



SoA_mapowanie zabezpieczeń
Zintegrowanego Systemu Zarządzania na
mechanizmy kontrolne Common Criteria
oraz SOC 2, Type II w Hadrone

2 Stycznia 2026 r.

Wersja obowiązująca
Final_V_1.00

Skrócona nazwa raportu:

SoA_mapowanie zabezpieczeń ZSZ na mechanizmy kontrolne ZSZ

Spis Treści

1	Cel dokumentu	2
2	Rozdział.....	3
3	Załączniki	117



1 Cel dokumentu

Głównym celem niniejszego dokumentu jest przedstawienie spójnego i ustrukturyzowanego mapowania zabezpieczeń wdrożonych w ramach **Zintegrowanego Systemu Zarządzania (ZSZ)** Hadrone Sp. z o.o. na wymagania i mechanizmy kontrolne standardów **Common Criteria (ISO/IEC 15408)** oraz **SOC 2 Type II (System and Organization Controls)**.

Jako wiodący dostawca rozwiązań chmurowych (SaaS) do zarządzania portfelem projektów i usługami IT, Hadrone opiera swój ZSZ na rygorystycznych normach międzynarodowych, takich jak ISO/IEC 27001:2022, ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 27701 oraz ISO 22301. Niniejsze mapowanie (Deklaracja Stosowania – SoA) stanowi kluczowe narzędzie dowodowe potwierdzające, że istniejące procedury, polityki oraz techniczne środki bezpieczeństwa w pełni pokrywają kryteria bezpieczeństwa wymagane przez globalnych partnerów biznesowych, instytucje sektora publicznego oraz audytorów zewnętrznych.

Opracowanie i utrzymanie tego dokumentu realizują następujące cele:

- **Zasada „Wdrażaj raz, spełniaj wiele wymagań” (Write Once, Comply with Many):** Wykazanie, w jaki sposób zintegrowane zabezpieczenia Hadrone (np.: kontrola dostępu, kryptografia, zarządzanie incydentami) jednocześnie realizują wymagania norm ISO, kryteriów SOC 2 oraz profili ochrony Common Criteria.
- **Wsparcie procesów audytowych (SOC 2, Type II):** Dostarczenie audytorom niezależnym bezpośredniego odniesienia (ang. *cross-reference*) pomiędzy dobowym funkcjonowaniem operacyjnym ZSZ w Hadrone a kryteriami zaufania SOC 2 (Trust Services Criteria), w szczególności w obszarach: *Security* (Bezpieczeństwo), *Availability* (Dostępność) oraz *Confidentiality* (Poufność).
- **Uwiarygodnienie bezpieczeństwa produktu (Common Criteria):** Odzwierciedlenie wymagań funkcjonalnych bezpieczeństwa (SFR) oraz wymagań zapewnienia bezpieczeństwa (SAR) według normy ISO/IEC 15408 w architekturze systemowej i procesach wytwórczych Hadrone (Secure SDLC).
- **Optymalizacja procesów zakupowych dla Klientów Enterprise i Sektora Publicznego:** Skrócenie czasu trwania analiz bezpieczeństwa (pre-evaluation) prowadzonych przez dział IT/Security u potencjalnych klientów poprzez natychmiastowe dostarczenie gotowej macierzy zgodności.
- **Identyfikacja luk (Gap Analysis) i ciągłe doskonalenie:** Monitorowanie spójności systemu oraz wykrywanie ewentualnych obszarów wymagających optymalizacji przy wprowadzaniu nowych wersji oprogramowania lub zmian w infrastrukturze chmurowej.



2 Rozdział

W rozdziale tym opisano wszystkie mechanizmy kontrolne wdrożone w Hadrone w ramach Zintegrowanego Systemu Zarządzania i dokonano mapowania na wymagania SOC 2, Type II w nomenklaturze COSO II i Common Criteria.

Przyjęto następujące mapowanie dla poziomu 0 oraz poziomu 1 (Level 0 oraz Level 1) jak zaprezentowano poniżej:

TCS (SOC 2, Type II)	Comon Criteria (ISO/IEC 15408)
Security	CC_S0 - Security / Bezpieczeństwo
	CC_S1 - Control Environment/ Kontrole Środowsikowe
	CC_S2 - Information and Communication / Komunikacja i informowanie
	CC_S3 - Risk Assessment / Ocena ryzyka
	CC_S4 - Monitoring Activities / Czynności monitorowania
	CC_S5 - Control Activities / Czynności kontrolne
	CC_S6 - Logical and Physical Access Control / Logiczna i fizyczna kontrola dostępu
	CC_S7 - System Operations / Operacje systemowe
	CC_S8 - Change Managment / Zarządzanie zmianą
	CC_S9 - Risk Mitigation / Osłabianie ryzyka
Availability	CC_A0 - Availability / Dostępność
Integrity	CC_I0 - Integrity / Integralność
Confidentiality	CC_C0 - Confidentiality / Poufność
Privacy	CC_P0 - Privacy / Prywatność
	CC_P1 - Pricacy - Objectives Related to Privacy / Cele związane z prywatnością
	CC_P3 - Collection / Zbieranie danych
	CC_P4 - Use, Retention and Disposal / Użycie, Retencja i wycofanie
	CC-P5 - Access / Dostęp
	CC_P6 - Disclosure and Nitification / Ujawnienie i powiadamianie
	CC_P7 - Quality / Jakość
	CC_P9 - Monitoring and Enforcement / Monitorowanie i egzekwowanie



ID.ISO	Domena	Nazwa Zabezpieczenia	Rozszerzenia (ISO 27001, ISO 27017, ISO 27018, ISO 27701, ISO 22301)	Kryteria Usług zaufania (Trust Services Criteria) - TSC	Wspólne Kryteria (Common Criteria) - CC	Wdrożone mechanizmy kontrolne stosowane w ZSZ przez Hadrone	stosowane w Hadrone mierniki efektywności dla wdrożonych mechanizmów kontrolnych	Ocena skuteczności wdrożonych kontroli	Spostrzeżenie / Wyłączenie / Uwaga dla wdrożonej kontroli	Dowody/Dokumentacja	Uzasadnienie	NISZ / DORA / AI Act	Status wdrożenia
5.1	Organizacyjne	Polityki bezpieczeństwa	ISO 27001	Security	CC_S2 - Information and Communication / Komunikacja i informowanie	<ul style="list-style-type: none">• Publikacja i dostęp: Umieszczenie dokumentów ZSZ na stronie www.hadrone.com dla każdego klienta w strefie Trust Center oraz w MS Teams dla pracownika Hadrone.• Metryka zapoznania: Obowiązkowe, udokumentowane potwierdzenie przeczytania polityki przez personel np.: w umowie.• Szkolenia: Regularne warsztaty i spotkania pracowników Hadrone z Hadrone CISO celem szerzenia zasad bezpieczeństwa i stosowania mechanizmów kontroli w obszarze ISMS, BCMS, PIMS i Cloud.• Ścieżka wyjątków: Oficjalna ścieżka zgłaszania i akceptacji odstępstw od polityki za zgodą Hadrone CISO.	<ul style="list-style-type: none">• Audyty: Regularne sprawdzanie przez audytorów Hadrone, czy teoria w dokumentach zgadza się z praktyką.• Wskaźniki (KPI): Monitorowanie wskaźników efektywności obszarów ZSZ.• Blokada techniczne: Hadrone wprowadza blokady systemowe i techniczne w obszarze sprzętowym, kont użytkowników, dostępu do sieci, aplikacji, systemu oraz dostępu do kodu źródłowego, dostępu do chmury obliczeniowej i w tym do infrastruktury IaaS.• Nadzór dostawców: Hadrone wprowadza weryfikacja dostawców, i potwierdza, że partnerzy zewnętrzni spełniają i przestrzegają wymagania Hadrone i standardy bezpieczeństwa.	Brak wyjątków, Brak uwag / No exception, No comments	Brak	Regulowany w kontekście ZSZ przez dokument: Polityka Zintegrowanego Systemu Zarządzania Hadrone Sp. z o.o. (Pełna wersja) - punkt: 2.5 Struktura nadzoru i zarządzania Zintegrowanym Systemem Zarządzania w Hadrone oraz dodatkowo przez: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone oraz systemowo przez: Zbiór procedur systemowych funkcjonujących w Hadrone dla Zintegrowanego Systemu Zarządzania (ZSZ)	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ obszar powiązany z obszarem systemowym ZSZ	Art. 21(2)a (NIS2) / Art. 6 (DORA)	tak

5.1	Organizacyjne	Zasady dotyczące bezpieczeństwa informacji	ISO 27001, ISO 27017, ISO 27701	Security	CC_S2 - Information and Communication / Komunikacja i informowanie	<ul style="list-style-type: none"> • Matryca RACI: Narzędzie w formie tabeli, które definiuje dla każdego procesu, kto jest za niego odpowiedzialny (Responsible), kto odpowiada przed zarządem (Accountable), z kim się konsultować (Consulted) i kogo informować (Informed). • Zakres obowiązków i umowy: Formalny proces wpisywania konkretnych odpowiedzialności za ZSZ do opisów stanowisk (HR) oraz do umów z zewnętrznymi dostawcami (B2B). • Proces powoływania i odwoływania (Wykazy): Centralny, na bieżąco aktualizowany rejestr wskazujący kto pełni kluczowe role CISO, KODO, CTO, IT DevOps, Developera, itp. • Szkolenia stanowiskowe: Proces wdrażania i doszkalania osób na dedykowanych stanowiskach z zakresu specyficznych dla nich procedur bezpieczeństwa w ramach ZSZ. 	<ul style="list-style-type: none"> • Przeglądy matrycy i weryfikacja kadrowa: Regularne (np.: raz na pół roku) sprawdzanie, czy przypisane role są aktualne i czy z powodu rotacji pracowników lub awansów nie powstały luki w i braki w przypisaniu osoby do roli. • Testy podziału obowiązków (SoD - Segregation of Duties): Audyt techniczny weryfikujący czy ta sama osoba nie posiada uprawnień wykonawczych i kontrolnych jednocześnie. • Wskaźniki pokrycia roli (KPI): Monitorowanie wskaźników efektywności obszarów ZSZ. • Testy gotowości (Ćwiczenia): Praktyczne sprawdzanie czy osoby przypisane do ról wiedzą, co robić, poprzez testy BCP, DRP czy testy obsługi incydentów. 	Brak wyjątków, Brak uwag / No exception, No comments	Brak	Regulowany w kontekście ZSZ przez dokument: Polityka Zintegrowanego Systemu Zarządzania Hadrone Sp. z o.o. (Pełna wersja) - punkt: 2.5 Struktura nadzoru i zarządzania Zintegrowanym Systemem Zarządzania w Hadrone oraz dodatkowo przez: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone oraz systemowo przez: Zbiór procedur systemowych funkcjonujących w Hadrone dla Zintegrowanego Systemu Zarządzania (ZSZ)	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ obszar powiązany z obszarem systemowym ZSZ	N/A	tak
-----	---------------	--	---------------------------------	----------	--	---	---	--	------	---	--	-----	-----



5.2	Organizacyjne	Role i odpowiedzialności	ISO 27001, ISO 27017, ISO 27701	Security	CC_S2 - Information and Communication / Komunikacja i informowanie	<ul style="list-style-type: none"> • Matryca RACI: Narzędzie w formie tabeli, które definiuje dla każdego procesu, kto jest za niego odpowiedzialny (Responsible), kto odpowiada przed zarządem (Accountable), z kim się konsultować (Consulted) i kogo informować (Informed). • Zakres obowiązków i umowy: Formalny proces wpisywania konkretnych odpowiedzialności za ZSZ do opisów stanowisk (HR) oraz do umów z zewnętrznymi dostawcami (B2B). • Proces powoływania i odwoływania (Wykazy): Centralny, na bieżąco aktualizowany rejestr wskazujący kto pełni kluczowe role CISO, KODO, CTO, IT DevOps, Developera, itp. • Szkolenia stanowiskowe: Proces wdrażania i doszkalania osób na dedykowanych stanowiskach z zakresu specyficznych dla nich procedur bezpieczeństwa w ramach ZSZ. 	<ul style="list-style-type: none"> • Przeglądy matrycy i weryfikacja kadrowa: Regularne (np.: raz na pół roku) sprawdzanie, czy przypisane role są aktualne i czy z powodu rotacji pracowników lub awansów nie powstały luki w i braki w przypisaniu osoby do roli. • Testy podziału obowiązków (SoD - Segregation of Duties): Audyt techniczny weryfikujący czy ta sama osoba nie posiada uprawnień wykonawczych i kontrolnych jednocześnie. • Wskaźniki pokrycia roli (KPI): Monitorowanie wskaźników efektywności obszarów ZSZ. • Testy gotowości (Ćwiczenia): Praktyczne sprawdzanie czy osoby przypisane do ról wiedzą, co robić, poprzez testy BCP, DRP czy testy obsługi incydentów. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Regulamin organizacyjny Hadrone, oraz w kontekście ZSZ przez dokument: Polityka Zintegrowanego Systemu Zarządzania Hadrone Sp. z o.o. (Pełna wersja) - punkt: 2.5 Struktura nadzoru i zarządzania Zintegrowanym Systemem Zarządzania w Hadrone	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ obszar powiązany z obszarem systemowym ZSZ	Art. 13 and 14 AI Act	tak
-----	---------------	--------------------------	---------------------------------	----------	--	---	---	---	------	---	--	-----------------------	-----



CL 5.2	Organizacyjne	Podział ról i odpowiedzialności	ISO 27001, ISO 27017	Security	CC_S2 - Information and Communication / Komunikacja i informowanie	<ul style="list-style-type: none"> • Matryca RACI: Narzędzie w formie tabeli, które definiuje dla każdego procesu, kto jest za niego odpowiedzialny (Responsible), kto odpowiada przed zarządem (Accountable), z kim się konsultować (Consulted) i kogo informować (Informed). • Zakres obowiązków i umowy: Formalny proces wpisywania konkretnych odpowiedzialności za ZSZ do opisów stanowisk (HR) oraz do umów z zewnętrznymi dostawcami (B2B). • Proces powoływania i odwoływania (Wykazy): Centralny, na bieżąco aktualizowany rejestr wskazujący kto pełni kluczowe role CISO, KODO, CTO, IT DevOps, Developera, itp. • Szkolenia stanowiskowe: Proces wdrażania i doszkalania osób na dedykowanych stanowiskach z zakresu specyficznych dla nich procedur bezpieczeństwa w ramach ZSZ. 	<ul style="list-style-type: none"> • Przeglądy matrycy i weryfikacja kadrowa: Regularne (np.: raz na pół roku) sprawdzanie, czy przypisane role są aktualne i czy z powodu rotacji pracowników lub awansów nie powstały luki w i braki w przypisaniu osoby do roli. • Testy podziału obowiązków (SoD - Segregation of Duties): Audyt techniczny weryfikujący czy ta sama osoba nie posiada uprawnień wykonawczych i kontrolnych jednocześnie. • Wskaźniki pokrycia roli (KPI): Monitorowanie wskaźników efektywności obszarów ZSZ. • Testy gotowości (Ćwiczenia): Praktyczne sprawdzanie czy osoby przypisane do ról wiedzą, co robić, poprzez testy BCP, DRP czy testy obsługi incydentów. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Regulamin organizacyjny Hadrone, oraz w kontekście ZSZ przez dokument: Polityka Zintegrowanego Systemu Zarządzania Hadrone Sp. z o.o. (Pełna wersja) - punkt: 2.5 Struktura nadzoru i zarządzania Zintegrowanym Systemem Zarządzania w Hadrone	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ obszar powiązany z obszarem systemowym ZSZ	N/A	tak
--------	---------------	---------------------------------	----------------------	----------	--	---	---	---	------	---	--	-----	-----



5.3	Organizacyjne	Podział obowiązków	ISO 27001, ISO 27701	Security	CC_S2 - Information and Communication / Komunikacja i informowanie	<ul style="list-style-type: none"> • Matryca konfliktów SoD (Segregation of Duties): Dokument lub tabela określająca, które uprawnienia systemowe i role w firmie są ze sobą sprzeczne i nie mogą być przypisane do jednego użytkownika. • Dwuetapowe procesy zatwierdzania (Workflow): Wdrożenie w systemach IT sztywnych ścieżek akceptacji, gdzie wykonawca (np.: programista) i zatwierdzający (np.: administrator) są inni i nie nakładają się rolami ani zakresem i uprawnieniami konta użytkownika. • Separacja środowisk (Prod / Test / Dev): Procesowe i techniczne rozdzielanie uprawnień. Programiści rozwijający kod nie mają prawa dostępu z uprawnieniami zapisu do systemów produkcyjnych, na których pracują klienci. • Rotacja stanowisk i urlopy: Mechanizm okresowego przenoszenia pracowników między zadaniami lub wymuszanie ciągłego urlopu (min. 14 dni), co pozwala na naturalne wykrycie ewentualnych nieprawidłowości ukrywanych przez jedną osobę. 	<ul style="list-style-type: none"> • Audyt kont i uprawnień (SoD): Regularny przegląd uprawnień użytkowników w systemach Hadrone w celu wykrycia osób, które w wyniku awansów lub zmian działów zgromadziły sprzeczne ze sobą uprawnienia. • Przegląd logów audytowych (Cross-checking): Automatyczna lub ręczna weryfikacja logów systemowych sprawdzająca, czy transakcje lub zmiany konfiguracyjne były realizowane zgodnie z zasadą "czterech oczu" (kto rozpoczął, a kto zatwierdził). • Wskaźnik naruszeń podziału obowiązków (KPI): Monitorowanie wskaźników efektywności obszarów ZSZ. • Testy i symulacje procesów: Próby przejścia krytycznej ścieżki procesowej przez jedną osobę (np.: próba samodzielnego wdrożenia zmiany na produkcji) w celu zweryfikowania, czy systemy skutecznie zablokują takie działanie. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Regulamin organizacyjny Hadrone, oraz w kontekście ZSZ przez dokument: Polityka Zintegrowanego Systemu Zarządzania Hadrone Sp. z o.o. (Pełna wersja) - punkt: 2.5 Struktura nadzoru i zarządzania Zintegrowanym Systemem Zarządzania w Hadrone	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ obszar powiązany z obszarem systemowym ZSZ	N/A	tak
-----	---------------	--------------------	----------------------	----------	--	---	--	---	------	---	--	-----	-----



5.4	Organizacyjne	Odpowiedzialność kierownictwa	ISO 27001, ISO 27701	Security	CC_S2 - Information and Communication / Komunikacja i informowanie	<ul style="list-style-type: none"> Przegląd Zarządzania: Formalny, cykliczny proces (np.: raz lub dwa razy w roku), podczas którego Kierownictwo Hadrone oficjalnie ocenia skuteczność systemu ZSZ, analizuje ryzyka i podejmuje decyzje o zmianach. Polityka Bezpieczeństwa Informacji: Dokument nadrzędny, podpisany osobiście przez Członka Zarząd Hadrone, będący oficjalnym stanowiskiem i nakazem stosowania norm bezpieczeństwa w Hadrone. Forum ds. ZSZ (Governance): Regularne spotkania Kierownictwa Hadrone i Pełnomocnika ds. ZSZ z liderami zespołów IT Dev, IT DevOps, PIMS, ISMS w celu koordynacji działań, zatwierdzania budżetów i rozwiązywania konfliktów interesów. System raportowania: Proces dostarczania Kierownictwu Hadrone skondensowanych raportów o stanie ZSZ w ramach corocznego procesu przeglądu ZSZ. 	<ul style="list-style-type: none"> Decyzje i protokoły z Przeglądu Zarządzania: Formalna weryfikacja (audyt) istnienia podpisanych protokołów, list obecności oraz decyzji (zadań dla zespołów) podjętych przez kierownictwo podczas przeglądów. Wskaźnik realizacji celów bezpieczeństwa (KPI): Monitorowanie wskaźników efektywności obszarów ZSZ. Weryfikacja budżetowa: Kontrola finansowa wykazująca czy zatwierdzony przez Kierownictwo Hadrone budżet na ZSZ jest realnie wydatkowany i wystarczający na pokrycie zidentyfikowanych ryzyk. Audyt zaangażowania (Wywiady audytowe): Bezpośrednia rozmowa audytora z członkami Zarządu Hadrone podczas audytu certyfikującego, weryfikująca ich realną wiedzę o systemie i zagrożeniach w organizacji. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Regulamin organizacyjny Hadrone, oraz w kontekście ZSZ przez dokument: Polityka Zintegrowanego Systemu Zarządzania Hadrone Sp. z o.o. (Pełna wersja) - punkt: 2.5 Struktura nadzoru i zarządzania Zintegrowanym Systemem Zarządzania w Hadrone oraz punkt: 3 Deklaracja Kierownictwa Hadrone Sp. z o.o.	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ obszar powiązany z obszarem systemowym ZSZ	N/A	tak
-----	---------------	-------------------------------	----------------------	----------	--	---	---	---	------	--	--	-----	-----



5.5	Organizacyjne	Kontakt z organami administracji	ISO 27001, ISO 27701	Security	CC_S2 - Information and Communication / Komunikacja i informowanie	<ul style="list-style-type: none"> Rejestr Kontaktów z organami: Centralna, bezpieczna baza danych (np.: w systemie SharePoint), w której ewidencjonuje się każde przychodzące i wychodzące pismo, wezwanie, decyzję oraz zgłoszenie incydentu. Procedura eskalacji i zgłaszania: Sztynny proces postępowania na wypadek wykrycia incydentu (np.: cyberataku), określający krok po kroku, kto przygotowuje raport, kto go opiniuje pod kątem prawnym i kto klika „wyślij” do organu. Konta i platformy dostępowe: Utrzymywanie i zabezpieczenie techniczne oficjalnych kanałów komunikacji elektronicznej z administracją państwową (np.: ePUAP, portale zgłoszeniowe PUODO czy CERT Polska). Szablony dokumentów i checklisty: Gotowe, zweryfikowane przez prawników wzory pism i formularzy zgłoszeniowych, które skracają czas reakcji w sytuacjach kryzysowych. 	<ul style="list-style-type: none"> Audyt terminowości (SLA): Regularna weryfikacja rejestru korespondencji pod kątem tego, czy wszystkie zgłoszenia i odpowiedzi na pisma organów zostały wysłane w wymaganym prawie terminie. Weryfikacja aktualności danych kontaktowych: Cykliczny (np.: coroczny) przegląd listy osób upoważnionych do kontaktu z organami oraz sprawdzenie, czy tokeny/hasła do platform typu ePUAP są aktywne. Wskaźnik poprawności formalnej (KPI): Monitorowanie wskaźników efektywności obszarów ZSZ. Testy i symulacje kryzysowe: Praktyczne ćwiczenia, podczas których symuluje się obowiązek zgłoszenia fikcyjnego incydentu do CERT lub PUODO w celu sprawdzenia drożności procedur. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 5.5 Kontakt z organami administracji. Dla obszaru PIMS dodatkowo regulowany przez dokument: Polityka Bezpieczeństwa Danych Osobowych w Hadrone Sp. z o.o. - punkt: 11. Postępowanie w sytuacji Naruszenia ochrony danych osobowych	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez RODO i w ramach ZSZ przez ZZPO_MK_ZS Z	N/A	tak
-----	---------------	----------------------------------	----------------------	----------	--	---	---	---	------	--	---	-----	-----



5.6	Organizacyjne	Kontakt z grupami interesu	ISO 27001, ISO 27701	Security	CC_S2 - Information and Communication / Komunikacja i informowanie	<ul style="list-style-type: none"> • Lista i rejestr grup interesu: Centralny spis organizacji, stowarzyszeń, forów i grup roboczych, w których firma bierze udział, wraz z przypisanymi do nich imiennymi reprezentantami z ramienia Hadrone. • Umowy członkowskie i NDA: Formalny proces weryfikacji regulaminów oraz podpisywania umów o zachowaniu poufności (NDA) przed przystąpieniem do sformalizowanych grup wymiany informacji. • Wewnętrzne repozytorium wiedzy: Proces transferu wiedzy z zewnątrz do organizacji – np.: dedykowany kanał (SharePoint, SLACK, MS Teams), gdzie reprezentanci dzielą się raportami, ostrzeżeniami o nowych zagrożeniach czy standardami pozyskanymi od grup interesu. • Procedura autoryzacji wystąpień: Proces zgłaszania i zatwierdzania przez dział prawny lub Zarząd Hadrone treści wszelkich publicznych prezentacji czy publikacji tworzonych w ramach członkostwa. 	<ul style="list-style-type: none"> • Coroczny przegląd zasadności członkostwa: Weryfikacja (np.: podczas przeglądu zarządzania), czy udział w danych grupach interesu nadal przynosi firmie wartość i czy wyznaczeni reprezentanci aktywnie w nich uczestniczą. • Wskaźnik transferu wiedzy (KPI): Monitorowanie wskaźników efektywności obszarów ZSZ. • Audyt incydentów "wycieku informacji": Kontrola sprawdzająca, czy podczas aktywności w grupach interesu nie doszło do nieautoryzowanego ujawnienia danych Hadrone (np.: weryfikacja publicznych postów, prezentacji czy wypowiedzi na forach). • Weryfikacja aktualności kontaktów alarmowych: Cykliczne sprawdzanie (np.: raz na pół roku), czy bezpośrednie kanały kontaktu do kluczowych grup (np.: wsparcia technicznego producentów systemów, grup reagowania) są drożne i aktualne. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 5.6 Kontakt z grupami interesu.	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z	N/A	tak
-----	---------------	----------------------------	----------------------	----------	--	---	--	---	------	---	--	-----	-----



5.7	Organizacyjne	Rozpoznanie zagrożeń / Threat Intelligence	ISO 27001, ISO 27017	Security	CC_S3 - Risk Assessment / Ocena ryzyka	<ul style="list-style-type: none"> • Zautomatyzowane źródła danych: Wdrożenie systemów (np.: platform SIEM, Microsoft Sentinel) automatycznie pobierających wskaźniki podatności (CVS, CVSS), oraz zagrożenia takie jak złośliwe adresy IP, domeny czy hashe złośliwych plików. • Proces analizy i korelacji: Cykliczna procedura porównywania pozyskanych baz zagrożeń z wewnętrznymi logami systemowymi w celu wykrycia, czy infrastruktura Hadrone nie komunikuje się już z serwerami stron trzecich w DarkWeb czy DeepWeb. • Biuletyny i alerty bezpieczeństwa: Proces subskrypcji i śledzenia ostrzeżeń od instytucji narodowych (np.: CERT Polska) oraz producentów oprogramowania używanego w Hadrone (np.: Microsoft, Attlessian). • Aktualizacja systemów i reguł (Patching): Proces przekładania wiedzy o zagrożeniach na natychmiastowe działania operacyjne w obszarze sieciowym (np.: dopisywanie reguł do Firewalla, systemów EDR/antywirusowych) oraz systemowym (np.: priorytetowe łatwanie luk w systemach). 	<ul style="list-style-type: none"> • Weryfikacja aktualności źródeł: Regularne sprawdzanie (np.: raz w miesiącu), czy podłączone strumienie danych Threat Intelligence są aktywne, poprawne technicznie i dostarczają świeże informacje. • Wskaźnik czasu reakcji (MTTR): Monitorowanie wskaźników efektywności obszarów ZSZ. • Audyt skuteczności reguł (Testy penetracyjne / Symulacje): Cykliczne sprawdzanie czy systemy chroniące dane i informacje Hadrone potrafią zablokować symulowany atak oparty na aktualnych, adekwatnych do profilu Hadrone podatnościach (np.: bazując na CVS czy CVSS scoring). • Raporty z analizy trendów: Coroczny przegląd statystyk wykrytych zagrożeń (w ramach przeglądu zarządzania), pozwalający Forum ds. ZSZ ocenić, czy inwestycje w konkretne systemy ochronne odpowiadają realnemu kierunkowi ewolucji cyber zagrożeń. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 5.7 Rozpoznanie zagrożeń / Threat Intelligence oraz system Microsoft Defender for Cloud oraz Microsoft Entra ID Protection.	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z	Art. 21(2)j (NIS2) / Art. 13 (DORA) / Art. 9 AI Act	tak
-----	---------------	--	----------------------	----------	--	---	--	---	------	---	--	---	-----



5.8	Organizacyjne	Bezpieczeństwo w zarządzaniu projektami	ISO 27001, ISO 27701	Security	CC_S3 - Risk Assessment / Ocena ryzyka	<ul style="list-style-type: none"> Włączenie bezpieczeństwa do metodyk (np.: Scrum, Agile, itp.): Wprowadzenie sztywnych punktów kontrolnych (tzw. Quality Gates lub kryteriów Definition of Done) do standardowego cyklu życia projektu, które uniemożliwiają przejście do kolejnej fazy bez zgody np.: CISO, CTO czy IT DevOps. Szablony dokumentacji projektowej: Umieszczenie dedykowanych sekcji dotyczących bezpieczeństwa w dokumentach inicjujących projekt (PID), kartach projektu czy formularzach zgłaszania wymagań. Matryca ról projektowych: Jasne określenie w strukturze projektu roli osoby odpowiedzialnej za bezpieczeństwo (np.: Architekta Bezpieczeństwa lub Konsultanta ds. Cyberbezpieczeństwa), która opiniuje działania zespołu. Proces szacowania ryzyka projektowego: Standardowa procedura identyfikacji zagrożeń specyficznych dla celów projektu (np.: ryzyko wycieku danych podczas migracji) wraz z planem ich mitygacji musi być prowadzona w narzędziu Hadrone PPM. 	<ul style="list-style-type: none"> Przeglądy etapowe (Bramki decyzyjne): Formalna weryfikacja (audyt) na koniec każdego etapu projektu sprawdzająca czy zaplanowane wymagania bezpieczeństwa zostały zrealizowane i przetestowane (np.: weryfikacja kody, testy penetracyjne, testy SAST lub DAST). Wskaźnik projektów zrealizowanych bezpiecznie (KPI): Monitorowanie wskaźników efektywności obszarów ZSZ. Audyty powdrożeniowe (Post-implementation review): Kontrola przeprowadzana po zakończeniu projektu i oddaniu produktu do użytku, weryfikująca czy końcowe rozwiązanie spełnia wszystkie założenia Polityki ZSZ Hadrone. Ewidencja ryzyk projektowych: Regularny przegląd rejestru ryzyk projektowych w narzędziu Hadrone PPM przez kierownika projektu w celu upewnienia się, że żadne zagrożenie wskazane w ZSZ nie zostało zignorowane przez zespół projektowy. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 5.8 Bezpieczeństwo w zarządzaniu projektami	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z	N/A	tak
-----	---------------	---	----------------------	----------	--	--	--	---	------	---	--	-----	-----



5.9	Organizacyjne	Inwentaryzacja informacji i aktywów	ISO 27001, ISO 27701	Security	CC_S4 - Monitoring Activities / Czynności monitorowania	<ul style="list-style-type: none"> Centralny rejestr aktywów (Asset Register): Jedna, zabezpieczona baza danych lub system (np.: bazy CMDb, w postaci pliku excel), zawierająca kompletną listę zasobów wraz z ich kopisem. Proces cyklu życia aktywów: Sztynna proces określający kroki postępowania z zasobem od momentu jego zakupu/wytworzenia, poprzez nadanie identyfikatorów, aż po bezpieczne wycofanie z eksploatacji i usunięcie z rejestru. Automatyczne skanowanie sieci (Discovery tools): Wykorzystanie narzędzi informatycznych, które stale skanują sieć firmową i automatycznie wykrywają nowe urządzenia, oprogramowanie lub bazy danych, zgłaszając je do rejestru. Standardy identyfikacji (Znakowanie): Fizyczne (np.: kody kreskowe, etykiety RFID na laptopach i telefonach) oraz logiczne (unikalne identyfikatory w systemach) oznaczanie zasobów ułatwiające ich ewidencję. 	<ul style="list-style-type: none"> Okresowe spisy z natury (Audyt aktywów): Cykliczne (np.: raz na dwa lata) weryfikacje polegające na porównaniu stanu faktycznego (co fizycznie znajduje się w firmie i systemach) z zapisami w Rejestrze Aktywów w celu wykrycia rozbieżności. Wskaźnik pokrycia rejestru (KPI): Monitorowanie wskaźników efektywności obszarów ZSZ. Kontrola Shadow IT: Monitorowanie logów sieciowych pod kątem wykrywania nieautoryzowanych urządzeń lub usług chmurowych, z których korzystają pracownicy, a które nie zostały zgłoszone do inwentarza. Weryfikacja procesu likwidacji (Uzgodnienie): Wyrzutowe sprawdzanie protokołów zniszczenia sprzętu i usuwania danych w celu upewnienia się, że wycofane aktywa zostały poprawnie wykreślone z aktywnego rejestru. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 5.9 Inwentaryzacja informacji i aktywów oraz excel pod analizę ryzyka: Risk Identification and analyse for ZSZ	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z oraz dodatkowo regulowany przez RODO i w ramach ZSZ	N/A	tak
-----	---------------	-------------------------------------	----------------------	----------	---	---	--	---	------	--	--	-----	-----



5.10	Organizacyjne	Dopuszczalne użytkowanie informacji	ISO 27001, ISO 27701	Security	CC_S4 - Monitoring Activities / Czynności monitorowania	<ul style="list-style-type: none"> Polityka czystego biurka i ekranu: Użytkownik ma obowiązek zablokować komputer / stację roboczą (skrót Win+L) przy każdym odejściu od stanowiska oraz chowanie dokumentów papierowych do zamykanych szafek. Systemy filtrowania treści (Web Filtering): Narzędzia informatyczne blokujące pracownikom automatyczny dostęp z komputerów firmowych do stron niebezpiecznych, hazardowych, pirackich czy niezwiązanych z pracą. System kontroli zgodności sprzętowej (Conditional Access): Narzędzia w Hadrone weryfikujące poziom zgodności komputera użytkownika z regulami wskazanymi w dostępie do sieci czy zasobów Hadrone. Systemy zarządzania urządzeniami (MDM/GPO): Centralne mechanizmy techniczne, które blokują możliwość instalowania samodzielnie oprogramowania przez użytkowników oraz uniemożliwiają podłączanie prywatnych nośników pamięci (pendrive'ów). Oświadczenie o dopuszczalnym użytkowaniu: Formalny proces (część onboardingu w Hadrone), podczas którego nowy pracownik podpisuje imienną deklarację, że zapoznał się z zasadami korzystania ze sprzętu i sieci. 	<ul style="list-style-type: none"> Monitorowanie ruchu sieciowego i logów: Regularne, zautomatyzowane sprawdzanie logów z systemów bezpieczeństwa w celu wykrycia prób obejścia blokad systemowych lub wejścia na zabronione strony internetowe. Wskaźnik incydentów nadużyć (KPI): Monitorowanie wskaźników efektywności obszarów ZSZ. Wyrwykowe audyty fizyczne: Okresowe kontrole czy komputery są odpowiednio skonfigurowane, mają zainstalowane łatę systemowe i są wolne od podatności. Kampanie testowe (Phishing / Socjotechnika): Regularne weryfikowanie zachowań użytkowników w praktyce poprzez kontrolowane symulacje ataków, sprawdzające czy pracownicy przestrzegają zasad bezpiecznego korzystania z poczty e-mail. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 5.10 Dopuszczalne użytkowanie informacji oraz wymagania dla użytkowników systemów informatycznych Hadrone oraz w ramach RODO: Instrukcja Zarządzania Systemem Informatycznym w Hadrone Sp. z o.o., oraz w zakresie Klasyfikacji Informacji przez: Zbiór procedur systemowych funkcjonujących w Hadrone dla Zintegrowanego Systemu Zarządzania (ZSZ) - punkt: 4.3 Procedura klasyfikacji informacji i danych dla ZSZ	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z oraz dodatkowo regulowany przez RODO i w ramach ZSZ	N/A	tak
------	---------------	-------------------------------------	----------------------	----------	---	---	--	---	------	---	--	-----	-----



