Dokument przygotwany na podstawie European Union Agency for Network and Information Security (ENISA) na podstawie załącznika A - Organizational and Technical Measures, Handbook on Security of Personal Data Processing (WP2017-0-2-2-5 GDPR Measures Handbook)

Kategoria	**ID**	**Opis kategorii**	**Opis stosowanego zabezpieczenia**
Polityka i procedury bezpieczeństwa ochrony danych osobowych	A1	Organizacja powinna udokumentować Politykę bezpieczeństwa danych osobowych.	Wdrożono
Polityka i procedury bezpieczeństwa ochrony danych osobowych	A2	Polityka bezpieczeństwa powinna być poddana przeglądowi w zaplanowanych odstępach czasu (na przykład raz do roku)	Wdrożono
Polityka i procedury bezpieczeństwa ochrony danych osobowych	A3	Organizacja powinna udokumentować odrębną dedykowaną Instrukcję Zarządzania Systemem Informatycznym. Instrukcja powinna zostać zatwierdzona przez kierownictwo i przekazana wszystkim pracownikom i właściwym stronom zewnętrznym.	Wdrożono

Kategoria	**ID**	**Opis kategorii**	**Opis stosowanego zabezpieczenia**
Polityka i procedury bezpieczeństwa ochrony danych osobowych	A4	Polityka bezpieczeństwa powinna przynajmniej odnosić się do: § ról i obowiązków personelu, § podstawowego stanu technicznego i przyjętych środków organizacyjnych dla bezpieczeństwa danych osobowych, § podmiotów przetwarzających dane lub inne strony trzecie zaangażowane w przetwarzanie dane osobowych.	Wdrożono
Polityka i procedury bezpieczeństwa ochrony danych osobowych	A5	Wykaz konkretnych zasad / procedur związanych z bezpieczeństwem danych osobowych powinien być stworzony i utrzymywany na podstawie ogólnej Polityki bezpieczeństwa.	Wdrożono
Role i odpowiedzialność za bezpieczeństwo informacji	B1	Odpowiedzialność za bezpieczeństwo informacji powinna być określona i przypisana zgodnie z postanowieniami Polityki bezpieczeństwa danych.	Wdrożono

Kategoria	ID	Opis kategorii	Opis stosowanego zabezpieczenia
Role i obowiązki	B2	W przypadku wewnętrznych zmian w organizacji lub wypowiedzeń i zmian zatrudnienia (w tym wypowiedzenia), odebranie uprawnień powinno być przeprowadzone w odpowiedni sposób tj. zgodnie z procedurami, które powinny być jasno określone i zdefiniowane.	Wdrożono
Role i obowiązki	B3	Jasne wyznaczenie osób odpowiedzialnych za określone zadania w zakresie ochrony informacji, w tym mianowanie Inspektora Ochrony Danych Osobowych	Wdrożono
Role i obowiązki	**B.4**	Inspektor Ochrony Danych powinien być formalnie wyznaczony (udokumentowany). Zadania i obowiązki Inspektora Ochrona Danych powinny być również jasno określone i udokumentowane.	Wdrożono
Role i obowiązki	**B.5**	Sprzeczne obowiązki i obszary odpowiedzialności np. role Administratora Systemów Informatycznych, audytora bezpieczeństwa i IOD, należy uznać za rozdzielone, aby	Wdrożono

Kategoria	**ID**	**Opis kategorii**	**Opis stosowanego zabezpieczenia**
		zmniejszyć możliwości nieuprawnionej lub niezamierzonej modyfikacji lub niewłaściwego wykorzystania danych osobowych.	
Polityka kontroli dostępu	C1	Konkretne prawa dostępu powinny być przypisane do każdej roli (zaangażowanej w przetwarzanie danych osobowych) kierując się „zasadą ścisłej potrzeby” (need to know basis)	Wdrożono
Polityka kontroli dostępu	C2	Organizacja powinna opracować szczegółową Politykę kontroli dostępu. Organizacja powinna określać i udokumentować odpowiednie zasady kontroli dostępu, prawa dostępu i ograniczenia dla określonych ról użytkowników.	Wdrożono
Polityka kontroli dostępu	C3	Zasady dotyczące rozdzielenia ról kontroli dostępu (np. żądanie dostępu, autoryzacja, administracja dostępem) powinny być jasno zdefiniowane i Udokumentowane.	Wdrożono

