REGULAMIN BEZPIECZEŃSTWA FIZYCZNEGO I ŚRODOWISKOWEGO

Spis treści:

§ 1.

Organizacja bezpieczeństwa fizycznego i środowiskowego

1. Działaniami w zakresie zapewniania bezpieczeństwa fizycznego i środowiskowego w Agencji bezpośrednio kierują: Administrator Zabezpieczeń Fizycznych w zakresie ochrony osób i mienia oraz administrator obiektu, w zakresie bezpieczeństwa środowiskowego, a w szczególności prawa budowlanego i ochrony przeciwpożarowej.
2. Administrator Zabezpieczeń Fizycznych sprawuje nadzór funkcjonalny nad działaniami realizowanymi przez agencje ochrony zabezpieczające obiekty Agencji.
3. Dyrektor komórki właściwej ds. bezpieczeństwa informacji w Centrali ARiMR a Inspektor Bezpieczeństwa Informacji w Oddziale Regionalnym lub Administrator Zabezpieczeń Fizycznych przynajmniej raz w roku organizuje szkolenie pracowników w zakresie ochrony osób i mienia Agencji.

§ 2.

Podstawowe zasady bezpieczeństwa fizycznego i środowiskowego

1. Środki bezpieczeństwa fizycznego dotyczą:
   1) rozmieszczenia i granic stref bezpieczeństwa,
   2) konstrukcji budowlanych wyznaczających granice stref bezpieczeństwa,
   3) sposobu zabezpieczenia wejścia do obiektu oraz do stref bezpieczeństwa,
   4) stosowania bezpośredniej ochrony fizycznej,
   5) stosowania systemu sygnalizacji napadu i włamania,
   6) stosowania systemu monitoringu wizyjnego,
   7) stosowania mechanicznych zabezpieczeń technicznych,
   8) dostępu do obszarów bezpiecznych oraz wykonywanie prac w obszarach bezpiecznych.
2. Bezpieczeństwo środowiskowe obejmuje:
   1) stosowanie urządzeń ochrony przeciwpożarowej,
   2) zabezpieczenie przed zalaniem wodą,
   3) zapewnienie właściwych warunków pracy w zakresie temperatury i wilgotności powietrza,
   4) stosowanie środków ochrony odgromowej na liniach telekomunikacyjnych,
   5) stosowanie zabezpieczeń przeciwprzepięciowych.
3. Zakres stosowania środków bezpieczeństwa fizycznego i środowiskowego wynika z przeprowadzonego i udokumentowanego szacowania ryzyka.
4. Szacowanie ryzyka i określanie wymagań bezpieczeństwa przeprowadza się w oparciu o:
   1) charakterystykę obiektu i pełnione przez niego funkcje, w szczególności rodzaj umieszczonych w nim zasobów podlegających ochronie (ludzie, dokumentacja, sprzęt komputerowy, itp.),
   2) określenie kategorii potencjalnych zagrożeń obiektu,
   3) opis topografii, konstrukcji obiektu i architektury, najbliższego otoczenia (zabezpieczenia budowlane i mechaniczne, ogrodzenie, bramy, furty, oświetlenie, miejsca do parkowania, drogi komunikacyjne i ewakuacyjne, inne budowle i elementy towarzyszące),
   4) odnotowane w przeszłości czyny przestępcze (rodzaj i typ czynu przestępczego, działania zewnętrzne, wewnętrzne, data, rozmiary, wartość szkody, wynik śledztwa),

5) aktualny stan bezpieczeństwa obiektu,
6) opis i ocenę funkcjonalności i poprawności zainstalowanych technicznych systemów zabezpieczenia, ich poprawności eksploatacji i aktualny stan techniczny (poziom technologiczny, sprawność, dokumentacja, serwisowanie),
7) aktualny stan ochrony fizycznej obiektu,
8) opis stosowanych procedur i rozwiązań organizacyjnych,
9) wnioski co do odpowiedniości (w stosunku do rodzaju i stopnia zagrożeń) kompletności i poprawności zastosowanych zabezpieczeń (mechanicznych, technicznych i proceduralno – organizacyjnych),
10) propozycje doskonalenia systemów oraz procedur ochrony obiektu.

§ 3.

Zapewnianie bezpieczeństwa fizycznego i środowiskowego

1. Dyrektor komórki właściwej ds. bezpieczeństwa informacji, dyrektorzy oddziałów regionalnych, kierownicy biur powiatowych ustalają podział powierzchni biurowych zajmowanych przez komórki i jednostki organizacyjne Agencji na:
   1) strefy administracyjne, do których dostęp posiadają wszyscy pracownicy Agencji,
   2) strefy bezpieczeństwa, do których dostęp jest ograniczony do osób posiadających specjalne prawa dostępu.
   3) strefy obsługi klienta, do której dostęp posiadają beneficjenci ARiMR, goście i inni interesanci.
2. Ochrona stref administracyjnych i stref bezpieczeństwa sprawowana jest na zasadach określonych w:
   1) przepisach o ochronie osób i mienia,
   2) planie ochrony obiektu (jeżeli został opracowany),
   3) niniejszym Regulaminie.
3. Na granicy strefy administracyjnej odbywa się kontrola ruchu osobowego i materiałowego. Wejścia gości do strefy administracyjnej jest rejestrowane. Wzór rejestru wejść stanowi załącznik nr 2 do niniejszego Regulaminu.
4. Strefa bezpieczeństwa powinna być ustalona na obszarze wydzielonym solidnymi konstrukcjami budowlanymi. Za solidne konstrukcje budowlane uznaje się takie, których ściany zewnętrzne i stropy budynków, w których zlokalizowane są strefy bezpieczeństwa, posiadają klasę odporności włamaniowej równoważnej murowi o grubości 25 cm wykonanemu z pełnej cegły. Natomiast pomieszczenia stref bezpieczeństwa powinny mieć ściany o odporności włamaniowej równoważnej murowi o grubości 12,5 cm. Zasady organizacji strefy bezpieczeństwa kancelarii niejawnej w ARiMR określają odrębne regulacje.
5. Wszystkie osoby przebywające w strefie administracyjnej muszą posiadać identyfikatory noszone w widocznym miejscu. Pracownicy Agencji posiadają identyfikatory zawierające: zdjęcie, imię i nazwisko, symbol lub nazwę jednostki organizacyjnej lub komórki organizacyjnej. Goście posiadają identyfikatory z napisem „Gość” i numerem identyfikatora.
6. Goście mogą poruszać się w obrębie strefy administracyjnej wyłącznie w asyście pracownika odpowiedzialnego za ich przyjęcie. Pracownik ten przed wprowadzeniem gości do strefy administracyjnej winien dopilnować pobrania przez nich w strefie obsługi klienta lub na stanowisku recepcyjnym identyfikatorów, o których mowa w ust. 5.

7. W jednostkach organizacyjnych, w których odbywa się masowa obsługa interesantów dopuszcza się wydzielenie z części strefy administracyjnej strefy obsługi klienta, w której goście – interesanci mogą przebywać bez identyfikatorów. Strefa obsługi klienta musi być oddzielona od pozostałych części strefy administracyjnej kontrolowanymi przejściami.
8. W przypadku stosowania systemu kontroli dostępu musi być to system z klasą dostępu B. Dla stref administracyjnych i bezpieczeństwa wymagana jest klasa rozpoznania 2 na wejściu i klasa rozpoznania 0 na wyjściu.
9. Klasa dostępu B oznacza, że w systemie możliwe jest przyznawanie dostępu w określonych godzinach oraz, że transakcje uzyskania dostępu są rejestrowane. Klasa rozpoznania 0 oznacza, że dostęp uzyskiwany jest bez sprawdzania tożsamości (np. wyjście po naciśnięciu przycisku). Klasa rozpoznania 2 oznacza, że dostęp uzyskiwany jest po sprawdzeniu tożsamości na podstawie danych zawartych na identyfikatorze lub na podstawie danych biometrycznych. (Według Polskiej Normy PN-EN 50133-1 - „Systemy alarmowe. Systemy kontroli dostępu. Wymagania systemowe").
10. Wszystkie drzwi z kontrolą dostępu muszą być zaopatrzone w urządzenia samozamykające.
11. Kontrolę ruchu osobowego i materiałowego na granicy strefy administracyjnej może sprawować pracownik ze strefy obsługi klienta lub stanowiska recepcyjnego, który wydaje identyfikatory gościom.
12. Pomieszczenia biurowe w strefie administracyjnej posiadają zamki klasy 0. Pomieszczenia w strefach bezpieczeństwa powinny posiadać zamki klasy C lub klasy 7 zabezpieczenia (wg normy PN-EN 12209:2005) oraz drzwi antywłamaniowe klasy C (wg normy PN-EN 14351-1) lub drzwi o odporności co najmniej klasy 4 (wg normy PN-EN 1627:2011), z odpornością ogniową co najmniej 60 minut.
13. Wejście oraz wyjście ze stref bezpieczeństwa jest rejestrowane. Rejestruje się tożsamość osób, cel pobytu oraz czas ich wejścia i wyjścia. Wzór rejestru stanowi załącznik nr 1 do niniejszego Regulaminu.

§ 4.

Zarządzanie kluczami

1. Klucze od pomieszczeń przechowywane są u ochrony obiektu, z tym, że klucze do pomieszczeń w strefach bezpieczeństwa muszą być zdawane na przechowanie w zaplombowanych pojemnikach.
2. Jeżeli obiekt nie posiada stałej ochrony po godzinach pracy, to klucze od pomieszczeń biurowych muszą być zdawane przez wyznaczonych pracowników Agencji w zaplombowanej kasecie pracownikowi firmy realizującej ochronę obiektu na zasadzie monitoringu, a następnego dnia roboczego pobierane z tej firmy. Przyjęcie kluczy przez pracownika firmy sprawującej monitoring jest równoznaczne z przyjęciem obiektu pod ochronę. Szczegółowe zasady takiej procedury określa umowa pomiędzy Agencją a firmą sprawującą ochronę. W przypadku braku możliwości obecności pracownika firmy monitorującej, klucze muszą być zdawane wyznaczonemu pracownikowi Agencji w celu zabezpieczenia ich w zaplombowanej kasetce, a następnego dnia roboczego pracownik ten zobowiązany jest wydać klucze upoważnionym pracownikom. Dopuszcza się, w biurach powiatowych Agencji, trwałe wydanie kluczy zewnętrznych do obiektu osobom funkcyjnym posiadającym indywidualny kod dostępu do Systemu Sygnalizacji Włamania i Napadu (SSWiN), w takim przypadku jeden z kluczy musi być zdeponowany w jednostce monitorującej obiekt, klucze

wewnętrzne mogą być przechowywane w skrytce wewnątrz obiektu, osoba otwierająca obiekt odpowiedzialna jest za wydanie kluczy, osoba zamykająca obiekt odpowiedzialna jest za przyjęcie do skrytki wszystkich kluczy wewnętrznych.

3. Klucze wydaje się na podstawie rejestru osób upoważnionych do ich pobierania. Fakt wydania kluczy i przyjęcia ich na przechowanie musi być odnotowany. Rejestr wydawania i zdawania kluczy prowadzony jest w formie papierowej w książce wydawania kluczy lub w formie elektronicznej w dedykowanym systemie elektromechanicznego depozytora kluczy. Wzór książki wydawania i zdawania kluczy stosowany w jednostce organizacyjnej określa Administrator Zabezpieczeń Fizycznych danej jednostki w porozumieniu z Inspektorem Bezpieczeństwa Informacji. Prowadzony rejestr musi określać:
   - nr pomieszczenia / nr klucza,
   - dokładną godzinę pobrania / zdania,
   - imię i nazwisko osoby pobierającej / zdającej bądź jej identyfikator (w systemie elektronicznego depozytora),
   - czytelny podpis osoby pobierającej / zdającej oraz przyjmującej klucz na przechowanie (w przypadku rejestru w formie papierowej).
4. Za przyznanie i odebranie prawa do pobierania kluczy do konkretnego pomieszczenia odpowiedzialny jest:
   1) w Centrali – dyrektor komórki organizacyjnej, któremu podlega dane pomieszczenie,
   2) w oddziale regionalnym – kierownicy biur w stosunku do pomieszczeń zajmowanych przez pracowników biura lub kierownik biura oddziału regionalnego w stosunku do pozostałych pomieszczeń oddziału,
   3) w biurze powiatowym – kierownik biura powiatowego.
5. Za organizację wydawania kluczy do pomieszczeń odpowiada administrator obiektu lub Administrator Zabezpieczeń Fizycznych. Organizacja wydawania kluczy musi być uzgodniona z:
   1) w Centrali Agencji - dyrektorem komórki właściwej ds. bezpieczeństwa informacji,
   2) w oddziale regionalnym i biurach powiatowych - Inspektorem Bezpieczeństwa Informacji.
6. Klucze do szaf i mebli biurowych, w których przechowywane są dokumenty zawierające informacje wrażliwe, nie mogą po zakończeniu pracy pozostawać w zamkach. Za organizację przechowywania takich kluczy odpowiada Administrator Zabezpieczeń Fizycznych, w uzgodnieniu z:
   1) w Centrali Agencji – dyrektorem komórki organizacyjnej, któremu podlega pomieszczenie z szafami i meblami biurowymi zawierającymi informacje wrażliwe,
   2) w oddziale regionalnym i biurze powiatowym – kierownikiem komórki organizacyjnej, któremu podlega pomieszczenie z szafami i meblami biurowymi zawierającymi informacje wrażliwe.
7. Zasady organizacji przechowywania kluczy do szaf, sejfów i mebli biurowych, w których przechowuje się informacje niejawne określają odrębne regulacje.

§ 5.

Zarządzanie uprawnieniami w systemie kontroli dostępu

1. W przypadku zastosowania systemu kontroli dostępu uprawnienia są jednoznacznie powiązane z urządzeniami aktywującymi przejście, które pełnią także role identyfikatorów.