5.11	Organizacyjne	Zwrot aktywów	ISO 27001	Security	CC_S5 - Control Activities / Czynności kontrolne	<ul style="list-style-type: none"> • Procedura offboardingu i karta obiegową: Zakończenia współpracy (wspierany przez workflow), wymagający zebrania zatwierdzeń od CISO, IT DevOps, przełożonego i potwierdzenia, że fizyczny zwrot sprzętu i dokumentów miał miejsce. • Ewidencja przypisania aktywów: Hadrone posiada centralną bazę danych zarządzania aktywami (Asset Management), która jednoznacznie wskazuje, jakie dokładnie zasoby (laptopy, telefony, systemy, licencje, subskrypcje) były przypisane do odchodzącej osoby. • Zautomatyzowane odbieranie dostępu i licencji: W momencie uruchomienia procedury zwrotu aktywów automatycznie blokuje się konta użytkownika, uniemożliwiając zdalne pobranie danych organizacji oraz obiera się subskrypcje do systemów i aplikacji online. • Protokoły zdawczo-odbiorcze: Oficjalne dokumenty (papierowe lub cyfrowe) podpisywane przez pracownika oraz przedstawiciela Hadrone, szczegółowo wymieniające zwracane pozycje wraz z ich numerami seryjnymi i stanowi formalny zapis zwrotu aktywu w modelu B2B. 	<ul style="list-style-type: none"> • Audyt kompletności kart obiegowych: Regularna (np.: miesięczna) weryfikacja losowo wybranych teczek personalnych byłych pracowników pod kątem obecności w pełni podpisanych i zamkniętych kart obiegowych oraz protokołów zwrotu. • Wskaźnik nieprzeprowadzonych zwrotów (KPI): Monitorowanie wskaźników efektywności obszarów ZSZ. • Weryfikacja kont osieroconych i urzędzeń: Porównywanie listy osób zwolnionych z aktywnymi urządzeniami w sieci i aktywnymi kontami w Entra ID i zamykanie lub blokowanie tych sprzętów i kont, które wykazują niezgodność. • Raportowanie strat i opóźnień: Cykliczne raporty dla Forum ds. ZSZ zawierające informacje o utraconych aktywach (np.: niezwróconych telefonach czy skradzionych laptopach) oraz o podjętych działaniach prawnych lub windykacyjnych w celu ich odzyskania. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 5.11 Zwrot aktywów oraz wymagania dla użytkowników systemów informatycznych Hadrone oraz w ramach RODO: Instrukcja Zarządzania Systemem Informatycznym w Hadrone Sp. z o.o., oraz w zakresie Klasyfikacji Informacji przez: Zbiór procedur systemowych funkcjonujących w Hadrone dla Zintegrowanego Systemu Zarządzania (ZSZ) - punkt: 4.3 Procedura klasyfikacji informacji i danych dla ZSZ	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z oraz dodatkowo regulowany przez RODO i w ramach ZSZ	N/A	tak
------	---------------	---------------	-----------	----------	--	---	--	---	------	---	--	-----	-----



5.12	Organizacyjne	Klasyfikacja informacji	ISO 27001, ISO 27701	Confidentiality	CC_CO - Confidentiality / Poufność	<ul style="list-style-type: none"> • Procedura klasyfikacji informacji: Sformalizowany dokument definiujący jasne stopnie poufności (np.: Publiczne, Wewnętrzne, Zastrzeżone, Poufne) oraz kryteria przypisywania informacji do danej kategorii. • Matryca klasyfikacji i postępowania: Praktyczna tabela dla pracowników, która dla każdej klasy informacji przypisuje konkretne instrukcje (np.: jak dany dokument przechowywać, jak go szyfrować, komu można go udostępnić i jak go niszczyć). • Warsztaty i proces mapowania danych: Regularne działania biznesowe polegające na identyfikacji kluczowych procesów w Hadrone i przypisywaniu klasyfikacji informacji i danych do powiązanych z nimi baz danych, systemów oraz dokumentów. • Narzędzia wspierające klasyfikację informacji i danych: Oprogramowanie do automatycznego określania wrażliwości informacji i danych, Hadrone wdrożył Microsoft Purview Information Protection, a domyślnym poziomem jest klasyfikacja Wewnętrzne. 	<ul style="list-style-type: none"> • Audyt zgodności klasyfikacji: Wyrwykowe, regularne kontrole (np.: raz na kwartał) wybranych repozytoriów danych (SharePoint, dyski sieciowe) i weryfikacja, czy znajdujące się tam pliki zostały prawidłowo sklasyfikowane przez użytkowników. • Wskaźnik poprawności klasyfikacji (KPI): Monitorowanie wskaźników efektywności obszarów ZSZ. • Przegląd ryzyka związanych z Nadklasyfikacją/Podklasyfikacją: Roczny przegląd incydentów bezpieczeństwa pod kątem sprawdzenia, czy nie doszło do wycieków danych z powodu zbyt niskiej klasyfikacji (podklasyfikacja) lub paraliżu procesów przez zbyt wysoką klasyfikację (nadklasyfikacja). • Testowanie świadomości pracowników: Okresowe testy i quizy dla personelu weryfikujące, czy pracownicy potrafią prawidłowo przyporządkować przykładowe dokumenty firmowe do odpowiednich klas poufności zgodnie z przyjętą w Hadrone procedurą. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 5.12 Klasyfikacja informacji oraz wymagania dla użytkowników systemów informatycznych Hadrone oraz w ramach RODO: Instrukcja Zarządzania Systemem Informatycznym w Hadrone Sp. z o.o., oraz w zakresie Klasyfikacji Informacji przez: Zbiór procedur systemowych funkcjonujących w Hadrone dla Zintegrowanego Systemu Zarządzania (ZSZ) - punkt: 4.3 Procedura klasyfikacji informacji i danych dla ZSZ	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z oraz dodatkowo regulowany przez RODO i w ramach ZSZ	Art. 10 AI Act	tak
------	---------------	-------------------------	----------------------	-----------------	------------------------------------	---	---	---	------	---	--	----------------	-----



5.13	Organizacyjne	Etykietowanie informacji	ISO 27001	Confidentiality	CC_CO - Confidentiality / Poufność	<ul style="list-style-type: none"> Systemy automatycznego znakowania (Microsoft Purview Information Protection): Narzędzia IT, które automatycznie (na podstawie zawartości, np.: obecności numerów PESEL) lub półautomatycznie (podpowiedź dla użytkownika) nakładają etykiety i metadane na pliki pakietu Office oraz wiadomości e-mail. Szablony dokumentacji ze znacznikami: Sformalizowane szablony dokumentów firmowych (Word, Excel, PowerPoint) posiadające na stałe wdrożone graficzne oznaczenia poziomu poufności w nagłówkach, stopkach lub jako znaki wodne. Etykietowanie fizyczne (Znakowanie nośników): Procesy operacyjne wymuszające fizyczne oznaczenie dokumentów papierowych (np.: pieczętka „POUFNE”) oraz zewnętrznych nośników danych, takich jak dyski (np.: kolorowe etykiety). Procedura reklasyfikacji i zmiany etykiet: Ścisły proces określający warunki, w jakich etykieta informacji może zostać zmieniona (np.: obniżenie stopnia poufności projektu po jego publicznym ogłoszeniu). 	<ul style="list-style-type: none"> Skanowanie repozytoriów danych (Audyt metadanych): Regularne, automatyczne przeszukiwanie dysków sieciowych, chmury (SharePoint/OneDrive) oraz skrzynek pocztowych w celu wykrycia plików, które nie posiadają przypisanej żadnej etykiety. Wskaźnik zaetykietowanych dokumentów (KPI): Monitorowanie wskaźników efektywności obszarów ZSZ. Weryfikacja skuteczności systemów DLP: Testowanie reguł systemowych (Data Loss Prevention) poprzez kontrolowane próby wysłania na zewnątrz plików z etykietą „Poufne”, sprawdzające czy system poprawnie blokuje taki transfer na podstawie metadanych etykiety. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 5.13 Etykietowanie informacji oraz wymagania dla użytkowników systemów informatycznych Hadrone oraz w ramach RODO: Instrukcja Zarządzania Systemem Informatycznym w Hadrone Sp. z o.o., oraz w zakresie Klasyfikacji Informacji przez: Zbiór procedur systemowych funkcjonujących w Hadrone dla Zintegrowanego Systemu Zarządzania (ZSZ) - punkt: 4.3 Procedura klasyfikacji informacji i danych dla ZSZ. Wykorzystane narzędzia w Hadrone to: Microsoft Purview Information Protection client (MPIP)	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ obszar powiązany z obszarem systemowym ZSZ	N/A	tak
------	---------------	--------------------------	-----------	-----------------	------------------------------------	---	--	---	------	---	--	-----	-----



5.14	Organizacyjne	Transfer informacji	ISO 27001, ISO 27701	Integrity	CC_IO - Integrity / Integralność	<ul style="list-style-type: none"> • Procedury i umowy transferu danych PII (PII Transfer Data Agreements): Sformalizowane zasady określające kroki postępowania przy wymianie danych, w tym danych osobowych z podmiotami zewnętrznymi, w tym stosowanie umów NDA i klauzul umownych chroniących transfer. • Bezpieczne systemy wymiany plików (SFTP / MFT): Wykorzystanie dedykowanych, szyfrowanych platform do przesyłania dużych zbiorów danych (np.: serwery SFTP, systemy Managed File Transfer) z automatycznym wygasaniem linków dostępowych. • Szyfrowanie poczty i wymuszenie TLS: Techniczne mechanizmy wdrożone w firmowym systemie pocztowym, które automatycznie szyfrują wiadomości zawierające załączniki lub wymuszają bezpieczne połączenie (TLS) z serwerem odbiorcy. • Ochrona fizycznego transportu nośników: Wymagania dla przesyłania danych fizycznie przez firmy kurierskie i logistyczne. Nośnik i danych muszą być oznaczone, zaplombowane, a elektroniczne nośniki danych dodatkowo zaszyfrowane. 	<ul style="list-style-type: none"> • Monitorowanie systemów DLP (Data Loss Prevention): Regularna kontrola i automatyczne alertowanie w przypadku wykrycia prób przesłania informacji niejawnych (np.: numerów PESEL, informacji o klientach, kodu źródłowego) poza sieć Hadrone. • Audyt logów transferu plików: Cykliczny przegląd logów z platformy wymiany danych w celu weryfikacji, kto, co, kiedy i do kogo przysyłał oraz czy odbiorca był do tego uprawniony. • Wskaźnik nieautoryzowanych transferów (KPI): Monitorowanie wskaźników efektywności obszarów ZSZ. • Testowanie odporności kanałów (Audyt techniczny): Okresowe weryfikacje konfiguracji protokołów kryptograficznych (np.: sprawdzanie wersji TLS, audyt konfiguracji VPN) w celu upewnienia się, że kanały transferu nie posiadają znanych podatności. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 5.14 Transfer informacji oraz wymagania dla użytkowników systemów informatycznych Hadrone oraz w ramach RODO: Polityka Bezpieczeństwa Danych Osobowych w Hadrone Sp. z o.o. - punkt: 6.9. Przekazywanie danych osobowych do państwa trzeciego oraz Instrukcja Zarządzania Systemem Informatycznym w Hadrone Sp. z o.o., oraz w zakresie Klasyfikacji Informacji przez: Zbiór procedur systemowych funkcjonujących w Hadrone dla Zintegrowanego Systemu Zarządzania (ZSZ) - punkt: 4.3 Procedura klasyfikacji informacji i danych dla ZSZ	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ obszar powiązany z obszarem systemowym ZSZ oraz dodatkowo regulowany przez RODO i w ramach ZSZ przez ZZPO_MK_ZS Z	N/A	tak
------	---------------	---------------------	----------------------	-----------	----------------------------------	--	---	---	------	--	---	-----	-----



5.15	Organizacyjne	Kontrola dostępu	ISO 27001, ISO 27017, ISO 27701	Security	CC_S5 - Control Activities / Czynności kontrolne	<ul style="list-style-type: none"> Polityka kontroli dostępu: Sformalizowany dokument i proces określający reguły nadawania, modyfikowania oraz odbierania uprawnień dla użytkowników własnych oraz partnerów biznesowych. Szyfrowane kanały zdalne (VPN / PAM): Wykorzystanie bezpiecznych, dedykowanych technologii (np.: dwuskładnikowy VPN, systemy Privileged Access Management) do zestawiania i nadzorowania sesji zdalnych dla pracowników i współpracowników Hadrone oraz dla dostawców usług IT dla Hadrone. Proces rejestracji i autoryzacji dostępu: Ustrukturyzowany proces wnioskowy (workflow), w którym każde nadanie uprawnień pracownikowi zewnętrznemu wymaga zgody menedżera/leadera danego obszaru ze strony Hadrone. Bramki sieciowe i segmentacja (Firewalle): Techniczne mechanizmy izolacji sieciowej, które automatycznie blokują ruch z kont dostawców do systemów i baz danych, które nie są objęte zakresem ich umowy. 	<ul style="list-style-type: none"> Cykliczny przegląd list dostępowych: Regularna (np.: raz w miesiącu) weryfikacja wszystkich aktywnych kont i uprawnień zewnętrznych w celu natychmiastowego usunięcia dostępów wygasłych, zbędnych lub „osieroconych”. Wskaźnik kont terminowych (KPI): Monitorowanie wskaźników efektywności obszarów ZSZ. Audyt logów aktywności stron trzecich: Regularne sprawdzanie i analiza logów systemowych pod kątem operacji wykonywanych przez firmy zewnętrzne w celu wykrycia nietypowych działań lub prób nadużyć. Testy odcięcia (Offboarding verification): Wyrwykowe sprawdzanie procesów zakończenia współpracy i weryfikacja, czy po zamknięciu projektu lub umowy z dostawcą wszystkie powiązane z nim dostępy zostały skutecznie zablokowane w czasie krótszym niż 48 godzin. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 5.15 Kontrola dostępu oraz wymagania dla użytkowników systemów informatycznych Hadrone	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z	Art. 21(2)g (NIS2) / Art. 9 (DORA)	tak
------	---------------	------------------	---------------------------------	----------	--	---	--	---	------	--	--	------------------------------------	-----



CL.P.5.15	Organizacyjne	Relacje z dostawcami	ISO 27018	Security	CC_S5 - Control Activities / Czynności kontrolne	<ul style="list-style-type: none"> • Polityka kontroli dostępu: Sformalizowany dokument i proces określający reguły nadawania, modyfikowania oraz odbierania uprawnień dla użytkowników własnych oraz partnerów biznesowych. • Szyfrowane kanały zdalne (VPN / PAM): Wykorzystanie bezpiecznych, dedykowanych technologii (np.: dwuskładnikowy VPN, systemy Privileged Access Management) do zestawiania i nadzorowania sesji zdalnych dla pracowników i współpracowników Hadrone oraz dla dostawców usług IT dla Hadrone. • Proces rejestracji i autoryzacji dostępu: Ustrukturyzowany proces wnioskowy (workflow), w którym każde nadanie uprawnień pracownikowi zewnętrznemu wymaga zgody menedżera/leadera danego obszaru ze strony Hadrone. • Bramki sieciowe i segmentacja (Firewalle): Techniczne mechanizmy izolacji sieciowej, które automatycznie blokują ruch z kont dostawców do systemów i baz danych, które nie są objęte zakresem ich umowy. 	<ul style="list-style-type: none"> • Cykliczny przegląd list dostępowych: Regularna (np.: raz w miesiącu) weryfikacja wszystkich aktywnych kont i uprawnień zewnętrznych w celu natychmiastowego usunięcia dostępu wygasłych, zbędnych lub „osieroconych”. • Wskaźnik kont terminowych (KPI): Monitorowanie wskaźników efektywności obszarów ZSZ. • Audyt logów aktywności stron trzecich: Regularne sprawdzanie i analiza logów systemowych pod kątem operacji wykonywanych przez firmy zewnętrzne w celu wykrycia nietypowych działań lub prób nadużyć. • Testy odcięcia (Offboarding verification): Wyrzawkowe sprawdzanie procesów zakończenia współpracy i weryfikacja, czy po zamknięciu projektu lub umowy z dostawcą wszystkie powiązane z nim dostępy zostały skutecznie zablokowane w czasie krótszym niż 48 godzin. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 5.16 Relacje z dostawcami oraz przez: Strategia Zarządzania Bezpieczeństwem Informacji i chmury obliczeniowej w ramach ZSZ dla Hadrone (integracja obszaru ISMS i Cloud) - punkt: 4 Strategia ISMS w Cloud Governance (ISO 27017 / ISO 27018)	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z	N/A	tak
-----------	---------------	----------------------	-----------	----------	--	---	--	---	------	---	--	-----	-----



5.16	Organizacyjne	Zarządzanie tożsamością	ISO 27001, ISO 27701	Security	CC_S5 - Control Activities / Czynności kontrolne	<ul style="list-style-type: none"> Systemy IAM (Identity and Access Management): Centralne narzędzia technologiczne (np.: Microsoft Entra ID) służące jako jedyne, autorytatywne źródło prawdy o tożsamościach w Hadrone. Półautomatyczny proces Onboarding / Offboarding: Sformalizowana procedura, w której system kadrowy (HR) półautomatycznie (Wymagane jest jeszcze potwierdzenie tożsamości) inicjuje w systemie IAM proces tworzenia konta dla nowego pracownika lub natychmiastowo blokuje tożsamość w dniu zakończenia umowy. Jednokrotne logowanie (Single Sign-On - SSO): Mechanizm techniczny pozwalający użytkownikowi na bezpieczne uwierzytelnianie się do wielu aplikacji firmowych za pomocą jednej, centralnie zarządzanej tożsamości cyfrowej. Rejestr kont technicznych i specjalnych: Prowadzona i regularnie aktualizowana baza danych zawierająca spis wszystkich kont systemowych, usługowych i testowych wraz z przypisanymi do nich systemami i osobami odpowiedzialnymi. 	<ul style="list-style-type: none"> Weryfikacja tożsamości nieaktywnych (Audyt uśpionych kont): Regularne (np.: raz na kwartał) zautomatyzowane skanowanie systemów w celu wykrywania i natychmiastowego blokowania kont, które nie były używane przez określony czas (np.: od 30 dni). Wskaźnik osieroconych tożsamości (KPI): Monitorowanie wskaźników efektywności obszarów ZSZ. Uzgadnianie baz danych (Reconciliation): Cykliczne porównywanie (reconciliation) stanów kont w poszczególnych aplikacjach biznesowych z centralnym systemem Enytra ID w celu wykrycia kont założonych ręcznie lub z pominięciem oficjalnej zatwierdzeń. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 5.16 Zarządzanie tożsamością oraz wymagania dla użytkowników systemów informatycznych Hadrone. Stosowane narzędzia i mechanizmy kontroli to: Azure Entra ID, recourse group na każdy vNET oraz VPN do Azure i Microsoft Entra ID Protection oraz Microsoft Defender for Cloud	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z	N/A	tak
------	---------------	-------------------------	----------------------	----------	--	--	---	---	------	---	--	-----	-----



5.17	Organizacyjne	Informacje uwierzytelniające	ISO 27001, ISO 27017	Security	CC_S5 - Control Activities / Czynności kontrolne	<ul style="list-style-type: none"> • Menedżery haseł (Password Managers): Wdrożenie centralnego, szyfrowanego narzędzia (np.: LastPass, 1Password) do bezpiecznego generowania, przechowywania i współdzielenia (w uzasadnionych przypadkach) haseł i kluczy dostępowych. • Polityki haseł w systemach (GPO/IAM): Systemowe wymuszenie technicznych parametrów haseł (np.: minimalna długość 14 znaków, użycie znaków specjalnych, blokada konta po 5 nieudanych próbach logowania). Hasło zmieniane jest co 180 dni, składa się co najmniej z 14 znaków i zawiera małe, duże litery, cyfry (co najmniej 3) oraz znaki specjalne (co najmniej 2) i jest utworzone jako passphrase. • Zautomatyzowany reset haseł tymczasowych: Automatyczny proces IT wymuszający na użytkowniku natychmiastową, samodzielną zmianę hasła tymczasowego podczas pierwszego logowania do systemu. • Szyfrowanie w locie i w spoczynku: Procesy techniczne gwarantujące, że bazy danych zawierające informacje uwierzytelniające są silnie haszowane (np.: algorytmem bcrypt/Argon2, AES-256), a ich przesyłanie przez sieć odbywa się wyłącznie kanałami szyfrowanymi (TLS/VPN). 	<ul style="list-style-type: none"> • Skanowanie podatności i audyty baz haseł: Regularne (np.: raz na pół roku) uruchamianie zautomatyzowanych narzędzi sprawdzających, czy pracownicy nie używają słabych haseł lub haseł, które wyciekły do sieci (np.: integracja z bazami typu Have I Been Pwned). • Wskaźnik wdrożenia MFA (KPI): Monitorowanie wskaźników efektywności obszarów ZSZ. • Monitorowanie logów pod kątem ataków (Brute-force): Ciągła, automatyczna analiza logów uwierzytelniania w celu natychmiastowego wykrywania i blokowania masowych prób zgadywania haseł lub logowań z nietypowych lokalizacji geograficznych. • Testy socjotechniczne (Phishing): Okresowe, kontrolowane symulacje ataków wyłudzenia informacji, sprawdzające czy pracownicy potrafią zidentyfikować zagrożenie i nie wpisać swoich poświadczeń na fałszywych stronach internetowych. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 5.17 Informacje uwierzytelniające oraz wymagania dla użytkowników systemów informatycznych Hadrone. Stosowane narzędzia i mechanizmy kontroli to: Azure Entra ID (login i hasło) oraz Microsoft MFA.	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z	N/A	tak
------	---------------	------------------------------	----------------------	----------	--	--	---	---	------	--	--	-----	-----



5.18	Organizacyjne	Uprawnienia dostępu	ISO 27001, ISO 27701	Security	CC_S5 - Control Activities / Czynności kontrolne	<ul style="list-style-type: none"> Systemy zarządzania tożsamością i dostępem (Identity & Access Management - IAM): Centralne narzędzia informatyczne (np.: Entra ID) służące do automatycznego nadawania, modyfikowania i odbierania uprawnień w systemach. Proces wnioskowania o dostęp (Workflow): Sformalizowana procedura (np.: zgłoszenie), w której pracownik składa wniosek, przełożony go zatwierdza, a support technicznie konfiguruje uprawnienia. Rola i grupy dostępowe (RBAC): Mechanizm przypisywania uprawnień na podstawie pełnionej funkcji w firmie (np.: grupa „IT DevOSP”, „Dev”), co zapobiega ręcznemu i chaotycznemu nadawaniu praw pojedynczym osobom. Procedura offboardingu (Natychmiastowe blokowanie): Automatyczne działanie HR-IT gwarantujące, że w momencie rozwiązania umowy z pracownikiem lub dostawcą wszystkie jego uprawnienia dostępu są natychmiastowo i bezpowrotnie dezaktywowane. 	<ul style="list-style-type: none"> Okresowy przegląd uprawnień (User Access Review): Cykliczna (np.: raz na kwartał) weryfikacja list dostępowych przez menedżerów i właścicieli systemów w celu usunięcia uprawnień nadmiarowych lub nieaktualnych. Wskaźnik kont osieroconych (KPI): Monitorowanie wskaźników efektywności obszarów ZSZ. Audyt zgodności z profilem roli: Wyrywkowa kontrola sprawdzająca, czy użytkownicy z danego zespołu nie posiadają uprawnień wykraczających poza standardowy profil przypisany do ich stanowiska. Monitorowanie nadania uprawnień (Logi): Automatyczne alertowanie i weryfikacja logów systemowych pod kątem wykrywania przypadków nadania uprawnień (szczególnie administracyjnych) z pominięciem oficjalnego procesu wnioskowego. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 5.18 Uprawnienia dostępu oraz wymagania dla użytkowników systemów informatycznych Hadrone. Dodatkowo w obszarze RODO regulowane przez: Polityka Bezpieczeństwa Danych Osobowych w Hadrone Sp. z o.o - punkt: 6.1. Upoważnienia do przetwarzania danych osobowych, Oświadczenia o zachowaniu poufności Stosowane narzędzia i mechanizmy kontroli to: Azure Entra ID, recourse group na każdy vNET oraz VPN do Azure i Microsoft Entra ID Protection oraz Microsoft Defender for Cloud	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ obszar regulowany przez RODO i w ramach ZSZ przez ZZPO_MK_ZS Z	N/A	tak
------	---------------	---------------------	----------------------	----------	--	---	--	---	------	--	--	-----	-----



5.19	Organizacyjne	Bezpieczeństwo w relacjach z dostawcami	ISO 27001, ISO 27017, ISO 27701	Security	CC_S4 - Monitoring Activities / Czynności monitorowania	<ul style="list-style-type: none"> Proces kwalifikacji i wyboru dostawców: Wstępna procedura oceny (Due Diligence) obejmująca weryfikację certyfikatów bezpieczeństwa (np.: ISO 27001, ISO 27701, GDPR, SOC 2, type II) oraz stabilności operacyjnej dostawcy przed podpisaniem umowy. Procedura bezpiecznego onboardingu i offboardingu: Sformalizowany proces nadawania, nadzorowania oraz natychmiastowego odbierania uprawnień i kont dostępowych dla pracowników dostawcy po zakończeniu prac. Połączenia VPN i dedykowane konta: Techniczne mechanizmy izolacji, co oznacza, że pracownicy dostawców korzystają wyłącznie z imiennych kont oraz zabezpieczonych, szyfrowanych kanałów dostępu zdalnego, podlegających pełnej rejestracji. Ankietyzacja i profile ryzyka: Narzędzia do okresowej oceny dojrzałości cyberbezpieczeństwa dostawców za pomocą ustrukturyzowanych kwestionariuszy i segmentacji ich na grupy ryzyka. 	<ul style="list-style-type: none"> Weryfikacja uprawnień zewnętrznych: Regularny (np.: kwartalny) przegląd aktywnych kont przypisanych do firm zewnętrznych w celu wykrycia i zablokowania dostępów "osieroconych" lub nadmiarowych. Audyty u dostawców (Second-party audits): Planowe lub doraźne kontrole i wizyty weryfikujące, czy dostawca w praktyce realizuje uzgodnione wymagania organizacyjne i techniczne. Wskaźnik incydentów z winy stron trzecich (KPI): Monitorowanie wskaźników efektywności obszarów ZSZ. Przegląd logów aktywności dostawców: Automatyczna kontrola i analiza działań podejmowanych przez konta zewnętrzne w sieci Hadrone pod kątem wykrywania nietypowych operacji lub prób nieautoryzowanego dostępu. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 5.19 Bezpieczeństwo w relacjach z dostawcami oraz dodatkowo przez poszczególne umowy z dostawcami i analizę prawną umów, stosowanie opracowanych i zatwierdzonych oraz zweryfikowanych template umów, a w obszarze usług SaaS, stosowanie odpowiedniego regulaminu i podziału odpowiedzialności jak wskazano w dokumencie: Strategia Zarządzania Bezpieczeństwem Informacji i chmury obliczeniowej w ramach ZSZ dla Hadrone (integracja obszaru ISMS i Cloud) - punkt: 4 Strategia ISMS w Cloud Governance (ISO 27017 / ISO 27018)	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z	Art. 21(2)d (NIS2) / Art. 28-30 (DORA)	tak
------	---------------	---	---------------------------------	----------	---	---	--	---	------	--	--	--	-----



5.20	Organizacyjne	Bezpieczeństwo w umowach z dostawcami	ISO 27001, ISO 27017	Security	CC_S5 - Control Activities / Czynności kontrolne	<ul style="list-style-type: none"> Standardowe klauzule bezpieczeństwa (SLA/NDA): Gotowe, zatwierdzone przez kancelarię prawną szablony umów, aneksów bezpieczeństwa oraz umów o zachowaniu poufności, dopasowane do poziomu ryzyka dostawcy. Proces klasyfikacji ryzyka dostawców: Procedura oceny przedkontraktowej, która kategoryzuje dostawców (np.: niski, średni, wysoki wpływ na bezpieczeństwo) i decyduje o surowości zapisów umownych. Wymóg zgłaszania incydentów: Procesowy zapis w umowie nakładający na dostawcę sztywny obowiązek (np.: w ciągu 24 godzin) informowania Hadrone o wszelkich cyberatakach lub wyciekach danych, które mogą mieć na nią wpływ. Zarządzanie podwykonawstwem: Klauzula umowna blokująca dostawcy możliwość przekazywania danych kolejnym podwykonawcom (subprocesorom) bez wcześniejszej, pisemnej zgody Hadrone. 	<ul style="list-style-type: none"> Weryfikacja kompletności umów (Audyt prawny): Cykliczny przegląd aktywnych kontraktów z dostawcami pod kątem obecności wymaganych zapisów i aneksów dotyczących bezpieczeństwa informacji. Wskaźnik umów zabezpieczonych (KPI): Monitorowanie wskaźników efektywności obszarów ZSZ. Monitorowanie parametrów SLA: Regularne sprawdzanie czy dostawca wywiązuje się z zapisanych w umowie wskaźników technicznych (np.: czasu dostępności usług chmurowych lub czasu reakcji na zgłoszenia podatności). Egzekwowanie prawa do audytu: Praktyczne przeprowadzanie okresowych weryfikacji (np.: wysyłanie ankiet bezpieczeństwa do kluczowych dostawców) w celu sprawdzenia, czy deklarowane w umowie zabezpieczenia są stosowane w rzeczywistości. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 5.20 Bezpieczeństwo w umowach z dostawcami	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z	N/A	tak
------	---------------	---------------------------------------	----------------------	----------	--	---	---	---	------	--	--	-----	-----



5.21	Organizacyjne	Zarządzanie łańcuchem dostaw ICT	ISO 27001, ISO 27017	Availability	CC_A0 - Availability / Dostępność	<ul style="list-style-type: none"> Proces oceny ryzyka dostawców ICT (Due Diligence): Procedura weryfikacji dostawców pod kątem praktyk bezpieczeństwa (np.: sprawdzanie certyfikatów ISO 27001, ISO 27701, deklaracji zgodności) przed włączeniem ich produktów do infrastruktury Hadrone. Zarządzanie zestawieniem komponentów: Narzędzie i proces wymagania od dostawców oprogramowania szczegółowej listy użytych bibliotek i komponentów open-source, co pozwala na szybkie wykrywanie znanych podatności. Testowanie i inspekcja przy odbiorze: Proces technicznej weryfikacji nowo zakupionego sprzętu i oprogramowania (np.: sprawdzanie sum kontrolnych, skanowanie podatności, testy w środowisku izolowanym) przed wdrożeniem produkcyjnym. Klauzule umowne dotyczące łańcucha dostaw: Zapisy w kontraktach nakładające na dostawców obowiązek audytowania ich własnych podwykonawców oraz natychmiastowego informowania o podatnościach typu zero-day w dostarczonych rozwiązaniach i ułomnościach ich produktów. 	<ul style="list-style-type: none"> Audyty procesów produkcyjnych i logistycznych: Cykliczna weryfikacja (np.: za pomocą ankiet lub audytów stron trzecich) sposobu, w jaki dostawcy zabezpieczają procesy tworzenia kodu, dostarczania usług IT i ICT do Hadrone. Skanowanie podatności komponentów stron trzecich: Automatyczne, regularne testy podatności i testy penetracyjne dla infrastruktury IT ukierunkowane na wykrywanie luk w oprogramowaniu i sprzęcie dostarczonym przez zewnętrznych producentów. Monitorowanie alertów o zagrożeniach łańcucha dostaw: Stałe śledzenie biuletynów bezpieczeństwa (np.: bazy CVE, ostrzeżenia CERT Polska) pod kątem wykrywania ataków na systemy i oprogramowanie, z których korzystają dostawcy firmy (tzw. Supply Chain Attacks). 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 5.21 Zarządzanie łańcuchem dostaw ICT oraz przez: Strategia Zarządzania Bezpieczeństwem Informacji i chmury obliczeniowej w ramach ZSZ dla Hadrone (integracja obszaru ISMS i Cloud) - punkt: 4.2 Kryteria wyboru i oceny dostawców usług chmurowych	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z	N/A	tak
------	---------------	----------------------------------	----------------------	--------------	-----------------------------------	---	--	---	------	--	--	-----	-----



5.22	Organizacyjne	Monitorowanie usług dostawców	ISO 27001, ISO 27017	Security	CC_S4 - Monitoring Activities / Czynności monitorowania	<ul style="list-style-type: none"> • Cykle spotkań i przeglądów operacyjnych: Regularne (np.: miesięczne lub kwartalne) spotkania statusowe z dostawcami w celu omówienia bieżących wyników, zrealizowanych prac oraz incydentów. • Automatyczne systemy monitorowania infrastruktury: Wykorzystanie narzędzi technicznych (np.: systemów klas VRM, narzędzi do pingowania i badania dostępności) do niezależnego sprawdzania czy systemy dostawcy działają bez zakłóceń. • Proces zarządzania zmianą u dostawcy: Formalne działania, w ramach której dostawca musi zgłaszać i uzgadniać z firmą wszelkie planowane okna serwisowe, aktualizacje i istotne zmiany w architekturze swoich usług. • Pulpity menedżerskie i raporty wydajności: Narzędzia i szablony agregujące dane operacyjne dostawcy (np.: czas dostępności systemów, czas reakcji na zgłoszenia serwisowe) w formie czytelnych raportów okresowych. 	<ul style="list-style-type: none"> • Weryfikacja realizacji wskaźników SLA: Regularne porównywanie faktycznych wyników dostawcy z zapisami w umowie (np.: sprawdzanie czy dostępność usługi chmurowej wyniosła wymagane i zakontraktowane poziomy SLA). • Wskaźnik niedotrzymania warunków umowy (KPI): Monitorowanie wskaźników efektywności obszarów ZSZ. • Przeglądy raportów z audytów stron trzecich: Cykliczna weryfikacja zewnętrznych certyfikatów i sprawozdań dostawcy (np.: aktualność certyfikatu ISO 27001 lub raportu SOC 2 Type II), aby upewnić się, że jego wewnętrzne kontrole są skuteczne. • Śledzenie statusu naprawy błędów i podatności: Kontrola terminowości usuwania przez dostawcę luk bezpieczeństwa oraz realizacji rekomendacji poincydentalnych i poaudytowych. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 5.22 Monitorowanie usług dostawców oraz przez: Strategia Zarządzania Bezpieczeństwem Informacji i chmury obliczeniowej w ramach ZSZ dla Hadrone (integracja obszaru ISMS i Cloud) - punkt: 4.2 Kryteria wyboru i oceny dostawców usług chmurowych	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z	N/A	tak
------	---------------	-------------------------------	----------------------	----------	---	---	--	---	------	---	--	-----	-----



CL.P.5.23	Organizacyjne	Bezpieczeństwo w usługach chmurowych	ISO 27017, ISO 27018	Security	CC_S7 - System Operations / Operacje systemowe	<ul style="list-style-type: none"> • Zarządzanie stanem bezpieczeństwa chmury (Cloud Security Posture Management - CSPM): Zautomatyzowane narzędzia (np.: Microsoft Defender for Cloud) do ciągłego skanowania konfiguracji chmury pod kątem błędów i luk bezpieczeństwa. • Brokery Bezpieczeństwa Dostępu do Chmury (CASB): Narzędzia techniczne pośredniczące między użytkownikami a usługami chmurowymi. Dopuszcza się użycie VPN'a i koncentratorów hostowania usług RDP w szyfrowanym kanale komunikacji. • Proces hardeningu środowisk chmurowych: Stosowanie oficjalnych standardów bezpiecznej konfiguracji (np.: profili Center for Internet Security - CIS Benchmarks level 1) dla specyficznych usług chmurowych (IaaS, PaaS, SaaS). • Zarządzanie kluczami szyfrującymi (BYOK / HYOK): Procesy i narzędzia (Key Management Services - KMS) pozwalające firmie na zachowanie pełnej kontroli nad kluczami kryptograficznymi używanymi do szyfrowania danych w chmurze. Odstępstwo od BYOK i HYOK: dopuszcza się użycie mechanizmów PKM (Platform Key Management) dla zarządzania kluczami komponentów chmury obliczeniowej, które są 	<ul style="list-style-type: none"> • Automatyczny audyt błędów konfiguracji: Regularna (lub ciągła) weryfikacja raportów z systemów CSPM w celu natychmiastowego wykrywania i naprawiania krytycznych błędów. • Wskaźnik pokrycia standardów CIS (KPI): Monitorowanie wskaźników efektywności obszarów ZSZ. • Weryfikacja raportów audytowych dostawcy chmury: Coroczny formalny przegląd niezależnych certyfikatów i raportów dostawcy (np.: ISO 27001, ISO 27017, SOC 2 Type II) w celu potwierdzenia, że infrastruktura fizyczna dostawcy jest bezpieczna. • Testowanie mechanizmów odtwarzania (Cloud Backup/DR): Okresowe (np.: raz w roku) próby odtworzenia systemów i danych z kopii zapasowych przechowywanych w odizolowanym środowisku chmurowym (lub u innego dostawcy chmury) w celu weryfikacji ciągłości działania. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 5.23 Bezpieczeństwo w usługach chmurowych oraz dodatkowo przez: oraz przez: Strategia Zarządzania Bezpieczeństwem Informacji i chmury obliczeniowej w ramach ZSZ dla Hadrone (integracja obszaru ISMS i Cloud) - punkt: 4.2 Kryteria wyboru i oceny dostawców usług chmurowych	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z	Art. 21(2)j (NIS2) / Art. 28 (DORA)	tak
-----------	---------------	--------------------------------------	----------------------	----------	--	---	--	---	------	--	--	-------------------------------------	-----



						przechowywane przed dostawę chmury w Key Vault.							
--	--	--	--	--	--	---	--	--	--	--	--	--	--