Kategoria	**ID**	**Opis kategorii**	**Opis stosowanego zabezpieczenia**
Polityka kontroli dostępu	**C.4**	Role z nadmiernymi prawami dostępu powinny być jasno określone i przypisane ograniczonej liczbie określonych członków personelu.	Wdrożono
Zarządzanie zasobami	D1	Organizacja powinna mieć rejestr wykorzystywanych zasobów informatycznych, które przetwarzają dane osobowe (sprzęt, oprogramowanie i sieć). Rejestr powinien zawierać co najmniej następujące informacje: zasób IT, typ (np. serwer, stacja robocza), lokalizacja (fizyczna lub elektroniczna). Należy wyznaczyć konkretną osobę do utrzymania i aktualizacji rejestru (może to być np. informatyk).	Wdrożono
Zarządzanie zasobami	D2	Należy dokonać przeglądu zasobów IT i aktualizować je na bieżąco	Wdrożono
Zarządzanie zasobami	D3	Należy określić i udokumentować role użytkowników mających dostęp do niektórych plików.	Wdrożono

Kategoria	**ID**	**Opis kategorii**	**Opis stosowanego zabezpieczenia**
Zarządzanie zasobami/aktywami	**D.4**	Zasoby IT powinny być poddawane przeglądowi i aktualizowane co roku.	Wdrożono
Zarządzanie zmianami	E1	Organizacja powinna się upewnić, że wszystkie zmiany w systemie informatycznym są zarejestrowane i monitorowane przez konkretną osobę (np. IT lub oficer bezpieczeństwa). Regularne monitorowanie zmian powinno być częścią procesu zarządzania zmianą.	Wdrożono
Zarządzanie zmianami	E2	Oprogramowanie powinno być wykonywane w specjalnym środowisku, które nie jest podłączone do systemu informatycznego wykorzystywanego do przetwarzania danych osobowych. Gdy potrzebne są testy, należy używać fikcyjnych danych (nierzeczywistych danych). Gdy nie jest to możliwe, w celu ochrony danych osobowych wykorzystywanych w testach powinny być wykorzystywane formalne procedury.	Wdrożono

Kategoria	**ID**	**Opis kategorii**	**Opis stosowanego zabezpieczenia**
Podmioty przetwarzające	F1	Formalne wytyczne i procedury obejmujące przetwarzanie danych osobowych przez podmioty przetwarzające dane powinny być zdefiniowane, udokumentowane i uzgodnione między administratorem danych a podmiotem przetwarzającym przed rozpoczęciem przetwarzania. Wytyczne i procedury powinny być obowiązkowe oraz powinny ustalać ten sam poziom bezpieczeństwa jak polityka bezpieczeństwa organizacji.	Wdrożono
Podmioty przetwarzające	F2	W wyniku naruszenia danych osobowych, podmiot przetwarzający dane powinien powiadomić administratora bez zbędnego opóźnienia.	Wdrożono
Podmioty przetwarzające	F3	Formalne wymogi i obowiązki powinny być formalnie uzgodnione między administratorem danych i podmiotem przetwarzającym. Podmiot przetwarzający powinien dostarczyć dokumentację jako dowód zgodności.	Wdrożono