2. Wstęp do poszczególnych stref, o których mowa w § 3 ust. 1 jest ograniczony tylko do tych osób, które uzyskały stosowne uprawnienia.
3. Uprawnienia przyznawane są zgodne z profilem dostępu (zakresem odpowiedzialności i uprawnień) na danym stanowisku pracy. Uprawnienia dostępu są nadawane wyłącznie w zakresie wynikającym z zajmowanego stanowiska i potrzebą wykonywania obowiązków służbowych na danym stanowisku pracy. Bezzasadne nadawanie uprawnień do pomieszczeń będzie kwalifikowane jako incydent związany z naruszeniem bezpieczeństwa informacji.
4. Za przyznawanie, zmianę oraz odbieranie uprawnień dostępu do stref bezpieczeństwa odpowiedzialny jest:
   1) w Centrali Agencji - dyrektor komórki organizacyjnej, któremu podlega dane pomieszczenie,
   2) w oddziale regionalnym i biurze powiatowym - kierownik biura oddziału regionalnego w stosunku do pomieszczeń oddziału regionalnego lub kierownik biura powiatowego w stosunku do pomieszczeń tego biura.
5. Przyznawanie, zmiana oraz odbieranie uprawnień jest realizowane w systemie kontroli dostępu przez Administratora Zabezpieczeń Fizycznych.
6. Administrator Zabezpieczeń Fizycznych jest obowiązany bezzwłocznie zablokować uprawnienia dostępu w przypadku:
   1) zgłoszenia przez pracownika Agencji utraty lub podejrzenia utraty urządzenia aktywującego przejście,
   2) zgłoszenia telefonicznego, za pośrednictwem faksu lub poczty elektronicznej, potwierdzonego bezzwłocznie pisemnym wnioskiem bezpośredniego przełożonego pracownika.
7. Ponowne nadanie uprawnień dostępu w przypadku zaistnienia okoliczności opisanych w ust. 6 pkt 1) odbywa się zgodnie z zasadami określonymi w ust. 4 i 5.
8. Uprawnienia dostępu są regularnie przeglądane zgodnie z zasadami opisanymi w Regulaminie nadzoru.

§ 6.

Pomieszczenia i zasoby chronione

1. Wnoszenie i wynoszenie do i ze stref bezpieczeństwa komputerowych nośników danych może mieć miejsce tylko w przypadkach wynikających z procedur eksploatacji zainstalowanego tam sprzętu teleinformatycznego.
2. Strefy bezpieczeństwa powinny być chronione systemem sygnalizacji włamania i napadu.
3. W uzasadnionych przypadkach, zarówno strefy administracyjne jak i strefy bezpieczeństwa, powinny być poddane monitoringowi wizyjnemu.
4. Strefy bezpieczeństwa nie posiadają oznakowania wewnątrz lub na zewnątrz, które wskazywałyby na to, że znajdują się w nich szczególnie chronione zasoby.
5. W strefach bezpieczeństwa dopuszcza się przebywanie osób bez uprawnień dostępu do tych stref tylko w wyjątkowych przypadkach, za zezwoleniem:
   1) dla pomieszczeń BP - kierownika biura powiatowego,
   2) dla pomieszczeń OR - kierownika Biura OR,
   3) dla pomieszczeń Centrali:

a) dyrektora komórki właściwej ds. informatyki dla pomieszczeń serwerowni, węzłów teletechnicznych i biblioteki kodów źródłowych,

b) dyrektora komórki właściwej ds. organizacyjno-gospodarczych dla pomieszczeń archiwum zakładowego,

c) Pełnomocnika ds. Ochrony Informacji Niejawnych w przypadku strefy bezpieczeństwa, w której przetwarzane są informacje niejawne.

6. Pobyt osoby, która nie posiada uprawnień do przebywania w strefie bezpieczeństwa jest rejestrowany. Za prowadzenie rejestru odpowiedzialne są osoby wskazane w ust. 5, a wpisy dokonywane są pod nadzorem osoby uprawnionej do przebywania w danej strefie.
7. Serwery, aktywne i pasywne urządzenia sieci teleinformatycznej, centrale telefoniczne i archiwa muszą być umieszczone w strefach bezpieczeństwa.
8. Zasoby, którym nadano status zasobu kluczowego podlegają szczególnej ochronie i są dodatkowo zabezpieczane przed pożarem i zalaniem.
9. Rozmieszczenie sprzętu służącego do przetwarzania informacji, zarówno w obszarach bezpiecznych, jak i w pozostałych pomieszczeniach, poprzedzone jest udokumentowanym szacowaniem ryzyk związanych z systemami zabezpieczeń technicznych oraz systemami wspomagającymi (wentylacyjno-klimatyzacyjnymi, zasilającymi, wodno-kanalizacyjnymi, grzewczymi).

§ 7.

Bezpieczeństwo środowiskowe

1. Przy planowaniu zabezpieczeń technicznych i organizacyjnych, ich rodzaju i siły, bierze się pod uwagę ryzyka związane z występującymi lokalnie zagrożeniami, takimi jak pożar, zalanie, trzęsienie ziemi, wybuch, wyładowania atmosferyczne, niepokoje społeczne i inne formy naturalnych lub spowodowanych przez działania umyślne bądź błędy człowieka katastrof. Ponadto analizie jest poddawany wpływ sąsiedztwa innych obiektów lub lokalnych instalacji i dróg (np. pożar w sąsiednim budynku, woda przeciekająca przez dach, powódź, bliska katastrofa komunikacyjna, eksplozja, zamieszki uliczne).
2. Pomieszczenia, w których zlokalizowane są zasoby kluczowe, wyposaża się w:
   1) system sygnalizujący wystąpienie pożaru,
   2) system klimatyzacji w serwerowniach.
3. Nie prowadzi się instalacji wodnych przez pomieszczenia, w których zlokalizowane są zasoby kluczowe do przetwarzania informacji (serwery, centra danych).
4. Urządzenia zapewniające bezpieczeństwo środowiskowe poddawane są regularnej kontroli zgodnie z obowiązującymi przepisami prawa, normami oraz zaleceniami producentów.
5. Na wypadek zagrożenia pożarem dla każdej z lokalizacji jednostek organizacyjnych Agencji opracowuje się instrukcje przeciwpożarowe. Ciągi komunikacyjne obiektów muszą być zaopatrzone w tabliczki informujące o kierunku ewakuacji i w miarę potrzeby wyposażone w oświetlenie awaryjne.
6. W przypadku, jeśli któreś z wymagań w zakresie bezpieczeństwa środowiskowego nie może być z przyczyn obiektywnych spełnione, Administrator Zabezpieczeń Fizycznych sporządza protokół opisujący: rodzaj odstępstwa, ryzyko wynikające z odstępstwa, zastosowane środki ochrony doraźnej lub zamiennej, plan dojścia do rozwiązania docelowego.

7. Parametry środowiska, w którym pracuje sprzęt systemu teleinformatycznego zaliczany do zasobów kluczowych, tj. temperatura, jest monitorowana w celu natychmiastowego wykrycia odchyleń, które mogłyby mieć negatywne skutki dla tego sprzętu.
8. Budynek, w którym znajdują się systemy teleinformatyczne wskazane w ust. 7 wyposażony jest, zgodnie z przepisami ppoż., w samoczynnie załączające się oświetlenie awaryjne (bezpieczeństwa i ewakuacyjne).
9. Oświetlenie bezpieczeństwa stosowane jest w pomieszczeniach, w których nawet krótkotrwałe wyłączenie oświetlenia podstawowego może spowodować zagrożenie zdrowia i życia podczas ewakuacji.
10. W przypadku, gdy oświetlenie bezpieczeństwa działa, co najmniej przez 2 godziny, nie ma potrzeby stosowania oświetlenia ewakuacyjnego.

§ 8.

Wymagania dla systemów wspomagających

1. Jeżeli jest to możliwe, należy projektować nadmiarową, modułową klimatyzację tak, aby w przypadku awarii lub przeglądu serwisowego jednego modułu pozostałe były w stanie zapewnić wymagane parametry środowiskowe, w szczególności środowiska eksploatacyjnego w serwerowniach.
2. Rozmieszczenie w obiekcie kanałów oraz czerpni należy zaprojektować uwzględniając ryzyko takich zdarzeń, jak przedostanie się przez nie do pomieszczeń chronionych wody, środków niebezpiecznych czy też zwierząt.
3. W przypadku prowadzenia instalacji wodno-kanalizacyjnych i grzewczych w sąsiedztwie (również nad lub bezpośrednio pod pomieszczeniem) serwerowni i pomieszczeń, w których usytuowano infrastrukturę techniczną służącą do przetwarzania w krytycznych systemach Agencji, należy wdrożyć systemy zapewniające wykrycie i alarmowanie w przypadku zalania pomieszczenia oraz zainstalować środki umożliwiające szybkie usunięcie wody (cieczy).
4. Przy ocenie sprawności instalacji wodno – kanalizacyjnej i grzewczej należy uwzględnić jej współdziałanie z innymi systemami wspomagającymi, takimi jak system klimatyzacyjno - wentylacyjny oraz w szczególności system przeciwpożarowy.

§ 9.

Eksploatacja technicznych systemów zabezpieczeń oraz systemów wspomagających

1. Systemy zabezpieczenia technicznego Agencji muszą spełniać następujące funkcje:
   1) zabezpieczenia budowlane i zabezpieczenia mechaniczne muszą zagwarantować uniemożliwienie dostępu osobom niepowołanym do chronionych pomieszczeń i urządzeń oraz zabezpieczyć osoby i mienie przed potencjalnymi zagrożeniami,
   2) system sygnalizacji napadu i włamania (SSWiN) musi zapewnić skuteczne przekazanie sygnału o realnym zagrożeniu do wskazanych osób, miejsc i urządzeń,
   3) system monitorowania w przypadku wystąpienia alarmu musi zapewnić podjęcie odpowiednich działań stosownych do zaistniałego zdarzenia,

4) system monitoringu (CCTV) musi zapewnić, poprzez rozmieszczone kamery, rozpoznanie rodzaju zagrożenia i śledzenie rozwoju sytuacji, prowadzenie obserwacji obrazu z kilku kamer oraz automatyczną jednoczesną rejestrację tych obrazów,
5) system kontroli dostępu (SKD) musi zabezpieczyć chronione pomieszczenie (grupę pomieszczeń) lub wydzieloną strefę przed dostępem do nich osób nieuprawnionych.

2. Wszystkie systemy zabezpieczeń podlegają regularnym przeglądom dokonywanym przez Administratora Zabezpieczeń Fizycznych lub pod jego nadzorem przez osoby posiadające odpowiednie uprawnienia. Przegląd polega na sprawdzeniu poprawności działania danego systemu zgodnie z dokumentacją techniczno-eksploatacyjną systemu. Przeglądy każdego systemu zabezpieczeń wykonywane są zgodnie z harmonogramem ustalonym przez Administratora Zabezpieczeń Fizycznych w porozumieniu z:
   1) w Centrali Agencji - dyrektorem komórki właściwej ds. bezpieczeństwa,
   2) w oddziale regionalnym i biurach powiatowych - Inspektorem Bezpieczeństwa Informacji.
3. Przeglądy dokonywane przez Administratora Zabezpieczeń Fizycznych co 6 miesięcy obejmują dodatkowo sprawdzenie stanu technicznego nośników elektronicznych SKD (identyfikatorów) przeznaczonych dla gości, jeśli mają zastosowanie w danej jednostce organizacyjnej.
4. Przeglądy systemów zabezpieczeń poza ustalonym harmonogramem przeprowadzane są każdorazowo w przypadku wystąpienia incydentów zagrażających lub mogących powodować zagrożenie dla bezpieczeństwa osób i mienia (np. katastrofa budowlana w sąsiedztwie obiektu, tąpnięcie, kolizja drogowa powodująca szczególne zagrożenie w pobliżu budynku, pożar, roboty budowlane w sąsiednich budynkach, ewakuacja osób i mienia z budynku, interwencja służb ratunkowych mająca wpływ na stan techniczny obiektu, wystąpienie anomalii pogodowych, itp.).
5. Administrator Zabezpieczeń Fizycznych odnotowuje przeprowadzenie przeglądu w dzienniku przeglądów prowadzonym dla każdego z funkcjonujących w Agencji systemów zabezpieczeń. Dziennik przeglądu zawiera następujące informacje:
   1) datę i czas przeglądu,
   2) dane personalne wykonującego przegląd,
   3) wynik przeglądu,
   4) dane personalne osoby nadzorującej/kontrolującej,
   5) uwagi z przeglądu.

   Dopuszcza się prowadzenie dziennika w systemie elektronicznym lub wersji elektronicznej umieszczonej na serwerze plików (fileserver).
6. Administrator Zabezpieczeń Fizycznych nadzoruje i dokumentuje bieżące prace konserwacyjne, w tym wymianę lub prostą naprawę elementów każdego z systemów zabezpieczeń, które nie wymagają posiadania stosownych uprawnień specjalistycznych. Pozostałe prace konserwacyjne wykonują pracownicy podmiotów zewnętrznych posiadający stosowne uprawnienia. Prace konserwacyjne polegają na wykonaniu niezbędnych czynności mających na celu utrzymanie systemu w sprawności techniczno-użytkowej zgodnie z dokumentacją techniczno-eksploatacyjną systemu. Prace konserwacyjne dla wszystkich systemów zabezpieczenia przeprowadzane są nie rzadziej niż raz na 12 miesięcy.
7. Administrator Zabezpieczeń Fizycznych nadzoruje i dokumentuje prace serwisowe przeprowadzane przez uprawnionych pracowników podmiotów zewnętrznych. Prace serwisowe

polegają na wykonaniu niezbędnych czynności mających na celu przywrócenie sprawności techniczno-użytkowej systemu zgodnie z dokumentacją techniczno-eksploatacyjną systemu.

8. Wymiany lub naprawy o wysokim poziomie technologicznym dokonuje podmiot zewnętrzny posiadający stosowne uprawnienia producenta, dystrybutora wyrobu lub specjalistyczne urządzenia do naprawy lub wymiany.
9. Dla każdego systemu alarmowego oraz dla każdego innego systemu technicznego zabezpieczeń funkcjonującego w Agencji jest założony dziennik/system rejestrowania zawierający:
   1) rejestr wyposażenia,
   2) rejestr zdarzeń,
   3) rejestr prac konserwacyjnych,
   4) rejestr prac serwisowych.

§ 10.