5.24	Organizacyjne	Zarządzanie incydentami - planowanie	ISO 27001, ISO 27701, ISO 22301	Availability	CC_A0 - Availability / Dostępność	<ul style="list-style-type: none"> Plany reagowania na incydenty: Sformalizowane i zatwierdzone procedury operacyjne krok po kroku, opisujące działania dla konkretnych typów zagrożeń (np.: atak ransomware, wyciek danych, DDoS) – dla Hadrone są to plany DRP. Matryca eskalacji i schematy powiadomień: Procesowy algorytm określający kogo, kiedy i w jaki sposób należy powiadomić o incydencie (w tym zarząd, podmioty zewnętrzne, takie jak PUODO czy CERT Polska) czy klientów Hadrone. Zestawy narzędziowe do reagowania: Przygotowane wcześniej, odizolowane narzędzia techniczne (oprogramowanie do analizy śledczej, czyste nośniki danych, zapasowy sprzęt sieciowy) niezbędne do natychmiastowego podjęcia działań w terenie. – w tym obszarze Hadrone korzysta z usług firm zewnętrznych, np.: dostarczających usługi SOC. Harmonogram i program szkoleń oraz symulacji: Cykliczny proces szkolenia członków zespołu BCP i DRP oraz kluczowych decydentów z procedur zawartych w planach kryzysowych. 	<ul style="list-style-type: none"> Testowanie planów poprzez symulacje: Regularne (np.: raz w roku) przeprowadzanie warsztatowych symulacji kryzysowych w celu praktycznego sprawdzenia, czy zapisane w planach kroki i działania są zrozumiałe i skuteczne. Wskaźnik aktualności planów i kontaktów (KPI): Monitorowanie wskaźników efektywności obszarów ZSZ. Ocena gotowości zasobów: Cykliczny przegląd dostępności narzędzi technicznych oraz uprawnień personelu zadeklarowanego w planach do działania w sytuacjach awaryjnych. Przeglądy po incydentalne: Obowiązkowa weryfikacja planu po każdym realnym incydencie. Oznacza to formalne sprawdzenie, które elementy planowania zadziałały poprawnie, a które wymagają modyfikacji. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 5.24 Zarządzanie incydentami - planowanie oraz dodatkowo przez obszar BCMS, tj.: Strategia Zarządzania Ciągłością Działania w ramach Zintegrowanego Systemu Zarządzania dla Hadrone i Plan BCP dla Hadrone i Plan DRP dla Hadrone i przez obszar PIMS: Polityka Bezpieczeństwa Danych Osobowych w Hadrone Sp. z o.o. - punkt: 11. Postępowanie w sytuacji Naruszenia ochrony danych osobowych	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z oraz dodatkowo obszar regulowany przez RODO i w ramach ZSZ i BCMS (DRP i BCP)	Art. 21(2)b (NIS2) / Art. 17-23 (DORA)	tak
------	---------------	--------------------------------------	---------------------------------	--------------	-----------------------------------	---	--	---	------	---	--	--	-----



5.25	Organizacyjne	Ocena zdarzeń bezpieczeństwa	ISO 27001, ISO 22301	Security	CC_S1 - Control Environment/ Kontrole Środowiskowe	<ul style="list-style-type: none"> • Funkcja / Usługa SOC: usługa mająca na celu weryfikację logów z serwerów, sieci oraz chmury, które automatycznie korelują zdarzenia i alarmują o podejrzeniu ataku. • Narzędzia Cloud Logging i Audytu: Wykorzystanie wbudowanych mechanizmów dostawców chmury (np.: Azure Monitor) do ciągłego zbierania i analizowania zdarzeń związanych ze zmianami konfiguracji i dostępem do danych w chmurze. • Procedura raportowania zdarzeń przez pracowników: Prosty, wewnętrzny proces (np.: dedykowany adres e-mail – incydenty@hadrone.com), umożliwiający każdemu pracownikowi szybkie zgłoszenie podejrzonej aktywności (np.: maila phishingowego). 	<ul style="list-style-type: none"> • Wskaźnik czasu oceny zdarzenia (KPI): Monitorowanie wskaźników efektywności obszarów ZSZ. • Audyt kompletności logowania (Log Coverage): Cykliczne sprawdzanie, czy wszystkie krytyczne systemy lokalne oraz wszystkie aktywne usługi chmurowe poprawnie przesyłają logi do centralnego punktu analizy zdarzeń. • Testowe symulacje zdarzeń: Kontrolowane prowokowanie nietypowych zdarzeń w systemach (w tym chmurowych) w celu sprawdzenia czy systemy monitoringu oraz ludzie prawidłowo je wykryją, ocenią i sklasyfikują. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 5.25 Ocena zdarzeń bezpieczeństwa oraz dodatkowo przez obszar BCMS, tj.: Strategia Zarządzania Ciągłością Działania w ramach Zintegrowanego Systemu Zarządzania dla Hadrone i Plan BCP dla Hadrone i Plan DRP dla Hadrone i przez obszar PIMS: Polityka Bezpieczeństwa Danych Osobowych w Hadrone Sp. z o.o. - punkt: 11. Postępowanie w sytuacji Naruszenia ochrony danych osobowych	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z oraz dodatkowo obszar regulowany przez RODO i w ramach ZSZ i BCMS (DRP i BCP)	Art. 9 AI Act	tak
------	---------------	------------------------------	----------------------	----------	--	---	--	---	------	---	--	---------------	-----



CL.5.25	Organizacyjne	Zasady korzystania z chmury	ISO 27017	Security	CC_S2 - Information and Communication / Komunikacja i informowanie	<ul style="list-style-type: none"> • Funkcja / Usługa SOC: usługa mająca na celu weryfikację logów z serwerów, sieci oraz chmury, które automatycznie korelują zdarzenia i alarmują o podejrzeniu ataku. • Narzędzia Cloud Logging i Audytu: Wykorzystanie wbudowanych mechanizmów dostawców chmury (np.: Azure Monitor) do ciągłego zbierania i analizowania zdarzeń związanych ze zmianami konfiguracji i dostępem do danych w chmurze. • Procedura raportowania zdarzeń przez pracowników: Prosty, wewnętrzny proces (np.: dedykowany adres e-mail – incydenty@hadrone.com), umożliwiający każdemu pracownikowi szybkie zgłoszenie podejrzonej aktywności (np.: maila phishingowego). 	<ul style="list-style-type: none"> • Wskaźnik czasu oceny zdarzenia (KPI): Monitorowanie wskaźników efektywności obszarów ZSZ. • Audyt kompletności logowania (Log Coverage): Cykliczne sprawdzanie, czy wszystkie krytyczne systemy lokalne oraz wszystkie aktywne usługi chmurowe poprawnie przesyłają logi do centralnego punktu analizy zdarzeń. • Testowe symulacje zdarzeń: Kontrolowane prowokowanie nietypowych zdarzeń w systemach (w tym chmurowych) w celu sprawdzenia czy systemy monitoringu oraz ludzie prawidłowo je wykryją, ocenią i sklasyfikują. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 5.25 Zasady korzystania z chmury oraz dodatkowo przez: Strategia Zarządzania Bezpieczeństwem Informacji i chmury obliczeniowej w ramach ZSZ dla Hadrone (integracja obszaru ISMS i Cloud) - patrz punkt: 4 Strategia ISMS w Cloud Governance (ISO 27017 / ISO 27018)	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZSZ oraz dodatkowo regulowany przez obszar systemowy ZSZ	N/A	tak
---------	---------------	-----------------------------	-----------	----------	--	--	--	---	------	--	--	-----	-----



5.26	Organizacyjne	Reagowanie na incydenty	ISO 27001, ISO 27018, ISO 22301	Security	CC_S5 - Control Activities / Czynności kontrolne	<ul style="list-style-type: none"> • Scenariusze reagowania: Precyzyjne instrukcje techniczne i proceduralne dla konkretnych typów ataków (np.: Ransomware, DDoS, Phishing), automatyzujące schemat działania zespołu. • Systemy automatycznej izolacji (EDR / XDR): Narzędzia informatyczne, które potrafią samoczynnie lub za jednym kliknięciem zablokować podejrzany proces, odciąć komputer od sieci czy unieważnić sesję użytkownika. Hadrone w tym obszarze korzysta z usług SOC. • Most konferencyjny i systemy powiadomień masowych: Narzędzia i dedykowane kanały komunikacji alarmowej (np.: wydzielone kanały Teams/Slack), służące do natychmiastowego zwołania zespołu reagowania kryzysowego. • Proces formalnej eskalacji: Ustrukturyzowana ścieżka informowania Zarządu Hadrone, klientów Hadrone oraz instytucji zewnętrznych (np.: CERT Polska, PUODO) o skali i skutkach trwającego incydentu. 	<ul style="list-style-type: none"> • Wskaźnik czasu reakcji i obsługi (KPI): Monitorowanie wskaźników efektywności obszarów ZSZ. • Weryfikacja kompletności logów z obsługi: Kontrola polegająca na sprawdzeniu, czy każda decyzja i działanie podjęte podczas incydentu zostały automatycznie lub manualnie zapisane w systemie zgłoszeń (tworzenie tzw. osi czasu). • Testowe symulacje: Praktyczne, niespodziewane testy techniczne (np.: kontrolowany atak na infrastrukturę), weryfikujące czy zespół potrafi prawidłowo i w wymaganym czasie zareagować na realne zagrożenie. • Przeglądy po incydentalne: Obowiązkowa weryfikacja planu po każdym realnym incydencie. Oznacza to formalne sprawdzenie, które elementy planowania zadziałały poprawnie, a które wymagają modyfikacji. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 5.26 Reagowanie na incydenty oraz dodatkowo przez obszar BCMS, tj.: Strategia Zarządzania Ciągłością Działania w ramach Zintegrowanego Systemu Zarządzania dla Hadrone i Plan BCP dla Hadrone i Plan DRP dla Hadrone i przez obszar PIMS: Polityka Bezpieczeństwa Danych Osobowych w Hadrone Sp. z o.o. - punkt: 11. Postępowanie w sytuacji Naruszenia ochrony danych osobowych	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z oraz dodatkowo obszar regulowany przez RODO i w ramach ZSZ i BCMS (DRP i BCP)	N/A	tak
------	---------------	-------------------------	---------------------------------	----------	--	--	---	---	------	--	--	-----	-----



5.27	Organizacyjne	Wnioski z incydentów	ISO 27001, ISO 22301	Security	CC_S5 - Control Activities / Czynności kontrolne	<ul style="list-style-type: none"> Proces przeglądu pi incydencie: Sformalizowane spotkanie kluczowych uczestników obsługi incydentu (analityków, IT, biznesu), mające na celu odtworzenie osi czasu ataku i wskazanie luk w obronie. Metodologia analizy przyczyn źródłowych (Root Cause Analysis - RCA): Stosowanie ustrukturyzowanych technik (np.: metody 5 Why – 5 razy, dlaczego?) do dotarcia do prawdziwej, głębokiej przyczyny zaistnienia incydentu. Rejestr działań korygujących: Centralny system (np.: moduł w Jira lub strona SharePoint) służący do zapisywania rekomendacji po incydentach, wyznaczania ich właścicieli oraz śledzenia terminów wdrożenia. Aktualizacja bazy wiedzy i scenariuszy: Proces techniczny polegający na modyfikacji procedur reagowania na incydenty oraz reguł wykrywania w systemach zdarzeń niebezpiecznych na podstawie nowo zdobytych doświadczeń. 	<ul style="list-style-type: none"> Wskaźnik powtarzalności incydentów (KPI): Monitorowanie wskaźników efektywności obszarów ZSZ. Kontrola terminowości realizacji zadań korygujących: Regularny (np.: miesięczny) przegląd statusu otwartych rekomendacji po incydentalnych pod kątem przekroczenia zaplanowanych terminów wdrożenia zabezpieczeń. Weryfikacja skuteczności wdrożonych poprawek: Ponowne przeprowadzenie ukierunkowanych testów bezpieczeństwa (np.: ponowny test penetracyjny lub kontrolowany phishing) w celu technicznego potwierdzenia, że dana podatność została trwale usunięta. Raportowanie trendów dla Forum ds. ZSZ: Cykliczne prezentowanie zagregowanych wniosków i statystyk z incydentów, umożliwiające podejmowanie decyzji o strategicznych zmianach w budżecie ZSZ. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 5.27 Wnioski z incydentów oraz dodatkowo przez obszar BCMS, tj.: Strategia Zarządzania Ciągłością Działania w ramach Zintegrowanego Systemu Zarządzania dla Hadrone i Plan BCP dla Hadrone i Plan DRP dla Hadrone i przez obszar PIMS: Polityka Bezpieczeństwa Danych Osobowych w Hadrone Sp. z o.o. - punkt: 11. Postępowanie w sytuacji Naruszenia ochrony danych osobowych	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z oraz dodatkowo obszar regulowany przez RODO i w ramach ZSZ i BCMS (DRP i BCP)	N/A	tak
------	---------------	----------------------	----------------------	----------	--	--	---	---	------	---	--	-----	-----



5.28	Organizacyjne	Zbieranie dowodów	ISO 27001	Security	CC_S5 - Control Activities / Czynności kontrolne	<ul style="list-style-type: none"> • Kryptograficzne sumy kontrolne (Haszowanie): Proces natychmiastowego generowania unikalnych skrótów (np.: SHA-256) dla zabezpieczonych plików lub obrazów dysków w celu późniejszego udowodnienia, że dane nie zostały zmienione. • Blokery zapisu: Specjalistyczne narzędzia techniczne odcinające możliwość jakiegokolwiek zapisu danych na badany nośnik podczas wykonywania jego kopii e celach inwestycji. • Oprogramowanie do informatyki śledczej (Computer Forensics): Narzędzia specjalistyczne do których Hadrone nie ma dostępu i nie ma kompetencji, obszar ten zamawia się w ramach potrzeb poza Hadrone w specjalistycznych firmach informatyki śledczej. • Procedura i szablon protokołowania: Sformalizowany proces komisijnego zabezpieczania dowodów, obejmujący m.in. fotografowanie miejsca zdarzenia, plombowanie fizycznego sprzętu oraz wypełnianie papierowych kart łańcucha dowodowego. 	<ul style="list-style-type: none"> • Weryfikacja zgodności sum kontrolnych: Kontrola polegająca na ponownym przeliczeniu skrótu kryptograficznego przed rozpoczęciem analizy i porównaniu go z wartością zapisaną w momencie zabezpieczenia (wynik musi być identyczny). • Wskaźnik poprawności procedury (KPI): Monitorowanie wskaźników efektywności obszarów ZSZ. • Szkolenia i certyfikacja personelu: Cykliczne sprawdzanie uprawnień oraz umiejętności osób wyznaczonych do zbierania dowodów (np.: posiadanie certyfikatów, kompetencje w wykorzystaniu narzędzi) w celu zapewnienia profesjonalizmu działań. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 5.28 Zbieranie dowodów oraz przez: Zbiór procedur systemowych funkcjonujących w Hadrone dla Zintegrowanego Systemu Zarządzania (ZSZ) - punkt: 4.3 Procedura klasyfikacji informacji i danych dla ZSZ	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ obszar powiązany z obszarem systemowym ZSZ	N/A	tak
------	---------------	-------------------	-----------	----------	--	---	---	---	------	--	--	-----	-----



5.29	Organizacyjne	Bezpieczeństwo podczas zakłóceń	ISO 27001, ISO 22301	Availability	CC_A0 - Availability / Dostępność	<ul style="list-style-type: none"> Procedury awaryjne zintegrowane z bezpieczeństwem (BCP): Plany ciągłości działania (Business Continuity Plans), które oprócz kroków odtworzeniowych zawierają specyficzne instrukcje dotyczące zachowania poufności i integralności danych w sytuacji kryzysowej. Konta awaryjne typu „Break-Glass”: Specjalne, wysoko uprawnione, ale głęboko ukryte i monitorowane konta dostępowe, używane wyłącznie w sytuacjach skrajnych, gdy standardowe metody zarządzania tożsamością zawiodą. Zapasowe, bezpieczne kanały łączności: Odizolowane systemy komunikacji (np.: szyfrowane komunikatory poza domeną Hadrone), które pozwalają zespołowi kryzysowemu na bezpieczną koordynację działań podczas niedostępności głównej sieci. Autonomiczne zasilanie i ochrona fizyczna: Systemy UPS, agregaty prądowórcze oraz systemy kontroli dostępu działające na zasilaniu bateryjnym, zapewniające ciągłość ochrony fizycznej serwerowni w trakcie przerw w dostawie prądu. 	<ul style="list-style-type: none"> Testowanie bezpieczeństwa w warunkach stresu (Symulacje BCP): Regularne (np.: raz w roku) ćwiczenia kryzysowe, podczas których celowo weryfikuje się, czy w trakcie symulowanej awarii pracownicy pamiętają o procedurach ochrony danych i czy systemy zapasowe są bezpieczne. Audyt logów z okresu zakłóceń: Obowiązkowa, po incydentalna kontrola wszystkich logów systemowych i rejestrów dostępu wygenerowanych w czasie trwania awarii, w celu wykrycia ewentualnych nadużyć lub prób nieautoryzowanego dostępu. Wskaźnik dostępności zabezpieczeń (KPI): Monitorowanie wskaźników efektywności obszarów ZSZ. Weryfikacja uprawnień po powrocie do normy: Natychmiastowa kontrola i cofnięcie wszelkich tymczasowych dostępu administracyjnych oraz haseł ratunkowych, które zostały wydane personelowi technicznemu na czas opanowywania kryzysu. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 5.29 Bezpieczeństwo podczas zakłóceń oraz dodatkowo przez obszar BCMS, tj.: Strategia Zarządzania Ciągłością Działania w ramach Zintegrowanego Systemu Zarządzania dla Hadrone i Plan BCP dla Hadrone i Plan DRP dla Hadrone	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z oraz dodatkowo obszar regulowany przez RODO i w ramach ZSZ i BCMS (DRP i BCP)	Art. 21(2)c (NIS2) / Art. 11 (DORA)	tak
------	---------------	---------------------------------	----------------------	--------------	-----------------------------------	--	--	---	------	--	--	-------------------------------------	-----



5.30	Organizacyjne	Gotowość ICT do ciągłości działania	ISO 27001, ISO 22301, ISO 27017	Availability	CC_A0 - Availability / Dostępność	<ul style="list-style-type: none"> • Analiza BIA i wyznaczenie parametrów RTO/RPO: Przegląd analizy BIA raz w roku i weryfikacja parametrów MTD, RPO i RTO. • Plany DRP: Szczegółowe, techniczne procedury operacyjne opisujące krok po kroku proces uruchamiania systemów w zapasowym centrum danych lub chmurze w sytuacjach kryzysowych. • Architektura wysokiej dostępności i replikacja: Narzędzia do ciągłego tworzenia kopii zapasowych (Backup) oraz mechanizmy replikacji danych w czasie rzeczywistym do geograficznie odizolowanej lokalizacji wtórnej. • Zautomatyzowane systemy przełączania (Failover): Rozwiązania sieciowe i serwerowe (np.: load balancery, klastry wysokiej dostępności), które w sposób automatyczny lub półautomatyczny przekierowują ruch użytkowników do sprawnej infrastruktury w razie awarii głównej jednostki. 	<ul style="list-style-type: none"> • Testy Disaster Recovery (DR Exercises): Regularne (np.: raz w roku) praktyczne próby odtworzenia systemów z backupu lub symulacje całkowitego wyłączenia głównego centrum danych i przełączenia biznesu na środowisko zapasowe. • Audyt spójności i kompletności backupów: Automatyczna, cykliczna weryfikacja poprawności wykonania kopii zapasowych oraz okresowe, próbne przywracanie losowych baz danych w celu potwierdzenia ich integralności. • Monitorowanie dostępności dostawców krytycznych (SLA): Ciągła kontrola zewnętrznych dostawców infrastruktury (np.: dostawców prądu, Internetu, usług chmurowych) pod kątem spełniania przez nich gwarantowanych wskaźników dostępności systemów. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 5.30 Gotowość ICT do ciągłości działania oraz dodatkowo przez obszar BCMS, tj.: Strategia Zarządzania Ciągłością Działania w ramach Zintegrowanego Systemu Zarządzania dla Hadrone i Plan BCP dla Hadrone i Plan DRP dla Hadrone	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z oraz dodatkowo obszar regulowany przez RODO i w ramach ZSZ i BCMS (DRP i BCP)	Art. 21(2)c (NIS2) / Art. 12 (DORA)	tak
------	---------------	-------------------------------------	---------------------------------	--------------	-----------------------------------	--	---	---	------	--	--	-------------------------------------	-----



5.31	Organizacyjne	Wymagania prawne i umowne	ISO 27001, ISO 27701	Security	CC_S5 - Control Activities / Czynności kontrolne	<ul style="list-style-type: none"> • Rejestr wymagań prawnych i umownych: Centralna, regularnie aktualizowana baza danych zawierająca listę wszystkich aktów prawnych (np.: RODO, DORA, NIS2, AI Act, itp.) i kontraktów Hadrone. • Współpraca z kancelarią prawną (Legal Desk): Sformalizowany sposób działania opiniowania nowych umów oraz projektów IT pod kątem zgodności z prawem i wymaganiami dla bezpieczeństwa informacji i ochrony danych osobowych. • Szkolenia z zakresu Legal Compliance: Program edukacyjny dla pracowników, uświadamiający ich w zakresie odpowiedzialności prawnej oraz specyficznych obowiązków regulacyjnych w ich codziennej pracy. • Subskrypcje i alerty legislacyjne: Narzędzia i serwisy zewnętrzne dostarczające automatyczne powiadomienia o planowanych i wprowadzanych zmianach w prawie (np.: serwisy rządowe, branżowe biuletyny prawnicze). 	<ul style="list-style-type: none"> • Audyty zgodności prawnej (Legal Compliance Audits): Okresowe, niezależne przeglądy (np.: raz w roku) realizowane przez audytorów, oceniające stopień realnego spełnienia wymagań regulacyjnych przez organizację. • Wskaźnik zidentyfikowanych niezgodności (KPI): Monitorowanie wskaźników efektywności obszarów ZSZ. • Weryfikacja klauzul bezpieczeństwa w umowach: Wyrównoważona kontrola podpisanych kontraktów handlowych w celu sprawdzenia, czy zawierają one standardowe i wymagane przez politykę ZSZ Hadrone zapisy dotyczące ochrony danych i informacji, w tym danych osobowych. • Monitorowanie kar i postępowań regulacyjnych: Śledzenie oraz raportowanie do Zarządu Hadrone wszelkich oficjalnych zapytań, skarg, postępowań wyjaśniających lub nałożonych kar przez organy państwowe i nadzorcze. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 5.31 Wymagania prawne i umowne oraz dodatkowo przez umowy o współpracy i Kodeks Pracy	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ obszar powiązany z obszarem systemowym ZSZ	N/A	tak
------	---------------	---------------------------	----------------------	----------	--	--	--	---	------	---	--	-----	-----



5.32	Organizacyjne	Prawa własności intelektualnej	ISO 27001	Security	CC_S5 - Control Activities / Czynności kontrolne	<ul style="list-style-type: none"> • Zarządzanie aktywami oprogramowania: Działania służące ewidencji zakupionych licencji, kluczy aktywacyjnych oraz instalacji oprogramowania. • Blokada praw administratora i White-listing: Techniczne mechanizmy ograniczające użytkownikom możliwość samodzielnego instalowania aplikacji na komputerach służbowych bez zgody i weryfikacji Hadrone CISO. • Skanery kodu i audyt Open-Source (SCA): Narzędzia (np.: skanery SAST) automatycznie sprawdzające kod źródłowy tworzony przez deweloperów pod kątem obecności i legalności użytych bibliotek open-source. • Zapisy w umowach (NDA / IP Clauses): Sformalizowane klauzule w umowach o pracę (UoP) oraz kontraktach B2B, precyzyjnie regulujące 	<ul style="list-style-type: none"> • Audyt zgodności licencyjnej: Cykliczne (np.: raz w roku) porównywanie liczby zakupionych licencji ze stanem faktycznym, czyli liczbą aplikacji realnie zainstalowanych na stacjach roboczych i serwerach Hadrone. • Wskaźnik nieautoryzowanego oprogramowania (KPI): Monitorowanie wskaźników efektywności obszarów ZSZ. • Przegląd praw dostępu do kodu źródłowego: Regularna weryfikacja list uprawnień do repozytoriów kodu GitHub, uniemożliwiająca dostęp osobom nieuprawnionym oraz byłym pracownikom. • Weryfikacja wygasania licencji i subskrypcji: Automatyczne alerty i systematyczny przegląd kalendarza umów, zapobiegające sytuacjom, w których Hadrone korzysta z oprogramowania po wygaśnięciu okresu subskrypcji. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 5.32 Prawa własności intelektualnej oraz dodatkowo przez umowy o współpracy i Kodeks Pracy	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ obszar powiązany z obszarem systemowym ZSZ	N/A	tak
------	---------------	--------------------------------	-----------	----------	--	--	---	---	------	--	--	-----	-----



5.33	Organizacyjne	Ochrona rekordów	ISO 27001, ISO 27701	Security	CC_S5 - Control Activities / Czynności kontrolne	<ul style="list-style-type: none"> • Harmonogram retencji rekordów (Retention Schedule): Sformalizowana macierz i powiązany z nią proces, określające typy dokumentów w organizacji wraz ze wskazaniem dokładnego czasu ich przechowywania i metody utylizacji. • Systemy Elektronicznego Zarządzania Dokumentacją (EZD / DMS): Specjalistyczne oprogramowanie z wdrożonym systemem uprawnień, metadanych oraz automatycznym śledzeniem historii zmian (Audit Trail) dla każdego dokumentu. • Procesy bezpiecznego niszczenia (Procedury utylizacji): Techniczne niszczenie rekordów elektronicznych (np.: demagnetyzacja, nadpisywanie wielokrotne) oraz fizycznych dokumentów papierowych (np.: niszczenie zgodnie z normą DIN 66399) przez certyfikowane podmioty. 	<ul style="list-style-type: none"> • Weryfikacja integralności i sum kontrolnych: Regularne, automatyczne sprawdzanie sum kontrolnych (np.: skrótów kryptograficznych SHA-256) przechowywanych rekordów w celu upewnienia się, że pliki nie uległy uszkodzeniu lub manipulacji. • Wskaźnik terminowości niszczenia (KPI): Monitorowanie wskaźników efektywności obszarów ZSZ. • Audyt próbny odtwarzania i odczytu archiwów: Okresowe (np.: raz w roku) testowe wyciąganie losowych, starych rekordów z archiwów cyfrowych i fizycznych w celu sprawdzenia czy procedury indeksowania działają, a formaty plików są nadal czytelne. • Kontrola uprawnień i logów dostępu: Cykliczny przegląd logów systemowych pod kątem wykrywania nietypowych prób masowego pobierania, modyfikacji lub usuwania rekordów, szczególnie przez konta o wysokich uprawnieniach (administratorów). 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 5.33 Ochrona rekordów	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ obszar powiązany z obszarem systemowym ZSZ	N/A	tak
------	---------------	------------------	----------------------	----------	--	--	--	---	------	---	--	-----	-----



CL.P.5.34	Organizacyjne	Prywatność i ochrona PII	ISO 27701, ISO 27018	Privacy	CC_P9 - Monitoring and Enforcement / Monitorowanie i egzekwowanie	<ul style="list-style-type: none"> Ocena skutków dla ochrony danych (DPIA): Sformalizowany proces analizy ryzyka przeprowadzany przed uruchomieniem operacji przetwarzania, które mogą powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych. Techniki pseudonimizacji i anonimizacji: Narzędzia kryptograficzne i algorytmiczne służące do ukrywania tożsamości (np.: poprzez maskowanie danych, haszowanie identyfikatorów lub usuwanie cech jednoznacznie identyfikujących osobę). System zarządzania zgodami: Formularze służące do rejestrowania, weryfikacji i łatwego wycofywania zgód marketingowych oraz preferencji prywatności przez użytkowników platformy SaaS oraz pracowników Hadrone. Rejestr Czynności Przetwarzania (RCP): Proces i centralna baza danych mapująca wszystkie przepływy danych osobowych w organizacji, zawierająca informacje o celach, kategoriach danych, odbiorcach i terminach ich retencji. 	<ul style="list-style-type: none"> Weryfikacja realizacji praw osób (DSAR): Regularna kontrola terminowości i poprawności realizacji wniosków od osób fizycznych (np.: żądanie wglądu do danych, prawo do zapomnienia, sprostowanie danych) w ustawowym czasie (np.: do 30 dni). Wskaźnik incydentów ochrony prywatności (KPI): Miara określająca liczbę oraz dotkliwość zdarzeń związanych z naruszeniem ochrony PII (np.: wyciek danych, nieuprawniony dostęp) i czas ich zgłoszenia do organu nadzorczego (cel: zgłoszenie w max 72h). Audyty procesorów i podmiotów przetwarzających: Cykliczna weryfikacja zewnętrznych dostawców (np.: firm hostingowych, systemów CRM, dostawców IaaS), którym powierzono dane, pod kątem spełniania przez nich wymagań umów powierzenia (DPA). Skanowanie baz pod kątem "dzikich" zbiorów PII: Zautomatyzowane testy i przeszukiwanie firmowych dysków oraz chmur w celu wykrycia nieszyfrowanych plików zawierających dane osobowe (np.: arkuszy Excel z bazami klientów) poza wyznaczonymi do tego systemami. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 5.34 Prywatność i ochrona PII oraz dodatkowo przez obszar RODO: Polityka Bezpieczeństwa Danych Osobowych w Hadrone Sp. z o.o.	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z oraz dodatkowo regulowany przez RODO i w ramach ZSZ	Art. 21(1) (NIS2) / Art. 12 (DORA) / Art. 10 AI Act	tak
-----------	---------------	--------------------------	----------------------	---------	---	--	---	---	------	---	--	---	-----



5.35	Organizacyjne	Niezależny przegląd bezpieczeństwa	ISO 27001, ISO 27701	Security	CC_S5 - Control Activities / Czynności kontrolne	<ul style="list-style-type: none"> • Program i harmonogram audytów: Sformalizowany proces planowania, który definiuje zakres, częstotliwość oraz metodologię przeprowadzania niezależnych weryfikacji w poszczególnych obszarach Hadrone. • Audyty zewnętrzne i certyfikacyjne: Procesy formalnej oceny realizowane przez akredytowane jednostki certyfikujące (np.: w celu odnowienia certyfikatu ISO 27001, ISO 27701, ISO 22301) lub zewnętrznych audytorów IT. • Testy penetracyjne i skanowanie podatności: Techniczne mechanizmy weryfikacji odporności infrastruktury, symulujące realne ataki hakerskie, zlecane wyspecjalizowanym firmom zewnętrznym. • Procedura zarządzania rekomendacjami poaudytowymi: Sformalizowane działania (często wspierany systemami typu Jira lub MS Planer), służący do rejestrowania wykrytych niezgodności, przypisywania działań naprawczych oraz monitorowania ich realizacji. 	<ul style="list-style-type: none"> • Ocena niezależności audytorów: Przedaudytowa kontrola formalna weryfikująca, czy zespół realizujący przegląd nie brał udziału w projektowaniu, wdrażaniu ani codziennym utrzymaniu kontrolowanych systemów. • Wskaźnik powtarzalności podatności: Miara sprawdzająca, czy podczas kolejnych, niezależnych przeglądów wykrywane są te same błędy lub luki (wysoki wskaźnik oznacza nieskuteczność wcześniejszych działań naprawczych). • Przegląd wyników przez Kierownictwo Hadrone: Formalna kontrola zarządcza polegająca na cyklicznym przedstawianiu raportów z niezależnych przeglądów Kierownictwu Hadrone w celu podjęcia decyzji o alokacji budżetu na poprawę funkcjonowania ZSZ. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 5.35 Niezależny przegląd bezpieczeństwa oraz dodatkowo przez: Zbiór procedur systemowych funkcjonujących w Hadrone dla Zintegrowanego Systemu Zarządzania (ZSZ) - punkt: 4.6 Procedura audytów i przeglądów dla ZSZ i punktem: 4.7 Procedura przeglądu zarządczego dla ZSZ	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ obszar powiązany z obszarem systemowym ZSZ	N/A	tak
------	---------------	------------------------------------	----------------------	----------	--	--	--	---	------	--	--	-----	-----



5.36	Organizacyjne	Zgodność z zasadami i standardami	ISO 27001	Security	CC_S5 - Control Activities / Czynności kontrolne	<ul style="list-style-type: none"> • Programy i systemy GRC (Governance, Risk and Compliance): Hadron, jako niewielka organizacja wykorzystuje przygotowany arkusz excel do mapowania wymagań prawnych i standardów na wewnętrzne procedury oraz monitorowania stanu zgodności firmy. • Proces przeglądu konfiguracji (Hardening Standards): Proces techniczny polegający na tworzeniu i wdrażaniu oficjalnych wytycznych bezpiecznej konfiguracji (np.: standardy CIS Benchmarks) dla systemów operacyjnych, baz danych i sieci. • System zarządzania dokumentacją normatywną: Proces cyklicznego przeglądu, aktualizacji i publikacji wewnętrznych polityk, zasad, wymagań i regulacji ZSZ w celu zapewnienia ich stałej spójności z dynamicznie zmieniającymi się przepisami prawa. • Automatyczne skanery zgodności (Compliance Scanners): Narzędzia IT, które automatycznie i bez przerwy weryfikują, czy serwery i stacje robocze posiadają konfigurację zgodną z przyjętymi w organizacji szablonami bezpieczeństwa. 	<ul style="list-style-type: none"> • Audyty zgodności (Compliance Audits): Planowe, niezależne kontrole wewnętrzne lub zewnętrzne (np.: audyt certyfikacyjny ISO 27001) weryfikujące faktyczny stan wdrożenia i przestrzegania określonych norm i standardów. • Weryfikacja odstępstw od standardów (Exceptions Tracking): Rejestr i regularny przegląd wszystkich zatwierdzonych, tymczasowych odstępstw od standardów bezpieczeństwa (tzw. security exceptions) wraz z analizą powiązanego ryzyka. • Testy i ocena świadomości normatywnej: Regularne sprawdzanie wiedzy personelu (np.: poprzez quizy compliance lub wywiady audytorskie) pod kątem znajomości kluczowych zasad i standardów postępowania obowiązujących w firmie. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadronie - punkt: 5.36 Zgodność z zasadami i standardami	W zakresie ZSZ Hadronie, nie wymaga uzasadnienia, ponieważ obszar powiązany z obszarem systemowym ZSZ	N/A	tak
------	---------------	-----------------------------------	-----------	----------	--	---	--	---	------	---	---	-----	-----



5.37	Organizacyjne	Udokumentowane procedury operacyjne	ISO 27001, ISO 27017	Security	CC_S5 - Control Activities / Czynności kontrolne	<ul style="list-style-type: none"> Baza wiedzy i repozytorium dokumentów (np.: Confluence, SharePoint): Centralna, uporządkowana platforma cyfrowa służąca do tworzenia, przechowywania i kategoryzowania wszystkich procedur operacyjnych z wdrożonym systemem uprawnień RBAC. Proces zarządzania cyklem życia dokumentu (Wersjonowanie): Formalna ścieżka tworzenia dokumentu, która obejmuje metrykę dokumentu, nazwę, wersję, tytuł, opcjonalnie skrót literowo-znakowy. Szablony i standardy dokumentacji: Ujednolicone szablony dokumentów w Hadrone gwarantują spójność i czytelność dokumentów w całej organizacji. System powiadomień o przeglądach: Działanie, które wymusza na właścicielu dokumentu jej weryfikację i ponowne zatwierdzenie. 	<ul style="list-style-type: none"> Audyt aktualności i przeglądów dokumentacji: Regularna weryfikacja (np.: raz w roku) rejestru dokumentów systemowych i operacyjnych Hadrone w celu wykrycia dokumentów, które nie były aktualizowane lub zatwierdzane w wymaganym terminie. Testowanie procedur w praktyce (Walkthrough): Wyrywkowe, praktyczne sprawdzanie skuteczności dokumentu polegające na zleceniu wykonania danej czynności (np.: odtworzenia bazy z backupu) nowemu lub innemu pracownikowi wyłącznie na podstawie zapisanej procedury. Weryfikacja zgodności działań z procedurą: Porównywanie logów systemowych z zapisami w procedurach (np.: sprawdzenie, czy faktyczne kroki podjęte podczas konfiguracji nowego serwera były w 100% zgodne z zatwierdzoną instrukcją instalacji). – dotyczy głównie IaaS uruchamianego z mechanizmu IaC. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 5.37 Udokumentowane procedury operacyjne (spis procedur) oraz instrukcje operacyjne dla np.: IaC czy Backup Restore.	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ obszar powiązany z obszarem systemowym ZSZ oraz dodatkowo regulowany przez RODO i w ramach ZSZ przez ZZPO_MK_ZS Z	N/A	tak
------	---------------	-------------------------------------	----------------------	----------	--	--	---	---	------	--	---	-----	-----