Kategoria	**ID**	**Opis kategorii**	**Opis stosowanego zabezpieczenia**
Podmioty przetwarzające	F4	Organizacja (Administrator danych) powinna regularnie kontrolować zgodność podmiotu przetwarzającego względem uzgodnionego poziomu wymagań i zobowiązań	Wdrożono
Procesor danych	**F.5**	Pracownicy podmiotu przetwarzającego dane osobowe powinni podlegać określonym udokumentowanym obowiązkom zachowania poufności/nieujawniania informacji.	Wdrożono
Obsługa incydentów / naruszenia danych osobowych	G1	Należy opracować procedurę obsługi incydentów, która będzie zawierała plan reagowania na incydenty. Plan powinien być tak zdefiniowany, aby zapewnić skuteczną i uporządkowaną reakcję na incydenty dotyczące danych osobowych.	Wdrożono

Kategoria	**ID**	**Opis kategorii**	**Opis stosowanego zabezpieczenia**
Obsługa incydentów / naruszenia danych osobowych	**G2**	Naruszenia danych osobowych należy niezwłocznie zgłaszać kierownictwu. Powinny istnieć procedury powiadamiania o naruszeniach do właściwych organów i osób, których dane dotyczą, zgodnie z art. 33 i 34 RODO	Wdrożono
Obsługa incydentów / naruszenia danych osobowych	G3	Plan reagowania na incydenty powinien być udokumentowany. Powinien wykazywać możliwe działania łagodzące i zawierać jasne przypisanie ról.	Wdrożono
Obsługa incydentów/osoby naruszające dane osobowe	**G.4**	Incydenty i naruszenia ochrony danych osobowych powinny być rejestrowane wraz ze szczegółami dotyczącymi zdarzenia i podjętych działań łagodzących.	Wdrożono
Poufność personelu	I1	Organizacja powinna zapewnić, aby wszyscy pracownicy rozumieli swoje obowiązki i obowiązki związane z przetwarzaniem danych osobowych. Role i obowiązki	Wdrożono

Kategoria	**ID**	**Opis kategorii**	**Opis stosowanego zabezpieczenia**
		powinny być jasno komunikowane podczas procesu poprzedzającego zatrudnienie i/lub integracji zawodowej.	
Poufność personelu	I2	Przed podjęciem obowiązków pracownicy powinni zostać poproszeni o zapoznanie się i uzgodnienie polityki bezpieczeństwa organizacji oraz podpisanie odpowiednich umów o zachowaniu poufności i poufności.	Wdrożono
Poufność personelu	**I.3**	Pracownicy zaangażowani w przetwarzanie danych osobowych pod wysokim ryzykiem powinni być zobowiązani do przestrzegania określonych klauzul poufności (wynikających z umowy o pracę lub innego aktu prawnego).	Wdrożono
Szkolenia	J1	Organizacja powinna zapewnić, że wszyscy pracownicy są odpowiednio poinformowani o środkach kontroli bezpieczeństwa systemu informatycznego, które dotyczą ich codziennej pracy. Pracownicy zaangażowani w przetwarzanie danych osobowych powinni być również odpowiednio informowani o	Wdrożono

Kategoria	ID	Opis kategorii	Opis stosowanego zabezpieczenia
		odpowiednich wymogach dotyczących ochrony danych i zobowiązaniach prawnych poprzez regularne kampanie informacyjne.	
Szkolenia	J2	Organizacja powinna mieć zorganizowane i regularne programy szkoleniowe dla pracowników, w tym dla określonych programistów w zakresie wprowadzania (do zagadnień związanych z ochroną danych) nowoprzybyłych.	Wdrożono
Kontrola dostępu i uwierzytelnianie	K1	Należy wdrożyć system kontroli dostępu obejmujący wszystkich użytkowników uzyskujących dostęp do systemu informatycznego. System powinien umożliwiać tworzenie, zatwierdzanie, przeglądanie i usuwanie kont użytkowników.	Wdrożono
Kontrola dostępu i uwierzytelnianie	K2	Należy unikać korzystania ze wspólnych kont użytkowników. W przypadkach, w których jest to konieczne, należy zapewnić, aby wszyscy użytkownicy wspólnego konta mieli te same role i obowiązki.	Wdrożono