Eksploatacja zabezpieczeń mechanicznych

1. Do zabezpieczeń mechanicznych zalicza się: kraty, żaluzje, okiennice, folie antywłamaniowe, zamki w drzwiach (w szczególności te, do których bezpośredni dostęp mają osoby postronne), inne zabezpieczenia otworów okiennych, włazów, kanałów wentylacyjnych, rygle, kłódki, zamki, zasuwy z blokadą mechaniczną.
2. Zabezpieczenia mechaniczne muszą być zamontowane przez uprawniony podmiot zgodnie z warunkami technicznymi wynikającymi z certyfikatu lub aprobaty technicznej.
3. Zabezpieczenia mechaniczne podlegają przeglądom przeprowadzanym przez Administratora Zabezpieczeń Fizycznych, zgodnie z harmonogramem - dotyczy tylko tych zabezpieczeń, które są dostępne dla osób postronnych i nie ma możliwości realizacji nadzoru przez inne systemy zabezpieczeń. Harmonogram przeglądów jest ustalany przez Administratora Zabezpieczeń Fizycznych w porozumieniu z:
   1) w Centrali Agencji - dyrektorem komórki właściwej ds. bezpieczeństwa,
   2) w oddziale regionalnym i biurach powiatowych – osobami pełniącymi funkcję Inspektora Bezpieczeństwa Informacji.
4. Przeglądy polegają na sprawdzeniu stanu technicznego elementów zabezpieczenia mechanicznego, przeprowadzanych w następujący sposób:
   1) w przypadku krat, żaluzji, okiennic i innych zabezpieczeń otworów okiennych, włazów, kanałów wentylacyjnych:
      a) sprawdzenie mocowań do murów (np. poprzez poruszenie elementów zabezpieczenia w pionie i poziomie i obserwacji reakcji elementów mocujących),
      b) sprawdzenie istnienia odkształceń mechanicznych na poszczególnych elementach, przy zastosowaniu metody porównawczej z opisem w dokumentacji technicznej,
      c) sprawdzenie występowania śladów po próbach penetracji lub usunięcia zabezpieczenia np. w postaci opiłków, śladów tynku, rysach na elementach zabezpieczeń, itp.,
      d) sprawdzić stan powłok lakierniczych i zabezpieczeń antykorozyjnych elementów narażonych na bezpośrednie działanie czynników atmosferycznych lub innych szkodliwych czynników dla mechanizmów kłódek, zamków, rygli (szczególnie kurz, pył),

2) w przypadku kłódek i zamków - sprawdzenie działania kluczy zapasowych oraz mechanizmu ryglującego przez otwarcie i zamknięcie kłódek i zamków, przegród mechanicznych i budowlanych,

3) w przypadku rygli i zasuw z blokadą mechaniczną - porównanie położenia elementów ruchomych z opisem w dokumentacji technicznej.

5. Przynajmniej dwa razy do roku Administrator Zabezpieczeń Fizycznych dokonuje oceny stanu powłoki lakierniczej, śladów korozji elementów narażonych na bezpośrednie działanie czynników atmosferycznych lub innych szkodliwych czynników dla mechanizmów.
6. Wycofane z użycia elementy zabezpieczeń mechanicznych zawierające informacje o kodzie zamków (klucze, wkładki, karty elektroniczne) niszczone są mechanicznie.
7. Zakup zamków (mechanizmów zamkowych) i wkładek dokonywany jest w sposób określany jako „zakup z półki".
8. Dla stref bezpieczeństwa każda faza procesu wymiany mechanizmów zamkowych, w tym zakup i transport, montaż zamków (mechanizmów zamkowych) i wkładek wykonywany jest co najmniej przez dwie osoby (w tym przez Administratora Zabezpieczeń Fizycznych sprawującego bezpośredni nadzór).
9. Wycofanie elementu zabezpieczenia mechanicznego przeprowadza się po uzyskaniu informacji od dystrybutora/producenta wyrobu o konieczności jego wymiany lub po uzyskaniu informacji o pojawieniu się metod/narzędzi powodujących przełamanie zabezpieczenia lub obniżenie jego właściwości.
10. Z zastrzeżeniem ust. 8, koniec okresu ważności certyfikatu lub świadectwa kwalifikacyjnego nie stanowi przyczyny demontażu elementu zabezpieczenia.

§ 11.

Eksploatacja zabezpieczeń techniczno-budowlanych

1. Do zabezpieczeń techniczno-budowlanych zalicza się drzwi, śluzy, ściany, stropy, ogrodzenia (wykonane z różnych materiałów), furtki, bramy, zapory, szlabany, kołowroty (w szczególności te, do których bezpośrednio dostęp mają osoby postronne).
2. Zabezpieczenia techniczno-budowlane podlegają przeglądowi przeprowadzanym przez Administratora Zabezpieczeń Fizycznych, zgodnie z harmonogramem - dotyczy tylko tych zabezpieczeń, które są dostępne dla osób postronnych i nie ma możliwości realizacji nadzoru przez inne systemy zabezpieczeń. Harmonogram przeglądów jest ustalany przez Administratora Zabezpieczeń Fizycznych w porozumieniu z:
    1) w Centrali Agencji - dyrektorem komórki właściwej ds. bezpieczeństwa,
    2) w oddziale regionalnym i biurach powiatowych – osobami pełniącymi funkcję Inspektora Bezpieczeństwa Informacji.
3. Przeglądy polegają na sprawdzeniu stanu technicznego elementów zabezpieczeń techniczno-budowlanych, przeprowadzanych w następujący sposób:
    1) sprawdzenie mocowań elementów ruchomych i elementów umocowanych na stałe do podłoża (np. poprzez poruszenie elementów konstrukcji zabezpieczenia i obserwacji reakcji elementów mocujących),
    2) sprawdzenie istnienia odkształceń mechanicznych na poszczególnych elementach, przy zastosowaniu metody porównawczej z opisem w dokumentacji technicznej,

3) sprawdzenie występowania śladów po próbach penetracji lub usunięcia zabezpieczenia np. w postaci opiłków, śladów tynku, rysach na elementach zabezpieczeń, rdzy, itp.,
4) sprawdzenie mechanizmów ryglowych (zamków, rygli, itp.),
5) porównanie położenia elementów ruchomych z opisem w dokumentacji technicznej.

4. Przynajmniej dwa razy do roku Administrator Zabezpieczeń Fizycznych dokonuje oceny stanu powłoki lakierniczej, śladów korozji elementów zabezpieczeń techniczno-budowlanych narażonych na bezpośrednie działanie czynników atmosferycznych lub innych czynników środowiskowych.
5. Wymiana/naprawa zabezpieczeń dokonywana jest pod nadzorem administratora obiektu w porozumieniu z Administratorem Zabezpieczeń Fizycznych.

§ 12.

Eksploatacja systemów okablowania zasilającego i teleinformatycznego w zakresie konstrukcyjno-mechanicznym

1. W skład systemów okablowania w zakresie konstrukcyjno-mechanicznym wchodzą: trakty kablowe (listwy PCV, szyny, rury, przepusty), osłony włazów i studzienek, szafy dystrybucyjne, tablice, krosownice.
2. Systemy okablowania znajdujące się w obszarze dostępnym publicznie podlegają przeglądom przeprowadzanym przez Administratora Zabezpieczeń Fizycznych oraz Administratora Systemu. Harmonogram przeglądów jest ustalany przez Administratora Zabezpieczeń Fizycznych w porozumieniu z:
   1) w Centrali Agencji - dyrektorem komórki właściwej ds. bezpieczeństwa,
   2) w oddziale regionalnym i biurach powiatowych – osobami pełniącymi funkcję Inspektora Bezpieczeństwa Informacji.
3. Przeglądy polegają na sprawdzeniu stanu technicznego (konstrukcyjno-mechanicznego) elementów systemu okablowania z dokumentacją techniczną.
4. Przeglądy zabezpieczeń elektronicznych systemów okablowania polegają na sprawdzeniu poprawności funkcjonowania np. systemów sygnalizacji włamania zastosowanych do zabezpieczenia szaf dystrybucyjnych, krosownic lub innych zabezpieczeń.
5. Przeglądy przeprowadzane lub nadzorowane przez Administratora Zabezpieczeń Fizycznych powinny obejmować sprawdzenie:
   1) ciągłości struktury (mocowanie listew) traktów kablowych w miejscach ogólnie dostępnych – np. narażonych na uszkodzenia mechaniczne spowodowane przez przenoszenie przedmiotów o dużych gabarytach (biurko, szafa), ruch osobowy,
   2) stanu powłoki lakierniczej, śladów korozji elementów narażonych na bezpośrednie działanie czynników atmosferycznych lub innych szkodliwych czynników dla obudów, osłon lub innych zabezpieczeń systemów okablowania,
   3) czy występują ślady po próbach penetracji lub usunięcia zabezpieczenia, np. w postaci opiłków, śladów tynku, rysach na elementach zabezpieczeń, itp.
6. Przeglądy prowadzone lub nadzorowane przez Administratora Systemu powinny obejmować sprawdzenie:

1) przestrzegania zasad ochrony okablowania oraz punktów połączeń okablowania (inspekcja pod kątem podłączonych nieautoryzowanych urządzeń przechwytujących, rejestrujących, transmitujących i zniekształcających sygnał transmisyjny),
2) zamknięcia szaf, tablic, osłon włazów i studzienek należących do Agencji,
3) zgodności stanu faktycznego z dokumentacją techniczną okablowania,
4) stanu technicznego instalacji poprzez wykonanie pomiarów okablowania.

§ 13.

Eksploatacja elektronicznych systemów zabezpieczeń

1. Do elektronicznych systemów zabezpieczeń zalicza się systemy sygnalizacji włamania i napadu (SSWiN), systemy kontroli dostępu (SKD), systemy telewizji dozorowej (CCTV) oraz inne systemy współdziałające z elektronicznymi systemami zabezpieczeniowymi, np. system oświetlenia podczerwienią dla systemu CCTV.
2. Elektroniczne systemy zabezpieczeniowe i systemy współdziałające podlegają przeglądom przeprowadzanym przez Administratora Zabezpieczeń Fizycznych zgodnie z harmonogramem i zakresem konserwacji systemu przeprowadzanej przez pracownika podmiotu zewnętrznego, posiadającego licencję pracownika zabezpieczenia technicznego.
3. Przeglądy SSWiN są przeprowadzane przez Administratora Zabezpieczeń Fizycznych i obejmują, w zależności od zastosowanego rozwiązania technicznego, sprawdzenie:
   1) trybu pracy urządzeń wg wskazań paneli sterujących poprzez porównanie z dokumentacją techniczno-eksploatacyjną systemu,
   2) działania przycisków sygnalizacji napadu/przycisków wezwania pomocy,
   3) działania poszczególnych klawiatur strefowych poprzez załączanie i rozłączanie systemu wprowadzając odpowiedni kod,
   4) ilości i rozmieszczenia klawiatur strefowych zgodnie z danymi w dzienniku systemu.
4. Czynności konserwacyjne dokonywane przez pracownika podmiotu zewnętrznego są przeprowadzane nie rzadziej niż raz na 12 miesięcy i obejmują:
   1) sprawdzenie prawidłowości funkcjonowania systemu SSWiN w zakresie określonym w dokumentacji technicznej,
   2) sprawdzenie ciągłości działania zasilania podstawowego i sprawności zasilania awaryjnego; (wymiana akumulatorów zgodnie z harmonogramem załączonym do dokumentacji technicznej systemu),
   3) sprawdzenie poprawności działania akustycznych lub optycznych sygnalizatorów alarmowych,
   4) sprawdzenie czujników systemu,
   5) sprawdzenie mocowania czujek do podłoża (uchwytów, ścian); szczególnie dotyczy to stref ogólnego i ograniczonego dostępu oraz znajdujących się poza pomieszczeniami Agencji (płaszczyzna ścian, ogrodzenia).
5. Przeglądy SKD są przeprowadzane przez Administratora Zabezpieczeń Fizycznych i obejmują, w zależności od zastosowanego rozwiązania technicznego, sprawdzenie:
   1) trybu pracy urządzeń wg wskazań paneli sterujących bądź aplikacji zarządzającej, poprzez porównanie z dokumentacją systemu,
   2) działania przycisków otwierających wyjścia z czytnikami działającymi jednostronnie, w tym działania przycisków ewakuacyjnych w przypadku, gdy SKD nie współpracuje z systemem ppoż.,

3) działania czytników systemu z odpowiednią kartą dostępu,
4) mocowania czytników, samozamykaczy, zamków elektromagnetycznych drzwi i przejść, w tym istnienia śladów prób penetracji (rysy, wgniecenia, próby podważania, demontażu),
5) ilości i rozmieszczenia czytników zgodnie z danymi w dzienniku systemu,
6) limitu użytkowników systemu.

6. Przeglądy dokonywane przez Administratora Zabezpieczeń Fizycznych co 6 miesięcy obejmują dodatkowo sprawdzenie stanu technicznego nośników elektronicznych SKD (identyfikatorów) przeznaczonych dla gości, jeśli mają zastosowanie w danej jednostce organizacyjnej.

7. Czynności konserwacyjne dokonywane przez pracownika podmiotu zewnętrznego są przeprowadzane nie rzadziej niż raz na 12 miesięcy i obejmują sprawdzenie:

1) prawidłowości funkcjonowania systemu SKD w zakresie określonym w dokumentacji technicznej,
2) ciągłości działania zasilania podstawowego i sprawności zasilania awaryjnego, w tym wymiana akumulatorów zgodnie z harmonogramem załączonym do dokumentacji technicznej systemu,
3) działania części elektromechanicznych (elektrozaczepów, trzymaczy elektromagnetycznych, śluz, tripodów itp.).

8. Przeglądy CCTV są przeprowadzane przez Administratora Zabezpieczeń Fizycznych i obejmują sprawdzenie:

1) trybu pracy urządzeń rejestrujących poprzez porównanie z dokumentacją techniczno-eksploatacyjną na podstawie wskazań paneli sterujących informujących o trybie pracy urządzeń,
2) jakości obrazu i pola obserwacji na monitorach poprzez porównanie z opisem oraz zdjęciem obrazu wykonanym w trybie dziennym i nocnym,
3) wymiany nośników w urządzeniu rejestrującym zgodnie z dokumentacją techniczną systemu,
4) poprawności pracy urządzeń rejestrujących poprzez nagranie i odtworzenie przebiegu zdarzeń w trybie czasu rzeczywistego oraz losowo wybranego zdarzenia w czasie przeszłym.