6.1	Ludzie	Badanie kandydatów	ISO 27001, ISO 27701	Security	CC_S1 - Control Environment/ Kontrola Środowiskowe	<ul style="list-style-type: none"> • Procedura Background Screeningu (Weryfikacja przeszłości): Sformalizowany proces określający kroki sprawdzania tożsamości, historii zatrudnienia, wykształcenia oraz, w uzasadnionych prawem przypadkach, niekaralności kandydata. • Szablony umów i kwestionariuszy rekrutacyjnych: Ujednolicone dokumenty zawierające klauzule informacyjne, oświadczenia kandydata o prawdziwości danych oraz formularze do zbierania referencji od poprzednich pracodawców. • Matryca ryzyka stanowisk rekrutacyjnych: Dokument procesowy przypisujący poziom wymaganej weryfikacji do roli w Hadrone. • Zewnętrzne usługi weryfikacyjne (Background check agencies): Narzędzia i współpraca z wyspecjalizowanymi podmiotami zewnętrznymi, które realizują audyt przeszłości kandydata na zlecenie Hadrone, gwarantując obiektywizm i zgodność prawną. 	<ul style="list-style-type: none"> • Wskaźnik kompletności weryfikacji przed zatrudnieniem (KPI): Monitorowanie wskaźników efektywności obszarów ZSZ. • Audyt dokumentacji rekrutacyjnej: Wyrzykowa, cykliczna kontrola teczek rekrutacyjnych w celu upewnienia się, że zawierają one wszystkie wymagane potwierdzenia (np.: kopie dyplomów, pisemne referencje, formularze zgód). 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 6.1 Badanie kandydatów oraz dodatkowo przez umowy o współpracy i Kodeks Pracy	W zakresie ZSZ regulowany przez przepisy prawa poliego - Kodeks Pracy oraz dodatkowo przez Regulami organizacyjny Hadrone	N/A	tak
-----	--------	--------------------	----------------------	----------	---	---	--	---	------	---	---	-----	-----



6.2	Ludzie	Zasady i warunki zatrudnienia	ISO 27001, ISO 27701	Security	CC_S2 - Information and Communication / Komunikacja i informowanie	<ul style="list-style-type: none"> • Umowy o zachowaniu poufności (NDA / Non-Disclosure Agreement): Formalne dokumenty prawne lub dedykowane klauzule w umowach o pracę (UoP) oraz kontraktach cywilnoprawnych B2B, precyzujące zakres informacji chronionych oraz warunki ochrony informacji i danych Hadrone. • Proces Onboardingu i podpisywania oświadczeń: Działanie, podczas którego nowo zatrudniana osoba podpisuje cyfrowo lub fizycznie Zasady Bezpieczeństwa funkcjonujące w ramach ZSZ w Hadrone oraz inne kluczowe regulaminy. • Regulamin Pracy i Kodeks Etyki: Centralne dokumenty organizacyjne zawierające formalne zapisy o procedurach dyscyplinarnych oraz odpowiedzialności pracownika za powierzone mienie i dane, w tym dane osobowe. • System archiwizacji dokumentów HR: Narzędzie informatyczne służące do bezpiecznego przechowywania podpisanych umów, aneksów oraz oświadczeń pracowników w ich cyfrowych teczkach osobowych lub folderach. 	<ul style="list-style-type: none"> • Wskaźnik podpisanych umów i NDA (KPI): Monitorowanie wskaźników efektywności obszarów ZSZ. • Audyt kompletności teczek osobowych: Wyrywkowa, cykliczna kontrola dokumentacji pracowniczej w firmie zajmującej się sprawami HR, sprawdzająca czy wszystkie oświadczenia dotyczące bezpieczeństwa są aktualne i prawidłowo podpisane. • Przegląd klauzul umownych (Legal Review): Okresowa (np.: raz w roku) weryfikacja wzorców umów przez kancelarię prawną w celu ich dostosowania do nowych przepisów (np.: zmian w prawie pracy lub nowych regulacji cyberbezpieczeństwa). 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 6.2 Zasady i warunki zatrudnienia oraz dodatkowo przez umowy o współpracy i Kodeks Pracy	W zakresie ZSZ regulowany przez przepisy prawa poliego - Kodeks Pracy oraz dodatkowo przez Regulami organizacyjny Hadrone	N/A	tak
-----	--------	-------------------------------	----------------------	----------	--	--	---	---	------	--	---	-----	-----



6.3	Ludzie	Świadomość i szkolenie	ISO 27001, ISO 27701, ISO 22301	Security	CC_S3 - Risk Assessment / Ocena ryzyka	<ul style="list-style-type: none"> Platformy e-learningowe (LMS): W przypadku specjalistycznych zagadnień Hadrone wykorzystuje zewnętrzne platformy szkoleniowe i kupuje szkolenia na zewnątrz. Szkolenia wprowadzające (Security Onboarding): Obowiązkowy moduł szkoleniowy realizowany w pierwszym tygodniu pracy nowo zatrudnionej osoby, kończący się testem wiedzy przed przystąpieniem do pracy w Hadrone. Systematyczne symulacje socjotechniczne: Narzędzia do przeprowadzania kontrolowanych kampanii phishingowych i vishingowych, które uczą pracowników rozpoznawania manipulacji w bezpiecznych warunkach. Kanały bieżącej komunikacji (Newsletters / Alert Security): Krótkie infografiki, cykliczne porady oraz błyskawiczne powiadomienia wysyłane przez komunikatory (Teams/Slack) lub email w przypadku wykrycia fali nowych oszustw. 	<ul style="list-style-type: none"> Wskaźnik ukończenia szkoleń obowiązkowych (KPI): Monitorowanie wskaźników efektywności obszarów ZSZ. Wskaźnik podatności na phishing (Click Rate): Statystyka określająca, jaki procent pracowników dał się nabrać na wewnętrzną, kontrolowaną kampanię testową poprzez kliknięcie w link lub podanie danych. Egzaminy i testy kompetencji: Okresowa (np.: raz w roku) weryfikacja wiedzy w formie sformalizowanych quizów, potwierdzająca zrozumienie kluczowych zasad z obszaru bezpieczeństwa, cyberbezpieczeństwa i ochrony danych osobowych. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 6.3 Świadomość i szkolenie oraz dodatkowo przez Kodeks Pracy (BHP) i przez: Zbiór procedur systemowych funkcjonujących w Hadrone dla Zintegrowanego Systemu Zarządzania (ZSZ) - punkt: 4.9 Procedura budowy świadomości organizacji dla obszaru ISMS, BCMS, PIMS dla ZSZ	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ obszar powiązany z obszarem systemowym ZSZ	Art. 13 and 14 AI Act	tak
-----	--------	------------------------	---------------------------------	----------	--	---	---	---	------	--	--	-----------------------	-----



6.4	Ludzie	Proces dyscyplinarny	ISO 27001	Security	CC_S2 - Information and Communication / Komunikacja i informowanie	<ul style="list-style-type: none"> Regulamin Pracy i Kodeks Pracy: Oficjalne dokumenty prawne organizacji (zgodne z Kodeksem Pracy), precyzyjnie definiujące katalog kar, ramy czasowe na ich nałożenie oraz procedurę odwoławczą. System raportowania naruszeń (Whistleblowing): Bezpieczne kanały zgłoszeniowe umożliwiające pracownikom lub systemom monitorującym (np. DLP) zgłaszanie podejrzeń łamania polityk bezpieczeństwa przez personel Hadrone. Szablony dokumentacji dyscyplinarnej: Przygotowane przez kancelarię prawną wzorce pism (np.: wezwanie do złożenia wyjaśnień, zawiadomienie o nałożeniu kary), zapewniające poprawność formalną i minimalizujące ryzyko przegrania ewentualnego sporu w sądzie pracy. 	<ul style="list-style-type: none"> Wskaźnik powtarzalności naruszeń (KPI): Miara określająca, ile osób ukaranych upomnieniem lub naganą ponownie złamało zasady bezpieczeństwa w wyznaczonym czasie (weryfikacja czy proces dyscyplinarny pełni funkcję odstraszającą). Audyt terminowości postępowań: Kontrola sprawdzająca, czy procesy dyscyplinarne są uruchamiane i kończone w ustawowych terminach (np.: zgodnie z prawem pracy). Przegląd statystyk i trendów naruszeń: Cykliczna (np.: raz w roku) analiza zgromadzonych spraw pod kątem identyfikacji najczęściej łamanych polityk (np.: masowe wynoszenie danych lub masowe wykorzystanie sprzętu Hadrone do celów prywatnych), służąca jako podstawa do aktualizacji szkoleń dla personelu. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 6.4 Proces dyscyplinarny oraz dodatkowo przez umowy o współpracy i Kodeks Pracy	W zakresie ZSZ regulowany przez przepisy prawa poliego - Kodeks Pracy oraz dodatkowo przez Regulami organizacyjny Hadrone	N/A	tak
-----	--------	----------------------	-----------	----------	--	---	---	---	------	---	---	-----	-----



6.5	Ludzie	Odpowiedzialność po ustaniu zatrudnienia	ISO 27001	Security	CC_S2 - Information and Communication / Komunikacja i informowanie	<ul style="list-style-type: none"> • Proces Offboarding (Proces zwolnienia pracownika): Sformalizowany w przepisach prawa polskiego, Kodeks Pracy sposób rozwiązania stosunku świadczenia pracy. • Deprovisioning kont (IdM / Identity Management): Techniczne narzędzia Microsoft Entra ID, które automatycznie blokują wszystkie konta, maile i dostęp VPN pracownika dokładnie w wyznaczonym dniu i godzinie. • Rozmowa wyjściowa: Formalne spotkanie z przełożonym, podczas którego pracownikowi składa się pisemne przypomnienie o jego zobowiązaniach prawnych (NDA) po ustaniu zatrudnienia, co zostaje potwierdzone jego podpisem. 	<ul style="list-style-type: none"> • Wskaźnik terminowości blokowania kont (KPI): Miara określająca procent kont byłych pracowników, które zostały pomyślnie zablokowane lub usunięte w czasie poniżej 48 godzin (lub natychmiast, zależnie od ryzyka) od momentu ustania zatrudnienia. • Audyt rozliczenia kart obiegowych: Cykliczna weryfikacja losowych teczek byłych pracowników w celu upewnienia się, że każda karta obiegowa jest kompletna, podpisana przez dział IT/Administrację i potwierdza fizyczny zwrot sprzętu (laptopa, telefonu, tokenów). • Kontrola "osieroconych dostępu": Regularne (np. raz na kwartał) automatyczne porównywanie bazy aktywnych kont w kluczowych systemach IT z bazą aktualnie zatrudnionych osób w systemie HR i MS Entra ID, mające na celu wykrycie kont osób, które już odeszły z firmy. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 6.5 Odpowiedzialność po ustaniu zatrudnienia oraz dodatkowo przez umowy NDA, umowy o współpracy i Kodeks Pracy	W zakresie ZSZ regulowany przez przepisy prawa polskiego - Kodeks Pracy oraz dodatkowo przez Regulami organizacyjny Hadrone	N/A	tak
-----	--------	--	-----------	----------	--	---	---	---	------	--	---	-----	-----



6.6	Ludzie	Umowy o zachowaniu poufności	ISO 27001, ISO 27701	Security	CC_S2 - Information and Communication / Komunikacja i informowanie	<ul style="list-style-type: none"> • Biblioteka standaryzowanych szablonów NDA: Zbiór zatwierdzonych przez kancelarię prawną wzorów umów NDA (dla pracowników, podwykonawców, partnerów handlowych), minimalizujący ryzyko błędów przy ręcznym pisaniu dokumentów. • Centralne repozytorium umów (System SharePoint): Cyfrowe narzędzie do bezpiecznego przechowywania, kategoryzowania i przeszukiwania wszystkich podpisanych zobowiązań NDA. • Zintegrowany proces elektronicznego podpisu (np.: DocuSign, Autenti, podpis kwalifikowany): Narzędzie i proces umożliwiający szybkie, zdalne i prawnie wiążące podpisywanie umów o poufności z pełną historią operacji (Audit Trail). • Proces przeglądu i eskalacji: Procedura weryfikacji umów w sytuacjach, gdy partner biznesowy odmawia podpisania standardowego szablonu firmy i narzuca własne, zmodyfikowane zapisy. 	<ul style="list-style-type: none"> • Wskaźnik pokrycia umowami NDA (KPI): Miara weryfikująca, czy 100% zewnętrznych dostawców i partnerów mających dostęp do zasobów informacyjnych firmy posiada przypisaną, ważną i podpisaną umowę NDA. • Przegląd terminów wygasania umów: Cykliczna (np.: raz na kwartał) weryfikacja bazy kontraktów pod kątem umów NDA, których okres ważności zbliża się do końca, w celu ich terminowego odnowienia lub aneksowania. • Audyt incydentów związanych z wyciekiem (Brak powiązania z NDA): Kontrola sprawdzająca, czy w przypadku wykrycia nieautoryzowanego ujawnienia danych przez partnera, pracownika, Hadrone dysponuje narzędziem prawnym (ważnym dokumentem NDA) mogącym służyć wyciągnięciu konsekwencji. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 6.6 Umowy o zachowaniu poufności oraz dodatkowo przez umowy NDA, umowy o współpracy i Kodeks Pracy	W zakresie ZSZ regulowany przez przepisy prawa poliego - Kodeks Pracy oraz dodatkowo przez Regulami organizacyjny Hadrone	N/A	tak
-----	--------	------------------------------	----------------------	----------	--	--	--	---	------	--	---	-----	-----



6.7	Ludzie	Praca zdalna	ISO 27001	Security	CC_S2 - Information and Communication / Komunikacja i informowanie	<ul style="list-style-type: none"> Polityka Pracy Zdalnej: Formalny zestaw reguł definiujący wymagania techniczne i organizacyjne, pracy zdalnej np.: z domu oraz obowiązki pracownika wykonującego obowiązki poza biurem Hadrone. Szyfrowane tunele VPN i uwierzytelnianie MFA: Wymóg techniczny wymuszający, aby każde połączenie zdalne z siecią Hadrone, lub zasobami Hadrone odbywało się przez bezpieczny protokół VPN z obowiązkowym drugim składnikiem logowania (Multi-Factor Authentication). Systemy Mobile Device Management (MDM / Intune): Narzędzia do centralnego zarządzania laptopami i smartfonami, umożliwiające zdalne wdrażanie poprawek, wymuszanie szyfrowania dysków (BitLocker) oraz zdalne czyszczenie danych w przypadku zgubienia sprzętu. Szyfrowana pamięć masowa i blokada portów USB: Techniczne blokady uniemożliwiające pracownikowi zdalnemu kopiowanie poufnych danych firmy na prywatne nośniki pendrive lub dyski zewnętrzne. 	<ul style="list-style-type: none"> Wskaźnik wdrożenia poprawek na urządzeniach zdalnych (KPI): Monitorowanie wskaźników efektywności obszarów ZSZ. Weryfikacja logów połączeń VPN pod kątem anomalii: Automatyczny przegląd rejestrów dostępu pod kątem wykrywania podejrzanych logowań. Audyt zgodności konfiguracji (Compliance Check): Blokowanie dostępu do sieci Hadrone urządzeniom, które podczas próby nawiązania połączenia zdalnego nie spełniają wymogów bezpieczeństwa (np. mają wyłączony firewall lub nieaktualny system). 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 6.7 Praca zdalna oraz dodatkowo przez umowy NDA, umowy o współpracy i Kodeks Pracy	W zakresie ZSZ regulowany przez przepisy prawa poliego - Kodeks Pracy oraz dodatkowo przez Regulami organizacyjny Hadrone	N/A	tak
-----	--------	--------------	-----------	----------	--	--	---	---	------	--	---	-----	-----



6.8	Ludzie	Zgłaszanie zdarzeń bezpieczeństwa	ISO 27001, ISO 27701	Security	CC_S2 - Information and Communication / Komunikacja i informowanie	<ul style="list-style-type: none"> • Dedykowany punkt kontaktu (Single Point of Contact - SPOC): Jeden, powszechnie znany kanał zgłoszeniowy (e-mail: incydnety@hadrone.com). • Przycisk "Zgłoś Phishing" w Outlook: Proste narzędzie wdrożone w programie pocztowym Outlook, umożliwiające użytkownikowi przesłanie podejrzanego wiadomości do zespołu bezpieczeństwa (SOC) za pomocą jednego kliknięcia. • Automatyczne kampanie uświadamiające: Regularne przypomnienia, plakaty oraz szkolenia przypominające pracownikom, gdzie, jak i co należy zgłaszać, utrzymujące wysoki poziom czujności w organizacji. 	<ul style="list-style-type: none"> • Wskaźnik liczby zgłoszeń od użytkowników (KPI): Monitorowanie wskaźników efektywności obszarów ZSZ. • Testy skuteczności zgłaszania (Symulowany Phishing): Regularne (np.: raz w roku) kontrolowane ataki phishingowe, mierzące jaki procent pracowników prawidłowo użył mechanizmu zgłoszeniowego zamiast kliknąć w link. • Audyt sprawności kanałów alarmowych: Okresowe testy techniczne (np.: raz na kwartał, raz na rok) sprawdzające, czy formularze zgłoszeniowe, telefony interwencyjne oraz skrzynki e-mail działają poprawnie i bez opóźnień sieciowych. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 6.8 Zgłaszanie zdarzeń bezpieczeństwa oraz dodatkowo przez obszar RODO: Polityka Bezpieczeństwa Danych Osobowych w Hadrone Sp. z o.o - punkt: 11. Postępowanie w sytuacji Naruszenia ochrony danych osobowych oraz obszar BCMS w dokumencie: Strategia Zarządzania Ciągłością Działania w ramach Zintegrowanego Systemu Zarządzania dla Hadrone - punkt: 4 Strategia reakcji na incydent w Hadrone oraz punkt: 5 Struktura reagowania na incydent (sytuację kryzysową)	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZSZ oraz dodatkowo regulowany przez RODO i w ramach ZSZ	N/A	tak
-----	--------	-----------------------------------	----------------------	----------	--	---	--	---	------	--	---	-----	-----



7.1	Fizyczne	Fizyczne dowody bezpieczeństwa	ISO 27001	Security	CC_S6 - Logical and Physical Access Control / Logiczna i fizyczna kontrola dostępu	<ul style="list-style-type: none"> Systemy Kontroli Dostępu (SKD): Narzędzia techniczne, takie jak zamki elektroniczne, czytniki kart zbliżeniowych, uniemożliwiające wejście osobom bez uprawnień. Telewizyjny System Nadzoru (CCTV): Kamery monitorujące całodobowo punkty wejścia/wyjścia, ogrodzenie zewnętrzne są połączone z systemem rejestracji obrazu. Procedura zarządzania gośćmi i przepustkami: Proces nakazujący rejestrację każdej osoby trzeciej w księdze wejść/wyjść, wydanie widocznego identyfikatora "GOŚĆ" oraz obowiązek stałej asysty pracownika Hadrone podczas pobytu na terenie biura w strefach pracy, Wyłącznie są toalety oraz kuchnia. 	<ul style="list-style-type: none"> Audyty ciągłości rejestracji wideo (KPI): Miara sprawdzająca dostępność i kompletność nagrań z monitoringu CCTV oraz weryfikująca, czy czas retencji (przechowywania) wideo jest zgodny z wymaganiami Hadrone – minimum ostatni tydzień (7 dni). Testy penetracji fizycznej (Tailgating Tests): Kontrole polegające na próbach kontrolowanego wtargnięcia do stref chronionych (np. poprzez "podczepienie się" pod pracownika otwierającego drzwi kartą) w celu oceny czujności personelu. Wskaźnik poprawności działania uprawnień SKD: Regularny, automatyczny audyt bazy kart dostępowych, mający na celu natychmiastowe wykrycie i deaktywację zagubionych przepustek oraz kart przypisanych do byłych pracowników. 	Wyjątek, Uwaga/Exception, Comment.	<p>Spostrzeżenie – data centers są zakupione w ramach usługi IaaS od Microsoft Inc. oraz od Hetzner. Ocena zabezpieczenia wymaga, aby Hadrone dokonał pełnej weryfikacji zabezpieczeń po stronie dostawcy przez proces oceny dostawcy (Vendor Risk Management Process) oraz identyfikował wszystkie zabezpieczenia występujące u dostawcy w celu potwierdzenia spełnienia punktu normy oraz wymagań mechanizmów kontrolnych – ryzyko wpisane w rejestr ryzyka Hadrone, z planem na jego wykonanie Q3 i Q4 2026 rok.</p>	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 7.1 Fizyczne dowody bezpieczeństwa. Wyklucza się elementy związane z infrastrukturą serwerową w ramach chmury obliczeniowej ze względu na dla modelu IaaS Hadrone nie jest dostawcą chmury obliczeniowej a jedynie jej klientem - zgodnie z przyjętą strategią: Strategia Zarządzania Bezpieczeństwem Informacji i chmury obliczeniowej w ramach ZSZ dla Hadrone (integracja obszaru ISMS i Cloud) - punkt: 4 Strategia ISMS w Cloud Governance (ISO 27017 / ISO 27018)	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z oraz dodatkowo regulowany przez RODO i w ramach ZSZ. Wyłączeniem jest wymaganie CSC oraz fakt że Hadrone nie jest dostawcą chmury obliczeniowej jako infrastruktury	N/A	częściowo
-----	----------	--------------------------------	-----------	----------	--	--	---	------------------------------------	---	---	--	-----	-----------



7.2	Fizyczne	Fizyczna kontrola wejścia	ISO 27001	Security	CC_S6 - Logical and Physical Access Control / Logiczna i fizyczna kontrola dostępu	<ul style="list-style-type: none"> • Karty zbliżeniowe i czytniki elektroniczne: Techniczne komponenty Systemu Kontroli Dostępu (SKD) blokujące fizyczne bariery (drzwi) i wymagające uwierzytelnienia przed ich otwarciem. • Recepcja i punkty ochrony budynku: Fizyczne stanowiska obsługiwane przez wykwalifikowany personel (ochronę, recepcję), stanowiące pierwszą linię weryfikacji tożsamości oraz wydawania przepustek czasowych. • Księga wejść/wyjść gości: Elektroniczny lub papierowy rejestr zawierający imię i nazwisko gościa, nazwę firmy, cel wizyty, nazwisko osoby wprowadzającej oraz dokładne godziny pobytu. 	<ul style="list-style-type: none"> • Audyt rejestrów systemu SKD (KPI): Cykliczny (np. raz na kwartał) przegląd logów systemowych w celu wykrycia anomalii, takich jak próby użycia karty poza godzinami pracy lub wielokrotne odrzucenia dostępu dla jednego konta. • Weryfikacja zgodności uprawnień fizycznych: Regularne porównywanie bazy aktywnych kart dostępowych z aktualną strukturą organizacyjną z bazy Entra ID, mające na celu natychmiastowe odebranie uprawnień osobom przeniesionym lub zwolnionym. • Testy czujności ochrony i personelu: Kontrolowane próby wejścia do budynku bez identyfikatora lub za plecami innej osoby w celu sprawdzenia czy pracownicy lub ochrona zareagują i zablokują intruza. • Inwentaryzacja fizycznych kluczy: Okresowa (np. raz na kwartał) kontrola stanów magazynowych oraz rejestrów wydań tradycyjnych kluczy metalowych do pokoi w biurze Hadrone wraz z rozliczeniem osób, które je pobrały. 	Wyjątek, Uwaga/ Exception, Comment.	<p>Spostrzeżenie – data centers są zakupione w ramach usługi IaaS od Microsoft Inc. oraz od Hetzner. Ocena zabezpieczenia wymaga, aby Hadrone dokonał pełnej weryfikacji zabezpieczeń po stronie dostawcy przez proces oceny dostawcy (Vendor Risk Management Process) oraz identyfikował wszystkie zabezpieczenia występujące u dostawcy w celu potwierdzenia spełnienia punktu normy oraz wymagań mechanizmów kontrolnych. – ryzyko wpisane w rejestr ryzyka Hadrone, z planem na jego wykonanie Q3 i Q4 2026 rok.</p>	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 7.2 Fizyczna kontrola wejścia. Wyklucza się elementy związane z infrastrukturą serwerową w ramach chmury obliczeniowej ze względu na model IaaS. Hadrone nie jest dostawcą chmury obliczeniowej a jedynie jej klientem - zgodnie z przyjętą strategią: Strategia Zarządzania Bezpieczeństwem Informacji i chmury obliczeniowej w ramach ZSZ dla Hadrone (integracja obszaru ISMS i Cloud) - punkt: 4 Strategia ISMS w Cloud Governance (ISO 27017 / ISO 27018)	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZSZ oraz dodatkowo regulowany przez RODO i w ramach ZSZ. Wyłączeniem jest wymagania CSC oraz fakt że Hadrone nie jest dostawcą chmury obliczeniowej jako	N/A	częściowo
-----	----------	---------------------------	-----------	----------	--	--	---	-------------------------------------	--	--	--	-----	-----------



A.7.2	Zabezpieczenia dla AD - Anex A	Warunki przetwarzania danych osobowych	ISO 27701	Privacy	CC_P1 - Privacy - Objectives Related to Privacy / Cele związane z prywatnością	<ul style="list-style-type: none"> Rejestr Czynności Przetwarzania (RCP) i ocena skutków (DPIA): Sformalizowane procesy mapowania wszystkich strumieni danych PII w Hadrone oraz przeprowadzanie formalnych ocen skutków dla ochrony danych (Data Protection Impact Assessment) dla procesów o wysokim ryzyku. Pseudonimizacja i szyfrowanie danych PII: Wykorzystanie narzędzi kryptograficznych do zabezpieczania danych osobowych zarówno w locie (TLS 1.2/1.3), jak i w spoczynku (AES-256 w bazach danych), połączone z oddzieleniem danych identyfikacyjnych od relacyjnych (pseudonimizacja). Systemy zarządzania prawami podmiotów danych (DSR Gateways): Narzędzia i procedury umożliwiające sprawną realizację praw użytkowników (np.: prawo do bycia zapomnianym, prawo do przenoszenia danych, wgląd w dane) w ustawowym czasie. Umowy powierzenia przetwarzania danych (DPA): Restrykcyjny proces prawno-organizacyjny weryfikacji i kontraktowania podmiotów przetwarzających (procesorów), którym Hadrone jako ADO zleca operacje na danych osobowych, wymuszający na nich identyczne standardy bezpieczeństwa. 	<ul style="list-style-type: none"> Wskaźnik terminowości realizacji żądań DSR (KPI): Miara określająca procent wniosków użytkowników (np.: o usunięcie danych) zrealizowanych poprawnie i w terminie wynikającym z przepisów prawa. Audyt i przegląd okresów retencji danych: Cykliczna (np.: raz w roku) kontrola techniczna baz danych i archiwów sprawdzająca, czy systemy automatycznie usuwają lub anonimizują rekordy, których maksymalny czas przechowywania właśnie upłynął. Weryfikacja incydentów i czas zgłaszania naruszeń: Monitorowanie sprawności procedury obsługi incydentów PII, mierzące czas od wykrycia naruszenia do momentu jego zabezpieczenia i ewentualnego zgłoszenia do organu nadzorczego. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: A.7.2 Warunki przetwarzania danych osobowych oraz dodatkowo przez obszar RODO: Polityka Bezpieczeństwa Danych Osobowych w Hadrone Sp. z o.o. i kolejny dokument: Instrukcja Zarządzania Systemem Informatycznym w Hadrone Sp. z o.o.	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez RODO i w ramach ZSZ	N/A	tak
-------	--------------------------------	--	-----------	---------	--	--	--	---	------	--	--	-----	-----



7.3	Fizyczne	Zabezpieczanie biur i obiektów	ISO 27001	Security	CC_S6 - Logical and Physical Access Control / Logiczna i fizyczna kontrola dostępu	<ul style="list-style-type: none"> • Fizyczne bariery i wzmocnienia: Montaż certyfikowanych drzwi antywłamaniowych, zamków o wysokiej klasie odporności. • Zasada zamykania i ochrona obiektu: Sformalizowana procedura opisująca obowiązki ostatniego pracownika opuszczającego biuro (sprawdzenie zamknięcia okien, wyłączenie urządzeń, uzbrojenie alarmu). • Bezpieczne strefy socjalne i kurierskie: Architektoniczne wydzielenie miejsc przyjmowania paczek (repcja), w celu odciążenia dostawców od wglądu w dokumenty i dane Hadrone. 	<ul style="list-style-type: none"> • Wskaźnik naruszeń i fałszywych alarmów (KPI): Monitorowanie liczby incydentów związanych z nieprawidłowym zamknięciem biura (np. niedomknięte drzwi, nieuzbrojony alarm) oraz analiza przyczyn wywołania fałszywych alarmów. • Obchody i patrole rewizyjne: Cykliczne, wieczorne i nocne kontrole fizyczne realizowane przez ochronę budynku weryfikujące status zamknięcia drzwi i ogólny stan bezpieczeństwa budynku. • Testy integracji systemów bezpieczeństwa: Okresowe (np. raz na pół roku) sprawdzanie automatycznego przesyłania sygnałów alarmowych z biura do zewnętrznej Stacji Monitorowania Agencji Ochrony (potwierdzenie czasu dojazdu grupy interwencyjnej). • Audyt odporności fizycznej i infrastruktury: Regularna (np. raz w roku) kontrola stanu technicznego uszczelek, zawiasów, zamków, rolet antywłamaniowych oraz kratki wentylacyjnych, mogących stanowić potencjalny punkt nieautoryzowanego wdarcia do obiektu lub co najmniej zaburzenia funkcjonowania biura Hadrone. 	Wyjątek, Uwaga/ Exception, Comment.	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 7.3 Zabezpieczanie biur i obiektów. Wyklucza się elementy związane z infrastrukturą serwerową w ramach chmury obliczeniowej ze względu na to, że dla modelu IaaS Hadrone nie jest dostawcą chmury obliczeniowej, a jedynie jej klientem - zgodnie z przyjętą strategią: Strategia Zarządzania Bezpieczeństwem Informacji i chmury obliczeniowej w ramach ZSZ dla Hadrone (integracja obszaru ISMS i Cloud) - punkt: 4 Strategia ISMS w Cloud Governance (ISO 27017 / ISO 27018)	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z oraz dodatkowo regulowany przez RODO i w ramach ZSZ. Wyłączeniem jest wymaganie CSC oraz fakt, że Hadrone nie jest dostawcą chmury obliczeniowej jako infrastruktury	N/A	częściowo
-----	----------	--------------------------------	-----------	----------	--	--	--	-------------------------------------	---	---	-----	-----------



A.7.3	Zabezpieczenia dla AD - Anex A	Obowiązki wobec osób, których dane dotyczą	ISO 27701	Privacy	CC_P1 - Privacy - Objectives Related to Privacy / Cele związane z prywatnością	<ul style="list-style-type: none"> • Polityki prywatności i klauzule informacyjne: Aktualne, publicznie dostępne dokumenty (na stronie WWW, w aplikacjach SaaS) realizujące obowiązek informacyjny w momencie zbierania danych, zawierające pełne dane kontaktowe Hadrone KODO (Koordynator Ochrony Danych Osobowych) • Scentralizowany proces obsługi żądań (DSR - Data Subject Requests): Sformalizowana procedura w systemie (np.: Jira) służąca do rejestrowania, weryfikacji tożsamości wnioskodawcy, przypisywania zadań do odpowiednich działów oraz wysyłki odpowiedzi. • Mechanizmy zarządzania zgodami (CMP - Consent Management Platforms): Narzędzia systemowe (np. bannery cookies) oraz odpowiednio zaprojektowane bazy danych, które w czasie rzeczywistym rejestrują statusy zgód marketingowych i profilowania. • Zautomatyzowane procedury czyszczenia i eksportu danych: Gotowe skrypty i narzędzia IT pozwalające na sprawne wyciągnięcie wszystkich danych klienta/pracownika w ustrukturyzowanym formacie (np.: XML/JSON/CSV dla prawa do przenoszenia) lub ich trwałe usunięcie (dla prawa do bycia zapomnianym). 	<ul style="list-style-type: none"> • Wskaźnik terminowości realizacji wniosków DSR (KPI): Procentowy udział zgłoszeń od osób, których dane dotyczą, zrealizowanych w pełnym zakresie i w ustawowym terminie w stosunku do wszystkich zarejestrowanych wniosków. • Średni czas procesowania zgłoszenia (MTTR for DSR): Miara operacyjna określająca, ile dni średnio zajmuje organizacji realizacja jednego wniosku (np. o usunięcie danych) od momentu poprawnej weryfikacji tożsamości. • Przegląd i walidacja rejestru zgód: Roczny audyt próbek losowych rekordów w bazie danych w celu upewnienia się, że systemy wysyłkowe (np.: newslettery) nie generują komunikatów do osób, które wycofały swoje zgody lub zgłosiły sprzeciw. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: A.7.3 Obowiązki wobec osób, których dane dotyczą oraz dodatkowo przez obszar RODO: Polityka Bezpieczeństwa Danych Osobowych w Hadrone Sp. z o.o	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez RODO i w ramach ZSZ	N/A	tak
-------	--------------------------------	--	-----------	---------	--	--	---	---	------	---	--	-----	-----



7.4	Fizyczne	Monitorowanie bezpieczeństwa fizycznego	ISO 27001	Security	CC_S4 - Monitoring Activities / Czynności monitorowania	<ul style="list-style-type: none"> • System CCTV: Kamery przemysłowe połączone z oprogramowaniem VMS (Video Management System), które potrafi automatycznie wykrywać ruch na terenie wokół biura Hadrone. • Reagowania na alarmy fizyczne: Sformalizowane działania operacyjne określające kroki, jakie operator lub patrol ochrony musi podjąć w przypadku wyzwolenia konkretnego alarmu (np.: wysłanie grupy interwencyjnej, powiadomienie Policji). • Czujniki środowiskowe z systemem powiadomień: Integracja monitoringu fizycznego z czujnikami zalań, dymu, temperatury i wilgotności w biurze, wysyłającymi automatyczne alerty SMS/e-mail do najemcy biura. 	<ul style="list-style-type: none"> • Wskaźnik czasu reakcji na incydent fizyczny (KPI): Miara określająca czas od momentu wygenerowania alarmu przez system monitorowania do fizycznego podjęcia interwencji na miejscu zdarzenia przez ochronę. • Kontrola retencji i ciągłości nagrań: Regularne (np. raz na rok) automatyczne lub manualne sprawdzanie czy rejestratory wideo zachowują wymagany czas przechowywania danych (np.: 7 dni) oraz czy żadna z kluczowych kamer nie straciła sygnału. • Testy sprawności i symulacje systemów alarmowych: Okresowe (np. raz na rok) kontrolowane wyzwalanie czujek ruchu, kontaktronów i przycisków alarmu w celu weryfikacji, czy sygnał poprawnie i bez opóźnień dociera do stacji monitorowania. 	Wyjątek, Uwaga/Exception, Comment.	<p>Spostrzeżenie – data centers są zakupione w ramach usługi IaaS od Microsoft Inc. oraz od Hetzner. Ocena zabezpieczenia wymaga, aby Hadrone dokonał pełnej weryfikacji zabezpieczeń po stronie dostawcy przez proces oceny dostawcy (Vendor Risk Management Process) oraz identyfikował wszystkie zabezpieczenia występujące u dostawcy w celu potwierdzenia spełnienia punktu normy oraz wymagań mechanizmów kontrolnych. – ryzyko wpisane w rejestr ryzyka Hadrone, z planem na jego wykonanie Q3 i Q4 2026 rok.</p>	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 7.4 Monitorowanie bezpieczeństwa fizycznego. Wyklucza się elementy związane z infrastrukturą serwerową w ramach chmury obliczeniowej ze względu że dla modelu IaaS Hadrone nie jest dostawcą chmury obliczeniowej a jedynie jej klientem - zgodnie z przyjętą strategią: Strategia Zarządzania Bezpieczeństwem Informacji i chmury obliczeniowej w ramach ZSZ dla Hadrone (integracja obszaru ISMS i Cloud) - punkt: 4 Strategia ISMS w Cloud Governance (ISO 27017 / ISO 27018)	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZSZ oraz dodatkowo regulowany przez RODO i w ramach ZSZ. Wyłączeniem jest wymaganie CSC oraz fakt że Hadrone nie jest dostawcą chmury obliczeniowej jako infrastruktury	N/A	częściowo
-----	----------	---	-----------	----------	---	---	--	------------------------------------	--	--	---	-----	-----------



A.7.4	Zabezpieczenia dla AD - Anex A	Prywatność w fazie projektowania (Privacy by Design)	ISO 27701	Privacy	CC_P7 - Quality / Jakość	<ul style="list-style-type: none"> Ocena skutków dla ochrony danych (DPIA / PIA): Obowiązkowy, formalny proces analizy ryzyka dla prywatności przeprowadzany przed uruchomieniem każdego nowego projektu IT, systemu lub zmiany w architekturze. Techniki minimalizacji danych i architektura Zero-Knowledge: Projektowanie baz danych i interfejsów w sposób, który fizycznie uniemożliwia zbieranie nadmiarowych informacji (np.: stosowanie tokenów zamiast jawnych danych identyfikacyjnych). Automatyczna pseudonimizacja i agregacja danych: Wykorzystanie narzędzi deweloperskich wdrażających mechanizmy "w locie", np.: automatyczne hashowanie identyfikatorów, szyfrowanie na poziomie kolumn bazy danych, oraz agregacja danych do celów statystycznych. Bramki prywatności w pipeline CI/CD (CI/CD Privacy Gates): Integracja automatycznych skanerów kodu i konfiguracji, które blokują wdrożenie oprogramowania, jeśli wykryją błędy w architekturze prywatności (np.: logowanie wrażliwych danych PII do plików tekstowych serwera w sposób jawny). 	<ul style="list-style-type: none"> Wskaźnik wdrożenia DPIA dla nowych projektów (KPI): Procent projektów technologicznych i biznesowych, dla których zrealizowano i zatwierdzono formalną ocenę skutków dla ochrony danych przed rozpoczęciem prac deweloperskich. Audyt domyślnych ustawień prywatności: Kwartalna weryfikacja techniczna nowych kont użytkowników sprawdzająca czy domyślne parametry (np.: zgody marketingowe, widoczność profilu, zbieranie geolokalizacji) są wyłączone. Weryfikacja retencji danych w architekturze systemowej: Regularne testy techniczne sprawdzające skuteczność mechanizmów automatycznego usuwania danych po upływie zdefiniowanego czasu przechowywania (testowanie integralności procesów usuwania i anonimizacji). 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: A.7.4 Prywatność w fazie projektowania (Privacy by Design) oraz dodatkowo przez obszar RODO: Polityka Bezpieczeństwa Danych Osobowych w Hadrone Sp. z o.o oraz przez: Strategia Zarządzania Bezpieczeństwem Informacji i chmury obliczeniowej w ramach ZSZ dla Hadrone (integracja obszaru ISMS i Cloud) - punkt: 7 Strategia ISMS w zakresie zarządzania prywatnością i ochroną danych osobowych (integracja z ISO 27701)	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez RODO i w ramach ZSZ	N/A	tak
-------	--------------------------------	--	-----------	---------	--------------------------	---	---	---	------	--	--	-----	-----