Kategoria	**ID**	**Opis kategorii**	**Opis stosowanego zabezpieczenia**
Kontrola dostępu i uwierzytelnianie	K3	Powinien istnieć mechanizm uwierzytelniania, umożliwiający dostęp do systemu informatycznego (w oparciu o politykę i system kontroli dostępu). Jako minimum należy użyć kombinacji nazwy użytkownika i hasła. Hasła powinny mieć określony (konfigurowalny) poziom złożoności.	Wdrożono
Kontrola dostępu i uwierzytelnianie	K4	System kontroli dostępu powinien mieć możliwość wykrywania haseł, które nie są zgodne z określonym (konfigurowalnym) poziomem złożoności, i nie zezwalać na użycie tych haseł.	Wdrożono
Kontrola dostępu i uwierzytelnianie	K5	Należy zdefiniować i udokumentować określoną politykę dotyczącą haseł. Polityka powinna obejmować przynajmniej długość hasła, złożoność, okres ważności, a także liczbę akceptowalnych nieudanych prób logowania.	Wdrożono

Kategoria	**ID**	**Opis kategorii**	**Opis stosowanego zabezpieczenia**
Kontrola dostępu i uwierzytelnianie	K6	Hasła użytkowników muszą być przechowywane w postaci „zaszyfrowanej”.	Wdrożono
Kontrola dostępu i uwierzytelnianie	**K.7**	W celu uzyskania dostępu do systemów przetwarzających dane osobowe najlepiej stosować uwierzytelnianie dwuetapowe. Czynnikami uwierzytelniającymi mogą być hasła, tokeny bezpieczeństwa, pendrive’y z tajnym tokenem, dane biometryczne itp.	Wdrożono
Kontrola dostępu i uwierzytelnianie	**K.8**	Należy stosować uwierzytelnianie urządzenia, które gwarantuje, że przetwarzanie danych osobowych odbywa się wyłącznie na określonych zasobach sieci.	Wdrożono
Logowanie i monitorowanie	L1	Pliki dziennika należy aktywować dla każdego systemu / aplikacji używanej do przetwarzania danych osobowych. Powinny obejmować wszystkie rodzaje dostępu do danych (przeglądanie, modyfikacja, usuwanie).	Wdrożono

Kategoria	**ID**	**Opis kategorii**	**Opis stosowanego zabezpieczenia**
Logowanie i monitorowanie	L2	Pliki dziennika powinny być opatrzone sygnaturą czasową i odpowiednio zabezpieczone przed manipulacją i nieautoryzowanym dostępem. Zegary powinny być zsynchronizowane z pojedynczym źródłem czasu odniesienia	Wdrożono
Rejestrowanie i monitorowanie	L3	Działania administratorów systemu i operatorów systemu, w tym dodawanie / usuwanie / zmiana uprawnień użytkowników, powinny być rejestrowane.	Wdrożono
Rejestrowanie i monitorowanie	L4	Nie powinno być możliwości usunięcia lub modyfikacji zawartości plików logów. Oprócz monitorowania w celu wykrycia nietypowej aktywności należy również rejestrować dostęp do plików dziennika.	Wdrożono
Rejestrowanie i monitorowanie	L5	System monitorowania powinien przetwarzać pliki dziennika i tworzyć raporty o stanie systemu oraz powiadamiać o potencjalnych alertach.	Wdrożono