9. Czynności konserwacyjne dokonywane przez pracownika podmiotu zewnętrznego są przeprowadzane nie rzadziej niż raz na 12 miesięcy i obejmują:

1) sprawdzenie ciągłości działania zasilania podstawowego i sprawności zasilania awaryjnego,
2) wyłączenie monitora i sprawdzenie „poświaty” (efekt „wypalania się” kineskopu objawiający się „pozostawaniem” obrazu na ekranie po odłączeniu źródła sygnału),
3) sprawdzenie jakości zarejestrowanego obrazu z kamer rejestrujących punkty newralgiczne (szczególnie z kamer zewnętrznych, rejestracja wykonana w godzinach nocnych),
4) sprawdzenie zapisu z wewnętrznych pamięci kamer (jeśli kamery posiadają taką pamięć),
5) sprawdzenie mocowania kamer zewnętrznych, jeśli są narażone na działania czynników atmosferycznych i innych np. konary drzew,
6) sprawdzenie działania wycieraczek, obwodów, grzałek (elementy przeciwśnieżne, jeśli zostały zainstalowane),
7) sprawdzenie działania głowic obrotowych i funkcji „zoom” (optyczny i elektroniczny),
8) sprawdzenie mocowania reflektorów podczerwieni i oświetlenia sztucznego związanego z CCTV (np. halogeny włączane automatycznie – z czasowym wyłącznikiem).

§ 14.

Systemy wspomagające oświetlenie

1. Przeglądy systemu są przeprowadzane przez Administratora Zabezpieczeń Fizycznych zgodnie z harmonogramem i obejmują sprawdzenie systemów sterujących (włączających i wyłączających oświetlenie). Harmonogram przeglądów jest ustalany przez Administratora Zabezpieczeń Fizycznych w porozumieniu z:
   1) w Centrali Agencji - dyrektorem komórki właściwej ds. bezpieczeństwa,
   2) w oddziale regionalnym i biurach powiatowych – osobami pełniącymi funkcję Inspektora Bezpieczeństwa Informacji.
2. Czynności konserwacyjne dokonywane przez pracownika podmiotu zewnętrznego są przeprowadzane nie rzadziej niż raz na 12 miesięcy i obejmują:
   1) sprawdzenie zasilania podstawowego i awaryjnego,
   2) sprawdzenie innych elementów, zgodnie z dokumentacją systemu.

§ 15.

Systemy transmisji sygnałów alarmowych do centrów monitoringu

1. Przeglądy systemu transmisji sygnałów alarmowych do centrów monitoringu są przeprowadzane przez podmiot zewnętrzny zgodnie z harmonogramem i obejmują sprawdzenie trybu pracy urządzenia wg wskazań paneli sterujących poprzez porównanie z dokumentacją systemu.
2. Czynności konserwacyjne dokonywane przez pracownika podmiotu zewnętrznego są przeprowadzane nie rzadziej niż raz na 12 miesięcy i obejmują:
   1) sprawdzenie ciągłości działania zasilania podstawowego i sprawności zasilania awaryjnego (wymiana akumulatorów zgodnie z harmonogramem załączonym do dokumentacji technicznej systemu),
   2) sprawdzenie systemu anten, masztów, stanu uziemienia,
   3) sprawdzenie/potwierdzenie prawidłowego działania systemu/systemów w centrum monitoringu.

§ 16.

Rejestrowanie i przechowywanie informacji w elektronicznych systemach zabezpieczeń

1. Zdarzenia rejestrowane w elektronicznych systemach zabezpieczeniowych podlegają regularnym przeglądom przeprowadzanym przez Administratora Zabezpieczeń Fizycznych.
2. Częstość przeglądu zapisów wyznacza się na podstawie pojemności pamięci zdarzeń danego systemu:
   1) przed czynnością włączenia/wyłączenia dla systemów, których pamięć zdarzeń jest kasowana podczas włączania/wyłączania, lub
   2) przed zapełnieniem pamięci systemu powodującej nadpisywanie danych (wg danych w dokumentacji techniczno-eksploatacyjnej systemu),

   nie rzadziej jednak niż raz 6 miesięcy.

3. Zapisy w systemach telewizji dozorowej (CCTV), kontroli dostępu (SKD) sygnalizacji włamania i napadu (SSWiN) oraz w dziennikach/rejestrach wejścia/wyjścia podlegają wyrywkowej kontroli korelacji rejestrowanych zdarzeń dokonywanej przez Administratora Zabezpieczeń Fizycznych.
4. W przypadku wystąpienia incydentu naruszenia bezpieczeństwa lub podejrzenia wystąpienia, którego okoliczności mogą być wyjaśnione dzięki zapisom z rejestrów elektronicznych systemów zabezpieczeń, Administrator Zabezpieczeń Fizycznych zapewnia utrwalenie zapisów z tych rejestrów elektronicznych systemów zabezpieczeń zgodnie z Regulaminem zarządzania incydentami.

§ 17.

Prowadzenie dokumentacji związanej z technicznymi systemami zabezpieczeń

1. Administrator Zabezpieczeń Fizycznych jest odpowiedzialny za prowadzenie wszelkich ewidencji, wykazów uprawnień, rejestrów, w tym rejestrów elektronicznych systemów zabezpieczeń.
2. Wszelka dokumentacja wskazana w ust. 1 jest klasyfikowana jako informacja wrażliwa.
3. Administrator Zabezpieczeń Fizycznych jest odpowiedzialny za aktualność i kompletność dokumentacji technicznych własnych systemów zabezpieczeń (tzn. dokumentacji powykonawczej, zmian w tej dokumentacji, aktualnych plików konfiguracyjnych systemów i urządzeń).

§ 18.

Zarządzanie zapisami pochodzącymi z elektronicznych systemów zabezpieczeń

1. Administrator Zabezpieczeń Fizycznych jest odpowiedzialny za utrzymanie rejestrów elektronicznych własnych systemów zabezpieczeń (SKD, SSWiN, CCTV). Okres przechowywania zapisów pochodzących z elektronicznych systemów zabezpieczeń powinien wynosić co najmniej 14 dni.
2. W przypadku powierzenia utrzymania rejestrów systemów kontroli dostępu, sygnalizacji napadu i włamania lub telewizji dozorowej podmiotowi zewnętrznemu, umowa z usługodawcą musi zapewniać Agencji skuteczną kontrolę nad zapisami przez umieszczenie w niej:
   1) warunków i czasu przechowywania rejestrów (min. 14 dni),
   2) wymagań bezpieczeństwa w odniesieniu do rejestrów,
   3) zasad dostępu Agencji do przechowywanych zapisów, w tym uzyskania kopii stanowiących materiał dowodowy, jeśli zachodzi taka potrzeba,
   4) sposobów komunikowania się Agencji z usługodawcą, w tym potwierdzania dostarczenia kopii rejestrów w trybie awaryjnym,
   5) zakres odpowiedzialności usługodawcy za utratę lub uszkodzenie rejestrów.
3. W przypadku stwierdzenia incydentu naruszenia bezpieczeństwa informacji Administrator Zabezpieczeń Fizycznych wykonuje kopie rejestrów elektronicznych systemów zabezpieczeń dla celów dowodowych.

Załącznik nr 1 do Regulaminu bezpieczeństwa fizycznego i środowiskowego – Wzór rejestru wejścia/wyjścia do strefy bezpieczeństwa

Rejestr osób przebywających w strefie bezpieczeństwa BP…./OR….

Lp.	Imię i nazwisko osoby otwierającej	Imię i nazwisko osoby wchodzącej	Data i godzina wejścia	Data i godzina wyjścia	Cel wejścia

Załącznik nr 2 do Regulaminu bezpieczeństwa fizycznego i środowiskowego – Wzór rejestru wejścia/wyjścia gości do strefy administracyjnej

Rejestr gości przebywających w strefie Administracyjnej Centrali/BP…./OR….

Lp.	Czas wejścia	Imię i nazwisko gościa	Rodzaj dokumentu tożsamości	Nr dokumentu tożsamości	Imię i nazwisko osoby wizytowanej	Nr identyfikatora	Czas wyjścia

REGULAMIN EKSPLOATACJI SYSTEMÓW TELEINFORMATYCZNYCH

Spis treści:

§ 1.

Definicje

Użyte w regulaminie określenia oznaczają:

1) blokowanie konta – administracyjne uniemożliwienie korzystania z konta w danym systemie teleinformatycznym;
2) dane uwierzytelniające – informacje wprowadzane do systemu, potwierdzające tożsamość użytkownika (np. hasła dostępu, kody zawarte w sprzętowych tokenach kryptograficznych);
3) hasło – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie teleinformatycznym;
4) integralność systemu - właściwość polegającą na tym, że system realizuje swoją zamierzoną funkcję w nienaruszony sposób, wolny od nieautoryzowanej manipulacji, celowej lub przypadkowej (PN-I-13335-1);
5) konto – część systemu teleinformatycznego (dane, oprogramowanie, zasoby sieciowe), które są przypisane do identyfikatora użytkownika;
6) kopia archiwalna – duplikat danych, przechowywanych z uwagi na przepisy prawa lub potrzeby dokumentowania działalności Agencji; kopia archiwalna nie służy do odtworzenia;
7) kopia zapasowa – duplikat danych, przechowywany na wymiennym nośniku komputerowym, służący do odtworzenia systemu, aplikacji, bazy danych lub dokumentu;
8) niezaprzeczalność – możliwość przeprowadzenia dowodu, że działanie lub zdarzenie miało miejsce, tak że nie można temu działaniu lub zdarzeniu później zaprzeczyć;
9) podatność – słabość aktywu lub grupy aktywów, która może być wykorzystana przez jedno lub więcej zagrożeń;
10) profil dostępu – zestaw uprawnień, funkcji i zasobów systemu informatycznego dostępnych poszczególnym użytkownikom systemu;
11) rozliczalność - właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi (ISO 7498-2: 1989);
12) spam – niepożądaną przesyłkę poczty elektronicznej kierowaną do niezdefiniowanego adresata;
13) uwierzytelnianie – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
14) zabezpieczenie danych w systemie teleinformatycznym - wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
15) zmiana – działanie lub ciąg działań mających na celu uzyskanie innego stanu systemu teleinformatycznego (konfiguracji lub funkcjonalności) niż przed podjęciem działania;
16) zmiana infrastruktury/ usługa rutynowa – uzgodnioną i zaakceptowaną wcześniej zmianę konfiguracji urządzeń lub sposobu/ zakresu świadczonych usług;
17) zmiana infrastruktury/ usługa awaryjna - zmianę podejmowaną w trybie nagłym wynikającym z konieczności usunięcia awarii lub błędu w systemie;

18) przywilej – specjalne uprawnienie posiadające wyższe od podstawowych prawa dostępu w systemie lub aplikacji, dostępne jedynie dla wybranych pracowników, w szczególności uprawnienie administracyjne.

Rozdział 1.
Podstawowe zasady eksploatacji systemów teleinformatycznych

§ 2.

Podział obowiązków w eksploatacji

1. Właściciel Procesu/Właściciel Zasobu może powierzyć administrowanie systemem (czynności wykonawcze) Administratorowi Systemu. Właściciel Zasobu sprawuje kontrolę nad działaniami wykonawczymi realizowanymi przez Administratora Systemu.
2. Administrator Systemu ponosi odpowiedzialność za bezpieczeństwo funkcjonowania systemu teleinformatycznego w ramach obowiązków powierzonych mu przez Właściciela Procesu/Właściciela Zasobu.
3. Role zarządcze (Właściciela Procesu/Właściciela Zasobu) i wykonawcze (Administratora Systemu) w zakresie eksploatacji systemów teleinformatycznych mogą być wykonywane przez tą samą komórkę organizacyjną.
4. Nadzór nad bezpieczeństwem informacji w systemach teleinformatycznych obejmującym kontrolę działań decyzyjnych i wykonawczych sprawuje dyrektor komórki właściwej ds. bezpieczeństwa informacji.
5. Obowiązki w zakresie eksploatacji sieci i serwerów są oddzielone od obowiązków w zakresie eksploatacji stacji roboczych poprzez przydzielenie ich różnym osobom (pracownikom Agencji lub pracownikom podmiotów zewnętrznych).
6. Wszystkie krytyczne czynności dotyczące realizacji szczególnie odpowiedzialnych zadań wymagają udziału, co najmniej dwóch osób działających jednocześnie lub wykonujących działania sekwencyjnie (dual control).

§ 3.

Monitorowanie pojemności i wydajności systemów

1. Administrator Systemu jest odpowiedzialny za prognozowanie wymagań dotyczących pojemności oraz wydajności kluczowych elementów systemów teleinformatycznych w celu ograniczenia ryzyka przeciążenia systemu.
2. Wymagania dotyczące pojemności nowych systemów, wynikające z rzeczywistych potrzeb Agencji, są definiowane i zatwierdzane przed dokonaniem zakupu, zaakceptowaniem i wdrożeniem tych systemów, zgodnie z Regulaminem rozwoju aplikacji, stanowiącym załącznik nr 11 do Polityki.
3. Administrator Systemu prowadzi monitorowanie eksploatowanych systemów teleinformatycznych, przez gromadzenie informacji dotyczących krytycznych elementów i parametrów systemów:
    1) infrastruktury sieciowej, w zakresie przepustowości i obciążenia łączy (interfejsów) oraz procesorów urządzeń sieciowych,

2) serwerów usług wewnętrznych Agencji (serwery plików, wydruków, faksów, itp.), w zakresie obciążenia procesora, zajętości pamięci dyskowej, przyrostu danych w okresie miesiąca,

3) serwerów aplikacyjnych i baz danych, w zakresie obciążenia procesora, zajętości pamięci dyskowej, przyrostu danych w okresie miesiąca.

4. Raz w roku oraz po wprowadzeniu istotnej zmiany do systemu Administrator Systemu przekazuje Komitetowi informację z monitorowania pojemności i wydajności systemów.
5. W sytuacji, w której analiza pojemności lub wydajności systemów wykazuje wzrost ryzyka niespełnienia celów statutowych Agencji, Administrator Systemu niezwłocznie przekazuje te informacje Przewodniczącemu Komitetu oraz dyrektorowi komórki właściwej ds. bezpieczeństwa informacji.