7.5	Fizyczne	Ochrona przed zagrożeniami środowiskowymi	ISO 22301	Security	CC_S1 - Control Environment/ Kontrola Środowiskowe	<ul style="list-style-type: none"> Automatyczne systemy przeciwpożarowe (Sash / Sugo): Systemy wczesnej detekcji dymu (np.: VESDA) połączone z instalacją gaszenia gazem obojętnym (bezpiecznym dla elektroniki), która gasi pożar bez użycia wody. Zasilanie awaryjne (UPS i Agregaty prądowłórcze): Centralne systemy akumulatorowe (UPS) zapewniające bezprzerwowe zasilanie w momencie tąpnięcia napięcia oraz generatory spalinowe (agregaty) z zapasem paliwa na minimum 24-48 godzin ciągłej pracy. Precyzyjna klimatyzacja dedykowana (HVAC): Systemy klimatyzacji szaf serwerowych pracujące w układzie zamkniętym (np.: korytarze zimne/ciepłe), wyposażone w automatyczne przełączanie na jednostki zapasowe (redundancja N+1). Czujniki zalania i zawory odcinające: Rozmieszczone pod podłogą techniczną detektory wilgoci, zintegrowane z systemem automatycznego odcinania dopływu wody do budynku w przypadku wykrycia wycieku. 	<ul style="list-style-type: none"> Wskaźnik dostępności środowiskowej (KPI): Miara określająca procent czasu, w którym temperatura, wilgotność oraz parametry zasilania w serwerowni mieściły się w normach technicznych. Przeglądy i certyfikacja instalacji ppoż. i HVAC: Regularna (zgodnie z przepisami prawa i zaleceniami producenta) techniczna weryfikacja szczelności butli z gazem gaśniczym, sprawności czujek dymu oraz ciśnienia w układach chłodzenia. Weryfikacja certyfikacji Data Center: Regularne, okresowe weryfikowanie certyfikatów data Center dostawców chmury obliczeniowej, weryfikacja raportów SOC 2, type II oraz ISO 27001, ISO 22310, oraz ISO 27701 w ramach zasad bezpieczeństwa monitorowania dostawcy zewnętrznego. 	Wyjątek, Uwaga/ Exception, Comment.	<p>Spostrzeżenie – data centers są zakupione w ramach usługi IaaS od Microsoft Inc. oraz od Hetzner. Ocena zabezpieczenia wymaga, aby Hadrone dokonał pełnej weryfikacji zabezpieczeń po stronie dostawcy przez proces oceny dostawcy (Vendor Risk Management Process) oraz identyfikował wszystkie zabezpieczenia występujące u dostawcy w celu potwierdzenia spełnienia punktu normy oraz wymagań mechanizmów kontrolnych – ryzyko wpisane w rejestr ryzyka Hadrone, z planem na jego wykonanie Q3 i Q4 2026 rok.</p>	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 7.5 Ochrona przed zagrożeniami środowiskowymi oraz dodatkowo dokument: Strategia Zarządzania Ciągłością Działania w ramach Zintegrowanego Systemu Zarządzania dla Hadrone. Wyklucza się elementy związane z infrastrukturą serwerową w ramach chmury obliczeniowej ze względu na model IaaS Hadrone nie jest dostawcą chmury obliczeniowej a jedynie jej klientem - zgodnie z przyjętą strategią: Strategia Zarządzania Bezpieczeństwem Informacji i chmury obliczeniowej w ramach ZSZ dla Hadrone (integracja obszaru ISMS i Cloud) - punkt: 4 Strategia ISMS w Cloud Governance (ISO 27017 / ISO 27018)	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z oraz dodatkowo regulowany przez BCP i DRP w ramach PIMS. Wyłączeniem jest wymaganie CSC oraz fakt że Hadrone nie jest dostawcą chmury obliczeniowej jako infrastruktury	N/A	częściowo
-----	----------	---	-----------	----------	---	---	---	--	---	---	--	-----	-----------



A.7.5	Zabezpieczenia dla AD - Anex A	Przekazywanie i udostępnianie PII	ISO 27701	Privacy	CC_P6 - Disclosure and Notification / Ujawnienie i powiadamianie	<ul style="list-style-type: none"> • Szyfrowane i bezpieczne kanały transmisji: Wykorzystanie protokołów bezpiecznego transferu plików (np.: SFTP z uwierzytelnianiem kluczem, HTTPS, dedykowane portale wymiany danych) oraz bezwzględne szyfrowanie paczek danych (np.: silne archiwum ZIP z hasłem przekazywanym osobnym kanałem). • Automatyczne mechanizmy maskowania i tokenizacji: Narzędzia, które przed wysyłką bazy danych do partnera zewnętrznego automatycznie usuwają zbędne kolumny (minimalizacja) lub zastępują realne identyfikatory (np.: IP) unikalnymi tokenami. • Proces kwalifikacji i weryfikacji dostawców (Vendor Assessment): Sformalizowany proces oceny bezpieczeństwa podmiotów trzecich przed podpisaniem umowy, polegający na analizie ich kwestionariuszy bezpieczeństwa, certyfikatów (np. ISO 27001) i raportów z audytów. • Scentralizowany Rejestr Udostępnień i Transferów: Rejestr, w którym ewidencjonowane jest każde masowe lub regularne przekazanie danych: kto, komu, kiedy, na jakiej podstawie prawnej i jaki zakres danych udostępnił. 	<ul style="list-style-type: none"> • Wskaźnik zatwierdzonych umów DPA (KPI): Procent podmiotów zewnętrznych, którym faktycznie przekazano dane PII, posiadających poprawnie podpisaną i aktualną umowę powierzenia przed momentem dokonania transferu. • Cykliczne audyty bezpieczeństwa u procesorów (Third-Party Audits): Regularne (np. raz w roku dla kluczowych dostawców) weryfikacje polegające na żądaniu dowodów zachowania bezpieczeństwa danych u partnera lub przeprowadzaniu audytów zdalnych/na miejscu. • Przegląd i walidacja mechanizmów transferów międzynarodowych: Coroczna kontrola prawno-techniczna aktualności stosowanych Standardowych Klauzul Umownych (SCC) oraz decyzji Komisji Europejskiej dotyczących stopnia ochrony danych w krajach, do których organizacja wysyła PII. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: A.7.5 Przekazywanie i udostępnianie PII oraz dodatkowo przez zobszar RODO: Polityka Bezpieczeństwa Danych Osobowych w Hadrone Sp. z o.o.	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez RODO i w ramach ZSZ	N/A	tak
-------	--------------------------------	-----------------------------------	-----------	---------	--	--	---	---	------	--	--	-----	-----



7.6	Fizyczne	Praca w obszarach bezpiecznych	ISO 27001	Security	CC_S6 - Logical and Physical Access Control / Logiczna i fizyczna kontrola dostępu	<ul style="list-style-type: none"> • Instrukcja bezpiecznego zachowania w strefach chronionych: Sformalizowany dokument proceduralny, z którym każdy uprawniony pracownik musi się zapoznać i podpisać przed nadaniem mu fizycznego dostępu do strefy chronionych serwerowni lub stref przetwarzania danych (danych osobowych). • Szafki depozytowe przed wejściem: Fizyczne skrytki zamykane na klucz lub kod, umieszczone bezpośrednio przed wejściem do obszaru bezpiecznego, służące do pozostawienia prywatnych telefonów i nośników danych. • Zasada dwóch pracowników (Four-Eyes Principle): Proces organizacyjny dla stref o najwyższym stopniu krytyczności, wymagający jednoczesnej obecności minimum dwóch uprawnionych osób do wykonania określonych operacji (np.: zmian w konfiguracji rdzenia sieci, instalacja nowego sprzętu). • Wydzielone i monitorowane punkty serwisowe: Proces nadzorowania prac konserwacyjnych, w ramach którego wszelkie naprawy infrastruktury w strefie bezpiecznej są rejestrowane w specjalnym harmonogramie i osobnym rejestrze wejść. 	<ul style="list-style-type: none"> • Wskaźnik incydentów naruszenia zasad strefy (KPI): Monitorowanie i rejestrowanie przypadków złamania reguł (np. wniesienie telefonu, niezablokowany ekran, brak asysty dla gościa) w celu wyciągnięcia konsekwencji dyscyplinarnych. • Weryfikacja certyfikacji Data Center: Regularne, okresowe weryfikowanie certyfikatów data Center dostawców chmury obliczeniowej, weryfikacja raportów SOC 2, type II oraz ISO 27001, ISO 22310, oraz ISO 27701 w ramach zasad bezpieczeństwa dostawcy zewnętrznego. 	Wyjątek, Uwaga/Exception, Comment.	<p>Spostrzeżenie – data centers są zakupione w ramach usługi IaaS od Microsoft Inc. oraz od Hetzner. Ocena zabezpieczenia wymaga, aby Hadrone dokonał pełnej weryfikacji zabezpieczeń po stronie dostawcy przez proces oceny dostawcy (Vendor Risk Management Process) oraz identyfikował wszystkie zabezpieczenia występujące u dostawcy w celu potwierdzenia spełnienia punktu normy oraz wymagań mechanizmów kontrolnych – ryzyko wpisane w rejestr ryzyka Hadrone, z planem na jego wykonanie Q3 i Q4 2026 rok.</p>	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 7.6 Praca w obszarach bezpiecznych. Wyklucza się elementy związane z infrastrukturą serwerową w ramach chmury obliczeniowej ze względu na model IaaS Hadrone nie jest dostawcą chmury obliczeniowej a jedynie jej klientem - zgodnie z przyjętą strategią: Strategia Zarządzania Bezpieczeństwem Informacji i chmury obliczeniowej w ramach ZSZ dla Hadrone (integracja obszaru ISMS i Cloud) - punkt: 4 Strategia ISMS w Cloud Governance (ISO 27017 / ISO 27018)	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZSZ oraz dodatkowo regulowany przez RODO i w ramach ZSZ. Wylaczeniem jest wymaganie CSC oraz fakt że Hadrone nie jest dostawcą chmury obliczeniowej jako	N/A	częściowo
-----	----------	--------------------------------	-----------	----------	--	--	---	------------------------------------	---	--	--	-----	-----------



7.7	Fizyczne	Zasada czystego biurka i ekranu	ISO 27001, ISO 27701	Confidentiality	CC_CO - Confidentiality / Poufność	<ul style="list-style-type: none"> • Polityka czystego biurka, kosza, drukarki i ekranu: Oficjalny, spisany standard organizacyjny, będący częścią onboardingu, precyzujący obowiązki pracownika w zakresie ochrony fizycznego stanowiska. • Wymuszenie automatycznej blokady ekranu (GPO / MDM): Techniczne narzędzie systemowe, które automatycznie blokuje komputer po określonym czasie bezczynności użytkownika (np.: maksymalnie po 30 minutach). • Zamykane kontenery i niszcarki dokumentów: Zapewnienie infrastruktury fizycznej – każdy pracownik musi posiadać szafkę zamykaną na klucz, a w biurze muszą znajdować się niszcarki o odpowiedniej klasie tajności (DIN 66399). • Bezpieczny druk poufny (Secure Print): Mechanizm wymagający podania kodu PIN bezpośrednio przy drukarce, aby urządzenie fizycznie rozpoczęło drukowanie dokumentu. 	<ul style="list-style-type: none"> • Wskaźnik naruszeń czystego biurka, kosza, druku (KPI): Miara określająca liczbę incydentów (np.: pozostawionych dokumentów, niezablokowanych ekranów, niezniszczonych dokumentów) wykrytych podczas cyklicznych audytów w cyklu rocznym. • Audyt logów blokowania stacji roboczych: Cykliczna weryfikacja automatycznych raportów z systemów IT sprawdzająca, czy użytkownicy sami blokują komputery, czy system najczęściej musi robić to za nich automatycznie (identyfikacja użytkowników o niskiej świadomości). 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 7.7 Zasada czystego biurka i ekranu	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z oraz dodatkowo regulowany przez RODO i w ramach ZSZ	N/A	tak
-----	----------	---------------------------------	----------------------	-----------------	------------------------------------	---	---	---	------	---	--	-----	-----



7.8	Fizyczne	Rozmieszczenie i ochrona wyposażenia	ISO 27001, ISO 27017	Security	CC_S1 - Control Environment/ Kontrolne Środowiskowe	<ul style="list-style-type: none"> • Zamykane szafy teleinformatyczne (Szafy RACK): Fizyczne szafy wyposażone w zamki mechaniczne lub elektroniczne (otwierane kartą SKD), chroniące serwery i przełączniki dystrybucyjne przed fizyczną ingerencją. • Bezpieczne trasowanie kabli (Koryta i peszle): Prowadzenie kabli sieciowych i zasilających w zamkniętych, podziemnych lub sufitowych korytach metalowych, a także stosowanie tras alternatywnych (redundantnych) dla zapewnienia ciągłości działania. • System Zarządzania Zasobami (Asset Management / CMDB): Narzędzie informatyczne ewidencjonujące dokładną, fizyczną lokalizację każdego urządzenia (budynek, piętro, pokój, numer szafy i półki). • Filtry zasilania i osłony fizyczne: Stosowanie systemów UPS, listew filtrujących oraz fizycznych osłon na krytyczne przełączniki zasilania (np.: kłapki zabezpieczające przyciski EPO), aby zapobiec przypadkowemu wyłączeniu sprzętu. 	<ul style="list-style-type: none"> • Weryfikacja certyfikacji Data Center: Regularne, okresowe weryfikowanie certyfikatów data Center dostawców chmury obliczeniowej, weryfikacja raportów SOC 2, type II oraz ISO 27001, ISO 22310, oraz ISO 27701 w ramach zasad bezpieczeństwa monitorowania dostawcy zewnętrznego. • Monitorowanie parametrów pracy urządzeń: Automatyczne systemy nadzoru IT (np. Zabbix, Nagios) wysyłające alerty w przypadku nagłego odłączenia sprzętu od sieci lub utraty zasobu w Azure, co pozwala na natychmiastowe wykrycie awarii / awarii fizycznej. 	Wyjątek, Uwaga/ Exception, Comment.	<p>Spostrzeżenie – data centers są zakupione w ramach usługi IaaS od Microsoft Inc. oraz od Hetzner. Ocena zabezpieczenia wymaga, aby Hadrone dokonał pełnej weryfikacji zabezpieczeń po stronie dostawcy przez proces oceny dostawcy (Vendor Risk Management Process) oraz identyfikował wszystkie zabezpieczenia występujące u dostawcy w celu potwierdzenia spełnienia punktu normy oraz wymagań mechanizmów kontrolnych. – ryzyko wpisane w rejestr ryzyka Hadrone, z planem na jego wykonanie Q3 i Q4 2026 rok.</p>	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 7.8 Rozmieszczenie i ochrona wyposażenia. Wyklucza się elementy związane z infrastrukturą serwerową w ramach chmury obliczeniowej ze względu że dla modelu IaaS Hadrone nie jest dostawcą chmury obliczeniowej a jedynie jej klientem - zgodnie z przyjętą strategią: Strategia Zarządzania Bezpieczeństwem Informacji i chmury obliczeniowej w ramach ZSZ dla Hadrone (integracja obszaru ISMS i Cloud) - punkt: 4 Strategia ISMS w Cloud Governance (ISO 27017 / ISO 27018)	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z. Wyłączeniem jest wymaganie CSC oraz fakt że Hadrone nie jest dostawcą chmury obliczeniowej jako infrastruktury	N/A	częściowo
-----	----------	--------------------------------------	----------------------	----------	--	---	--	-------------------------------------	--	---	--	-----	-----------



7.9	Fizyczne	Bezpieczeństwo aktywów poza siedzibą	ISO 27001, ISO 27017	Security	CC_S1 - Control Environment/ Kontrolę Środowiskowe	<ul style="list-style-type: none"> • Pełne szyfrowanie dysków (FDE) i ochrona danych: Wymóg techniczny (np.: BitLocker) zapewniający, że w przypadku kradzieży sprzętu poza firmą, odczytanie danych przez osoby nieuprawnione będzie niemożliwe. • Systemy lokalizacji i zdalnego czyszczenia (MDM): Narzędzia (np. Microsoft Intune) umożliwiające administratorom namierzenie skradzionego laptopa/telefonu oraz natychmiastowe, zdalne wykasowanie całej zawartości pamięci (Remote Wipe). • Procedura autoryzacji i paszportyzacji sprzętu: Proces rejestracji wynoszonych aktywów w systemie Asset Management, ze wskazaniem osoby odpowiedzialnej, celu wyniesienia oraz planowanej daty zwrotu. • Fizyczne zabezpieczenia transportowe: Stosowanie certyfikowanych toreb/plecaków bezpiecznych, filtrów prywatyzujących na ekrany (utrudniających podglądanie w pociągu czy samolocie) oraz linków zabezpieczających typu Kensington Lock. 	<ul style="list-style-type: none"> • Wskaźnik utraconych aktywów poza firmą (KPI): Statystyka mierząca liczbę zgubionych lub skradzionych urządzeń w danym okresie, wraz z analizą finansową i informatyczną skutków tych zdarzeń. • Audyt zgodności szyfrowania urządzeń mobilnych: Automatyczna, codzienna kontrola systemowa weryfikująca, czy 100% laptopów i smartfonów pracujących poza siecią lokalną firmy ma aktywne i sprawne szyfrowanie pamięci. 	Wyjątek, Uwaga/ Exception, Comment.	<p>Spostrzeżenie – data centers są zakupione w ramach usługi IaaS od Microsoft Inc. oraz od Hetzner. Ocena zabezpieczenia wymaga, aby Hadrone dokonał pełnej weryfikacji zabezpieczeń po stronie dostawcy przez proces oceny dostawcy (Vendor Risk Management Process) oraz identyfikował wszystkie zabezpieczenia występujące u dostawcy w celu potwierdzenia spełnienia punktu normy oraz wymagań mechanizmów kontrolnych – ryzyko wpisane w rejestr ryzyka Hadrone, z planem na jego wykonanie Q3 i Q4 2026 rok.</p>	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 7.9 Bezpieczeństwo aktywów poza siedzibą. Wyklucza się elementy związane z infrastrukturą serwerową w ramach chmury obliczeniowej ze względu na model IaaS Hadrone nie jest dostawcą chmury obliczeniowej a jedynie jej klientem - zgodnie z przyjętą strategią: Strategia Zarządzania Bezpieczeństwem Informacji i chmury obliczeniowej w ramach ZSZ dla Hadrone (integracja obszaru ISMS i Cloud) - punkt: 4 Strategia ISMS w Cloud Governance (ISO 27017 / ISO 27018)	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZSZ	N/A	częściowo
-----	----------	--------------------------------------	----------------------	----------	---	--	--	--	---	--	---	-----	-----------



7.10	Fizyczne	Nośniki pamięci	ISO 27001, ISO 27701, ISO 27018	Security	CC_S7 - System Operations / Operacje systemowe	<ul style="list-style-type: none"> Systemy Endpoint Protector / DLP (Blokada portów USB): Narzędzia informatyczne centralnie blokujące możliwość podłączenia nieautoryzowanych nośników wymiennych do komputerów Hadrone. Oprogramowanie do bezpiecznego czyszczenia (Wiping Tools): Narzędzia realizujące wielokrotne nadpisywanie sektorów dysku (np.: zgodnie ze standardem NIST SP 800-88), generujące nadrzędny certyfikat usunięcia danych. Procedura fizycznego niszczenia (Degaussing i niszcarki): Proces polegający na poddawaniu uszkodzonych nośników działaniu silnego pola magnetycznego (demagnetyzacja) lub ich fizycznemu zmieleniu w młynkach przemysłowych o klasie H-5 (DIN 66399). Rejestr nośników i znakowanie (Asset Tracking): Ewidencja w bazie danych, w której każdy nośnik posiada unikalny identyfikator (numer/kod kreskowy/QR), przypisanego właściciela oraz aktualny status (w użyciu / zdeponowany / zniszczony). 	<ul style="list-style-type: none"> Audyt zgodności szyfrowania nośników wymiennych: Cykliczny przegląd logów systemowych sprawdzający, czy dane kopiowane na dozwolone, służbowe pendrive'y są automatycznie i wymuszenie szyfrowane przez system (np. BitLocker To Go). Inwentaryzacja szaf depozytowych i sejfów: Kwartalna, fizyczna weryfikacja stanów magazynowych w miejscach przechowywania zapasowych lub wycofanych nośników, w celu upewnienia się, że żadne urządzenie nie zaginęło. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 7.10 Nośniki pamięci	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z	N/A	tak
------	----------	-----------------	---------------------------------------	----------	--	--	---	--	------	---	--	-----	-----



7.11	Fizyczne	Media wspierające (zasilanie itp.)	ISO 27001, ISO 22301	Security	CC_S1 - Control Environment/ Kontrole Środowiskowe	<ul style="list-style-type: none"> Systemy UPS i Agregaty prądoworcze: Zestawy akumulatorów (UPS) filtrujące zakłócenia i podtrzymujące zasilanie do czasu uruchomienia generatorów spalinowych (agregatów) z automatycznym przełącznikiem faz (ATS). Multi-homing i redundantne łącza internetowe: Wykorzystanie protokołu BGP oraz kilku niezależnych dostawców Internetu, zapewniające automatyczne przekierowanie ruchu sieciowego w przypadku awarii jednego ze światłowodów. Automatyka klimatyzacyjna i sensoryczna (BMS): System zarządzania budynkiem (Building Management System) stale monitorujący parametry pracy klimatyzacji (HVAC), ciśnienia wody oraz czystości powietrza z systemem wczesnego ostrzegania. Umowy serwisowe z gwarancją czasu naprawy (SLA): Kontrakty z dostawcami mediów i firmami konserwacyjnymi, wymuszające rygorystyczne czasy reakcji i naprawy (np.: 24/7/4h) w przypadku awarii infrastruktury budynkowej. 	<ul style="list-style-type: none"> Wskaźnik ciągłości działania mediów (KPI): Miara określająca procent czasu bezawaryjnej dostępności energii, chłodzenia i Internetu w skali roku. Weryfikacja certyfikacji Data Center: Regularne, okresowe weryfikowanie certyfikatów data Center dostawców chmury obliczeniowej, weryfikacja raportów SOC 2, type II oraz ISO 27001, ISO 22310, oraz ISO 27701 w ramach zasad bezpieczeństwa monitorowania dostawcy zewnętrznego. 	Wyjątek, Uwaga/ Exception, Comment.	<p>Spostrzeżenie – data centers są zakupione w ramach usługi IaaS od Microsoft Inc. oraz od Hetzner. Ocena zabezpieczenia wymaga, aby Hadrone dokonał pełnej weryfikacji zabezpieczeń po stronie dostawcy przez proces oceny dostawcy (Vendor Risk Management Process) oraz identyfikował wszystkie zabezpieczenia występujące u dostawcy w celu potwierdzenia spełnienia punktu normy oraz wymagań mechanizmów kontrolnych – ryzyko wpisane w rejestr ryzyka Hadrone, z planem na jego wykonanie Q3 i Q4 2026 rok.</p>	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 7.11 Media wspierające (zasilanie itp.). Wyklucza się elementy związane z infrastrukturą serwerową w ramach chmury obliczeniowej ze względu na model IaaS Hadrone nie jest dostawcą chmury obliczeniowej a jedynie jej klientem - zgodnie z przyjętą strategią: Strategia Zarządzania Bezpieczeństwem Informacji i chmury obliczeniowej w ramach ZSZ dla Hadrone (integracja obszaru ISMS i Cloud) - punkt: 4 Strategia ISMS w Cloud Governance (ISO 27017 / ISO 27018)	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS z i dodatkowo w ramach identyfikacji zabezpieczeń pod BIA w obszarze PIMS. Wylaczeniem jest wymaganie CSC oraz fakt że Hadrone nie jest dostawcą chmury obliczeniowej jako infrastruktury	N/A	częściowo
------	----------	------------------------------------	----------------------	----------	--	--	--	-------------------------------------	---	---	--	-----	-----------



7.12	Fizyczne	Bezpieczeństwo okablowania	ISO 27001	Security	CC_S1 - Control Environment/ Kontrola Środowiskowe	<ul style="list-style-type: none"> • Zamknięte systemy prowadzenia kabli: Wykorzystanie metalowych koryt kablowych, rur ochronnych (peszli) oraz zamykanych szachtów instalacyjnych (pionów technicznych) uniemożliwiających łatwy dostęp do wiązek przewodów. • Zamykane punkty dystrybucyjne (MDF / IDF): Umieszczanie przełączników sieciowych i paneli krosowych (patch paneli) wewnątrz dedykowanych, zamkniętych na klucz szaf RACK, znajdujących się w monitorowanych pomieszczeniach technicznych. 	<ul style="list-style-type: none"> • Wskaźnik nieaktywnych portów sieciowych (KPI): Miara weryfikująca, czy 100% gniazd sieciowych w strefach publicznych i open space, które nie są aktualnie przypisane do konkretnego sprzętu firmowego, jest fizycznie odłączonych na krosownicy lub zablokowanych systemowo. • Weryfikacja dostępu do punktów dystrybucji: Kontrola logów systemowych (SKD/CCTV) oraz fizycznych zamknięć szaf krosowych, mająca na celu upewnienie się, że żadna osoba nieuprawniona nie manipulowała przy krosowaniu przewodów. 	Wyjątek, Uwaga/ Exception, Comment.	<p>Spostrzeże nie – data centers są zakupione w ramach usługi IaaS od Microsoft Inc. oraz od Hetzner. Ocena zabezpieczenia wymaga, aby Hadrone dokonał pełnej weryfikacji zabezpieczeń po stronie dostawcy przez proces oceny dostawcy (Vendor Risk Management Process) oraz identyfikował wszystkie zabezpieczenia występujące u dostawcy w celu potwierdzenia spełnienia punktu normy oraz wymagań mechanizmów kontrolnych. – ryzyko wpisane w rejestr ryzyka Hadrone, z planem na jego wykonanie Q3 i Q4 2026 rok.</p>	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 7.12 Bezpieczeństwo okablowania. Wyklucza się elementy związane z infrastrukturą serwerową w ramach chmury obliczeniowej ze względu na dla modelu IaaS Hadrone nie jest dostawcą chmury obliczeniowej a jedynie jej klientem - zgodnie z przyjętą strategią: Strategia Zarządzania Bezpieczeństwem Informacji i chmury obliczeniowej w ramach ZSZ dla Hadrone (integracja obszaru ISMS i Cloud) - punkt: 4 Strategia ISMS w Cloud Governance (ISO 27017 / ISO 27018)	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZSZ. Wyłączeniem jest wymaganie CSC oraz fakt że Hadrone nie jest dostawcą chmury obliczeniowej jako infrastruktury	N/A	częściowo
------	----------	----------------------------	-----------	----------	---	--	--	--	---	--	---	-----	-----------



7.13	Fizyczne	Konserwacja wyposażenia	ISO 27001	Security	CC_S1 - Control Environment/ Kontrola Środowiskowe	<ul style="list-style-type: none"> Procedura "Serwis zewnętrzny" i asysta IT/Security: Zasady wpuszczania serwisantów do stref bezpiecznych, wymagający weryfikacji ich tożsamości, podpisania dokumentów np.: NDA oraz zapewnienia stałego nadzoru pracownika w trakcie naprawy. Umowy utrzymaniowe z producentami (Vendor Support): Kontrakty serwisowe typu Care Pack, gwarantujące wsparcie inżynierów producenta oraz dostawę komponentów sprzętowych w rygorystycznym reżimie czasowym (np. Next Business Day lub 4h on-site). 	<ul style="list-style-type: none"> Audyt poserwisowy i testy sprawności: Obowiązkowa procedura weryfikacyjna, w ramach której po zakończeniu prac konserwacyjnych sprzęt jest poddawany testom operacyjnym przed oficjalnym przywróceniem go do produkcyjnej pracy w sieci. Analiza awarii spowodowanych brakiem konserwacji: Kontrola badająca każdą awarię sprzętową pod kątem tego, czy bezpośrednią przyczyną usterki nie było pominięcie lub nienależyte wykonanie okresowego serwisu. 	Wyjątek, Uwaga/ Exception, Comment.	<p>Spostrzeżenie – data centers są zakupione w ramach usługi IaaS od Microsoft Inc. oraz od Hetzner. Ocena zabezpieczenia wymaga, aby Hadrone dokonał pełnej weryfikacji zabezpieczeń po stronie dostawcy przez proces oceny dostawcy (Vendor Risk Management Process) oraz identyfikował wszystkie zabezpieczenia występujące u dostawcy w celu potwierdzenia spełnienia punktu normy oraz wymagań mechanizmów kontrolnych – ryzyko wpisane w rejestr ryzyka Hadrone, z planem na jego wykonanie Q3 i Q4 2026 rok.</p>	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 7.13 Konserwacja wyposażenia. Wyklucza się elementy związane z infrastrukturą serwerową w ramach chmury obliczeniowej ze względu na dla modelu IaaS Hadrone nie jest dostawcą chmury obliczeniowej a jedynie jej klientem - zgodnie z przyjętą strategią: Strategia Zarządzania Bezpieczeństwem Informacji i chmury obliczeniowej w ramach ZSZ dla Hadrone (integracja obszaru ISMS i Cloud) - punkt: 4 Strategia ISMS w Cloud Governance (ISO 27017 / ISO 27018)	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z. Wyłączeniem jest wymaganie CSC oraz fakt że Hadrone nie jest dostawcą chmury obliczeniowej jako infrastruktury	N/A	częściowo
------	----------	-------------------------	-----------	----------	---	--	---	--	---	---	--	-----	-----------



7.14	Fizyczne	Bezpieczne usuwanie sprzętu	ISO 27001, ISO 27017, ISO 27018	Security	CC_S7 - System Operations / Operacje systemowe	<ul style="list-style-type: none"> • Procedura EOL (End-of-Life) i wycofania zasobów: Sformalizowane zasady określające krok po kroku ścieżkę wyrejestrowania sprzętu z systemów IT, odpięcia go od sieci korporacyjnej oraz przekazania do strefy kwarantanny/utylizacji. • Współpraca z licencjonowanymi firmami utylizacyjnymi: Proces przekazywania e-odpadów wyspecjalizowanym podmiotom zewnętrznym, które na mocy umowy (i pod nadzorem) dokonują fizycznego zmielenia lub przetopienia sprzętu, wystawiając Kartę Przekazania Odpadu (KPO). 	<ul style="list-style-type: none"> • Wskaźnik certyfikacji utylizacji (KPI): Miara weryfikująca, czy 100% wycofanych z użycia urządzeń posiada powiązany, unikalny certyfikat bezpiecznego zamazania danych lub fizycznego zniszczenia. • Kontrola poprawności usuwania logów konfiguracyjnych: Weryfikacja, czy przed usunięciem urządzeń sieciowych (routery, przełączniki) zresetowano je do ustawień fabrycznych, usuwając zapisane klucze kryptograficzne, adresy IP i hasła dostępowe. 	Wyjątek, Uwaga/ Exception, Comment.	<p>Spostrzeżenie – data centers są zakupione w ramach usługi IaaS od Microsoft Inc. oraz od Hetzner. Ocena zabezpieczenia wymaga, aby Hadrone dokonał pełnej weryfikacji zabezpieczeń po stronie dostawcy przez proces oceny dostawcy (Vendor Risk Management Process) oraz identyfikował wszystkie zabezpieczenia występujące u dostawcy w celu potwierdzenia spełnienia punktu normy oraz wymagań mechanizmów kontrolnych – ryzyko wpisane w rejestr ryzyka Hadrone, z planem na jego wykonanie Q3 i Q4 2026 rok.</p>	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 7.14 Bezpieczne usuwanie sprzętu. Wyklucza się elementy związane z infrastrukturą serwerową w ramach chmury obliczeniowej ze względu na model IaaS. Hadrone nie jest dostawcą chmury obliczeniowej, a jedynie jej klientem - zgodnie z przyjętą strategią: Strategia Zarządzania Bezpieczeństwem Informacji i chmury obliczeniowej w ramach ZSZ dla Hadrone (integracja obszaru ISMS i Cloud) - punkt: 4 Strategia ISMS w Cloud Governance (ISO 27017 / ISO 27018)	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZSZ oraz dodatkowo regulowany przez RODO i w ramach ZSZ. Wyłączeniem jest wymaganie CSC oraz fakt, że Hadrone nie jest dostawcą chmury obliczeniowej jako	N/A	częściowo
------	----------	-----------------------------	---------------------------------	----------	--	---	--	-------------------------------------	---	--	---	-----	-----------



8.1	Techniczne	Urządzenia końcowe użytkownika	ISO 27001, ISO 27701	Security	CC_S1 - Control Environment/ Kontrolę Środowiskowe	<ul style="list-style-type: none"> Systemy MDM / UEM (Unified Endpoint Management): Narzędzia centralne (np.: Microsoft Intune) służące do zdalnego zarządzania konfiguracją, wymuszania polityk bezpieczeństwa oraz zdalnego czyszczenia (Remote Wipe) urządzeń. Ochrona przed malware: Zaawansowane oprogramowanie antywirusowe nowej generacji instalowane na każdym urządzeniu, stale monitorujące zachowanie systemu i blokujące cyberzagrożenia w czasie rzeczywistym. Proces rejestracji i uwierzytelniania (MFA/biometria): Wymóg stosowania silnego, wieloskładnikowego uwierzytelniania (MFA) lub mechanizmów biometrycznych (Windows Hello, FaceID) przy każdym logowaniu do urządzenia. Zasady bezpiecznego BYOD (Bring Your Own Device): Zasady i ramy prawne definiujące warunki techniczne i bezpieczeństwa, na jakich pracownicy mogą używać prywatnego sprzętu do celów służbowych. 	<ul style="list-style-type: none"> Wskaźnik aktualności oprogramowania (KPI): Miara określająca procent urządzeń końcowych, które posiadają zainstalowane najnowsze krytyczne łatki bezpieczeństwa w określonym oknie czasowym. Automatyczna kontrola stanu zgodności (Compliance Check): Mechanizmy dostępu warunkowego (Conditional Access), które automatycznie blokują urządzeniu dostęp do poczty i chmury, jeśli system wykryje, że antywirus lub szyfrowanie są wyłączone. Inwentaryzacja i testy podatności punktów końcowych: Regularne, automatyczne skanowanie urządzeń w celu wykrycia zainstalowanych nieautoryzowanych aplikacji oraz podatności w konfiguracji systemowej. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 8.1 Urządzenia końcowe użytkownika oraz dodatkowo konfigurowane zgodnie z: Zasady konfiguracji aplikacji i usług M365 w Hadrone Sp. z o.o. Stosowane narzędzia to: M365 oraz polisy konfiguracyjne dla każdego komputera dodanego do domeny.	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z oraz dodatkowo regulowany przez RODO i w ramach ZSZ	Art. 21(2)g (NIS2) / Art. 9 (DORA)	tak
-----	------------	--------------------------------	----------------------	----------	---	--	--	---	------	--	--	------------------------------------	-----