Kategoria	ID	Opis kategorii	Opis stosowanego zabezpieczenia
Bezpieczeństwo baz danych i serwerów	M1	Serwery baz danych i aplikacji powinny być skonfigurowane do pracy przy użyciu oddzielnego konta, z minimalnymi uprawnieniami systemu operacyjnego, aby działały poprawnie.	Wdrożono
Bezpieczeństwo baz danych i serwerów	M2	Serwery baz danych i aplikacji powinny przetwarzać tylko te dane osobowe, które są rzeczywiście potrzebne do przetwarzania do osiągnięcia celów przetwarzania.	Wdrożono
Bezpieczeństwo serwera / bazy danych	M3	Rozwiązania szyfrujące należy rozważyć w odniesieniu do określonych plików lub rekordów poprzez implementację oprogramowania lub sprzętu.	Wdrożono
Bezpieczeństwo serwera / bazy danych	M4	Należy rozważyć szyfrowanie dysków do przechowywania danych	Wdrożono

Kategoria	**ID**	**Opis kategorii**	**Opis stosowanego zabezpieczenia**
Bezpieczeństwo serwera / bazy danych	M5	Techniki pseudonimizacji należy stosować poprzez oddzielenie danych od bezpośrednich identyfikatorów, aby uniknąć łączenia z osobą, której dane dotyczą, bez dodatkowych informacji	Wdrożono
Bezpieczeństwo baz danych i serwerów	**M.6**	Należy rozważyć techniki wspierające prywatność na poziomie bazy danych, takie jak autoryzowane zapytania, zapytania do baz danych chroniące prywatność, szyfrowanie z możliwością przeszukiwania itp.	Wdrożono
Bezpieczeństwo stacji roboczej	N1	Użytkownicy nie powinni mieć możliwości dezaktywowania ani ominięcia ustawień zabezpieczeń.	Wdrożono
Bezpieczeństwo stacji roboczej	N2	Aplikacje antywirusowe i sygnatury detekcji należy aktualizować co tydzień.	Wdrożono

Kategoria	**ID**	**Opis kategorii**	**Opis stosowanego zabezpieczenia**
Bezpieczeństwo stacji roboczej	N4	System powinien mieć limity czasu sesji, gdy użytkownik nie był aktywny przez określony czas.	Wdrożono
Bezpieczeństwo stacji roboczej	N5	Krytyczne aktualizacje zabezpieczeń wydane przez programistę systemu operacyjnego powinny być regularnie instalowane.	Wdrożono
Bezpieczeństwo stacji roboczej	N6	Aplikacje antywirusowe i sygnatury wykrywania należy aktualizować codziennie.	Wdrożono
Bezpieczeństwo stacji roboczej	**N.7**	Nie należy zezwalać na przenoszenie danych osobowych ze stacji roboczych na zewnętrzne urządzenia magazynujące (np. USB, DVD, zewnętrzne dyski twarde itp.)	Wdrożono
Bezpieczeństwo stacji roboczej	**N.8**	W miarę możliwości stacje robocze wykorzystywane do przetwarzania danych osobowych nie powinny być połączone z internetem, chyba że zastosowane środki	Wdrożono

Kategoria	ID	Opis kategorii	Opis stosowanego zabezpieczenia
		bezpieczeństwa zapobiegające nieuprawnionemu przetwarzaniu, kopiowaniu i przekazywaniu danych osobowych w magazynie.	
Bezpieczeństwo stacji roboczej	**N.9**	Szyfrowanie całego dysku powinno być włączone na dyskach z systemem operacyjnym stacji roboczej.	Wdrożono
Bezpieczeństwo sieci / komunikacji	O1	Ilekroć dostęp odbywa się przez Internet, komunikacja powinna być szyfrowana za pomocą protokołów kryptograficznych (TLS / SSL).	Wdrożono
Bezpieczeństwo sieci / komunikacji	O2	Bezprzewodowy dostęp do systemu informatycznego powinien być możliwy tylko dla określonych użytkowników i procesów. Powinien być chroniony mechanizmami szyfrowania.	Wdrożono
Bezpieczeństwo sieci / komunikacji	O3	Generalnie należy unikać zdalnego dostępu do systemu informatycznego. W przypadkach, gdy jest to absolutnie konieczne, powinno się to odbywać tylko pod	Wdrożono