§ 4.

Ochrona przed szkodliwym oprogramowaniem

1. Stacje robocze i serwery w Agencji są objęte ochroną w czasie rzeczywistym za pomocą oprogramowania antywirusowego oraz zapory (firewall), zapewniających integralność zasobów przechowywanych i przetwarzanych w systemie teleinformatycznym Agencji.
2. Użytkowane poza systemem Agencji wymienne nośniki komputerowe, przed rozpoczęciem pracy z tymi nośnikami w systemach teleinformatycznych Agencji, są sprawdzane za pomocą aktualnego oprogramowania antywirusowego.
3. W systemach Agencji wdrożono scentralizowany system antywirusowy.
4. Aktualizacja baz wirusów odbywa się automatycznie, przynajmniej raz dziennie.
5. Po każdej naprawie i konserwacji urządzenia a przed ponownym włączeniem do systemu teleinformatycznego Agencji zawartość stałych nośników komputerowych jest sprawdzana za pomocą aktualnego oprogramowania antywirusowego zawierającego najnowsze bazy antywirusowe.
6. W przypadku, gdy stacje robocze oraz serwery nie są objęte ochroną w czasie rzeczywistym Administrator Systemu, co najmniej raz w tygodniu dokonuje rutynowej kontroli pod kątem obecności złośliwego oprogramowania, przy czym kontrola może być realizowana w sposób:
   1) automatyczny, zgodnie z harmonogramem zdefiniowanym w scentralizowanym systemie zarządzającym,
   2) automatyczny, zgodnie z harmonogramem zdefiniowanym w każdym systemie teleinformatycznym osobno,
   3) ręczny na żądanie, centralnie lub w każdym systemie teleinformatycznym osobno.
7. Działania Administratora Systemu są dokumentowane stosownymi zapisami w Dzienniku pracy systemu, którego wzór zamieszczono w załączniku nr 3 do niniejszego Regulaminu.

§ 5.

Kontrola licencjonowanego oprogramowania

1. Dla wszystkich systemów i aplikacji użytkowanych w Agencji Administrator Systemu prowadzi spisy licencjonowanego oprogramowania zawierające:
    1) nośniki instalacyjne (i ich kopie, przechowywane w innej lokalizacji),
    2) licencje wraz z okresami ich ważności,
    3) kopie dowodów zakupu licencji,
    4) miejsce zainstalowania,
    5) dane dotyczące użytkownika/Właściciela Procesu/Właściciela Zasobu.
2. Standardowa konfiguracja stacji użytkownika określona jest w Regulaminie standaryzacji stacji roboczych, zatwierdzonym przez Komitet.
3. Za utrzymanie standardu stacji roboczych odpowiada komórka właściwa ds. informatyki.
4. Przeglądy licencjonowanego oprogramowania mogą być przeprowadzane w trybie doraźnym lub w terminie ustalonym w harmonogramie przeglądów, zatwierdzanym przez Prezesa Agencji.
5. Spis licencjonowanego oprogramowania jest sprawdzany przez dyrektora komórki właściwej ds. bezpieczeństwa informacji pod kątem kompletności ewidencji.
6. Okresowo, nie rzadziej niż raz w roku, stacje robocze i udostępnione udziały sieciowe użytkowników są sprawdzane przez Administratora Systemu pod kątem obecności nieautoryzowanego oprogramowania.
7. Przesłanką do podjęcia przeglądu doraźnego jest:
    1) żądanie kierownika komórki organizacyjnej, Właściciela Procesu/Właściciela Zasobu, dyrektora komórki właściwej ds. bezpieczeństwa informacji, Komitetu lub uprawnionych organów ścigania, w związku z informacją o popełnieniu lub podejrzeniu popełnienia czynu niedozwolonego przez pracownika,
    2) otrzymanie zgłoszenia od pracownika o pojawieniu się lub podejrzeniu pojawienia się w systemie teleinformatycznym nieautoryzowanego oprogramowania.
8. Do przeprowadzenia przeglądu zgodności zainstalowanego oprogramowania z posiadanymi licencjami, a także zgodności z konfiguracją standardową, Administrator Systemu może stosować narzędzia programowe umożliwiające m.in.:
    1) automatyczne sprawdzanie stacji roboczych i serwerów,
    2) centralne zarządzanie spisem licencjonowanego oprogramowania,
    3) automatyczne ostrzeganie przed przekroczeniem liczby licencji.
9. Nieautoryzowane oprogramowanie jest niezwłocznie usuwane z systemu teleinformatycznego, a informacje o przypadkach używania nieautoryzowanego oprogramowania są przedstawiane przez Administratora Systemu Komitetowi z rekomendacją podjęcia odpowiednich działań.

§ 6.

Zarządzanie kopiami zapasowymi i archiwalnymi

1. Kopie zapasowe systemów, aplikacji baz danych i dokumentów użytkowanych w Agencji służą do zapewnienia możliwości odtworzenia w przypadku utraty aktualnie użytkowanych danych i/lub konfiguracji systemów i aplikacji.
2. Kopie zapasowe sporządza się w następujących przypadkach:
   1) przed dokonaniem zmiany konfiguracyjnej (np. aktualizacji oprogramowania, ustawień systemowych),
   2) po przeprowadzeniu udanej zmiany konfiguracyjnej (np. aktualizacji oprogramowania, ustawień systemowych).
3. Kopie archiwalne sporządza się w celu utrwalenia istotnych dokumentów, systemów, baz danych i aplikacji, które nie są aktualnie wykorzystywane, a których obowiązek przechowywania wynika z obowiązujących aktów prawnych lub potrzeb wewnętrznych Agencji.
4. Kopie archiwalne przechowywane są przez okres wynikający z uwarunkowań prawnych lub wewnętrznych Agencji.
5. Kopie zapasowe i archiwalne są wykonywane dla systemów, baz danych i aplikacji oraz dokumentów użytkowanych w Agencji.
6. Za tworzenie kopii zapasowych i archiwalnych odpowiedzialny jest Administrator Systemu, któremu Właściciel Procesu/Właściciel Zasobu zlecił wykonywanie kopii.
7. Dla wskazanych dokumentów, systemów, baz danych i aplikacji podlegających tworzeniu kopii Właściciel Procesu/Właściciel Zasobu w porozumieniu z Administratorem Systemu określa:
   1) strategię tworzenia kopii uwzględniającą: częstotliwość tworzenia kopii, rodzaj kopii (przyrostowa, pełna, różnicowa), ilość kopii, miejsce, okres i sposób przechowywania kopii, rotację nośników,
   2) warunki techniczne realizacji procesu zarządzania kopiami zapasowymi i archiwalnymi, w tym określenie urządzenia/oprogramowania do wykonywania kopii, rodzaj nośnika, sposób wykonywania kopii (automatyczny, ręczny), okno eksploatacyjne wykonywania kopii (jeśli ma zastosowanie), sposób weryfikacji poprawności wykonanej kopii.
8. Użytkownicy mogą zlecać Administratorowi Systemu wykonanie kopii przetwarzanych przez nich danych (np. kopii folderów osobistych skrzynek pocztowych).
9. Postępowanie dotyczące nagrywania na nośnikach optycznych danych, zawierających informacje przetwarzane w Agencji opisane zostało w Książce Procedur KP-611-186-ARiMR.
10. Tworzenie kopii odbywa się zgodnie z procedurą tworzenia i odtwarzania kopii zapasowych i podlega rejestracji. Wzór rejestru określa załącznik nr 1 do niniejszego Regulaminu. Rejestr prowadzony jest w postaci papierowej lub elektronicznej.
11. Po utworzeniu kopii automatycznie (jeżeli jest technicznie realizowalne) jest generowany raport o przebiegu wykonania kopii. Raport podlega weryfikacji przez Administratora Systemu.

12. Miejsce przechowywania kopii jest zabezpieczone przed nieuprawnionym dostępem oraz skutkami zdarzeń takich, jak pożar, zalanie, oddziaływanie silnego pola elektromagnetycznego, promieniowanie, zanieczyszczenie środowiska na takim poziomie, jak jest zabezpieczony system, z którego kopia zapasowa została wykonana.
13. Kopie są przechowywane w bezpiecznej odległości (w innej lokalizacji) od miejsca, w którym jest prowadzona eksploatacja systemów. Proces przekazywania nośników zawierających kopie zapasowe i archiwalne do innej lokalizacji jest udokumentowany.
14. Regularnie, co najmniej raz w roku, Administrator Systemu w porozumieniu z Właścicielem Procesu/Właścicielem Zasobu przeprowadza testowe sprawdzenie odtworzenia systemu, aplikacji, bazy danych lub dokumentów z kopii. Testowe odtworzenie podlega udokumentowaniu w dzienniku pracy systemu.
15. W przypadku, gdy okres trwałości zapisu na nośniku elektronicznym lub magnetycznym jest krótszy od wymaganego okresu przechowywania wynikającego z uwarunkowań prawnych dane z nośników są przenoszone na inny nośnik.
16. Kopię na inny nośnik wykonuje Administrator Systemu. Nośnik, z którego przeniesiono zapis, jest niszczony zgodnie z zasadami obowiązującymi w Agencji, a całość operacji przeniesienia jest dokumentowana.
17. Po upływie wymaganego okresu przechowywania kopie archiwalne są niszczone zgodnie z zasadami obowiązującymi w Agencji.
18. Usługi transportowania lub przechowywania kopii zapasowych lub archiwalnych mogą być powierzone podmiotowi zewnętrznemu.
19. Umowa z podmiotem zewnętrznym na transportowanie lub przechowywanie kopii zapasowych lub archiwalnych powinna zawierać:
    1) wymagania bezpieczeństwa transportowania (przechowywania) kopii zapasowych,
    2) tryb przekazywania (odbierania) kopii zapasowych lub archiwalnych:
        a) zwykły (rotacja kopii zapasowych),
        b) awaryjny (w celu użycia kopii zapasowej lub archiwalnej),
    3) sposoby komunikowania się Agencji z usługodawcą, w tym potwierdzania dostarczenia kopii zapasowych w trybie awaryjnym,
    4) zakres odpowiedzialności usługodawcy za utratę lub uszkodzenie kopii zapasowych lub archiwalnych.

§ 7.

Zarządzanie poprawkami technicznymi

1. Zarządzanie poprawkami ma na celu eliminowanie lub ograniczanie zidentyfikowanych podatności systemów teleinformatycznych.
2. Administrator Systemu zobowiązany jest do monitorowania pojawiania się poprawek do poszczególnych usług sieciowych, systemów operacyjnych i aplikacji ARiMR.
3. Administrator Systemu obowiązany jest do wprowadzania poprawek w oparciu informacje uzyskane od producentów urządzeń sieciowych, systemów operacyjnych i apli-

kacji oraz od profesjonalnych organizacji zajmujących się tematyką bezpieczeństwa informacji i systemów teleinformatycznych.

4. Poprawki techniczne, w zależności od ich krytyczności, są testowane w środowisku testowym zanim zostaną wprowadzone do środowiska produkcyjnego. Administrator Systemu prowadzi rejestr dokonywanych zmian.
5. Wprowadzanie poprawek bezpośrednio do środowiska produkcyjnego może być wykonane wyłącznie po uzyskaniu akceptacji Właściciela Procesu / Właściciela Zasobu. Wprowadzanie poprawek podlega dokumentowaniu w Dzienniku pracy systemu.

Rozdział 2.
Zasady bezpieczeństwa sieci

§ 8.

Ogólne mechanizmy bezpieczeństwa sieci

1. Agencja zapewnia bezpieczeństwo sieci za pomocą następujących mechanizmów:
   1) aplikacji i urządzeń typu firewall oraz systemów wykrywania i przeciwdziałania włamaniom na poziomie sieci i hostów,
   2) aplikacji antywirusowych stosowanych podczas wymiany danych pomiędzy siecią Agencji a sieciami należącymi do innych organizacji lub sieciami publicznymi,
   3) rozdzielania sieci; użytkownicy poszczególnych komórek i jednostek organizacyjnych są grupowani w logicznie rozdzielonych segmentach sieciowych (VLAN),
   4) uwierzytelniania użytkowników i urządzeń (o ile istnieją możliwości techniczne),
   5) wyłączenia (zablokowania) usług sieciowych, które są niewykorzystywane, nie mają uzasadnienia biznesowego lub technicznego albo są uznawane za niebezpieczne, niezależnie do tego czy są udostępniane wewnątrz sieci Agencji, czy także na zewnątrz,
   6) właściwie (z punktu widzenia bezpieczeństwa informacji) skonfigurowanie aplikacji, usług lub systemów operacyjnych,
   7) aktualizowanie aplikacji, systemów operacyjnych oraz usług sieciowych do najnowszej oraz bezpiecznej i stabilnej wersji,
   8) fizycznych zabezpieczeń dostępu do systemów,
   9) rozdzielenia środowisk produkcyjnych od testowych.
2. Podsieci logiczne VLAN wewnątrz sieci Agencji tworzy się dla elementów systemu o różnych wymaganiach bezpieczeństwa. Każda z takich podsieci stanowi odrębną strefę bezpieczeństwa, do której dostęp musi być kontrolowany z wykorzystaniem zapory ogniowej zapewniającej realizację ścisłej kontroli oraz selektywnego dostępu do wybranych usług i systemów w danej strefie.
3. Ruch między podsieciami jest kontrolowany za pomocą reguł filtrujących wprowadzonych w urządzeniach sieciowych oraz serwerach.
4. W Agencji wdrożono mechanizmy kontroli rutingu w sieciach oparte na zdefiniowaniu możliwych tras pakietów w sieci.