8.2	Techniczne	Uprzywilejowane prawa dostępu	ISO 27001, ISO 27017	Security	CC_S6 - Logical and Physical Access Control / Logiczna i fizyczna kontrola dostępu	<ul style="list-style-type: none"> Systemy klasy PAM (Privileged Access Management): Dedykowane rozwiązania informatyczne (np.: Microsoft PAM/PIM) służące do bezpiecznego przechowywania haseł administracyjnych, rotowania ich oraz nagrywania sesji administratorów. Wieloskładnikowe uwierzytelnianie (MFA): Obowiązkowy mechanizm drugiego składnika (token sprzętowy, aplikacja uwierzytelniająca) wymagany przy każdym logowaniu użytkownika, w tym na konto o podwyższonych uprawnieniach. Sformalizowany proces wnioskowania: Działania wymagające pisemnego uzasadnienia biznesowego i formalnej akceptacji (email) właściciela systemu, Hadrone CISO, przed nadaniem uprawnień admina. Automatyczna rotacja haseł i kluczy: Techniczne algorytmy systemowe, które automatycznie zmieniają hasła do kont administracyjnych po każdym ich użyciu lub w regularnych, krótkich odstępach czasu (np.: co 24 godziny). 	<ul style="list-style-type: none"> Wskaźnik liczby kont uprzywilejowanych (KPI): Miara kontrolna monitorująca łączną liczbę aktywnych kont administratorów w organizacji i dążąca do jej stałego ograniczania. Cykliczny przegląd i reatestacja uprawnień: Regularny (np.: raz na kwartał) formalny przegląd listy kont z dostępem root/admin w celu wykrycia i natychmiastowego usunięcia uprawnień osobom, które zmieniły stanowisko lub odeszły z firmy. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 8.2 Uprzywilejowane prawa dostępu oraz dodatkowo konfigurowane zgodnie z: Zasady konfiguracji aplikacji i usług M365 w Hadrone Sp. z o.o. Stosowane narzędzia to: M365 oraz polity konfiguracyjne dla każdego komputera dodanego do domeny. możliwość użycia kont w ramach procedury "braking glass" - włączone monitorowanie.	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z oraz dodatkowo regulowany przez RODO i w ramach ZSZ	N/A	tak
-----	------------	-------------------------------	----------------------	----------	--	---	---	---	------	--	--	-----	-----



B.8.2	Zabezpieczenia dla PP - Annex B	Warunki przetwarzania	ISO 27701	Privacy	CC_P4 - Use, Retention and Disposal / Użycie, Retencja i wycofanie	<ul style="list-style-type: none"> • Matryca Mapowania Instrukcji na Procesy IT: Sformalizowany dokument techniczny przekładający zapisy umowne na konkretne reguły systemowe (np.: blokowanie funkcji eksportu danych, jeśli umowa pozwala wyłącznie na ich wyświetlanie). • System zarządzania zmianą instrukcji (Change Management): Proces weryfikacji i autoryzacji nowych wytycznych od Administratora, każda zmiana warunków przetwarzania musi przejść formalną ścieżkę zatwierdzenia przed wdrożeniem w systemach. • Scentralizowany Rejestr Podwykonawców (Sub-processor Registry): Narzędzie i powiązany z nim proces informowania Administratorów z odpowiednim wyprzedzeniem o planowanych zmianach sub-procesorów, umożliwiając ADO wyrażenie sprzeciwu. • Techniczne blokady cross-data (Izolacja środowisk): Konfiguracja systemów bazodanowych i aplikacji (np. za pomocą sztynowego podziału na logiczne kontenery/tenanty), uniemożliwiająca mieszanie danych różnych Administratorów i przetwarzanie ich na innych warunkach. 	<ul style="list-style-type: none"> • Wskaźnik zgodności operacji z umową (KPI): Wynik cyklicznych (np. miesięcznych) wewnętrznych testów sprawdzających czy wszystkie realizowane procesy na danych PII posiadają bezpośrednie odzwierciedlenie w aktualnych umowach Electricity (cel: 100% zgodności). • Weryfikacja i testy zgłaszania sprzeciwów prawnych: Coroczny przegląd procedury eskalacyjnej sprawdzający, czy pracownicy Procesora potrafią zidentyfikować i prawidłowo zaraportować instrukcje ADO naruszające prawo (test skuteczności mechanizmu "whistleblowing"). • Audyt zgodności umów z sub-procesorami (Back-to-Back Agreement Check): Roczna kontrola losowych umów z dalszymi podwykonawcami w celu upewnienia się, że warunki przetwarzania i wymagania techniczne nie są mniej rygorystyczne niż te, które Procesor podpisał z głównym Administratorem. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: B.8.2 Warunki przetwarzania oraz dodatkowo przez dokument: Polityka Bezpieczeństwa Danych Osobowych w Hadrone Sp. z o.o i przez dokument: Instrukcja Zarządzania Systemem Informatycznym w Hadrone Sp. z o.o.	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez RODO i w ramach ZSZ	N/A	tak
-------	---------------------------------	-----------------------	-----------	---------	--	---	--	---	------	---	--	-----	-----



8.3	Techniczne	Ograniczenie dostępu do informacji	ISO 27001, ISO 27701	Security	CC_S2 - Information and Communication / Komunikacja i informowanie	<ul style="list-style-type: none"> Kontrola dostępu oparta na rolach (RBAC) lub cechach (ABAC): Mechanizm technologiczny automatycznie przypisujący uprawnienia do kont na podstawie pełnionej funkcji w strukturze (np.: Rola: "Specjalista") lub atrybutów (np.: „Zespół”). Macierz uprawnień (Access Control Matrix): Sformalizowany, regularnie aktualizowany dokument, definiujący relacje między rolami użytkowników a poziomem dostępu do zasobów (Odczyt/Zapis/Usuwanie). Dostęp Warunkowy (Conditional Access) i MFA: Polityki bezpieczeństwa uzależniające przyznanie dostępu do informacji od dodatkowych kryteriów, takich jak logowanie z zaufanego urządzenia, właściwa lokalizacja geograficzna oraz pomyślna weryfikacja drugim składnikiem (MFA). Znakowanie i klasyfikacja informacji: Proces technicznego etykietowania dokumentów i wiadomości e-mail (np.: przy użyciu Microsoft Purview Information Protection), który automatycznie nakłada restrykcje (np.: zakaz kopiowania/drukowania) na pliki oznaczone jako "Poufne" lub te które mają podkategorię „Privacy Data”. 	<ul style="list-style-type: none"> Proces cyklicznej weryfikacji i przeglądu dostępu: Kwartalny lub półroczny formalny proces, w którym właściciele informacji muszą elektronicznie zatwierdzić (podpisać) listę osób mających dostęp do podległych im zasobów wrażliwych. Testy segregacji obowiązków (SoD - Segregation of Duties): Automatyczna lub manualna weryfikacja krzyżowa mająca na celu wykrycie konfliktów uprawnień, np. sprawdzenie, czy ta sama osoba nie posiada jednocześnie uprawnień do wprowadzania faktury oraz jej finansowego zatwierdzania. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 8.3 Ograniczenie dostępu do informacji oraz dodatkowo konfigurowane zgodnie z: Zasady konfiguracji aplikacji i usług M365 w Hadrone Sp. z o.o. Stosowane narzędzia to: M365 oraz polisy konfiguracyjne dla każdego komputera dodanego do domeny. Wdrożone narzędzia to: Microsoft Purview Information Protection client (MPIP) oraz RG dla środowiska Azure.	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z oraz dodatkowo regulowany przez RODO i w ramach ZSZ	N/A	tak
-----	------------	------------------------------------	----------------------	----------	--	--	--	---	------	--	--	-----	-----



B.8.3	Zabezpieczenia dla PP - Anex B	Obowiązki wobec klienta	ISO 27701	Privacy	CC_P3 - Collection / Zbieranie danych	<ul style="list-style-type: none"> • Sformalizowana procedura powiadamiania o incydentach: Zautomatyzowany proces eskalacji, który po wykryciu naruszenia automatycznie generuje i wysyła precyzyjny raport do wyznaczonych osób po stronie klienta. • Dedykowane interfejsy i narzędzia samoobsługowe (DSR Portals): Udostępnienie klientowi funkcji systemowych (np. przez API lub panel administracyjny) pozwalających na samodzielny eksport, modyfikację lub trwałe kasowanie danych PII w odpowiedzi na wnioski jego użytkowników. – dotyczy systemów SaaS. • Pakiety dowodowe dla klienta (Compliance Packages): Gotowe zestawy dokumentów (np.: certyfikaty ISO 27001/27701, wyniki testów penetracyjnych) udostępniane klientom na żądanie w celu redukcji konieczności przeprowadzania audytów manualnych. • SLA i procesy zarządzania zapytaniami klientów: Wydzielony kanał komunikacji, służący wyłącznie do obsługi zapytań klientów związanych z prywatnością, audytami oraz zmianami w architekturze systemowej. 	<ul style="list-style-type: none"> • Czas powiadomienia o incydencie (KPI / MTTE): Miara sprawdzająca czas, jaki upłynął od momentu potwierdzenia incydentu w infrastrukturze Procesora do momentu skutecznego doręczenia powiadomienia klientowi (zgodność z umową, np.: mniej niż 24 godziny). • Wskaźnik terminowości wsparcia wniosków DSR: Procentowy udział zapytań od klientów dotyczących realizacji praw ich użytkowników (np.: wyciąg danych z bazy), które zostały obsłużone przez inżynierów Procesora w zdefiniowanym w umowie czasie. • Przegląd gotowości do audytów zewnętrznych (Mock Audits): Coroczny test wewnętrzny (symulacja), w którym zespół Procesora przechodzi przez ścieżkę audytu narzuconą przez fikcyjnego, rygorystycznego klienta, w celu zweryfikowania sprawności wyciągania dowodów bezpieczeństwa. 	Brak wyjątków, Brak uwag / No exception, No comments.	brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: B.8.3 Obowiązki wobec klienta oraz dodatkowo przez dokument: Polityka Bezpieczeństwa Danych Osobowych w Hadrone Sp. z o.o i przez umowy z klientami Hadrone w ramach umów DPA czy samych zapisów o powierzchni danych do przetwarzania. - dokument dodatkowy: Strategia Zarządzania Bezpieczeństwem i Ochroną Danych Osobowych w ramach ZSZ dla Hadrone (Integracja z PIMS i PII w Cloud) - punkt: 4.2 Matryca współdzielonej odpowiedzialności za PII w Chmurze.	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez RODO i w ramach ZSZ	N/A	tak
-------	--------------------------------	-------------------------	-----------	---------	---------------------------------------	--	---	---	------	---	--	-----	-----



8.4	Techniczne	Dostęp do kodu źródłowego	ISO 27001	Security	CC_S2 - Information and Communication / Komunikacja i informowanie	<ul style="list-style-type: none"> Systemy Kontroli Wersji (Git) z uwierzytelnieniem MFA: Centralne, bezpieczne repozytoria (np.: GitHub) wymagające logowania hasło lub np.: kluczami FIDO2 oraz obowiązkowego stosowania wieloskładnikowego uwierzytelniania MFA. Blokady gałęzi (Protected Branches) i proces Pull Request: Konfiguracja repozytorium uniemożliwiająca bezpośredni wypych kodu (push) do gałęzi produkcyjnej bez przejścia formalnego procesu recenzji (Pull/Merge Request) i pomyślnego zaliczenia testów automatycznych. Skanery kodu i sekretów (SAST / Secret Detection): Narzędzia automatyczne zintegrowane z pipeline CI/CD, które skanują kod w poszukiwaniu podatności oraz przypadkowo pozostawionych haseł przed jego wdrożeniem. Scentralizowane zarządzanie kluczami (Vaults): Wykorzystanie zewnętrznych systemów zarządzania sekretami (np. HashiCorp Vault, Microsoft KeyVault), z których aplikacja pobiera hasła dynamicznie w czasie uruchamiania, zamiast czytać je z kodu. 	<ul style="list-style-type: none"> Wskaźnik pokrycia recenzją kodu (KPI): Miara weryfikująca, jaki procent zmian wprowadzonych do gałęzi produkcyjnej przeszedł poprawny proces Peer Review zatwierdzony przez drugiego programistę. Audyt i przegląd uprawnień do repozytoriów: Regularna (np.: raz na kwartał/pół roku) kontrola listy użytkowników posiadających dostęp do kodu, skutkująca natychmiastowym blokowaniem kont pracowników odchodzących z Hadrone lub zmieniających projekt. Monitorowanie pobrań kodu (Anti-exfiltration logs): Automatyczne alerty systemowe weryfikujące anomalie w pobieraniu kodu, takie jak masowe klonowanie (git clone) całych repozytoriów przez pojedynczego użytkownika w krótkim czasie (wczesne wykrywanie kradzieży własności intelektualnej). Cykliczne testy podatności i penetracyjne: Wyrwykowe, manualne audyty bezpieczeństwa kodu źródłowego oraz konfiguracji repozytoriów, mające na celu wykrycie luk w logice aplikacji lub błędów w uprawnieniach dostępu do systemów CI/CD. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 8.4 Dostęp do kodu źródłowego. Stosowane narzędzia to: GitHub logowanie przez Entra ID (login i hasło) oraz Microsoft MFA jako 2FA. Dostęp tylko dla tych osób, które są w odpowiedniej RG w Azure Entra ID i mają zdefiniowane role w GitHub.	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z	N/A	tak
-----	------------	---------------------------	-----------	----------	--	--	---	---	------	--	--	-----	-----



B.8.4	Zabezpieczenia dla PP - Anex B	Prywatność w fazie projektowania	ISO 27701	Privacy	CC_P7 - Quality / Jakość	<ul style="list-style-type: none"> • Techniczne funkcje zarządzania danymi (Privacy Features): Wbudowanie w system gotowych narzędzi dla Administratora, takich jak mechanizmy automatycznego maskowania danych, szyfrowanie baz danych (w spoczynku i w locie) oraz funkcje trwałego usuwania rekordów. • Granularne zarządzanie uprawnieniami (RBAC): Mechanizm kontroli dostępu oparty na rolach, umożliwiający Klientowi precyzyjne odseparowanie uprawnień swojego personelu od personelu Procesora. • Automatyzacja polityk retencji danych: Implementacja w architekturze systemu konfigurowalnych reguł (np.: zadań harmonogramu), które automatycznie usuwają lub anonimizują dane PII po upływie okresu zdefiniowanego przez Klienta. • Modelowanie zagrożeń dla prywatności (Threat Modeling): Włączenie analizy ryzyka dla prywatności (np.: przy użyciu metodologii STRIDE) do standardowego procesu projektowania każdej nowej funkcji systemu lub infrastruktury. 	<ul style="list-style-type: none"> • Wskaźnik pokrycia testami bezpieczeństwa i prywatności (KPI): Automatyczne testy bezpieczeństwa (SAST/DAST) pod kątem wycieków danych PII przed każdym wydaniem nowej wersji. • Weryfikacja integralności rejestrów aktywności (Audit Logs): Kontrola poprawności działania logów systemowych i upewnienie się, że system bezbłędnie rejestruje każdą operację na danych PII (kto, kiedy, co zmienił) i udostępnia te logi Administratorowi w nienaruszalnej formie. • Cykliczne testy penetracyjne dostarczanych rozwiązań: Regularne (np. raz w roku) zlecenie niezależnych testów bezpieczeństwa gotowego produktu lub platformy w celu wykrycia luk architektonicznych zagrażających prywatności danych Klientów. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: B.8.4 Prywatność w fazie projektowania oraz dodatkowo przez dokument: Polityka Bezpieczeństwa Danych Osobowych w Hadrone Sp. z o.o. - punkt: 6.5. Uwzględnienie ochrony danych osobowych w fazie projektowania oraz domyślna ochrona danych osobowych Dodatkowo ma zastosowanie dokument dodatkowy: Strategia Zarządzania Bezpieczeństwem i Ochroną Danych Osobowych w ramach ZSZ dla Hadrone (Integracja z PIMS i PII w Cloud) - punkt: 6 Operacjonalizacja zasad prywatności (PIMS Operations - ISO 27701)	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez RODO i w ramach ZSZ	N/A	tak
-------	--------------------------------	----------------------------------	-----------	---------	--------------------------	--	---	---	------	---	--	-----	-----



8.5	Techniczne	Bezpieczne uwierzytelnianie	ISO 27001, ISO 27017	Security	CC_S6 - Logical and Physical Access Control / Logiczna i fizyczna kontrola dostępu	<ul style="list-style-type: none"> • Uwierzytelnianie wieloskładnikowe (MFA / 2FA): Wykorzystanie kombinacji wiedzy (hasło/PIN), posiadania (klucz sprzętowy U2F/FIDO2, aplikacja Authenticator z powiadomieniem push) oraz cech biometrycznych (odcisk palca, skan twarzy). • Scentralizowane systemy Identity Provider (IdP / SSO): Rozwiązania klasy Single Sign-On (np.: Microsoft Entra ID), które pozwalają użytkownikowi na jednokrotne bezpieczne zalogowanie się i uzyskanie dostępu do wielu aplikacji bez wpisywania osobnych haseł. • Polityka blokowania kont: Automatyczny mechanizm techniczny, który czasowo blokuje konto lub drastycznie opóźnia czas kolejnej próby logowania po wprowadzeniu 5 razy błędnego hasła (ochrona przed atakami Brute Force). 	<ul style="list-style-type: none"> • Wskaźnik pokrycia systemów przez MFA (KPI): Miara określająca procentowy udział aplikacji i systemów w organizacji, które wymagają drugiego składnika uwierzytelniania przed przyznaniem dostępu. • Audyt siły i podatności haseł (Password Auditing): Cykliczne (np.: raz do roku), automatyczne skanowanie baz skrótów haseł (w sposób bezpieczny/offline) w celu wykrycia kont używających haseł słabych, domyślnych lub ujawnionych w publicznych wyciekach. • Kontrolowane testy socjotechniczne (Phishing Campaigns): Regularne symulacje ataków phishingowych nakierowanych na wyłudzenie poświadczeń pracowników, pozwalające ocenić skuteczność wdrożonych mechanizmów MFA oraz poziom czujności personelu. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 8.5 Bezpieczne uwierzytelnianie oraz dodatkowo konfigurowane zgodnie z: Zasady konfiguracji aplikacji i usług M365 w Hadrone Sp. z o.o. Stosowane narzędzia to: M365 oraz polisy konfiguracyjne dla każdego komputera dodanego do domeny. Stosowane narzędzia to: Entra ID (login i hasło) oraz Microsoft MFA jako 2FA. Dla systemów Hadrone dostarczanych w modelu SaaS stosuje się identyfikację i uwierzytelnianie bazując na API w standardzie OpenID i stosowanie mechanizmów kontroli jest po stronie klienta usługi SaaS Hadrone.	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z	N/A	tak
-----	------------	-----------------------------	----------------------	----------	--	--	--	---	------	--	--	-----	-----



B.8.5	Zabezpieceni a dla PP - Anex B	Przekazywanie i udostępnianie	ISO 27701	Privacy	CC_P6 - Disclosure and Nitification / Ujawnienie i powiadamiani e	<ul style="list-style-type: none"> • Kryptograficzne zabezpieczenia transferu (Secure In-Transit): Wdrożenie wymogu stosowania wyłącznie bezpiecznych i autoryzowanych kanałów transmisji (np. szyfrowane tunele VPN, protokół SFTP z kluczami SSH) przy jakimkolwiek technicznym przekazywaniu danych do systemów podwykonawców. • Standardowe Klauzule Umowne (SCC / B2B DPA): Gotowe szablony umów powierzenia danych dla podwykonawców (sub-DPA) oraz mechanizmy prawne (SCC) regulujące transfery międzynarodowe, z góry zweryfikowane przez dział prawny pod kątem zgodności z wymaganiami głównych Klientów. • Scentralizowany rejestr przepływu danych (Data Flow Mapping): Narzędzie do mapowania procesów, które w przejrzysty sposób dokumentuje każdą relację udostępniania danych wskazując dokładnie kto, komu, jakie kategorie PII, w jakim celu i do jakiego kraju przekazuje. 	<ul style="list-style-type: none"> • Wskaźnik zatwierdzonych sub-procesorów (KPI): Procentowy udział podmiotów trzecich, którym faktycznie przekazano dane PII, posiadających formalną, pisemną akceptację ze strony Administratora oraz podpisaną umowę sub-DPA przed rozpoczęciem transferu. • Cykliczny audyt techniczny i operacyjny sub-procesorów: Coroczny przegląd procedur bezpieczeństwa u dostawców trzecich (np. weryfikacja ważności ich certyfikatów ISO 27001, raportów SOC 2) w celu upewnienia się, że stale spełniają oni warunki ochrony danych. • Kontrola integralności lokalizacji danych (Geo-fencing Audits): Automatyczne skanowanie konfiguracji chmurowej i bazodanowej w celu fizycznego zweryfikowania, czy dane PII nie są replikowane lub backupowane do regionów geograficznych zabronionych umową z Klientem. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: B.8.5 Przekazywanie i udostępnianie oraz dodatkowo przez dokument: Polityka Bezpieczeństwa Danych Osobowych w Hadrone Sp. z o.o. - punkt: 6.9. Przekazywanie danych osobowych do państwa trzeciego. Dodatkowo ma zastosowanie dokument dodatkowy: Strategia Zarządzania Bezpieczeństwem i Ochroną Danych Osobowych w ramach ZSZ dla Hadrone (Integracja z PIMS i PII w Cloud) - punkt: 7 Cykl życia, geokalizacja i retencja danych osobowych	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez RODO i w ramach ZSZ	N/A	tak
-------	--------------------------------------	----------------------------------	-----------	---------	---	---	---	--	------	--	--	-----	-----



8.6	Techniczne	Zarządzanie wydajnością	ISO 27001, ISO 27017, ISO 22301	Availability	CC_A0 - Availability / Dostępność	<ul style="list-style-type: none"> Systemy ciągłego monitorowania wydajności (Monitoring Tools): Narzędzia automatyczne (np.: Azure Monitoring) zbierające w czasie rzeczywistym parametry zużycia zasobów sprzętowych i aplikacyjnych. Progi ostrzegawcze i systemy alertowania: Konfiguracja automatycznych powiadomień (np.: e-mail, SMS), które są wysyłane do administratorów po przekroczeniu krytycznych wartości (np.: zajętość dysku serwera powyżej 70%). Mechanizmy automatycznego skalowania (Autoscaling): Wykorzystanie technologii chmurowych i konteneryzacji, które automatycznie uruchamiają dodatkowe zasoby/serwery w momencie wzrostu ruchu automatycznie np.: przez wykorzystanie mechanizmów microserwisów IaC. Testy obciążeniowe i wydajnościowe (Load/Stress Testing): Procesy symulacji masowego ruchu użytkowników, realizowane przed wdrożeniem systemu na produkcję w celu określenia jego maksymalnych limitów. 	<ul style="list-style-type: none"> Wskaźnik użycia zasobów krytycznych (KPI): Regularna analiza średniego i szczytowego poziomu zużycia CPU, RAM i dysków w celu identyfikacji systemów wymagających natychmiastowej rozbudowy. Monitorowanie trendów wzrostu danych: Cykliczna (np.: raz w miesiącu) analiza prędkości przyrostu baz danych i logów systemowych, pozwalająca precyzyjnie określić moment, w którym zabraknie przestrzeni dyskowej. Przegląd logów opóźnień i czasu odpowiedzi (Response Time): Miara weryfikująca czas realizacji zapytań przez aplikację SaaS Hadrone. Audyt konfiguracji i usuwania zbędnych danych: Okresowe sprawdzanie systemów pod kątem czyszczenia starych logów, plików tymczasowych oraz optymalizacji indeksów bazodanowych, co pozwala odzyskać wydajność bez nakładów finansowych. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 8.6 Zarządzanie wydajnością oraz dodatkowo konfigurowane zgodnie z: Zasady konfiguracji aplikacji i usług M365 w Hadrone Sp. z o.o. Stosowane narzędzia to: M365 oraz polityki konfiguracyjne dla każdego komputera dodanego do domeny.	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z	N/A	tak
-----	------------	-------------------------	---------------------------------	--------------	-----------------------------------	--	--	---	------	---	--	-----	-----



8.7	Techniczne	Ochrona przed złośliwym oprogramowaniem	ISO 27001, ISO 27017	Security	CC_S3 - Risk Assessment / Ocena ryzyka	<ul style="list-style-type: none"> Systemy EDR / XDR i Antywirusy: Nowoczesne oprogramowanie ochronne (Endpoint Detection and Response) zainstalowane na punktach końcowych, łączące tradycyjne skanowanie sygnatur z zaawansowaną analizą behawioralną AI. Bramki sieciowe (Secure Email & Web Gateways): Filtry na poziomie serwerów pocztowych i ruchu internetowego, które skanują załączniki e-mail oraz blokują dostęp do niebezpiecznych lub zainfekowanych stron WWW (phishing, drive-by download), HIPS, HBFW, WAF. Technologia piaskownicy (Sandboxing): Mechanizm izolowanego środowiska w chmurze lub sieci, w którym podejrzane, nowo napotkane pliki są bezpiecznie uruchamiane i testowane przed dopuszczeniem ich do systemu użytkownika. Scentralizowane zarządzanie (Konsola administracyjna): Centralny system (np.; Microsoft Defender) dający administratorom pełen wgląd w stan bezpieczeństwa wszystkich urządzeń, umożliwiający zdalne usuwanie złośliwego oprogramowania i wymuszanie skanowania. 	<ul style="list-style-type: none"> Wskaźnik aktualności agentów ochrony (KPI): Miara określająca procent urządzeń w sieci posiadających aktualne bazy definicji wirusów i najnowszą wersję oprogramowania EDR/AV. Monitorowanie niechronionych punktów (CAC): Automatyczne skanowanie sieci (np. przez systemy NAC) w celu natychmiastowego wykrywania i blokowania urządzeń, które próbują uzyskać dostęp do zasobów, a nie mają zainstalowanego antywirusa. Przegląd i analiza alertów bezpieczeństwa: Codzienna weryfikacja logów z konsoli antywirusowej, mająca na celu identyfikację powtarzających się incydentów, podatnych użytkowników lub systemów wymagających dodatkowego utwardzenia (hardeningu). 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 8.7 Ochrona przed złośliwym oprogramowaniem oraz dodatkowo konfigurowane zgodnie z: Zasady konfiguracji aplikacji i usług M365 w Hadrone Sp. z o.o. Stosowane narzędzia to: M365 oraz polisy konfiguracyjne dla każdego komputera dodanego do domeny.	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z	N/A	tak
-----	------------	---	----------------------	----------	--	--	---	---	------	---	--	-----	-----



8.8	Techniczne	Zarządzanie podatnościami	ISO 27001, ISO 27017	Security	CC_S9 - Risk Mitigation / Osłabianie ryzyka	<ul style="list-style-type: none"> • Skanery podatności (Vulnerability Scanners): Automatyczne narzędzia (np.: Nessus) wykonujące regularne, zaplanowane audyty sieci, systemów operacyjnych i aplikacji w poszukiwaniu znanych luk bezpieczeństwa. • Proces zarządzania poprawkami (Patch Management): Scentralizowane systemy (np.: Microsoft Intune) automatyzujące pobieranie, testowanie i masową dystrybucję łat bezpieczeństwa na urządzenia Hadrone. • Subskrypcja alertów zagrożeń (Threat Intelligence): Proces stałego monitorowania biuletynów bezpieczeństwa producentów oprogramowania oraz powiadomień od zespołów ds. cyberbezpieczeństwa (np.: CERT Polska) o nowo odkrytych podatnościach (w tym typu Zero-Day). • Testy penetracyjne: Manualne próby przełamania zabezpieczeń wykonywane przez zewnętrznych ekspertów (etycznych hakerów), pozwalające wykryć złożone luki logiczne, których nie zauważyły automatyczne skanery. 	<ul style="list-style-type: none"> • Średni czas naprawy podatności (MTTR - Mean Time to Repair): Kluczowy wskaźnik (KPI) mierzący czas, jaki upływa od wykrycia podatności do jej skutecznego załatwienia, porównywany z limitami określonymi w polityce Hadrone. • Wskaźnik okna ekspozycji (Vulnerability Window): Miara weryfikująca liczbę oraz procent urządzeń w organizacji, które pozostają niezafatane po upływie oficjalnego terminu SLA luki bezpieczeństwa. • Skanowanie re-weryfikacyjne (Rescanning): Obowiązkowa kontrola techniczna polegająca na ponownym uruchomieniu skanera podatności natychmiast po wdrożeniu poprawek, mająca na celu potwierdzenie, że luka została trwale zamknięta. • Audyt wyjątków bezpieczeństwa: Regularny przegląd i zatwierdzanie rejestru tzw. „akceptowanych ryzyk”, czyli systemów, na których z przyczyn technicznych nie można zainstalować poprawki (wymaga wdrożenia alternatywnych mechanizmów kompensacyjnych, np. izolacji sieciowej). 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 8.8 Zarządzanie podatnościami oraz dodatkowo konfigurowane zgodnie z: Zasady konfiguracji aplikacji i usług M365 w Hadrone Sp. z o.o. Stosowane narzędzia to: M365 oraz polisy konfiguracyjne dla każdego komputera dodanego do domeny.	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z	Art. 21(2)g (NIS2) / Art. 6 (DORA) / Art. 9 AI Act	tak
-----	------------	---------------------------	----------------------	----------	---	---	---	---	------	---	--	--	-----



8.9	Techniczne	Zarządzanie konfiguracją	ISO 27001, ISO 27017	Security	CC_S8 - Change Managment / Zarządzanie zmianą	<ul style="list-style-type: none"> Bazy danych zarządzania konfiguracją (CMDB): Rejest ewidencji przechowujący informacje o zasobach IT, ich parametrach oraz wzajemnych powiązaniach. Infrastruktura jako Kod (IaC) i automatyzacja: Narzędzia do automatycznego wdrażania i egzekwowania identycznej konfiguracji (np.: Terraform, Microsoft Intune, GPO), które eliminują błędy ludzkie przy ręcznym ustawianiu parametrów. Szablony utwardzania systemów (Hardening Guides): Wykorzystanie uznanych standardów rynkowych (np.: wytyczne CIS Benchmarks, NIST) jako podstawy do tworzenia bezpiecznej konfiguracji. Wersjonowanie konfiguracji (Git): Przechowywanie plików konfiguracyjnych systemów i sieci w bezpiecznych repozytoriach kodu, co pozwala na śledzenie historii zmian oraz szybkie przywrócenie stabilnej wersji w razie awarii. 	<ul style="list-style-type: none"> Wskaźnik zgodności konfiguracyjnej (KPI): Miara określająca procent urządzeń i aplikacji w sieci, których rzeczywiste parametry pracy są w 100% zgodne z oficjalnie zatwierdzonym szablonem bezpieczeństwa (domena laaS). Automatyczne wykrywanie zmian (Configuration Drift Detection): Stałe monitorowanie systemów przez narzędzia audytowe, które natychmiast generują alert bezpieczeństwa (lub automatycznie cofają zmianę), gdy użytkownik lub administrator samowolnie zmodyfikuje chroniony parametr. Wyrównanie audyty weryfikacyjne: Regularne (np.: raz na kwartał) manualne lub automatyczne przeglądy konfiguracji losowo wybranych systemów krytycznych pod kątem obecności nieautoryzowanych kont lub otwartych portów. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 8.9 Zarządzanie konfiguracją oraz dodatkowo konfigurowane zgodnie z: Zasady konfiguracji aplikacji i usług M365 w Hadrone Sp. z o.o. Stosowane narzędzia to: M365 oraz polisy konfiguracyjne dla każdego komputera dodanego do domeny.	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z	N/A	tak
-----	------------	--------------------------	----------------------	----------	---	---	---	---	------	--	--	-----	-----



CL.P.8.10	Techniczne	Usuwanie informacji	ISO 27017, ISO 27018, ISO 27701	Privacy	CC_P4 - Use, Retention and Disposal / Użycie, Retencja i wycofanie	<ul style="list-style-type: none"> • Zapisy dotyczące retencji danych: Oficjalny harmonogram określający dokładne okresy przechowywania dla poszczególnych kategorii danych (np. rekrutacje – 1 rok, dane fakturowe – 5 lat) wraz ze wskazaniem ról odpowiedzialnych za ich kasowanie. • Automatyczne skrypty i polityki usuwania (Data Lifecycle): Narzędzia systemowe (np.: reguły retencji w Microsoft Purview, polityki cyklu życia w Azure), które automatycznie i bez udziału człowieka trwale kasują pliki po upływie ich ważności. • Oprogramowanie do bezpiecznego nadpisywania (Wiping Tools): Wykorzystanie certyfikowanych algorytmów (np. standard NIST SP 800-88, DoD 5220.22-M), które wielokrotnie nadpisują przestrzeń dyskową losowymi cyframi, uniemożliwiając odzyskanie plików narzędziami śledczymi. • Fizyczne pojemniki bezpieczne i niszczarki DIN 3 do 5: Rozmieszczenie w biurze zamkniętych kontenerów na dokumenty przeznaczone do utylizacji przez wyspecjalizowaną firmę zewnętrzną lub stosowanie niszczarek tnących papier na mikrościnki. 	<ul style="list-style-type: none"> • Wskaźnik terminowości czyszczenia danych (KPI): Miara weryfikująca procent zasobów informacyjnych (baz danych, folderów), które zostały skutecznie wyczyszczone zgodnie z harmonogramem retencji. • Certyfikaty zniszczenia i Karty Przekazania Odpadu: Obowiązkowa weryfikacja dokumentacji dostarczonej przez firmy zewnętrzne realizujące niszczenie nośników lub dokumentów (potwierdzenie, że proces odbył się zgodnie z normami bezpieczeństwa). • Audyt logów systemowych kasowania danych: Regularny przegląd automatycznych raportów generowanych przez systemy IT w celu potwierdzenia, że zaplanowane zadania (cron jobs, polityki chmurowe) odpowiedzialne za usuwanie danych wykonały się bez błędów. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zarządzania w Hadrone - punkt: CL.P.8.10 Usuwanie informacji oraz dodatkowo w dokumencie: Polityka Bezpieczeństwa Danych Osobowych w Hadrone Sp. z o.o. - punkt: 6.8. Retencja danych osobowych	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z oraz dodatkowo regulowany przez RODO i w ramach ZSZ	Art. 10 AI Act	tak
-----------	------------	---------------------	---------------------------------	---------	--	---	--	---	------	---	--	----------------	-----



8.11	Techniczne	Maskowanie danych	ISO 27001, ISO 27018, ISO 27701	Security	CC_S9 - Risk Mitigation / Osłabianie ryzyka	<ul style="list-style-type: none"> Dynamiczne maskowanie danych (DDM): Narzędzia bazodanowe (np.: wbudowane funkcje MS SQL, lub narzędzia firm trzecich), które modyfikują dane "w locie" w momencie wykonywania zapytania przez użytkownika, w zależności od jego uprawnień. Statyczne maskowanie danych (SDM): Procesy ETL (Extract, Transform, Load), które pobierają dane produkcyjne, trwale je zamazują/mieszają i dopiero w takiej bezpiecznej formie zapisują w bazie środowiska testowego. Techniki transformacji (Pseudonimizacja i Anonimizacja): Zastąpienie danych losowym identyfikatorem (tokenem). <ul style="list-style-type: none"> Zacieranie (Blurring/Substitution): Podmiana realnych nazwisk na fikcyjne z przygotowanego słownika. Redakcja (Redaction): Zastąpienie znaków symbolem "X" (np.: 4444-XXXX-XXXX-1111). 	<ul style="list-style-type: none"> Wskaźnik pokrycia danych wrażliwych (KPI): Miara określająca procent zidentyfikowanych pól z danymi poufnymi/osobowymi w środowiskach nieprodukcyjnych, które zostały skutecznie poddane procesowi statycznego maskowania. Automatyczne skanowanie podatności baz testowych: Regularne używanie narzędzi do wykrywania danych (Data Discovery), które sprawdzają środowiska deweloperskie w poszukiwaniu tzw. "wycieków produkcyjnych" (np.: obecności realnych adresów e-mail). Audyty uprawnień i logów dostępu do danych jawnych: Kwartalny przegląd listy osób posiadających specjalne uprawnienia do oglądania danych w wersji nieodmaskowanej (unmasked) oraz analiza logów pod kątem nadużyć tych uprawnień. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	<p>Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 8.11 Maskowanie danych.</p> <p>Maskowanie danych występuje głównie w systemach SaaS Hadrone i nie są widoczne dla pracowników Hadrone. Jest to zabezpieczenie programowe oraz ograniczone prawa dostępu do danych i widoków dla pracowników Hadrone. Dodatkowe zastosowania mają zapisu dokumentu: Strategia Zarządzania Bezpieczeństwem i Ochroną Danych Osobowych w ramach ZSZ dla Hadrone (Integracja z PIMS i PII w Cloud) - punkt: 5.2 Pseudonimizacja i minimalizacja danych osobowych w systemach SaaS Hadrone oraz: 5.3 Bezpieczeństwo środowisk nieprodukcyjnych w obszarze przetwarzania danych osobowych w systemach SaaS Hadrone.</p>	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z oraz dodatkowo regulowany przez RODO i w ramach ZSZ	N/A	tak
------	------------	-------------------	---------------------------------	----------	---	--	---	---	------	--	--	-----	-----