Kategoria	ID	Opis kategorii	Opis stosowanego zabezpieczenia
		kontrolą i monitoringiem określonej osoby z organizacji (np. Administratora IT / pracownika bezpieczeństwa) za pośrednictwem predefiniowanych urządzeń.	
Bezpieczeństwo sieci / komunikacji	O4	Ruch do iż systemu informatycznego powinien być monitorowany i kontrolowany przez zapory ogniowe i systemy wykrywania włamań.	Wdrożono
Bezpieczeństwo sieci / komunikacji	**O.5**	Nie powinno się zezwalać na połączenia internetowe z serwerami i stacjami roboczymi używanymi do przetwarzania danych osobowych.	Wdrożono
Bezpieczeństwo sieci / komunikacji	**O.6**	Sieć systemu informatycznego powinna być oddzielona od innych sieci administratora danych.	Wdrożono

Kategoria	**ID**	**Opis kategorii**	**Opis stosowanego zabezpieczenia**
Bezpieczeństwo sieci / komunikacji	**O.7**	Dostęp do systemu informatycznego powinien odbywać się wyłącznie za pomocą uprzednio autoryzowanych urządzeń i terminali z wykorzystaniem technik takich jak filtrowanie adresów MAC czy NAC (Network Access Control).	Wdrożono
Kopie zapasowe	P1	Procedury tworzenia kopii zapasowych i przywracania danych powinny być zdefiniowane, udokumentowane i jasno powiązane z rolami i obowiązkami.	Wdrożono
Kopie zapasowe	P2	Kopie zapasowe powinny mieć odpowiedni poziom ochrony fizycznej i środowiskowej, zgodny ze standardami stosowanymi w odniesieniu do danych, z których pochodzą.	Wdrożono
Kopie zapasowe	P3	Wykonywanie kopii zapasowych powinno być monitorowane w celu zapewnienia kompletności.	Wdrożono

Kategoria	**ID**	**Opis kategorii**	**Opis stosowanego zabezpieczenia**
Kopie zapasowe	P4	Pełne kopie zapasowe należy wykonywać regularnie.	Wdrożono
Kopie zapasowe	P5	Nośniki kopii zapasowych powinny być regularnie testowane, aby mieć pewność, że można na nich polegać w sytuacjach awaryjnych.	Wdrożono
Kopie zapasowe	P6	Zaplanowane przyrostowe kopie zapasowe należy wykonywać przynajmniej codziennie.	Wdrożono
Kopie zapasowe	P7	Kopie kopii zapasowej powinny być bezpiecznie przechowywane w różnych lokalizacjach.	Wdrożono

Kategoria	**ID**	**Opis kategorii**	**Opis stosowanego zabezpieczenia**
Kopie zapasowe	P8	W przypadku korzystania z usługi innej firmy do przechowywania kopii zapasowych, kopia musi zostać zaszyfrowana przed przesłaniem jej przez administratora danych.	Wdrożono
Kopie zapasowe	**P.9**	Kopie kopii zapasowych powinny być zaszyfrowane i bezpiecznie przechowywane również w trybie offline.	Wdrożono
Bezpieczeństwo w cyklu życia aplikacji	R1	Podczas cyklu życia rozwoju należy przestrzegać najlepszych praktyk, najnowocześniejszych i powszechnie uznanych praktyk, ram i standardów bezpiecznego rozwoju.	Wdrożono
Bezpieczeństwo w cyklu życia aplikacji	R2	Konkretne wymagania dotyczące bezpieczeństwa należy zdefiniować na wczesnych etapach cyklu rozwoju.	Wdrożono