5. Sygnatury systemów wykrywania i przeciwdziałania włamaniom podlegają regularnej aktualizacji.
6. Komunikacja systemów zewnętrznych z systemami Agencji musi być realizowana poprzez routery dostępowe przyłączone w jednej ze stref zapory ogniowej – strefy dostępowej dedykowanej dla komunikacji z systemami zewnętrznymi.
7. Do realizacji połączeń z systemami zewnętrznymi wymagane jest wykorzystanie łączy dedykowanych. W szczególnych przypadkach oraz do celów testowych zezwala się na dostęp do systemów aplikacyjnych Agencji za pośrednictwem łączy wirtualnych realizowanych poprzez sieć publiczną z wykorzystaniem technologii VPN (połączenia terminowane w zaporze ogniowej lub koncentratorze VPN zlokalizowanym w strefie dostępowej).

§ 9.

Uwierzytelnianie węzłów

1. Agencja wykorzystuje mechanizm identyfikacji urządzeń do uwierzytelniania połączeń z określonych lokalizacji lub urządzeń. Identyfikacja urządzeń realizowana jest w oparciu o przydzielanie stałego adresu IP, na podstawie unikalnego adresu MAC, dla każdego urządzenia podłączanego do sieci Agencji.
2. Agencja może nie stosować mechanizmu określonego w ust. 1, jeśli wynika to z uzasadnionych potrzeb biznesowych.

§ 10.

Ochrona urządzeń sieciowych

1. Wszelkie zmiany topologii sieci lub konfiguracji urządzeń sieciowych są przeprowadzane w oparciu o proces zarządzania zmianami.
2. Wszędzie, gdzie jest to technicznie możliwe, urządzenia sieciowe są chronione hasłem dostępu przechowywanym w postaci zaszyfrowanej.
3. Zarządzanie siecią odbywa się z wydzielonych stacji roboczych zlokalizowanych w sieci lokalnej lub przez konsole podłączone bezpośrednio do urządzeń sieciowych.

§ 11.

Bezpieczeństwo zdalnego dostępu do portów diagnostycznych i konfiguracyjnych

1. Ustawienia parametrów konfiguracyjnych oraz przeprowadzenie diagnostyki urządzeń systemu teleinformatycznego wykonuje się z lokalnej konsoli administracyjnej, wykorzystując do tego celu dedykowane konta administracyjne (lokalny dostęp administracyjny).
2. W szczególnych przypadkach przewidzianych umowami z podmiotami zewnętrznymi oraz sytuacjach awaryjnych, działania administracyjne można wykonywać w trybie zdalnego dostępu. Zdalny dostęp administracyjny jest realizowany wyłącznie ze stacji dedykowanych dla systemów administracyjnych.
3. Do nawiązywania zdalnych połączeń administracyjnych stosuje się:
   1) mechanizmy zapewniające uwierzytelnianie stacji i użytkownika,

2) szyfrowanie komunikacji z wykorzystaniem bezpiecznych protokołów, zapewniających poufność i integralność przesyłanych danych,

3) ograniczenie dostępu do określonej grupy adresacji oraz usług niezbędnych do realizacji powierzonych zadań.

4. Warunki techniczne zdalnego dostępu podlegają zatwierdzeniu przez Komitet.

§ 12.

Bezpieczeństwo dostępu do sieci publicznych (Internet)

1. Sieć teleinformatyczna Agencji, w tym sieci lokalne jednostek organizacyjnych, może być podłączona do sieci ogólnodostępnych (np. sieć publiczna Internet) tylko na poziomie WAN'u i jedynie przy użyciu specjalnych systemów zabezpieczających (aplikacje i urządzenia typu firewall, systemy IDS/IPS).
2. Za zgodą Komitetu, sieć teleinformatyczna Agencji może być połączona z innymi sieciami zewnętrznymi. Warunki takiego połączenia określane są przez reguły filtrowania zapór sieciowych ustalane przez Administratora Systemu we współpracy z dyrektorem komórki właściwej ds. bezpieczeństwa informacji.
3. Wszystkie połączenia pomiędzy sieciami publicznymi a siecią Agencji są realizowane przy użyciu specjalnych systemów zabezpieczających (aplikacje i urządzenia typu firewall, systemy wykrywania włamań).
4. Architekturę zapory ogniowej (firewall) oddzielającej sieć publiczną od sieci wewnętrznych Agencji skonfigurowano na zasadzie przepuszczania tylko ściśle zdefiniowanego ruchu przychodzącego i wychodzącego.
5. Serwery zewnętrznych usług sieciowych muszą być zlokalizowane w wydzielonych strefach DMZ.
6. Usługi udostępniane w sieci publicznej oraz uprawnienia dostępu użytkowników do tych usług są autoryzowane przez Komitet. Wykaz dostępnych usług prowadzi Administrator Systemu. Wykaz ten zawiera zestawienia usług oraz profile użytkowników uprawnionych do korzystania z określonych usług.

Rozdział 3.
Bezpieczeństwo systemów operacyjnych

§ 13.

Ogólne mechanizmy bezpieczeństwa

1. W Agencji stosuje się następujące mechanizmy bezpieczeństwa systemów operacyjnych:

   1) uwierzytelnianie użytkowników, zgodnie z przyjętymi w Agencji zasadami kontroli dostępu,

   2) rejestrowanie nieudanych prób dostępu do systemu,

   3) rejestrowanie korzystania z przywilejów systemowych,

   4) generowanie alarmów w przypadku naruszenia reguł bezpieczeństwa systemu,

5) ograniczanie czasu nieaktywności sesji użytkowników.

2. Systemy operacyjne pracujące w Agencji muszą mieć włączone mechanizmy bezpiecznego logowania zapewniające (w zależności od możliwości technicznych):
   1) ujawnianie minimum informacji o systemie,
   2) wyświetlanie ostrzeżenia, że dostęp do systemu jest dozwolony jedynie dla uprawnionych użytkowników,
   3) unikanie wyświetlania komunikatów pomocniczych, które mogłyby pomóc nieuprawnionemu użytkownikowi przy nieautoryzowanych próbach dostępu,
   4) unikanie wskazywania, która część danych jest poprawna lub niepoprawna w przypadku wystąpienia błędu podczas logowania,
   5) ograniczenie liczby nieudanych prób logowania się do systemu,
   6) blokowanie konta po co najwyżej sześciu następujących po sobie nieudanych próbach logowania,
   7) wykonywanie zapisu każdego nieudanego logowania w logach zdarzeń,
   8) ograniczenie możliwości zalogowania się do systemu tylko w określonych przedziałach czasowych („oknach logowania”),
   9) blokowanie wyświetlania hasła w trakcie jego wprowadzania,
   10) blokowanie domyślnego wyświetlania identyfikatora (konieczność wpisania identyfikatora),
   11) szyfrowanie przesyłanych haseł.

§ 14.

Identyfikacja i uwierzytelnianie użytkowników

1. Wszyscy użytkownicy systemów muszą posiadać unikalne identyfikatory użytkownika (ID użytkownika) do swojego wyłącznego użytku.
2. Stosowane identyfikatory użytkownika nie wskazują na poziom uprawnień danego użytkownika.
3. W celu uwierzytelnienia użytkowników Agencja wykorzystuje hasła lub klucze kryptograficzne chronione hasłem.
4. Dostęp do systemu dla użytkownika, który sześciokrotnie pod rząd podał błędne hasło jest blokowany; odblokowania dokonuje ręcznie Administrator Systemu na wniosek złożony zgodnie z KP-611-101-ARiMR. Tworzenie automatów (skryptów) programowych odblokowujących dostęp np. po określonym czasie jest zabronione.

§ 15.

System zarządzania hasłami

1. Ustawienia zasad zarządzania hasłami w systemach teleinformatycznych zapewniają:
   1) wymuszanie użycia indywidualnych haseł,
   2) wybór i zmianę haseł przez użytkowników,

3) potwierdzanie zmiany haseł dla uniknięcia błędów podczas ich wprowadzania,
4) wymuszenie wyboru haseł o odpowiedniej jakości, tj.: składających się co najmniej z 8 znaków, zawierających małe i wielkie litery oraz cyfry lub znaki specjalne,
5) wymuszenie zmiany haseł z ustaloną częstotliwością, w przypadku systemów przetwarzających dane osobowe zmiana hasła następuje nie rzadziej niż co 30 dni,
6) wymuszenie zmiany haseł tymczasowych przy pierwszym rejestrowaniu się w systemie,
7) pamiętanie haseł przez system w celu zapobiegania ponownemu ich użyciu, minimalna liczba haseł pamiętanych przez system wynosi 5.

2. Hasła administracyjne mogą być w szczególnych sytuacjach stosowane dłużej niż zaznaczono to w ust. 1 pkt 5, jednak nie dłużej niż 6 miesięcy.

§ 16.

Użycie programów narzędziowych

1. Uprawnienia umożliwiające uruchamianie programów narzędziowych są przydzielane na czas niezbędny do wykonania określonego zadania, na podstawie wniosku złożonego przez kierownika komórki organizacyjnej lub Właściciela Procesu / Właściciela Zasobu, którego wzór zamieszczono w załączniku nr 4 do niniejszego Regulaminu.
2. Poziom uprawnień umożliwiający uruchamianie programów narzędziowych jest udokumentowany.
3. Administrator Systemu rejestruje w Dzienniku pracy systemu, którego wzór zamieszczono w załączniku nr 3 do niniejszego Regulaminu, wszystkie przypadki użycia systemowych programów narzędziowych.
4. Systemowe programy narzędziowe oraz aplikacje, które nie są wykorzystywane przez użytkowników podczas pracy w systemach teleinformatycznych, są w miarę możliwości technicznych usuwane ze stacji roboczych i serwerów.

§ 17.

Ograniczenia czasowe sesji połączeniowej

1. W celu wymuszenia ochrony urządzeń systemu teleinformatycznego stosuje się następujące mechanizmy włączane w przypadku stwierdzenia braku aktywności użytkownika:
   1) blokowanie lub wyłączanie stacji roboczej (sesji połączeniowej),
   2) powtarzanie identyfikacji i uwierzytelnianie użytkownika.
2. System operacyjny po ustalonym okresie bezczynności użytkownika, jednak nie dłużej niż 10 minut, przechodzi w stan nieaktywny, w którym blokowany jest dostęp do konsoli. Powrót do stanu aktywności wymaga podania hasła.
3. Dla zapewnienia bezpieczeństwa systemów teleinformatycznych Agencji stosuje się ograniczenia czasu pracy w systemach operacyjnych do godzin pracy Agencji.

4. O ograniczeniu czasu trwania połączenia decyduje Właściciel Procesu/Właściciel Zasobu odpowiedzialny za funkcjonowanie i bezpieczeństwo danego systemu teleinformatycznego.
5. W przypadku konieczności pracy w systemie w innym czasie niż wyżej określony, zgodę wydaje Właściciel Procesu/Właściciel Zasobu na wniosek kierownika komórki organizacyjnej, której pracownicy potrzebują dostępu do systemu poza ustalonymi godzinami pracy.

§ 18.

Eksploatacja aplikacji w systemach teleinformatycznych Agencji

1. O przyznawaniu dostępu i zakresie nadanych uprawnień użytkowników do aplikacji decyduje Właściciel Procesu / Właściciel Zasobu w Centrali oraz, w razie potrzeby, dyrektor oddziału regionalnego dla użytkowników w oddziale regionalnym i biurze powiatowym, na podstawie upoważnienia nadanego przez Właściciela Procesu / Właściciela Zasobu.
2. Uprawnienia administratora są nadawane ograniczonej liczbie użytkowników.
3. Mechanizm dziedziczenia uprawnienia administratora aplikacji na podstawie uprawnień administratora nadanych w systemie operacyjnym lub na platformie bazodanowej jest zablokowany.
4. Właściciel Procesu / Właściciel Zasobu jest odpowiedzialny za aktualność i dokumentowanie przydzielonych uprawnień udzielonych użytkownikom do pracy w aplikacjach Agencji. Dotyczy to uprawnień wszystkich użytkowników w tym również pracowników podmiotów zewnętrznych świadczących usługi informatyczne dla Agencji.

§ 19.

Świadczenie usług informatycznych przez podmioty zewnętrzne

1. Dostęp podmiotu zewnętrznego do systemów Agencji wymaga przeprowadzenia udokumentowanego szacowania ryzyka.
2. Szacowanie ryzyka przeprowadza Właściciel Procesu/Właściciel Zasobu na podstawie informacji dostarczonych przez Administratora Systemu.
3. W szczególności, Właściciel Procesu/Właściciel Zasobu otrzymuje następujące informacje:
   1) podstawę udzielenia dostępu dla danego podmiotu zewnętrznego,
   2) zakres i sposób dostępu do sieci Agencji, w tym zakres przydzielanych uprawnień,
   3) proponowane rozwiązania techniczne i organizacyjne służące ograniczeniu ryzyka dla bezpieczeństwa systemów teleinformatycznych Agencji.
4. Zgodę na udzielenie dostępu podmiotowi zewnętrznemu wydaje Właściciel Procesu/ Właściciel Zasobu, po zaakceptowaniu i wdrożeniu rozwiązań, o których mowa w ust. 3 pkt 3.
5. W umowie z podmiotem zewnętrznym dotyczącej utrzymania systemów teleinformatycznych Agencji uwzględnia się zapis zobowiązujący podmiot zewnętrzny do stosowania zasad i procedur wynikających z dokumentów polityki bezpieczeństwa informa-

cji i systemu zarządzania bezpieczeństwem informacji. Umowa z podmiotem zewnętrznym może zawierać uszczegółowienie bądź rozszerzenie zasad wynikających z dokumentów polityki bezpieczeństwa informacji i systemu zarządzania bezpieczeństwem informacji wynikające ze specyfiki danego projektu.

6. Doraźne działania serwisowe podmiotów zewnętrznych (nie mające charakteru stałego utrzymania systemów teleinformatycznych) są dokumentowana przez Administratora Systemu w dzienniku pracy systemu. Zapis w dzienniku zawiera, co najmniej:
   1) dokładny czas rozpoczęcia i zakończenia działania serwisowego,
   2) identyfikacja osoby realizującej działania serwisowe po stronie podmiotu zewnętrznego oraz nadzorującej te działania po stronie Agencji,
   3) dokładny opis przeprowadzonych działań wraz ze wskazaniem statusu tych działań (wymagające kontynuacji, zakończone).
7. Doraźne działania serwisowe w systemie teleinformatycznym osób, nie będących uprawnionymi pracownikami Agencji dokonywane są w obecności Administratora Systemu.
8. Osobie reprezentującej podmiot zewnętrzny, wykonującej działania serwisowe, nie mogą zostać nadane uprawnienia administratora. Jeśli wyjątkowa sytuacja uzasadnia taką potrzebę, to nadanie uprawnienia wymaga zgody Właściciela Procesu/Właściciela Zasobu. Niezwłocznie po zakończeniu pracy uprawnienia administratora oraz jakiekolwiek inne uprawnienia nadane osobie reprezentującej podmiot zewnętrzny muszą zostać odebrane.
9. W przypadku dokonywania zmian konfiguracji (naprawy, rekonfiguracje) przez stronę trzecią Agencja zapewnia odpowiednie uprawnienia do użycia oprogramowania narzędziowego służącego do celów zarządzania konfiguracją.