CL.P.8.12	Techniczne	Zapobieganie wyciekowi danych	ISO 27701, ISO 27018	Privacy	CC_P9 - Monitoring and Enforcement / Monitorowanie i egzekwowanie	<ul style="list-style-type: none"> Systemy klasy DLP (Data Loss Prevention): Narzędzia informatyczne wdrożone na stacjach roboczych (Endpoint DLP) oraz sieci (Network DLP), które rozpoznają wrażliwe wzorce danych (np.: oznaczenia „Poufne”) i automatycznie blokują ich kopiowanie na USB, wysyłkę prywatną pocztą czy wgrywanie do chmury. Zarządzanie prawami do informacji (IRM / E-DRM): Technologie (np.: Microsoft Purview Information Protection), które trwale szyfrują plik i przypisują do niego prawa dostępu, gdzie nawet po pobraniu pliku na prywatny komputer, osoba nieuprawniona nie zdoła go otworzyć, wydrukować ani zrobić zrzutu ekranu. Filtrowanie ruchu i blokowanie stron (Web URL Filtering): Narzędzia sieciowe uniemożliwiające pracownikom wchodzenie na portale hostujące pliki (np. WeTransfer, Dropbox) oraz niezaufane serwisy, gdzie mogłoby dojść do niekontrolowanego transferu. – z wyjątkiem zatwierdzonych wyjątków. Proces bezpiecznej współpracy z partnerami (NDA): Procedura wymuszająca podpisywanie restrykcyjnych umów o poufności (NDA) oraz audytowanie systemów bezpieczeństwa dostawców zewnętrznych przed 	<ul style="list-style-type: none"> Wskaźnik incydentów i prób wycieku (KPI): Miara określająca liczbę oraz powtarzalność zablokowanych przez system DLP prób nieautoryzowanego transferu danych w danym okresie. Audyt fałszywych alarmów (False Positive Rate): Regularna kontrola reguł systemu DLP mająca na celu dopasowanie filtrów tak, aby blokowały realne zagrożenia, nie paraliżując przy tym codziennej, legalnej pracy operacyjnej biznesu. Weryfikacja logów dostępu warunkowego: Stały monitoring alertów o próbach pobierania masowych ilości danych z nietypowych lokalizacji lub w godzinach nocnych. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: CL.P.8.12 Zapobieganie wyciekowi danych. Stosowane narzędzia to klasyfikacja informacji i oznaczanie informacji przez Microsoft Purview Information Protection client (MPIP), monitorowanie służbowych skrzynek email Hadrone, mechanizm RMS w ramach Microsoft Purview Information Protection client (MPIP). Dla obszaru robot zastosowanie mają: Polityka Bezpieczeństwa Danych Osobowych w Hadrone Sp. z o.o - punkt: 6.1. Upoważnienia do przetwarzania danych osobowych	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z oraz dodatkowo regulowany przez RODO i w ramach ZSZ	N/A	tak
-----------	------------	-------------------------------	----------------------	---------	---	--	---	---	------	--	--	-----	-----



						przekazaniem im jakichkolwiek danych – vendor risk managment.							
--	--	--	--	--	--	--	--	--	--	--	--	--	--



8.13	Techniczne	Tworzenie kopii zapasowych	ISO 27001, ISO 27017, ISO 22301	Security	CC_S7 - System Operations / Operacje systemowe	<ul style="list-style-type: none"> Oprogramowanie do automatyzacji backupu: Wykorzystanie profesjonalnych systemów do automatycznego, bezobsługowego wykonywania kopii według harmonogramu (backupy pełne, przyrostowe). Szyfrowanie kopii w spoczynku i w locie: Techniczne wymuszenie szyfrowania (np.: algorytm AES-256) wszelkich danych backupowych podczas ich przesyłania przez sieć oraz w trakcie przechowywania na docelowym nośniku. Fizyczna i chmurowa ochrona lokalizacji off-site: Wykorzystanie bezpiecznych repozytoriów chmurowych (Object Storage z blokadą zapisu) dla kopii zapasowej. Sformalizowana procedura odtwarzania (Runbook): Aktualizowana krok po kroku instrukcja techniczna opisująca sekwencję i sposób przywracania systemów z kopii zapasowych, dostępna dla administratorów nawet w przypadku całkowitej awarii sieci podstawowej. 	<ul style="list-style-type: none"> Cykliczne testy odtwarzania (DR Restor test): Obowiązkowe, regularne (np. raz roku) próbne przywracanie danych do odizolowanego środowiska testowego w celu weryfikacji czy kopie nie są uszkodzone i czy proces przebiega pomyślnie. Wskaźnik sukcesu zadań backupu (KPI): Codzienna kontrola procentu poprawnie wykonanych zadań backupowych w stosunku do wszystkich zaplanowanych w systemie. Weryfikacja metryk RTO i RPO w praktyce: Mierzenie i rejestrowanie rzeczywistego czasu odtwarzania podczas testów i porównywanie go z założonymi celami biznesowymi RTO i RPO. Audyt uprawnień do infrastruktury backupu: Coroczny przegląd kont i uprawnień dostępowych do serwera kopii zapasowych. Dostęp ten musi być skrajnie ograniczony, oddzielony od kont administratorów domeny produkcyjnej i chroniony przez mechanizm uwierzytelniania MFA. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 8.13 Tworzenie kopii zapasowych, dodatkowo kopia danych dla systemów SaaS Hadrone realizowana jest w ramach IaC i zaimplementowanych skryptów w reżimie 3 kopii, ostatni dzienny backup, ostatni tygodniowy backup, ostatni dzienny backup zapasowy. Kopie są szyfrowane kluczem PKM Azure.	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z oraz dodatkowo przez DRP w ramach obszaru PIMS	Art. 21(2)c (NIS2) / Art. 12 (DORA)	tak
------	------------	----------------------------	---------------------------------	----------	--	--	---	---	------	---	---	-------------------------------------	-----



8.14	Techniczne	Nadmiarowość zasobów przetwarzania	ISO 27001, ISO 27017, ISO 22301	Security	CC_S1 - Control Environment/ Kontrole Środowiskowe	<ul style="list-style-type: none"> • Klastry wysokiej dostępności (HA - High Availability) i Load Balancing: Wykorzystanie systemów Load Balancers, które rozdzielają zapytania użytkowników na wiele serwerów jednocześnie i automatycznie odcinają maszyny, które uległy awarii. • Geograficzne systemy Disaster Recovery (DR Site): Utrzymywanie zapasowego centrum danych (w chmurze) z uruchomioną ciągłą, asynchroniczną replikacją danych z lokalizacji głównej. • Nadmiarowość infrastruktury fizycznej i sprzętowej: <ul style="list-style-type: none"> - Zasilanie: Podwójne linie zasilające, systemy zasilania awaryjnego (UPS) oraz generatory prądotwórcze z zapasem paliwa. – dotyczy Data Center w IaaS - Sieć: Łąca internetowe od niezależnych dostawców (podpięte osobnymi trasami kablowymi). – dotyczy Data Center w IaaS / Hadrone - Pamięć masowa: Macierze dyskowe pracujące w konfiguracjach RAID chroniących przed awarią fizycznych dysków. – dotyczy Data Center w IaaS • Architektura Microservices i Autoscaling: Projektowanie aplikacji w postaci niezależnych kontenerów, które potrafią automatycznie replikować się i skalować w przypadku 	<ul style="list-style-type: none"> • Testy przełączenia awaryjnego (Failover Tests): Cykliczne kontrolowane wyłączanie głównych systemów lub odcinanie zasilania w celu zmierzenia realnego czasu przełączenia na infrastrukturę nadmiarową. • Wskaźnik dostępności systemów (Uptime / SLA): Kluczowa miara (KPI) wyliczana procentowo w skali roku weryfikująca skuteczność działania mechanizmów HA. • Ciągły monitoring kondycji zasobów (Health Checks): Automatyczne systemy nadzoru, które co kilka sekund wysyłają zapytania kontrolne (ping/HTTP request) do wszystkich nadmiarowych elementów i natychmiastowo alarmują o awarii pojedynczej linii. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 8.14 Nadmiarowość zasobów przetwarzania. Dodatkowe zastosowania mają następujące regulacje: Strategia Zarządzania Bezpieczeństwem Informacji i chmury obliczeniowej w ramach ZSZ dla Hadrone (integracja obszaru ISMS i Cloud) oraz: Strategia Zarządzania Bezpieczeństwem i Ochroną Danych Osobowych w ramach ZSZ dla Hadrone (Integracja z PIMS i PII w Cloud) - punkt: 3.1 Granice systemu PIMS w Hadrone.	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z oraz dodatkowo przez DRP w ramach obszaru PIMS	N/A	tak
------	------------	------------------------------------	---------------------------------	----------	--	---	---	---	------	---	---	-----	-----



						awarii pojedynczych węzłów serwerowych.							
--	--	--	--	--	--	---	--	--	--	--	--	--	--



8.15	Techniczne	Logowanie	ISO 27001, ISO 27017, ISO 27018, ISO 27701	Security	CC_S4 - Monitoring Activities / Czynności monitorowani a	<ul style="list-style-type: none"> Systemy Log Management: Centralne platformy (np.: Microsoft Sentinel) służące do bezpiecznego, automatycznego agregowania logów z całej sieci w jednym, odizolowanym miejscu w czasie rzeczywistym. Synchronizacja czasem NTP: Wdrożenie i egzekwowanie konfiguracji serwerów Network Time Protocol (NTP) na każdym serwerze, komputerze i urządzeniu sieciowym w strukturze IaaS i w siedzibie Hadrone. Reguły korelacji i automatyczne alertowanie: Algorytmy i reguły analityczne, które automatycznie wykrywają podejrzane wzorce (np.: 5 nieudanych logowań na jedno konto z rzędu w ciągu 10 sekund) i natychmiast wywołują zdarzenie / alert. Procedura retencji i archiwizacji logów: Działanie określające czas przechowywania logów (np.: minimum 12 miesięcy) oraz mechanizmy ich bezpiecznego kompresowania i przenoszenia do pamięci długoterminowej (WORM). 	<ul style="list-style-type: none"> Wskaźnik pokrycia centralnym logowaniem (KPI): Miara techniczna sprawdzająca procent systemów i aplikacji produkcyjnych, które skutecznie i bezprzerwowo wysyłają swoje logi do centralnego systemu np.: Azure Log Hub. Przegląd uprawnień do repozytorium logów: Kwartalna kontrola dostępu do logów. Prawa do odczytu logów muszą być ograniczone do minimum, a prawa do konfiguracji – odseparowane od tradycyjnej administracji systemami. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 8.15 Logowanie. Dodatkowe zastosowania mają następujące regulacje: Strategia Zarządzania Bezpieczeństwem i Ochroną Danych Osobowych w ramach ZSZ dla Hadrone (Integracja z PIMS i PII w Cloud) - punkt: 5.3 Bezpieczeństwo środowisk nieprodukcyjnych w obszarze przetwarzania danych osobowych w systemach SaaS Hadrone. Zastosowane narzędzia to: logowanie wyłącznie przez Entra ID dla pracowników Hadrone z MFA. Dla usług SaaS Hadrone, logowanie wyłącznie przez dostępne i monitorowane API w ramach protokołu OpenID.	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z oraz dodatkowo regulowany przez RODO i w ramach ZSZ	Art. 21(2)e (NIS2) / Art. 10 (DORA) / Art. 15 AI Act	tak
------	------------	-----------	---	----------	---	--	---	--	------	---	--	--	-----



8.16	Techniczne	Monitorowanie aktywności	ISO 27001, ISO 27017	Security	CC_S4 - Monitoring Activities / Czynności monitorowania	<ul style="list-style-type: none"> Narzędzia klasy Activity Logs: Wykorzystanie natywnych mechanizmów dostawców chmurowych (np.: Azure Activity Log) stosowane w celu agregacji i analizy zdarzeń administracyjnych w chmurze. Systemy IDPS i monitorowania sieci (NPM / NDR): Wdrożenie systemów wykrywania i zapobiegania intruzom (Intrusion Detection/Prevention Systems) oraz narzędzi analizujących ruch sieciowy (Network Detection and Response) pod kątem złośliwego oprogramowania lub prób eksfiltracji danych. Scentralizowane pulpity nawigacyjne (Dashboards): Ekran operatorskie (np.: Azure Monitor) prezentujące w czasie rzeczywistym kluczowe parametry zdrowia i bezpieczeństwa systemów w modelu hybrydowym. Reagowanie na incydenty: Sformalizowane ścieżki postępowania, które automatycznie uruchamiają się (lub są wdrażane przez zespół SOC) w momencie wykrycia określonego typu anomalii, np.: logowania z dwóch skrajnych lokalizacji jednocześnie. 	<ul style="list-style-type: none"> Wskaźnik czasu wykrycia i reakcji (MTTD / MTTR): Kluczowe miary (KPI) określające średni czas od momentu wystąpienia anomalii do jej wykrycia przez systemy monitorujące oraz średni czas potrzebny na zablokowanie zagrożenia. Przegląd reguł korelacji i redukcji fałszywych alarmów: Kwartalne działanie dostrajania filtrów i progów alarmowych, mający na celu utrzymanie wskaźnika fałszywych alarmów (False Positive Rate) na poziomie, który nie zakłóca pracy. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 8.16 Monitorowanie aktywności oraz dodatkowo konfigurowane zgodnie z: Zasady konfiguracji aplikacji i usług M365 w Hadrone Sp. z o.o. Stosowane narzędzia to: M365 oraz polisy konfiguracyjne dla każdego komputera dodanego do domeny. Monitorowanie aktywności pracowników Hadrone w systemach będzie docelowo relizowane przez Hadrone SOC na zasadzie usługi zewnętrznej. - usługa w przygotowaniu do wdrożenia. Dla usług SaaS Hadrone logowanie aktywności użytkowników na IaaS jest pełne, w aplikacji Hadrone jest pełne - logi mogą być dostarczone przez Azure Hub do dowolnego narzędzia SIEM klienta.	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z oraz dodatkowo regulowany przez RODO i w ramach ZSZ	N/A	tak
------	------------	--------------------------	----------------------	----------	---	--	--	---	------	---	--	-----	-----



CL.8.16	Techniczne	Monitorowanie aktywności w chmurze	ISO 27017	Security	CC_S4 - Monitoring Activities / Czynności monitorowania	<ul style="list-style-type: none"> Narzędzia klasy Activity Logs: Wykorzystanie natywnych mechanizmów dostawców chmurowych (np.: Azure Activity Log) stosowane w celu agregacji i analizy zdarzeń administracyjnych w chmurze. Systemy IDPS i monitorowania sieci (NPM / NDR): Wdrożenie systemów wykrywania i zapobiegania intruzom (Intrusion Detection/Prevention Systems) oraz narzędzi analizujących ruch sieciowy (Network Detection and Response) pod kątem złośliwego oprogramowania lub prób eksfiltracji danych. Scentralizowane pulpity nawigacyjne (Dashboards): Ekran operatora (np.: Azure Monitor) prezentujące w czasie rzeczywistym kluczowe parametry zdrowia i bezpieczeństwa systemów w modelu hybrydowym. Reagowanie na incydenty: Sformalizowane ścieżki postępowania, które automatycznie uruchamiają się (lub są wdrażane przez zespół SOC) w momencie wykrycia określonego typu anomalii, np.: logowania z dwóch skrajnych lokalizacji jednocześnie. 	<ul style="list-style-type: none"> Wskaźnik czasu wykrycia i reakcji (MTTD / MTTR): Kluczowe miary (KPI) określające średni czas od momentu wystąpienia anomalii do jej wykrycia przez systemy monitorujące oraz średni czas potrzebny na zablokowanie zagrożenia. Przegląd reguł korelacji i redukcji fałszywych alarmów: Kwartalne działanie dostrajania filtrów i progów alarmowych, mający na celu utrzymanie wskaźnika fałszywych alarmów (False Positive Rate) na poziomie, który nie zakłóca pracy. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: CL.8.16 Monitorowanie aktywności w chmurze oraz dodatkowo konfigurowane zgodnie z: Zasady konfiguracji aplikacji i usług M365 w Hadrone Sp. z o.o. Stosowane narzędzia to: M365 oraz polisy konfiguracyjne dla każdego komputera dodanego do domeny. Monitorowanie aktywności pracowników Hadrone w systemach będzie docelowo relizowane przez Hadrone SOC na zasadzie usługi zewnętrznej. - usługa w przygotowaniu do wdrożenia. Dla usług SaaS Hadrone logowanie aktywności użytkowników na IaaS jest pełne, w aplikacji Hadrone jest pełne - logi mogą być dostarczone przez zAzure Hub do dowolnego narzędzia SIEM klienta.	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z oraz dodatkowo regulowany przez RODO i w ramach ZSZ	N/A	tak
---------	------------	------------------------------------	-----------	----------	---	---	--	---	------	---	--	-----	-----



8.17	Techniczne	Synchronizacja czasu	ISO 27017	Security	CC_57 - System Operations / Operacje systemowe	<ul style="list-style-type: none"> • Protokół NTP / PTP: Wykorzystanie protokołu Network Time Protocol (NTP) dla standardowej infrastruktury lub Precise Time Protocol (PTP) w środowiskach wymagających mikrosekundowej dokładności (np.: systemy finansowe, automatyka przemysłowa). • Polityki centralne (GPO / MDM): Automatyczne wymuszenie konfiguracji klientów NTP na stacjach roboczych i serwerach za pomocą polityk grupowych (GPO) lub systemów zarządzania urządzeniami (MDM/Intune). • Uwierzytelnianie pakietów NTP: Włączenie kryptograficznego uwierzytelniania komunikatów NTP pomiędzy serwerem a klientami, co uniemożliwia napastnikom podrzucenie fałszywego czasu do sieci firmowej. 	<ul style="list-style-type: none"> • Wskaźnik maksymalnego przesunięcia (Clock Skew KPI): Miara weryfikująca maksymalne dopuszczalne odchylenie czasu na dowolnym urządzeniu w sieci względem wzorca (np.: alert bezpieczeństwa uruchamia się, gdy przesunięcie przekroczy sekunda dla serwerów IaaS). • Automatyczne monitorowanie statusu daemona NTP: Stała weryfikacja przez systemy monitorujące (np. Azure Monitor), czy usługa synchronizacji czasu na serwerach produkcyjnych i urządzeniach sieciowych jest uruchomiona i poprawnie skomunikowana z serwerem nadrzędnym. • Audyt spójności czasu podczas analizy logów: Regularne testy operacyjne polegające na losowym porównaniu znaczników czasu (timestamps) tego samego zdarzenia zarejestrowanego przez różne systemy (np. logowanie na firewallu vs logowanie w bazie danych) w celu potwierdzenia idealnej korelacji. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 8.17 Synchronizacja czasu oraz dodatkowo konfigurowane zgodnie z: Zasady konfiguracji aplikacji i usług M365 w Hadrone Sp. z o.o. Stosowane narzędzia to: M365 oraz polisy konfiguracyjne dla każdego komputera dodanego do domeny. Dla systemów SaaS Hadrone wykorzystanie natywnych mechanizmów Azure: Windows Azure używa wbudowanej usługi Windows Time Service (W32Time)	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z	N/A	tak
------	------------	----------------------	-----------	----------	--	--	--	---	------	---	--	-----	-----



8.18	Techniczne	Używanie uprzywilejowanych programów narzędziowych	ISO 27001	Security	CC_S7 - System Operations / Operacje systemowe	<ul style="list-style-type: none"> • Rozwiązania klasy PAM (Privileged Access Management): Systemy kontrolujące i nagrywające sesje, podczas których administratorzy korzystają z uprzywilejowanych narzędzi, automatycznie rotujące hasła po zakończeniu pracy. • Szablony utwardzania (VM Hardening Blueprints): Konfiguracja maszyn wirtualnych według rygorystycznych wytycznych (np.: CIS Benchmarks level 1) – wyłączenie funkcji kopiuj-wklej między hostem a VM, odpięcie wirtualnych napędów CD/dyskietek, wyłączenie nieużywanych portów. • Białe listy aplikacji (Application Whitelisting): Mechanizmy techniczne, które blokują możliwość uruchomienia jakichkolwiek programów narzędziowych (np. edytorów dysków, snifferów sieciowych), jeśli nie zostały one jawnie dopuszczone przez politykę bezpieczeństwa organizacji. • Szyfrowanie maszyn wirtualnych i vTPM: Wdrożenie wirtualnych modułów zaufanej platformy (vTPM) oraz pełnego szyfrowania dysków maszyn wirtualnych (np.: BitLocker), co chroni dane przed kradzieżą w przypadku skopiowania plików samej maszyny wirtualnej (.vmdk/.vhdx) z hiperwizora. 	<ul style="list-style-type: none"> • Wskaźnik zgodności z szablonem utwardzania (KPI): Miara weryfikująca procent maszyn wirtualnych w organizacji, które pomyślnie przechodzą automatyczny test zgodności z oficjalnym standardem bezpieczeństwa. • Audyt uruchomień narzędzi uprzywilejowanych: Regularny, automatyczny przegląd logów systemowych pod kątem wykrycia przypadków użycia programów administratorских bez powiązanego i zatwierdzonego zgłoszenia. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 8.18 Używanie uprzywilejowanych programów narzędziowych, dodatkowo lista tych aplikacji jest brana pod analizę ryzyka i jest na bieżąco inwentaryzowana w ramach excela: Risk Identification and analyse for ZSZ_Hadrone	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z	N/A	tak
------	------------	--	-----------	----------	--	--	--	---	------	--	--	-----	-----



8.19	Techniczne	Instalacja oprogramowania	ISO 27001	Security	CC_S7 - System Operations / Operacje systemowe	<ul style="list-style-type: none"> Systemy scentralizowanej dystrybucji: Wykorzystanie systemów zarządzania urządzeniami (np.: Microsoft Intune), które pozwalają na zdalną, automatyczną i bezpieczną instalację zatwierdzonych aplikacji bez udziału użytkownika. Technologie Whitelisting / AppLocker: Wdrożenie mechanizmów kontroli aplikacji (np. Windows Defender Application Control, AppLocker), które blokują uruchomienie jakichkolwiek plików instalacyjnych (.exe, .msi), jeśli nie zostały one podpisane cyfrowo przez zaufanego wydawcę. Request for Software (RFS): Formalne ogłoszenie zapotrzebowania na nowe oprogramowanie poprzez kontakt z Hadrone CISO / Członkiem Zarządu Hadrone wymagający weryfikacji wpływu aplikacji na bezpieczeństwo oraz zatwierdzenia zakupu licencji. 	<ul style="list-style-type: none"> Wskaźnik wykrywania nieautoryzowanego software (KPI): Miara bazująca na raportach systemów antywirusowych lub inwentaryzacyjnych, określająca liczbę zainstalowanych aplikacji spoza oficjalnej listy dozwolonej. Cykliczne skanowanie inwentaryzacyjne (Software Inventory Audits): Automatyczny, okresowe przeglądy rejestrów wszystkich stacji roboczych i serwerów w celu wykrycia aplikacji zainstalowanych w sposób niestandardowy (np.: wersje portable uruchamiane z katalogów użytkownika). Weryfikacja podpisów cyfrowych i sum kontrolnych: Automatyczna kontrola w pipeline wdrożeniowych (CI/CD) sprawdzająca czy instalowane na serwerach pakiety oprogramowania są oryginalne, nienaruszone i pochodzą z legalnego, oficjalnego źródła. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 8.19 Instalacja oprogramowania oraz dodatkowo konfigurowane zgodnie z: Zasady konfiguracji aplikacji i usług M365 w Hadrone Sp. z o.o. Stosowane narzędzia to: M365 oraz polisy konfiguracyjne dla każdego komputera dodanego do domeny. - tylko osoby z odpowiednimi uprawnieniami mogą zainstalować oprogramowanie lub programy narzędziowe.	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z	N/A	tak
------	------------	---------------------------	-----------	----------	--	--	--	---	------	--	--	-----	-----



CL.8.18	Techniczne	Utwardzanie maszyn wirtualnych	ISO 27017	Security	CC_S9 - Risk Mitigation / Osłabianie ryzyka	<ul style="list-style-type: none"> • Rozwiązania klasy PAM (Privileged Access Management): Systemy kontrolujące i nagrywające sesje, podczas których administratorzy korzystają z uprzywilejowanych narzędzi, automatycznie rotujące hasła po zakończeniu pracy. • Szablony utwardzania (VM Hardening Blueprints): Konfiguracja maszyn wirtualnych według rygorystycznych wytycznych (np.: CIS Benchmarks level 1) – wyłączenie funkcji kopiuj-wklej między hostem a VM, odpięcie wirtualnych napędów CD/dyskietek, wyłączenie nieużywanych portów. • Białe listy aplikacji (Application Whitelisting): Mechanizmy techniczne, które blokują możliwość uruchomienia jakichkolwiek programów narzędziowych (np. edytorów dysków, snifferów sieciowych), jeśli nie zostały one jawnie dopuszczone przez politykę bezpieczeństwa organizacji. • Szyfrowanie maszyn wirtualnych i vTPM: Wdrożenie wirtualnych modułów zaufanej platformy (vTPM) oraz pełnego szyfrowania dysków maszyn wirtualnych (np.: BitLocker), co chroni dane przed kradzieżą w przypadku skopiowania plików samej maszyny wirtualnej (.vmdk/.vhdx) z hiperwizora. 	<ul style="list-style-type: none"> • Wskaźnik zgodności z szablonem utwardzania (KPI): Miara weryfikująca procent maszyn wirtualnych w organizacji, które pomyślnie przechodzą automatyczny test zgodności z oficjalnym standardem bezpieczeństwa. • Audyt uruchomień narzędzi uprzywilejowanych: Regularny, automatyczny przegląd logów systemowych pod kątem wykrycia przypadków użycia programów administratorów bez powiązanego i zatwierdzonego zgłoszenia. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: CL.8.19 Utwardzanie maszyn wirtualnych oraz dodatkowo konfigurowane zgodnie z: Zasady konfiguracji aplikacji i usług M365 w Hadrone Sp. z o.o. Stosowane narzędzia to: M365 oraz polisy konfiguracyjne dla każdego komputera dodanego do domeny. Dla systemów SaaS Hadrone, przy uruchamianiu IaaS wybiera się obraz maszyny wirtualnej, dostępne są obrazy w standardzie CIS Benchmarks Level 1 lub wyższym.	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z	N/A	tak
---------	------------	--------------------------------	-----------	----------	---	--	--	---	------	---	--	-----	-----



8.20	Techniczne	Bezpieczeństwo sieci	ISO 27001, ISO 27017	Security	CC_S5 - Control Activities / Czynności kontrolne	<ul style="list-style-type: none"> • Zapory sieciowe nowej generacji (NGFW) i ACL: Filtrowanie ruchu na granicach stref sieciowych przy użyciu zaawansowanych firewalli, które analizują nie tylko porty, ale i aplikacje (Deep Packet Inspection), blokując nieautoryzowane połączenia. • Systemy Kontroli Dostępu do Sieci (NAC): Narzędzia, które identyfikują urządzenia próbujące podłączyć się do sieci i automatycznie przypisują je do właściwego segmentu (VLAN) na podstawie certyfikatu standardu lub stanu bezpieczeństwa. • Szyfrowany dostęp zdalny (VPN): Wykorzystanie bezpiecznych tuneli VPN, które wpuszczają zdalnych użytkowników wyłącznie do konkretnych aplikacji, a nie do całej sieci. • Wirtualne sieci lokalne (VLAN) i mikrosegmentacja: Logiczny podział fizycznej infrastruktury sieciowej na mniejsze, niezależne podsieci, co uniemożliwia rozprzestrzenianie się ataków w przypadku zainfekowania jednej stacji. 	<ul style="list-style-type: none"> • Wskaźnik wykrywania nieautoryzowanych urządzeń (KPI): Miara określająca liczbę oraz czas reakcji systemu NAC/CAC na próby podłączenia do sieci urządzeń obcych lub niespełniających wymogów polityki bezpieczeństwa. • Cykliczne skanowanie portów i podatności sieciowych: Regularne automatyczne testy sprawdzające, czy w sieci nie pojawiły się nowe, nieautoryzowane usługi lub otwarte porty wystawione na świat zewnętrzny. • Audyt i przegląd reguł firewalli: Weryfikacja bazy reguł na zaporach sieciowych (Firewall Rule Base Review) w celu wykrycia i usunięcia reguł przestarzałych, zbyt ogólnych lub konfliktowych. • Analiza anomalii w ruchu sieciowym: Stały monitoring wolumenu i kierunków transferu danych pod kątem wykrywania nietypowych zachowań, takich jak masowy transfer danych w nocy na zewnętrzne serwery. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 8.20 Bezpieczeństwo sieci oraz dodatkowo konfigurowane zgodnie z: Zasady konfiguracji aplikacji i usług M365 w Hadrone Sp. z o.o. Stosowane narzędzia to: M365 oraz polisy konfiguracyjne dla każdego komputera dodanego do domeny. Dla systemów Saas Hadrone, przy uruchamianiu laC wybiera domyślnie tworzona jest private vNET oraz dodatkowe private end-point, dostęp jest przez odpowiednie RG w ramach uprawnień na Entra ID. Dostęp do Azure wyłącznie przez VPN. Dostęp do sieci Hadrone w HQ wyłącznie po Wi-Fi z uwierzytelnieniem AES WPA3 Enterprise.	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z	Art. 21(2)g (NIS2) / Art. 9 (DORA)	tak
------	------------	----------------------	----------------------	----------	--	--	--	---	------	--	--	------------------------------------	-----



8.21	Techniczne	Bezpieczeństwo usług sieciowych	ISO 27001, ISO 27017	Security	CC_S7 - System Operations / Operacje systemowe	<ul style="list-style-type: none"> • Bramki API (API Gateways) i WAF: Wdrożenie scentralizowanych bramek dla usług sieciowych, które kontrolują ruch (rate limiting), walidują zapytania i chronią przed atakami aplikacyjnymi (np.: SQL Injection, Cross-Site Scripting) przy użyciu Web Application Firewall. • Bezpieczne protokoły transportowe i DNSSEC: Wymuszenie stosowania wyłącznie bezpiecznych wersji usług sieciowych, np. HTTPS zamiast HTTP, SFTP zamiast FTP oraz wdrożenie protokołu DNSSEC w celu ochrony przed sfałszowaniem odpowiedzi serwerów DNS. • Rozwiązania chroniące przed atakami DDoS: Wykorzystanie zaawansowanych usług ochrony sieciowej zdolnych do filtrowania i pochłaniania masowego ruchu wolumetrycznego na brzegu sieci, zanim dotrze on do serwerów organizacji. • Scentralizowany rejestr usług: Prowadzenie dokładnego spisu wszystkich aktywnych usług sieciowych i ich punktów końcowych (endpoints) wraz z wdrożeniem zasad mikroautoryzacji (każda usługa ufa innej tylko po pomyślnej weryfikacji tożsamości). 	<ul style="list-style-type: none"> • Automatyczne testy penetracyjne interfejsów (API Security Testing): Regularne (np. raz w miesiącu), zautomatyzowane skanowanie publicznie wystawionych interfejsów i usług sieciowych pod kątem obecności znanych podatności lub błędów w konfiguracji uprawnień. • Audyt zgodności i certyfikacji dostawców (Vendor Assessment): Cykliczny (np.: raz w roku) przegląd raportów z niezależnych audytów dostawców kluczowych usług sieciowych (np.: weryfikacja certyfikatów ISO 27001, raportów SOC 2 Type II). • Monitorowanie i korelacja logów wywołań (Anomaly Detection): Stała analiza logów generowanych przez bramki API i systemy firewall pod kątem wykrywania nietypowych skoków liczby zapytań lub prób masowego wywoływania błędów autoryzacji (kod HTTP 401/403). 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	<p>Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 8.21 Bezpieczeństwo usług sieciowych oraz dodatkowo konfigurowane zgodnie z: Zasady konfiguracji aplikacji i usług M365 w Hadrone Sp. z o.o. Stosowane narzędzia to: M365 oraz polisy konfiguracyjne dla każdego komputera dodanego do domeny. Dla systemów SaaS Hadrone, przy uruchamianiu IaC tworzony jest zawsze WAF i Proxy dla aplikacji oraz zakładane są domyślne policy ACL na poszczególne VNET i private endpoint w Azure.</p> <p>W sieci Hadrone domyślne protokoły sieciowe to HTTPS 443 oraz SFTP na niestandardowym porcie 2222. Dodatkowo każda stacja robocza posiada włączony usługi Microsoft HIPS oraz HPFW.</p>	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z	N/A	tak
------	------------	---------------------------------	----------------------	----------	--	--	---	---	------	---	--	-----	-----



8.22	Techniczne	Separacja sieci	ISO 27001, ISO 27017	Security	CC_S7 - System Operations / Operacje systemowe	<ul style="list-style-type: none"> • Wirtualne sieci lokalne (VLAN) i VxLAN: Logiczny podział fizycznej infrastruktury sieciowej na poziomie warstwy drugiej (L2) i trzeciej (L3), uniemożliwiający urządzeniom z różnych stref bezpośrednią komunikację bez pośrednictwa firewalla. • Mikrosegmentacja i Zapory Ogniowe (Firewalle) Nowej Generacji: Wdrożenie zapór sieciowych (NGFW) na granicach segmentów oraz oprogramowania do mikrosegmentacji wewnątrz chmury, które kontroluje ruch na poziomie pojedynczych maszyn wirtualnych. • Izolacja zasobów wirtualnych na hiperwizorze: Konfiguracja wirtualnych przełączników (vSwitches) w sposób gwarantujący, że uszkodzenie lub przejście jednej maszyny wirtualnej nie pozwoli na podsłuchanie ruchu innej (ochrona przed VLAN hopping). • Bezpieczne strefy DMZ (Demilitarized Zones): Umieszczanie systemów mających kontakt z Internetem (np.: serwerów IIS) w specjalnej strefie buforowej (DMZ), która jest rygorystycznie odizolowana od wewnętrznej, wrażliwej sieci korporacyjnej. 	<ul style="list-style-type: none"> • Automatyczna weryfikacja architektury sieciowej: Cykliczne, automatyczne skanowanie topologii sieci i konfiguracji vSwitchy w celu wykrycia tzw. „mostków sieciowych” (np.: maszyn wirtualnych podpiętych jednocześnie do dwóch różnych, odizolowanych sieci). • Audyt i testy penetracyjne z wnętrza segmentu: Regularne (np.: raz na pół roku) próby przełamania izolacji (testy typu pivoting i lateral movement), polegające na symulacji przejścia maszyny w strefie testowej i próbie dotarcia z niej do systemów produkcyjnych. • Cykliczny przegląd i czyszczenie reguł routingu i ACL: Coroczne przegląd list kontroli dostępu (Access Control Lists) oraz reguł firewalli w celu natychmiastowego usunięcia tymczasowych zezwoleń, które zostały otwarte np. na czas wdrożenia projektu i nie zostały zamknięte. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 8.22 Separacja sieci. Techniczne zabezpieczenia stosowane przez Hadrone to a) stosowanie czystego i brudnego Internetu od dwóch różnych dostawców. Pełne rozdzielanie środowisk produkcyjnych i developerskich oraz developerskich i testowych. - rozdzielanie na poziomie subskrypcji. Usługi SaaS posiadają pełną separację na fron-end i back-end z private end-pointami, w private vNET. Osobne rebuy Host FW są ustawiane w zakresie komunikacji.	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z	N/A	tak
------	------------	-----------------	-------------------------	----------	--	---	--	--	------	---	--	-----	-----



CL.8.22	Technologia CL	Izolacja środowisk wirtualnych	ISO 27017	Security	CC_S7 - System Operations / Operacje systemowe	<ul style="list-style-type: none"> • Wirtualne sieci lokalne (VLAN) i VxLAN: Logiczny podział fizycznej infrastruktury sieciowej na poziomie warstwy drugiej (L2) i trzeciej (L3), uniemożliwiający urządzeniom z różnych stref bezpośrednią komunikację bez pośrednictwa firewalla. • Mikrosegmentacja i Zapory Ogniowe (Firewall) Nowej Generacji: Wdrożenie zapór sieciowych (NGFW) na granicach segmentów oraz oprogramowania do mikrosegmentacji wewnątrz chmury, które kontroluje ruch na poziomie pojedynczych maszyn wirtualnych. • Izolacja zasobów wirtualnych na hiperwizorze: Konfiguracja wirtualnych przełączników (vSwitches) w sposób gwarantujący, że uszkodzenie lub przejście jednej maszyny wirtualnej nie pozwoli na podsłuchanie ruchu innej (ochrona przed VLAN hopping). • Bezpieczne strefy DMZ (Demilitarized Zones): Umieszczanie systemów mających kontakt z Internetem (np.: serwerów IIS) w specjalnej strefie buforowej (DMZ), która jest rygorystycznie odizolowana od wewnętrznej, wrażliwej sieci korporacyjnej. 	<ul style="list-style-type: none"> • Automatyczna weryfikacja architektury sieciowej: Cykliczne, automatyczne skanowanie topologii sieci i konfiguracji vSwitchy w celu wykrycia tzw. „mostków sieciowych” (np.: maszyn wirtualnych podpiętych jednocześnie do dwóch różnych, odizolowanych sieci). • Audyt i testy penetracyjne z wnętrza segmentu: Regularne (np.: raz na pół roku) próby przełamania izolacji (testy typu pivoting i lateral movement), polegające na symulacji przejścia maszyny w strefie testowej i próbie dotarcia z niej do systemów produkcyjnych. • Cykliczny przegląd i czyszczenie reguł routingu i ACL: Coroczne przegląd list kontroli dostępu (Access Control Lists) oraz reguł firewalli w celu natychmiastowego usunięcia tymczasowych zezwoleń, które zostały otwarte np. na czas wdrożenia projektu i nie zostały zamknięte. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: CL.8.22 Izolacja środowisk wirtualnych. Techniczne zabezpieczenia dla SaaS jakie stosuje Hadrone to: Pełne rozdzielanie środowisk produkcyjnych i developerskich oraz developerskich i testowych. - rozdzielanie na poziomie subskrypcji. Usługi SaaS posiadają pełną separację na front-end i back-end z private end-pointami, w private vNET. Osobne reguły Host FW są ustawiane w zakresie komunikacji.	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z	N/A	tak
---------	----------------	--------------------------------	-----------	----------	--	--	--	---	------	--	--	-----	-----