Kategoria	**ID**	**Opis kategorii**	**Opis stosowanego zabezpieczenia**
Bezpieczeństwo w cyklu życia aplikacji	R3	Konkretne technologie i techniki przeznaczone do wspierania prywatności i ochrony danych (zwane również technologiami zwiększającymi prywatność (PET)) powinny być przyjmowane analogicznie do wymogów bezpieczeństwa.	Wdrożono
Bezpieczeństwo w cyklu życia aplikacji	R4	Należy przestrzegać standardów i praktyk bezpiecznego kodowania.	Wdrożono
Bezpieczeństwo w cyklu życia aplikacji	R5	Podczas opracowywania należy przeprowadzić testy i walidację pod kątem wdrożenia wstępnych wymagań bezpieczeństwa.	Wdrożono
Usunięcie / utylizacja danych	S1	Programowe nadpisywanie powinno być wykonywane na wszystkich nośnikach przed ich usunięciem. W przypadkach, gdy nie jest to możliwe (płyty CD, DVD itp.), Należy dokonać fizycznego zniszczenia.	Wdrożono

Kategoria	ID	Opis kategorii	Opis stosowanego zabezpieczenia
Usunięcie / utylizacja danych	S2	Należy przeprowadzić niszczenie papieru i nośników przenośnych służących do przechowywania danych osobowych.	Wdrożono
Usunięcie / utylizacja danych	S3	Przed wyrzuceniem należy wykonać wiele przebiegów nadpisywania w oparciu o oprogramowanie na wszystkich nośnikach.	Wdrożono
Usunięcie / utylizacja danych	S4	Jeśli usługi strony trzeciej są wykorzystywane do bezpiecznego usuwania nośników lub zapisów papierowych, należy zawrzeć umowę o świadczenie usług i sporządzić stosowny protokół zniszczenia zapisów.	Wdrożono
Usunięcie / utylizacja danych	**S.5**	Po usunięciu oprogramowania należ wykonać dodatkowe środki techniczne, takie jak rozmagnesowanie. W zależności od przypadku należy również rozważyć fizyczne zniszczenie.	Wdrożono

Kategoria	**ID**	**Opis kategorii**	**Opis stosowanego zabezpieczenia**
Usunięcie / utylizacja danych	**S.6**	Jeżeli osoba trzecia czyli podmiot przetwarzający dane, jest wykorzystywana do niszczenia nośników lub plików papierowych, należy wziąć pod uwagę, że proces ten odbywa się w siedzibie administratora danych (i unikać przekazywania danych poza lokalizację)	Wdrożono
Bezpieczeństwo fizyczne	T1	Fizyczny obwód infrastruktury systemu IT nie powinien być dostępny dla osób nieupoważnionych.	Wdrożono
Bezpieczeństwo fizyczne	T2	Jasna identyfikacja za pomocą odpowiednich środków, np. W stosownych przypadkach należy założyć identyfikatory dla całego personelu i gości wchodzących na teren organizacji.	Wyłączenie, ze względu na wielkość organizacji
Bezpieczeństwo fizyczne	T4	We wszystkich strefach bezpieczeństwa należy zainstalować systemy wykrywania intruzów.	Wdrożono

Kategoria	**ID**	**Opis kategorii**	**Opis stosowanego zabezpieczenia**
Bezpieczeństwo fizyczne	T5	Tam, gdzie ma to zastosowanie, należy budować bariery fizyczne, aby zapobiec nieuprawnionemu dostępowi fizycznemu.	Wdrożono
Bezpieczeństwo fizyczne	T6	Wolne obszary bezpieczne należy fizycznie zamknąć i okresowo przeglądać	Wdrożono
Bezpieczeństwo fizyczne	T7	W serwerowni należy zaimplementować automatyczny system gaszenia pożaru, dedykowany system klimatyzacji ze sterowaniem zamkniętym oraz zasilacz awaryjny (UPS)	Wdrożono
Bezpieczeństwo fizyczne	T8	Personel serwisowy strony zewnętrznej powinien mieć ograniczony dostęp do bezpiecznych obszarów.	Wdrożono