Rozdział 4.
Zarządzanie zmianami w systemach teleinformatycznych Agencji

§ 20.

Odbiór systemu teleinformatycznego

1. Kryteria odbioru obejmują dostarczenie:
   1) w przypadku oprogramowania - dokumentacji technicznej, instrukcji dla administratora i użytkownika,
   2) w przypadku infrastruktury – dokumentacji powykonawczej obejmującej w szczególności schemat połączeń fizycznych i logicznych elementów infrastruktury.
2. Ponadto, kryteria odbioru obejmują:
   1) wymagania wydajnościowe i pojemnościowe systemu teleinformatycznego,
   2) dokumenty potwierdzające, że instalacja nowych systemów nie będzie miała negatywnego wpływu na istniejące systemy, szczególnie w chwilach największego obciążenia (jeżeli ma zastosowanie),
   3) dokumenty potwierdzające, że wpływ nowych systemów na bezpieczeństwo informacji został uwzględniony,

4) szkolenia z zakresu posługiwania się i działania nowych systemów,

5) w przypadku oprogramowania, odbiór obejmuje dodatkowo zapisy zawarte w § 7 Regulaminu rozwoju aplikacji.

§ 21.

Kontrola zmian w eksploatacji

1. Kontrola zmian sieci, systemów operacyjnych i aplikacji ma na celu zapewnianie poprawnego i bezpiecznego działania systemów teleinformatycznych pracujących w Agencji.
2. Zarządzanie zmianami polega na koordynacji, nadawaniu priorytetów, zatwierdzaniu, planowaniu zasobów i oceny ryzyka w związku ze zmianami dokonywanymi w systemach teleinformatycznych Agencji.
3. Każda zmiana w systemie teleinformatycznym Agencji musi być udokumentowana.
4. Zasady wskazane w niniejszym rozdziale odnoszą się do:
   1) zmian infrastruktury technicznej systemów sprowadzających się do wprowadzenia nowego elementu infrastruktury, zmodyfikowania lub usunięcia istniejącego elementu infrastruktury, poprawiania błędu w infrastrukturze, przy czym:
      a) zmiana infrastruktury regularna – oznacza zmianę, która nie wymaga natychmiastowego wdrożenia,
      b) zmiana infrastruktury awaryjna - stosowana w sytuacjach awaryjnych, gdzie czas implementacji zmiany jest krytyczny, z pominięciem lub uproszczeniem niektórych etapów (np. testów) przy założonym ryzyku,
      c) zmiana infrastruktury rutynowa - zaakceptowane wcześniej działanie związane z relatywnie prostymi czynnościami np. wymiana drukarki lub monitora,
   2) zmian aplikacyjnych będących poprawkami (w tym usuwanie błędów) albo modyfikacjami, zmiany aplikacyjne są klasyfikowane jako:
      a) zmiany aplikacyjne regularne – oznaczają zmiany, które nie wymagają natychmiastowego wdrożenia,
      b) zmiany aplikacyjne awaryjne – wprowadzane w stanie pilnej konieczności z powodu zagrożenia działania aplikacji,
   3) zmian w sposobie i/ lub zakresie świadczenia usług przez podmiot zewnętrzny.
5. Za proces zarządzania zmianami w poszczególnych obszarach jest odpowiedzialny Właściciel Procesu/Właściciel Zasobu, zaś za wykonywane zmian Administrator Systemu (jeżeli działania te zostały na niego delegowane).
6. Każda zmiana regularna jest poprzedzona udokumentowanym:
   1) opisem zmiany,
   2) opisem przyczyny zmiany (wraz z podaniem aktów prawnych uzasadniających zmianę – jeżeli ma zastosowanie),
   3) opisem rodzaju wymaganych działań,
   4) szacowaniem ryzyka potencjalnego wpływu zmian,

5) harmonogramem wprowadzanych zmian,
6) wykonaniem kopii zapasowej z możliwością odtworzenia stanu poprzedniego na wypadek nieprzewidzianych zdarzeń (jeżeli ma zastosowanie),
7) przetestowaniem zmian.

7. Jeżeli zmiana ma charakter awaryjny, dokumentacja może być opracowana najpóźniej w przeciągu 7 dni od dokonania zmiany.
8. Zmiana mająca charakter awaryjny, którą trzeba wprowadzić bezzwłocznie w celu ograniczenia ryzyka poważnego zakłócenia działalności Agencji wymaga zgody Właściciela Procesu / Właściciela Zasobu.
9. Dokonywane zmiany: regularne, awaryjne i rutynowe podlegają rejestracji w Dzienniku pracy systemu prowadzonym przez Administratora Systemu.
10. Wpisu dokonuje osoba przeprowadzająca zmianę. Wpis zawiera w szczególności odnośniki do dokumentów określonych w ust. 6.

§ 22.

Bezpieczeństwo dokumentacji systemu

1. Dokumentacja powykonawcza infrastruktury oraz dokumentacja techniczna systemu podlega ochronie zgodnie z zasadami ochrony informacji wrażliwych przedstawionymi w Polityce.
2. Osobą odpowiedzialną za aktualność i kompletność dokumentacji jest dyrektor komórki właściwej ds. informatyki.
3. Dokumentacja systemów jest udostępniana na zasadzie „wiedzy koniecznej”. Udostępnienie dokumentacji jest rejestrowane.

Rozdział 5.
Zarządzanie wymiennymi nośnikami komputerowymi

§ 23.

Użytkowanie nośników

1. Nośniki komputerowe są przechowywane i eksploatowane zgodnie z zaleceniami producenta, z uwzględnieniem wymagań w zakresie ochrony informacji, które są umieszczone na nośnikach.
2. Nośniki zawierające informacje wrażliwe przechowywane są w specjalnych, atestowanych szafach (np. S120 DIS) zlokalizowanych w strefie administracyjnej. Szafy do przechowywania nośników zapewniają ochronę przed:
   1) pożarem,
   2) eksplozją towarzyszącą pożarowi,
   3) działaniem gazów powstałych podczas pożaru,
   4) zalaniem,
   5) działaniem pola elektromagnetycznego.

3. Wymienne nośniki komputerowe takie, jak: przenośne dyski twarde, kamery taśmy magnetyczne, optyczne nośniki danych, pamięci typu flash, podlegają ewidencji prowadzonej przez Administratora Systemu. Rejestr wymiennych nośników komputerowych prowadzony jest w postaci papierowej lub elektronicznej.
4. Etykiety nośników informacji posiadają identyfikator lub numer umożliwiający ich jednoznaczną identyfikację (np.: nr seryjny, kod kreskowy, itp.). Na podstawie etykiety nośnika informacji i danych zawartych w ewidencji nośników możliwe jest ustalenie:
   1) numeru ewidencyjnego nośnika,
   2) typu nośnika,
   3) daty zapisu na nośniku (informacja nieobowiązkowa dla nośników wielokrotnego zapisu),
   4) nazwy komórki organizacyjnej składującej informacje,
   5) określenia rodzaju przechowywanej informacji (informacja nieobowiązkowa dla nośników wielokrotnego zapisu),
   6) imienia i nazwiska osoby dokonującej zapisu (w przypadku nośników wielokrotnego zapisu imię i nazwisko osoby, na stanie której jest dany nośnik).
5. Nośniki wymienne zawierające informacje wrażliwe przewożone są przez pracowników Agencji do innych lokalizacji w pojemniku zapewniającym ochronę nośników przed zagrożeniami wskazanymi w ust. 2.

§ 24.

Wycofanie z eksploatacji nośników komputerowych

1. Wycofanie z eksploatacji wymiennych nośników komputerowych, przekazanie do naprawy lub ponownego użycia jest poprzedzone archiwizacją, a następnie skutecznym usunięciem zapisanych danych.
2. Uszkodzone wymienne nośniki komputerowe zawierające informacje wrażliwe są niszczone w sposób uniemożliwiający odczytanie zapisanych na nich informacji.
3. Zasady i tryb postępowania z nośnikami przekazanymi do archiwum określają odrębne przepisy Agencji.

Rozdział 6.
Bezpieczeństwo wymiany danych

§ 25.

Bezpieczeństwo serwisów intranetowych i ekstranetowych

1. Serwisy intranetowe i ekstranetowe są lokalizowane na serwerach, do których dostęp wymaga identyfikacji i uwierzytelnienia.
2. Udostępnienie informacji w serwisach intranetowych i ekstranetowych wymaga zatwierdzenia przez Właściciela Procesu/Właściciela Zasobu.
3. Dostęp do serwisów ekstranetowych posiadają wyłącznie pracownicy Agencji.

4. Dostęp do serwisów ekstranetowych mogą posiadać uprawnione z mocy prawa podmioty zewnętrzne współpracujące z Agencją.

§ 26.

Bezpieczeństwo wymiany poczty elektronicznej wewnętrznej i zewnętrznej

1. System poczty elektronicznej zapewnia:
   1) ochronę przed szkodliwym oprogramowaniem rozpowszechnianym za pomocą poczty elektronicznej,
   2) ochronę antywirusową załączników przesyłanych w poczcie elektronicznej,
   3) ochronę antyspamową,
   4) możliwość użycia dostępnych technik kryptograficznych do ochrony poufności i integralności wiadomości poczty elektronicznej,
   5) monitorowanie i rejestrowanie poczty elektronicznej.
2. Zasoby poczty elektronicznej (wszystkie skrzynki pocztowe) podlegają sporządzaniu kopii zapasowej. Kopia zapasowa sporządzana jest każdego dnia. Okres przechowywania kopii zapasowych wynosi co najmniej 3 dni.
3. System poczty elektronicznej nakłada ograniczenia, co do rozmiaru pojedynczej skrzynki pocztowej oraz wielkości przesyłanej wiadomości.

Rozdział 7.
Konserwacja i naprawy sprzętu

§ 27.

Konserwacja i naprawa sprzętu

1. Konserwacja sprzętu i urządzeń pracujących w systemach teleinformatycznych Agencji ma na celu zapewnienie nieprzerwanej i bezpiecznej pracy tych systemów, zapobieganie utraty, uszkodzenia lub naruszenia bezpieczeństwa.
2. Sprzęt podlega konserwacji według ustalonego planu, wynikającego z zaleceń producentów.
3. Konserwacja i naprawy muszą być prowadzone jedynie przez uprawnionych pracowników Agencji lub podmiot zewnętrzny świadczącą usługi konserwacyjne na podstawie umowy lub w ramach gwarancji.
4. W przypadku, gdy na nośnikach komputerowych, stanowiących integralną część sprzętu przekazywanego do naprawy, znajdują się informacje wrażliwe, sprzęt taki naprawiany jest pod nadzorem Administratora Systemu. Jeżeli zaś taki nadzór nie jest możliwy, to informacje wrażliwe są, po zapewnieniu możliwości ich odtworzenia, skutecznie usuwane z nośnika.
5. Wszelkie konserwacje i naprawy są odnotowywane w dzienniku pracy danego sprzętu.

§ 28.

Zabezpieczenie sprzętu poza siedzibą

1. Wynoszenie sprzętu (np. komputery przenośne, notesy elektroniczne itp.) jest możliwe tylko w przypadku uzyskania zgody Właściciela Procesu/Właściciela Zasobu.
2. Pracownik wyznaczony przez Właściciela Procesu/Właściciela Zasobu prowadzi ewidencję sprzętu pracującego poza Agencją.
3. Wszelkie informacje wrażliwe nie mogą być przechowywane w urządzeniach przenośnych, które pracują poza Agencją w postaci niezaszyfrowanej.
4. Sprzęt wykorzystywany poza Agencją podlega ubezpieczeniu.
5. Ustala się, że wynoszenie sprzętu komputerowego poza Agencję, w tym sposób programowego zabezpieczenia komputerów, odbywa się w sposób opisany w „Procedurze wydawania zezwoleń na wynoszenie sprzętu komputerowego z ARiMR" zawartej w Książce Procedur KP-611-206-ARiMR.
6. Wynoszenie sprzętu komputerowego poza Agencję dotyczy również sytuacji, kiedy praca odbywa się na terenie Agencji, ale poza pomieszczeniami przystosowanymi do przetwarzania informacji wrażliwych.

Rozdział 8.
Zarządzanie dostępem do systemów teleinformatycznych

§ 29.

Rejestrowanie użytkowników i przypisanie praw dostępu

1. Użytkownik systemu teleinformatycznego jest jednoznacznie identyfikowany poprzez indywidualny identyfikator (nazwę) użytkownika.
2. Niedopuszczalne jest korzystanie z tego samego identyfikatora przez więcej niż jednego użytkownika (chyba, że z przyczyn technicznych nie ma możliwości stosowania osobistych identyfikatorów).
3. Raz użyty identyfikator nie może być przydzielony innemu użytkownikowi.
4. Uprawnienia dostępu są nadawane wyłącznie w zakresie wynikającym z zajmowanego stanowiska i potrzeby wykonywania obowiązków służbowych na danym stanowisku pracy. Bezzasadne nadawanie uprawnień administratora (przywilejów) będzie kwalifikowane jako incydent związany z bezpieczeństwem informacji.
5. Nadawanie uprawnień dostępu do systemu teleinformatycznego Agencji odbywa się zgodnie z procedurą nadawania/zmiany/odbierania uprawnień pracownikom ARiMR zawartą w Książce Procedur KP-611-101-ARiMR.
6. W przypadku konieczności natychmiastowego odebrania/ograniczenia praw dostępu dopuszcza się możliwość zastosowania uproszczonego trybu polegającego na przekazaniu stosownej informacji pocztą elektroniczną od bezpośredniego przełożonego do Administratora Systemu, która niezwłocznie jest potwierdzana w zwykłym trybie.
7. Rejestr użytkowników wraz z przyznanymi uprawnieniami do systemu lub aplikacji prowadzi Administrator Systemu. Rejestr publikowany jest w sieci wewnętrznej

na stronie intranetowej Agencji i aktualizowany nie rzadziej niż raz na miesiąc. Weryfikację aktualności tego rejestru prowadzą Właściciele Procesów/Właściciele Zasobów w odniesieniu do nadzorowanych przez siebie zasobów.