8.23	Techniczne	Filtrowanie treści stron	ISO 27001	Security	CC_S7 - System Operations / Operacje systemowe	<ul style="list-style-type: none"> • Bramki sieciowe Secure Web Gateway (SWG) i Web proxy: Scentralizowane rozwiązania (chmurowe), które filtrują każde zapytanie HTTP/HTTPS wysyłane z urządzeń firmowych i blokują dostęp na podstawie stale aktualizowanej bazy kategorii. • Filtrowanie oparte na inspekcji SSL/TLS (SLL Decryption): Mechanizm bezpiecznego odszyfrowywania ruchu HTTPS „w locie” przez bramkę sieciową. Bez tego narzędzia nowoczesne systemy filtrujące nie są w stanie zweryfikować pełnego adresu URL ani pobieranej zawartości pod kątem wirusów. • Agenci końcowi (Endpoint Agents): Oprogramowanie zainstalowane bezpośrednio na laptopach i telefonach służbowych (zintegrowane np. z systemami antywirusowymi lub MDM), zapewniające ciągłe filtrowanie treści również wtedy, gdy pracownik przebywa poza biurem i nie korzysta z firmowego VPN. • Filtrowanie i ochrona na poziomie DNS: Blokowanie zapytań o złośliwe domeny już na etapie rozwiązywania nazw (np.: poprzez bezpieczne serwery DNS), co uniemożliwia nawiązanie połączenia z serwerem przestępców zanim przeglądarka w ogóle zacznie łączyć stronę. 	<ul style="list-style-type: none"> • Cykliczne testy skuteczności filtrowania (Evasion Tests): Regularne (np.: raz na kwartał) próby wejścia z losowo wybranych stacji roboczych na nowo powstałe, testowe domeny o złej reputacji w celu weryfikacji, czy system SWG poprawnie odcina do nich dostęp. • Audyt wniosków i udzielonych wyjątków: Coroczny przegląd listy unikalnych reguł (białych list) dopisanych ręcznie przez administratorów na żądanie użytkowników, mający na celu usunięcie uprawnień, które wygasły lub nie są już potrzebne. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: CL.8.23 Filtrowanie treści stron. Techniczne zabezpieczenia to: HIPS oraz HPFW, oraz podatkowe filtrowanie treści www dostarczane przez operatora sieci Internet w ramach umowy i mechanizmu Business Protection Network. - dla Hadrone są to wystarczające zabezpieczenia w warstwie sieci.	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z	N/A	tak
------	------------	--------------------------	-----------	----------	--	---	---	---	------	--	--	-----	-----



CL.P.8.24	Techniczne	Zarządzanie konfiguracją - logowanie	ISO 27018	Security	CC_S5 - Control Activities / Czynności kontrolne	<ul style="list-style-type: none"> Systemy zarządzania kluczami (KMS / PKM): Wykorzystanie dedykowanych systemów zarządzania kluczami (np.: Azure Key Vault) do bezpiecznego generowania i izolowania kluczy szyfrujących. Szyfrowanie danych w spoczynku i w locie (At-Rest & In-Transit): Wdrożenie mechanizmów pełnego szyfrowania dysków (np. BitLocker) oraz baz danych (TDE), a także wymuszenie stosowania protokołów TLS 1.3 dla wszystkich połączeń sieciowych. Scentralizowane logowanie konfiguracji (Audit Trails): Wykorzystanie mechanizmów takich jak chmurowe dzienniki zdarzeń, skonfigurowanych tak, aby natychmiast rejestrowały i chroniły logi dotyczące operacji na kluczach (np.: użycie klucza, eksport, unieważnienie). Zautomatyzowana rotacja kluczy (Key Rotation Lifecycle): Procesy automatycznej, cyklicznej wymiany kluczy kryptograficznych i certyfikatów (np.: za pomocą protokołu ACME / Let's Encrypt) bez konieczności ręcznej interwencji administratora. 	<ul style="list-style-type: none"> Wskaźnik pokrycia szyfrowaniem (KPI): Miara techniczna określająca procent zasobów informacyjnych (baz danych, laptopów, dysków sieciowych), które są skutecznie zaszyfrowane zgodnie z zasadami Hadrone. Automatyczna kontrola ważności certyfikatów i kluczy: Systemy monitorujące, które wysyłają alerty o zbliżającym się terminie wygasania certyfikatów SSL/TLS (np.: na 30, 14 i 7 dni przed wygaśnięciem), zapobiegając przerwom w działaniu usług. Wyrwykowe testy odtwarzania (Decryption Audits): Przegląd procedur awaryjnych (Key Recovery), polegający na kontrolowanej próbie odszyfrowania danych z kopii zapasowej przy użyciu klucza odzyskiwania, sprawdzający czy organizacja nie utraci dostępu do danych w przypadku awarii systemu KMS. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: CL.P.8.24 Bezpieczeństwo usług sieciowych oraz dodatkowo konfigurowane zgodnie z: Zasady konfiguracji aplikacji i usług M365 w Hadrone Sp. z o.o. Stosowane narzędzia to: M365 oraz polisy konfiguracyjne dla każdego komputera dodanego do domeny. Techniczne zabezpieczenia stosowane przez Hadrone dla systemów chmury obliczeniowej to konto w Entra ID oraz MFA, dla Azura dodatkowo MFA + VPN wraz ze spełnieniem wymagań CAL przy logowaniu. Obowiązuje zasada „minimalizacji uprawnień” oraz „zasady wiedzy koniecznej”.	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z	N/A	tak
-----------	------------	--------------------------------------	-----------	----------	--	--	--	---	------	--	--	-----	-----



8.24	Techniczne	Stosowanie kryptografii	ISO 27001, ISO 27017, ISO 27701	Security	CC_S9 - Risk Mitigation / Osłabianie ryzyka	<ul style="list-style-type: none"> Systemy zarządzania kluczami (KMS / PKM): Wykorzystanie dedykowanych systemów zarządzania kluczami (np.: Azure Key Vault) do bezpiecznego generowania i izolowania kluczy szyfrujących. Szyfrowanie danych w spoczynku i w locie (At-Rest & In-Transit): Wdrożenie mechanizmów pełnego szyfrowania dysków (np. BitLocker) oraz baz danych (TDE), a także wymuszenie stosowania protokołów TLS 1.3 dla wszystkich połączeń sieciowych. Scentralizowane logowanie konfiguracji (Audit Trails): Wykorzystanie mechanizmów takich jak chmurowe dzienniki zdarzeń, skonfigurowanych tak, aby natychmiast rejestrowały i chroniły logi dotyczące operacji na kluczach (np.: użycie klucza, eksport, unieważnienie). Automatyzowana rotacja kluczy (Key Rotation Lifecycle): Procesy automatycznej, cyklicznej wymiany kluczy kryptograficznych i certyfikatów (np.: za pomocą protokołu ACME / Let's Encrypt) bez konieczności ręcznej interwencji administratora. 	<ul style="list-style-type: none"> Wskaźnik pokrycia szyfrowaniem (KPI): Miara techniczna określająca procent zasobów informacyjnych (baz danych, laptopów, dysków sieciowych), które są skutecznie zaszyfrowane zgodnie z zasadami Hadrone. Automatyczna kontrola ważności certyfikatów i kluczy: Systemy monitorujące, które wysyłają alerty o zbliżającym się terminie wygaśnięcia certyfikatów SSL/TLS (np.: na 30, 14 i 7 dni przed wygaśnięciem), zapobiegając przerwom w działaniu usług. Wyrównane testy odtwarzania (Decryption Audits): Przegląd procedur awaryjnych (Key Recovery), polegający na kontrolowanej próbie odszyfrowania danych z kopii zapasowej przy użyciu klucza odzyskiwania, sprawdzający czy organizacja nie utraci dostępu do danych w przypadku awarii systemu KMS. 	Wyjątek, Uwaga/Exception, Comment.	<p>Spostrzeżenie – dla mechanizmów kontrolnych realizowanych w ramach zabezpieczeń kryptograficznych dostarczanych jako element usługi IaaS lub serwis SaaS do wykorzystania, zaleca się weryfikację tego zabezpieczenia poprzez pentesty oraz testy konfiguracji IaaS dla usługi SaaS PPM i SPM oraz weryfikację kodu Terraform i skryptów PowerShell uruchamianych w ramach procesu infrastruktury as a Code (IaC) przez Hadrone. Weryfikacja pozwoli na ocenę czy poprawnie skonfigurowana jest usługa, oraz czy zminimalizowano do niezbędnego minimum ingerencję pracowników w Hadrone w tworzenie,</p>	<p>Obszar częściowo regulowany przez Hadrone a częściowo regulowany przez dostawcę chmury obliczeniowej w ramach mechanizmu PKM (Platform Key management) stosowanego przy np.: szyfrowaniu kopii zapasowych - generowaniem i przechowywaniem kluczy do operacji szyfrowania i deszyfrowania zajmuje się w 100% Microsoft, Hadrone tylko wykorzystuje ten mechanizm w ramach IaaS. Wyłączenie ze względu na fakt, że Hadrone nie jest dostawcą chmury obliczeniowej, a jedynie klientem IaaS. decyzja oparta na materiałach źródłowych Microsoft:</p> <p>a) https://learn.microsoft.com/en-us/azure/security/fundamentals/key-management</p> <p>b) https://learn.microsoft.com/en-us/azure/virtual-machines/disk-encryption-overview</p>	<p>Częściowo w zakresie ZSZ Hadrone, wymaga uzasadnienia wykluczenia dla zarządzania kluczami kryptograficznymi w ramach mechanizmu PKM (Platform Key Management), poza tym regulowany przez w ramach ZSZ przez ZZPO_MK_ZS</p>	<p>Art. 21(2)h (NIS2) / Art. 9 (DORA) / Art. 15 AI Act</p>	częściowo
------	------------	-------------------------	---------------------------------	----------	---	---	--	------------------------------------	--	---	--	--	-----------



									uruchamia nia oraz zarządzanie usługą KeyVault w Microsoft Azure w ramach IaaS.				
--	--	--	--	--	--	--	--	--	---	--	--	--	--



8.25	Techniczne	Cykl życia bezpiecznego rozwoju SDLC	ISO 27001, ISO 27701	Security	CC_S8 - Change Managment / Zarządzanie zmianą	<ul style="list-style-type: none"> Modelowanie zagrożeń (Threat Modeling): Proces analityczny (np.: przy użyciu metodologii STRIDE) realizowany na etapie projektowania, mający na celu identyfikację potencjalnych wektorów ataku na architekturę aplikacji. Automatyczne testy bezpieczeństwa w pipeline CI/CD: <ul style="list-style-type: none"> SAST: skanujące surowy kod źródłowy w poszukiwaniu błędów logicznych i luk. SCA: Skanery wykrywające znane podatności w używanych bibliotekach Open Source. Dynamiczne testy i audyty (DAST & Testy Penetracyjne): Automatyczne testowanie uruchomionej aplikacji "od zewnątrz" (np.: OWASP ZAP) uzupełniane manualnymi testami penetracyjnymi przed każdym dużym wydaniem produkcyjnym. Zarządzanie sekretami (Secrets Management): Wykorzystanie bezpiecznych repozytoriów (np.: Microsoft Key Vaults) do wstrzykiwania kluczy API i haseł do aplikacji w czasie jej uruchamiania, zamiast umieszczania ich w kodzie. 	<ul style="list-style-type: none"> Bramki jakościowe (Quality Gates): Techniczne reguły wdrożeniowe w systemie CI/CD, które automatycznie przerywają proces budowania aplikacji (build failure), jeśli skaner SAST/SCA wykryje nową, krytyczną lukę. Audyt zgodności z polityką kodowania: Regularny przegląd procedur Code Review (weryfikacja krzyżowa kodu przez drugiego programistę) pod kątem sprawdzania czy kryteria bezpieczeństwa są realnie weryfikowane przed zatwierdzeniem zmian do głównej gałęzi kodu (main branch). 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 8.25 Cykl życia bezpiecznego rozwoju SDLC. Zabezpieczenia techniczne to pipeline CI/CD w GitHub z ograniczonym dostępem, do tego manualny przegląd kodu źródłowego przez Hadrone, testy penetracyjne na kodzie w środowisku produkcyjnym i testowym. Dodatkowo zlecane są testy SAST i DAST dla rozwijanego kodu.	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z oraz dodatkowo regulowany przez RODO i w ramach ZSZ	Art. 21(2)g (NIS2) / Art. 6 (DORA) / Art. 15 AI Act	tak
------	------------	--------------------------------------	----------------------	----------	---	---	--	---	------	---	--	---	-----



8.26	Techniczne	Wymagania bezpieczeństwa aplikacji	ISO 27001, ISO 27701	Security	CC_S9 - Risk Mitigation / Oslabianie ryzyka	<ul style="list-style-type: none"> Standardy i checklisty wymagań (np.: OWASP ASVS): Wykorzystanie uznanych standardów (Application Security Verification Standard) do tworzenia powtarzalnych list wymagań technicznych dla programistów i dostawców. Mechanizmy tożsamości i kontroli dostępu: Wdrażanie w architekturze aplikacji wymagań dotyczących silnego uwierzytelniania (MFA), integracji z firmowym systemem Single Sign-On (SSO) oraz kontroli dostępu opartej na rolach (RBAC). Walidacja i sanitaryzacja danych wejściowych: Projektowanie procesów, które bezwzględnie filtrują i oczyszczają wszelkie dane wprowadzane przez użytkownika w formularzach i zapytaniach API, co technicznie uniemożliwia ataki typu SQL Injection czy XSS. Bezpieczna komunikacja i obsługa błędów: Wymóg stosowania protokołu TLS dla całego ruchu oraz projektowanie generycznych komunikatów o błędach. 	<ul style="list-style-type: none"> Wskaźnik pokrycia wymagań bezpieczeństwa (KPI): Miara określająca procent wymagań bezpieczeństwa, które zostały pomyślnie zaimplementowane i przetestowane przed dopuszczeniem aplikacji do użytku produkcyjnego. Matryca identyfikowalności wymagań (Requirements Traceability Matrix): Proces weryfikacji, w którym każdy zdefiniowany na początku wymóg bezpieczeństwa jest mapowany na konkretny test techniczny (manualny lub automatyczny) potwierdzający jego działanie. Automatyczne i manualne testy akceptacyjne (UAT / Security Testing): Przeprowadzanie dedykowanych testów bezpieczeństwa (w tym testów penetracyjnych) w celu empirycznego potwierdzenia, że aplikacja spełnia założone wymagania odporności na ataki. Przegląd architektury i modelowania zagrożeń: Formalny proces kontrolny przed wdrożeniem, polegający na ocenie architektury aplikacji przez dedykowany zespół ds. cyberbezpieczeństwa (Security Sign-off) pod kątem realizacji założeń polityki bezpieczeństwa organizacji. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 8.26 Wymagania bezpieczeństwa aplikacji, oraz w obszarze RODO: Polityka Bezpieczeństwa Danych Osobowych w Hadrone Sp. z o.o - punkt: 6.5. Uwzględnienie ochrony danych osobowych w fazie projektowania oraz domyślna ochrona danych osobowych, oraz dokument: Strategia Zarządzania Bezpieczeństwem i Ochroną Danych Osobowych w ramach ZSZ dla Hadrone (Integracja z PIMS i PII w Cloud) - punkt: 6.1 Privacy by Design oraz Privacy by Default. Zabezpieczenia techniczne to pipeline CD/CD z weryfikacją punktów SAST	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z oraz dodatkowo regulowany przez RODO i w ramach ZSZ	N/A	tak
------	------------	------------------------------------	----------------------	----------	---	--	--	---	------	--	--	-----	-----



8.27	Techniczne	Architektura i inżynieria systemów	ISO 27001	Security	CC_S7 - System Operations / Operacje systemowe	<ul style="list-style-type: none"> Wzorce i szablony bezpiecznej architektury: Wykorzystanie sprawdzonych standardów inżynierskich (np.: wytyczne NIST SP 800-160, wzorce projektowe architektur trójwarstwowych lub mikroservisów) jako fundamentu każdego nowego projektu IT. Modelowanie zagrożeń na poziomie systemowym: Formalny proces analizy architektury (np.: diagramów przepływu danych DFD) przed rozpoczęciem prac inżynierskich, pozwalający zidentyfikować luki w logice połączeń i autoryzacji. Infrastruktura jako Kod (IaC) i konteneryzacja: Narzędzia do powtarzalnego, bezpiecznego wdrażania środowisk (np.: Terraform), które wymuszają z góry zdefiniowaną i niezmienną architekturę systemową. 	<ul style="list-style-type: none"> Wskaźnik zgodności architektonicznej (KPI): Miara określająca procent wdrożonych systemów, które przeszły formalną weryfikację pod kątem zgodności z zatwierdzonymi standardami inżynierii bezpieczeństwa. Formalny przegląd i zatwierdzenie projektu (Architecture Sign-off): Obowiązkowa kontrola proceduralna realizowana przez architekta bezpieczeństwa przed uruchomieniem budowy systemu, potwierdzająca uwzględnienie wszystkich wymagań odpornościowych. Testy odporności warstwowej (Component Testing): Praktyczne próby podatnościowe polegające na testowaniu pojedynczych komponentów inżynierskich (np.: konfiguracji serwerów, komunikacji między API a bazą), aby zweryfikować czy izolacja warstw działa w praktyce. Audyt konfiguracji bazowej (Hardening Baseline Audit): Automatyczna weryfikacja gotowego systemu tuż przed oddaniem go do użytku, sprawdzająca, czy inżynierowie wyłączyli domyślne konta, testowe usługi i niezabezpieczone protokoły zgodnie z założeniami projektu. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 8.27 Architektura i inżynieria systemów. Techniczne zabezpieczenia to: .net Framework oraz technologia webowa, oraz wykorzystanie mechanizmów IaaS od Microsoft Azure, dodatkowo Hadrone stosuje IaC na bazie Terraform i automatyzacja działań celem eliminacji błędów ludzkich.	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS	N/A	tak
------	------------	------------------------------------	-----------	----------	--	--	--	---	------	---	--	-----	-----



8.28	Techniczne	Bezpieczne kodowanie	ISO 27001	Security	CC_S7 - System Operations / Operacje systemowe	<ul style="list-style-type: none"> • Zautomatyzowana analiza kodu (SAST): Wdrożenie narzędzi do statycznej analizy bezpieczeństwa kodu, które automatycznie skanują strukturę kodu źródłowego przy każdym wypchnięciu zmian (git push) pod kątem znanych podatności (np.: z listy OWASP Top 10). • Parametryzacja zapytań (Prepared Statements): Obowiązkowe stosowanie zapytań parametryzowanych w komunikacji z bazami danych, co na poziomie programistycznym całkowicie uniemożliwia przeprowadzenie ataków typu SQL Injection. • Bezpieczne API do zarządzania sekretami: Wykorzystanie dedykowanych systemów (np.: Azure Key Vault), które wstrzykują klucze i hasła bezpośrednio do pamięci uruchomionej aplikacji (environment variables) bez ujawniania ich w plikach kodu. • Zasada wzajemnego przeglądu kodu (Peer Code Review): Sformalizowany proces, w którym żadna linijka kodu nie trafia do głównego repozytorium bez uprzedniej weryfikacji i zatwierdzenia przez drugiego, doświadczonego programistę pod kątem poprawności i bezpieczeństwa. 	<ul style="list-style-type: none"> • Bramki bezpieczeństwa w procesie budowania (CI/CD Quality Gates): Blokada automatycznego wdrażania nowej wersji aplikacji, jeśli skanery kodu wykryją błędy bezpieczeństwa o statusie "Krytyczny" lub "Wysoki". • Testy penetracyjne aplikacji przed wydaniem: Cykliczne (manualne i automatyczne) testy bezpieczeństwa gotowego oprogramowania, mające na celu praktyczne zweryfikowanie odporności aplikacji na ataki i próby złamania jej logiki biznesowej. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 8.28 Bezpieczne kodowanie. Techniczne zabezpieczenia to pipeline CI/CD w GitHub z ograniczonym dostępem, do tego manualny przegląd kodu źródłowego przez Hadrone, testy penetracyjne na kodzie w środowisku produkcyjnym i testowym. Dodatkowo zlecane są testy SAST i DAST dla rozwijanego kodu.	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS	N/A	tak
------	------------	----------------------	-----------	----------	--	--	--	---	------	---	--	-----	-----



8.29	Techniczne	Testowanie bezpieczeństwa	ISO 27001	Security	CC_S7 - System Operations / Operacje systemowe	<ul style="list-style-type: none"> • Automatyczne skanowanie podatności (Vulnerability Scanning): Wykorzystanie narzędzi (np.: Nessus) do regularnego, automatycznego przeszukiwania sieci, systemów operacyjnych i baz danych pod kątem znanych luk i brakujących poprawek. • Testy penetracyjne (Pentesty): Kontrolowane, manualne próby przełamania zabezpieczeń realizowane przez wykwalifikowanych specjalistów (Etycznych Hakerów) symulujących realne techniki cyberprzestępców (podejścia Black Box, Grey Box, White Box). • Automatyzacja DAST i SAST w pipeline CI/CD: Wdrożenie dynamicznych testów bezpieczeństwa aplikacji (np. przy użyciu OWASP ZAP, Burp Suite Enterprise) uruchamianych automatycznie przy każdym wdrożeniu nowej wersji w celu wykrycia luk w działającym środowisku. 	<ul style="list-style-type: none"> • Wskaźnik podatności w czasie (KPI / Vulnerability Density): Liczba i krytyczność zidentyfikowanych luk w podziale na systemy, monitorowana w ujęciu miesięcznym lub kwartalnym w celu oceny ogólnego trendu poziomu bezpieczeństwa firmy. • Średni czas usuwania podatności: Kluczowa miara operacyjna sprawdzająca, jak szybko organizacja naprawia wykryte błędy. • Audyt i śledzenie realizacji zaleceń po-testowych: Formalny, kwartalny przegląd statusu raportów z testów penetracyjnych. Każda wykryta podatność musi posiadać przypisanego właściciela biznesowego, plan naprawczy lub formalną, podpisaną przez zarząd akceptację ryzyka. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 8.29 Testowanie bezpieczeństwa Techniczne zabezpieczenia to pipeline CI/CD w GitHub z ograniczonym dostępem, do tego manualny przegląd kodu źródłowego przez Hadrone, testy penetracyjne na kodzie w środowisku produkcyjnym i testowym. Dodatkowo zlecane są testy SAST i DAST dla rozwijanego kodu.	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS	N/A	tak
------	------------	---------------------------	-----------	----------	--	--	--	---	------	---	--	-----	-----



8.30	Techniczne	Outsourcing rozwoju oprogramowania	ISO 27001	Security	CC_S7 - System Operations / Operacje systemowe	<ul style="list-style-type: none"> • Kontraktowe zapisy bezpieczeństwa: Aneksowanie umów o precyzyjne wytyczne techniczne (np.: nakaz zgodności z OWASP Top 10, obowiązek naprawy krytycznych podatności w określonym czasie na koszt dostawcy). • Niezależne pipeline CI/CD wdrożeniowe (Staging / Escrow): Proces przyjmowania kodu, w którym dostawca przekazuje oprogramowanie do odizolowanego repozytorium organizacji, gdzie przechodzi ono automatyczne testy, zanim trafi do środowiska testowego. • Automatyczne skanowanie kodu dostawcy (SAST / SCA): Wykorzystanie narzędzi do bezwzględnego skanowania każdej dostarczonej paczki kodu pod kątem ukrytych luk, podatnych bibliotek Open Source oraz celowo zaszytych podatności (backdoors). • Zarządzanie tożsamością (IdM/PAM): Przekazywanie zewnętrznym wykonawcom dedykowanych, imiennych kont z wymuszonym MFA, kontrolowanych przez systemy PAM (Privileged Access Management), które rejestrują całą aktywność na serwerach organizacji. 	<ul style="list-style-type: none"> • Niezależne testy penetracyjne (Pentesting): Obowiązkowe, manualne testy bezpieczeństwa realizowane przez zewnętrzną firmę trzecią (niezależną od dostawcy kodu) przed formalnym podpisaniem protokołu odbioru oprogramowania. • Audyty i inspekcje dostawcy (Third-Party Audits): Cykliczna (np.: raz w roku) weryfikacja dojrzałości procesowej dostawcy, polegająca na przeglądzie jego certyfikatów (np.: ISO 27001) lub audycie sposobu, w jaki zabezpiecza on stacje robocze swoich programistów. • Ewidencja i monitoring praw własności i licencji: Kontrola prawno-techniczna weryfikująca, czy dostawca nie umieścił w kodzie komponentów Open Source na licencjach wykluczających użycie komercyjne (np.: GPL), co mogłoby narazić organizację na straty prawne lub wizerunkowe. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 8.30 Outsourcing rozwoju oprogramowania. Techniczne zabezpieczenie: kod jest odebrany jako końcowy produkt po testach bezpieczeństwa tj. po testach SAST, DAST, pentestach oraz po weryfikacji na poziom ASVS level 1. Testy DAST i pentesty są prowadzone na zgodność z wymaganiami OWASP Web Top 10 lub Top 25 (wersja najnowsza)	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS	N/A	tak
------	------------	------------------------------------	-----------	----------	--	--	--	---	------	---	--	-----	-----



8.31	Techniczne	Separacja środowisk	ISO 27001, ISO 27017	Security	CC_S1 - Control Environment/ Kontrole Środowiskowe	<ul style="list-style-type: none"> • Mikrosegmentacja i osobne konta chmurowe: Wykorzystanie fizycznie oddzielonej infrastruktury sieciowej (VLAN/VNET) lub osobnych subkont/subskrypcji w chmurze (np.: Azure Tenants) dla każdego ze środowisk. • Narzędzia do anonimizacji i maskowania danych: Wdrożenie automatycznych skryptów lub narzędzi (np. Delphix, Redgate), które przed skopiowaniem bazy danych do środowiska testowego trwale nadpisują wrażliwe rekordy (np.: zamiana nazwisk i email na ciągi losowe). • Zautomatyzowane pipeline CI/CD (Deployment Pipelines): Używanie systemów takich jak GitHub do automatycznego budowania i wdrażania kodu. Przeniesienie paczki na produkcję odbywa się bez ręcznej interwencji człowieka, na podstawie zatwierdzonego skryptu. • Zarządzanie tożsamością i dostępem (IAM): Restrykcyjna konfiguracja ról dostępów. Dostęp do środowisk testowych i deweloperskich opiera się na kontach domenowych deweloperów, podczas gdy dostęp do produkcji jest skrajnie ograniczony i zabezpieczony osobnym MFA. 	<ul style="list-style-type: none"> • Wskaźnik szczelności izolacji środowisk (KPI): Miara weryfikująca liczbę nieautoryzowanych prób nawiązania połączeń sieciowych lub transferu danych ze strefy deweloperskiej bezpośrednio do produkcyjnej. • Audyt konfiguracji kont i uprawnień użytkowników: Coroczny przegląd list dostępowych (ACL) do środowiska produkcyjnego. Weryfikacja, czy żadne konto przypisane do roli programisty lub zewnętrznego kontraktora nie posiada uprawnień modyfikacji systemów produkcyjnych. • Weryfikacja logów potoku wdrożeniowego (Deployment Audits): Bieżąca kontrola sprawdzająca czy każda zmiana wprowadzona na produkcji posiada unikalny identyfikator powiązany z zaliczonymi testami w środowisku UAT oraz formalną akceptacją właściciela biznesowego (Change Managera). 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 8.31 Separacja środowisk. Techniczne zabezpieczenia stosowane przez Hadrone to pełne rozdzielenie środowisk produkcyjnych i deweloperskich oraz deweloperskich i testowych. - rozdzielenie na poziomie subskrypcji.	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS	Art. 15 AI Act	tak
------	------------	---------------------	----------------------	----------	--	--	---	---	------	---	--	----------------	-----



8.32	Techniczne	Zarządzanie zmianami	ISO 27001, ISO 27017	Security	CC_S8 - Change Managment / Zarządzanie zmianą	<ul style="list-style-type: none"> Systemy zarządzania zgłoszeniami: Wykorzystanie oprogramowania (np.: Jira) do rejestracji cyklu życia zmiany – od wniosku, przez testy, oceny ryzyka, po wdrożenie i zamknięcie. Proces Zarządzania Zmianami Awaryjnymi (Emergency Change): Sformalizowana ścieżka pozwalająca na natychmiastowe wdrożenie poprawki (np.: załatanie krytycznej podatności zero-day) za zgodą Hadrone CISO, z obowiązkiem pełnego udokumentowania i audytu wstecznego w ciągu 24–48 godzin po incydencie. Automatyczne potoki wdrażania (CI/CD) i testy automatyczne: Integracja procesu zmian z narzędziami automatyzacji (np.: Terraform), co eliminuje błędy ludzkie i implementacja tych zmian z poziomu pipeline CI/CD. Kalendarz Zmian (Change Calendar) i okna serwisowe: Narzędzie planistyczne zapobiegające nakładaniu się na siebie wielu krytycznych modyfikacji infrastruktury, wymuszające wdrażanie zmian w wyznaczonych oknach czasowych o najmniejszym natężeniu ruchu biznesowego. 	<ul style="list-style-type: none"> Wskaźnik zmian zakończonych sukcesem (KPI / Success Rate): Miara określająca procent zmian wdrożonych prawidłowo za pierwszym razem w stosunku do wszystkich modyfikacji. Wskaźnik incydentów powdrożeniowych: Mierzenie liczby awarii lub incydentów bezpieczeństwa, których bezpośrednią przyczyną było wprowadzenie konkretnej zmiany w ciągu ostatnich 72 godzin od wdrożenia. Audyt powdrożeniowy (Post-Implementation Review - PIR): Obowiązkowa, cykliczna weryfikacja losowo wybranych lub nieudanych zmian, mająca na celu ustalenie przyczyn niepowodzenia, ocenę poprawności wykonania planu rollback oraz wyciągnięcie wniosków na przyszłość (Lessons Learned). 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 8.32 Zarządzanie zmianami. Techniczne zabezpieczenia to: stosowne uprawnienia na IaaS Azure, dodatkowo paczka kod musi być skompilowana, zamrożona i odblokowana do wdrożenia z pipeline CI/CD.	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS	N/A	tak
------	------------	----------------------	----------------------	----------	---	--	--	---	------	---	--	-----	-----



8.33	Techniczne	Informacje testowe	ISO 27001, ISO 27018, ISO 27701	Security	CC_S8 - Change Managment / Zarządzanie zmianą	<ul style="list-style-type: none"> • Generator danych syntetycznych: Wykorzystanie specjalistycznego oprogramowania (np. Mockaroo, Faker, dedykowane skrypty) do masowego tworzenia realistycznych, ale całkowicie fikcyjnych zestawów danych (np.: fikcyjne adresy e-mail). • Narzędzia do maskowania danych (Data Masking / Obfuscation): Wdrożenie systemów (np.: Delphix, Redgate Data Masker), które automatycznie podmieniają wrażliwe produkcyjne rekordy w bazie danych (np.: email algorytmicznie poprawnymi, ale fałszywymi ciągami cyfr). • Formalny proces zatwierdzania użycia danych (Data Request Process): Wydana zgoda Właściciela Danych (Data Owner) i Hadrone KOOD na czasowe użycie wycinka danych produkcyjnych na teście – wymaga analizy ryzyka, w tym DPIA. • Zautomatyzowane niszczenie danych: Skrypty czyszczące, które automatycznie i nieodwracalnie usuwają (nadpisują zerami) tabele testowe po upływie zdefiniowanego w zgłoszeniu okna czasowego. 	<ul style="list-style-type: none"> • Skanowanie środowisk testowych pod kątem wycieku produkcji: Regularne automatyczne przeszukiwanie baz i systemów plików środowisk testowych w celu wykrycia realnych struktur danych produkcyjnych. • Audyt uprawnień do bazy danych testowych: Coroczna weryfikacja list dostępu (ACL) sprawdzająca, czy deweloperzy lub zewnętrzni kontraktorzy nie posiadają uprawnień do eksportowania informacji testowych na lokalne stacje robocze. • Weryfikacja logów usuwania danych (Purge Audit): Cykliczny przegląd potwierdzeń realizacji procedur niszczenia danych testowych po zamknięciu zgłoszeń projektowych, weryfikujący czy żadne archiwalne dumpy baz danych nie zalegają na serwerach deweloperskich. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 8.33 Informacje testowe. Technicznie Hadrone stosuje tzw. Dumy-data. Wynika to z następujących dokumentacji: Strategia Zarządzania Bezpieczeństwem i Ochroną Danych Osobowych w ramach ZSZ dla Hadrone (Integracja z PIMS i PII w Cloud) - punkt: 5 Techniczna ochrona danych osobowych w chmurze (ISO 27018) oraz z Polityka Bezpieczeństwa Danych Osobowych w Hadrone Sp. z o.o - punkt: 9. Określenie środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS Z oraz dodatkowo regulowany przez RODO i w ramach ZSZ	N/A	tak
------	------------	--------------------	---------------------------------	----------	---	---	--	---	------	--	--	-----	-----



8.34	Techniczne	Ochrona systemów podczas audytów	ISO 27001	Security	CC_S5 - Control Activities / Czynności kontrolne	<ul style="list-style-type: none"> • Dedykowane, tymczasowe konta audytowe: Tworzenie unikalnych, imiennych kont dla audytorów z automatyczną datą wygaśnięcia (np. na koniec dnia roboczego), zabezpieczonych MFA i restrykcyjnymi uprawnieniami typu Read-Only. • Izolowane sesje i nagrywanie aktywności (PAM): Uruchamianie dostępu dla audytorów przez systemem PAM (Privileged Access Management), które nie tylko izolują połączenie, ale w pełni rejestrują każdą komendę wpisaną przez audytora. • Ekstrakcja danych i logów na żądanie (Data Offloading): Hadrone generuje techniczne raporty, zrzuty ekranu lub eksporty logów i przekazuje je audytorowi w sposób kontrolowany. • Procedura okien audytowych: Wyznaczanie ścisłych ram czasowych na testy audytowe (np.: poza godzinami szczytu biznesowego) oraz definiowanie okresów krytycznych (np.: wdrożenia), podczas których wszelkie działania audytowe są zabronione. 	<ul style="list-style-type: none"> • Wskaźnik incydentów spowodowanych audytem (KPI): Miara określająca liczbę przestojów, awarii lub alertów bezpieczeństwa, których bezpośrednią przyczyną były działania weryfikacyjne prowadzone przez audytorów. • Audyt rozliczalności i zamknięcia kont: Natychmiastowa weryfikacja techniczna po zakończeniu audytu, sprawdzająca czy wszystkie tymczasowe konta, dostępy VPN oraz reguły sieciowe otwarte na czas kontroli zostały skutecznie zablokowane lub usunięte. • Weryfikacja integralności logów systemowych: Kontrola upewnijająca się, że logi z przebiegu audytu (kto, kiedy i co sprawdzał) zostały automatycznie przesłane do nienaruszalnego repozytorium i nie zostały zmodyfikowane. • Przegląd zgodności używanych narzędzi audytowych: Weryfikacja czy oprogramowanie, którym posługuje się audytor posiada aktualne sygnatury, licencje i jest bezpieczne dla infrastruktury Hadrone. 	Brak wyjątków, Brak uwag / No exception, No comments.	Brak	Regulowany przez dokument: Zbiór zasad i procedur operacyjnych dla zarządzania mechanizmami kontrolnymi dla Zintegrowanego Systemu Zarządzania w Hadrone - punkt: 8.34 Ochrona systemów podczas audytów. Techniczne zabezpieczenia stosowane w Hadrone do systemów własnych wynikają z Zasady konfiguracji aplikacji i usług M365 w Hadrone Sp. z o.o. natomiast dla systemów SaaS w Azure zapisy audytowe bazują na IaC i odkładaniu każdego logu w osobnej bazie danych. Aplikacje SaaS Hadrone logują i zapisują, każdą akcję na danych w ramach logów aplikacyjnych i odkładają je do osobnego pliku bazy danych. Logi mogą być udostępniane do audytu lub weryfikacji poprzez mechanizmy Azure Hub do dowolnego narzędzia SIEM dla klienta Hadrone.	W zakresie ZSZ Hadrone, nie wymaga uzasadnienia, ponieważ regulowany przez w ramach ZSZ przez ZZPO_MK_ZS	N/A	tak
------	------------	----------------------------------	-----------	----------	--	---	--	---	------	--	--	-----	-----



3 Załączniki

Lista załączników:

- Załącznik nr 1 – Mapowanie_SoA_Hadrone_ZSZ_na_wymagania_SOC2, TYPE II-CC_Styczeń_2026



Mapowanie_SoA_H
adrone_ZSZ_na_wyn