8. Prawa dostępu do wielu aktywów (plików, katalogów, aplikacji, stron internetowych) jednocześnie przydzielane są dla każdego z aktywów za osobną zgodą danego Właściciela Procesu/Właściciela Zasobu. W przypadku, gdy w Agencji wykorzystuje się domenowe mechanizmy zarządzania dostępem (usługi katalogowe, active directory, itp.) aktywa są grupowane, za uprzednią zgodą odpowiednich Właścicieli Procesów / Właścicieli Zasobów.
9. Administrator Systemu raz na miesiąc dokonuje przeglądu stanu aktywności kont użytkowników.
10. Konta nieużywane przez okres 30 dni są automatycznie blokowane.

§ 30.

Zarządzanie przywilejami

1. Nadawane przywileje (większe uprawnienia niż wynika to z realizowanych rutynowych zadań użytkownika) podlegają ścisłej ewidencji prowadzonej przez Administratora Systemu.
2. Przywileje w systemie nadaje Administrator Systemu zgodnie z procedurami obsługi kont użytkowników systemów informatycznych zamieszczonymi w Książce Procedur KP-611-101-ARiMR.
3. Uprzywilejowane konto nie może służyć do realizacji przez użytkownika rutynowych zadań.
4. Przywileje podlegają cofnięciu niezwłocznie po ustaniu potrzeby uzasadniającej ich nadanie.
5. Przywileje nadawane są osobie zastępującej danego administratora na czas jego nieobecności.
6. Osobie zastępującej przekazywane są hasła dostępu oraz procedury wykonywane nadanym stanowisku.
7. Nadawane przywileje podlegają regularnym przeglądom i kontroli.

§ 31.

Zarządzanie hasłami użytkowników

1. Niedopuszczalne jest występowanie w systemie teleinformatycznym kont niezabezpieczonych hasłem.
2. Administrator Systemu, za pomocą ustawień systemowych, wymusza natychmiastową zmianę hasła początkowego, przydzielonego użytkownikowi, na nowe przez niego wybrane (o ile istnieją możliwości techniczne wymuszenia).
3. Zabronione jest przekazywanie haseł przez osoby trzecie lub za pośrednictwem otwartych wiadomości poczty elektronicznej (nie dotyczy to haseł tymczasowych do systemów wyposażonych w mechanizm wymuszający zmianę hasła przy pierwszej próbie uwierzytelnienia się w danym systemie).

4. Hasła tymczasowe, dostarczane w przypadku utraty hasła, są wydawane dopiero po pozytywnej weryfikacji tożsamości użytkownika.
5. Przy konfigurowaniu mechanizmów logowania do systemów uwzględnia się następujące zasady:
   1) użytkownik musi podać swój identyfikator oraz hasło,
   2) w polu logowania nie jest prezentowana ostatnio użyta nazwa użytkownika (o ile system to umożliwia),
   3) wpisywane hasło nie pojawia się w postaci jawnej na ekranie logowania,
   4) hasło przesyłane jest w postaci zaszyfrowanej (o ile system to umożliwia).
6. Systemy operacyjne i aplikacje spełniają wymagania dotyczące możliwości ustawienia następujących parametrów haseł:
   1) siły hasła (długość i złożoność haseł),
   2) maksymalnego okresu ważności,
   3) ograniczenia możliwości ponownego wykorzystania hasła (pamięć ostatnio używanych haseł).
7. Specjalne warunki przechowywania duplikatów haseł dotyczą:
   1) elementów aktywnych sieci teleinformatycznej,
   2) haseł administracyjnych do systemów, aplikacji i baz danych,
   3) konfiguracji komputerów, w tym hasła do BIOS.
8. Hasła administracyjne przechowuje się w postaci zaszyfrowanej. Dopuszcza się przechowywanie haseł w wersji elektronicznej poprzez zastosowanie oprogramowania typu „password manager” z bazą szyfrowaną algorytmem AES lub Twofish.
9. Do przechowywania hasła głównego do zaszyfrowanej bazy haseł, bądź innych haseł zapisanych na papierze, stosuje się wyłącznie koperty, które uniemożliwiają otwarcie bez uszkodzenia ich struktury (tzw. „koperty bezpieczne”). Koperty z hasłami przechowuje się w sejfie, w miejscu zapewniającym dostęp tylko osobom upoważnionym.
10. Dane umieszczone na bezpiecznej kopercie zawierają:
    1) numer koperty adekwatny do numeru ewidencyjnego podanego w książce ewidencji haseł,
    2) datę jej złożenia i podpis osoby składającej kopertę,
    3) skróconą nazwę przynależności hasła.
11. Koperty z hasłami podlegają oznaczaniu zgodnie z załącznikiem nr 2 do niniejszego Regulaminu oraz ścisłej ewidencji prowadzonej przez Administratora Systemu.
12. Ewidencja haseł przechowywana jest w miejscu zabezpieczonym przed utratą i dostępem osób niepowołanych.
13. Za aktualność przechowywanych haseł odpowiedzialny jest Administrator Systemu.
14. Awaryjne otwarcie bezpiecznej koperty oraz pobranie kopii hasła znajdującego się w kopercie wymaga uprzedniej pisemnej akceptacji Właściciela Procesu / Właściciela Zasobu lub osoby przez niego upoważnionej i jest udokumentowane w ewidencji kopert.

15. Po użyciu, hasło ulega zniszczeniu, a w to miejsce jest generowane nowe hasło, którego kopia jest przechowywana na identycznych zasadach jak w przypadku zniszczonego hasła.

§ 32.

Zasady dostępu do plików i katalogów

1. Uprawnienia dostępu do plików i katalogów z poziomu systemu operacyjnego są nadawane przez Administratora Systemu po zatwierdzeniu przez Właściciela Procesu/Właściciela Zasobu odpowiedzialnego za dany zasób.
2. Uprawnienia dostępu do katalogów i plików aplikacji, w tym do baz danych, są nadawane przez Administratora Systemu po zatwierdzeniu przez Właściciela Procesu/Właściciela Zasobu odpowiadającego za dany zasób.

Rozdział 9.
Zasady monitorowania systemów i ich użycia

§ 33.

Mechanizmy monitorowania systemów

1. Monitorowanie systemów i ich użycia ma na celu wykrywanie nieuprawnionych działań.
2. Rejestrowane i monitorowane są wszystkie zdarzenia polegające na użyciu urządzeń przetwarzania informacji oraz programów narzędziowych, diagnostycznych zapewniając weryfikację i rozliczalność użytkowników wykonujących zadania, do których zostali uprawnieni. W szczególności rejestrowaniu podlegają:
   1) identyfikatory użytkowników,
   2) daty i czasy zarejestrowania i wyrejestrowania w systemie,
   3) identyfikator stacji roboczej lub terminala (nazwę komputera w systemie),
   4) nieudane próby logowania do systemu,
   5) zmiany zapisów w rejestrach,
   6) błędy systemu i procedury obsługi tych błędów,
   7) zawieszenie i ponowne uruchomienia systemu,
   8) uruchamianie programów narzędziowych,
   9) zmiany w plikach konfiguracyjnych i krytycznych zmiennych systemowych,
   10) wersje systemu i stan uaktualnień w porównaniu z zalecanymi przez producenta, (jeśli ma zastosowanie).
3. Rejestry są utrzymywane i przechowywane dla wszystkich krytycznych dla Agencji systemów i aplikacji.
4. Systemy rejestrów są objęte standardową procedurą tworzenia kopii archiwalnych. Kopie archiwalne rejestrów przechowywane są przez 2 lata.

5. Serwery kontrolujące dostęp do Internetu tworzą zdalne pliki rejestrów lub mają wdrożony system przesyłania rejestrów zdarzeń na inne, wewnętrzne serwery.
6. W celu wykrywania incydentów związanych z bezpieczeństwem Administrator Systemu regularnie monitoruje zapisy dokonywane automatycznie przez systemy w rejestrach zdarzeń pod kątem właściwego wykorzystania systemu teleinformatycznego i zarządzania nim.
7. Systemy zapisu zdarzeń są zabezpieczone przed manipulacją i nieuprawnionymi zmianami.
8. W ramach weryfikacji zgodności systemów teleinformatycznych względem standardów bezpieczeństwa przeprowadzane są, na podstawie zatwierdzonego przez Prezesa Agencji harmonogramu oraz procedury KP-611-298-ARiMR, testy bezpieczeństwa systemów teleinformatycznych ARiMR.

§ 34.

Dziennik pracy systemu

1. Administrator Systemu prowadzi dziennik wykonywanych czynności oraz zdarzeń zachodzących w systemie. Dzienniki pracy systemu, zgodnie ze wzorem zamieszczonym w załączniku nr 3 do niniejszego Regulaminu, zawierają zapisy dotyczące następujących zdarzeń lub czynności:
   1) informacje o nadaniu, modyfikacji lub cofnięciu przywilejów w systemie,
   2) przejęcie obowiązków administratora,
   3) błędy systemowe i podjęte działania naprawcze,
   4) zdarzenie związane z bezpieczeństwem informacji,
   5) błędy zgłaszane przez użytkowników oraz innych administratorów, a także uzyskane od stron trzecich świadczących usługi na rzecz systemu użytkowanego w Agencji oraz podjęte działania naprawcze,
   6) informacje o sesjach połączeń zdalnych wykonywanych przez podmioty zewnętrzne (jeżeli ma zastosowanie) zawierające:
      a) cel połączenia,
      b) opis działań,
      c) specyfikację danych i systemów, do których firma serwisowa będzie miała dostęp,
      d) nazwisko osoby nawiązującej połączenie ze strony firmy zewnętrznej oraz nazwę firmy,
      e) datę i godzinę połączenia,
   7) instalacje oprogramowania lub zmiany wersji,
   8) użycie programów narzędziowych,
   9) zmiany konfiguracji sprzętu i systemu operacyjnego.
2. Każdy zapis w dzienniku pracy systemu zawiera informacje dodatkowe o czynnościach lub zdarzeniu, takie jak:

1) czas rozpoczęcia i zakończenia pracy w systemie;
2) nazwisko osoby wykonującej wpis do dziennika,
3) identyfikator konta, z którego wykonano czynności (jeśli ma zastosowanie).

3. Administrator Systemu odnotowuje w dzienniku wszelkie dodatkowe informacje, które pozwolą zlokalizować przyczynę błędu:
   1) w przypadku awarii sprzętu lub usługi, w szczególności:
      a) powtórzenie błędu (np. analogiczny wcześniejszy zapis w dzienniku),
      b) objawy towarzyszące (np. komunikaty systemowe, logi połączeń),
      c) krytyczność awarii, zgodnie z klasyfikacją uzgodnioną z dostawcą usług (np. w umowie SLA),
   2) w przypadku awarii oprogramowania, w szczególności:
      a) powtórzenie błędu (np. analogiczny wcześniejszy zapis w dzienniku),
      b) zrzuty ekranów,
      c) konfiguracje oprogramowania i baz danych (np. otwarte pliki, zapisy w logach),
      d) krytyczność błędu, zgodnie z klasyfikacją uzgodnioną z dostawcą oprogramowania.
4. Lista działań wykonywanych przez administratorów podlegających bezwzględnemu odnotowywaniu w dziennikach może zostać poszerzona lub ograniczona dla danego systemu teleinformatycznego po ówczesnym przeprowadzeniu udokumentowanego szacowanie ryzyka i zatwierdzeniu przez Komitet.
5. Dzienniki mogą być prowadzone oddzielnie dla każdego serwera, urządzenia sieciowego, aplikacji.
6. Dzienniki prowadzone są przez administratora odpowiedzialnego za dany serwer, urządzenie sieciowe, aplikację.
7. Dzienniki systemowe lub ich części prowadzone są w formie elektronicznej lub papierowej.
8. Rejestracja błędów może być prowadzona poza dziennikiem administratora, w dedykowanym rejestrze.

§ 35.

Synchronizacja zegarów

1. Odpowiednia dokładność i możliwość korelacji rejestrów zdarzeń, których zapisy mogą służyć jako dowody w postępowaniu w przypadku wykrycia naruszenia bezpieczeństwa, jest zapewniona przez właściwe ustawienie zegarów urządzeń teleinformatycznych.
2. Do synchronizacji czasu wykorzystuje się protokół NTP.
3. Źródłem synchronizacji powinien być zewnętrzny wzorzec czasu.
4. Stacje robocze synchronizują czas z kontrolerów domen.

§ 36.

Bezpieczeństwo okablowania

1. W Agencji przyjęto następujące zasady instalowania i ochrony okablowania:
    1) sposób instalacji okablowania uwzględnia ochronę okablowania przed nieautoryzowanym dostępem lub uszkodzeniem, poprzez prowadzenie kabli w rurach kablowych, listwach PCV, podłogach technologicznych,
    2) okablowanie, w miarę możliwości, nie jest prowadzone przez ogólnie dostępne strefy; w przypadku prowadzenia okablowania przez takie miejsca stosowane są środki uniemożliwiające bądź ograniczające dostęp do okablowania przez osoby nieupoważnione,
    3) przy projektowaniu przebiegu linii sieci teleinformatycznej poza strefami administracyjnymi wykorzystywane są w maksymalnym stopniu rozwiązania wykorzystujące technologie światłowodowe,
    4) w instalacji okablowania oddzielono kable zasilające od okablowania komunikacyjnego w celu unikania interferencji,
    5) w instalacji okablowania zastosowano jednoznaczne i wyraźne oznakowanie umożliwiające identyfikację kabli i sprzętu w celu zmniejszenia ryzyka błędów takich, jak niewłaściwe połączenie lub zastosowanie nieodpowiedniego kabla,
    6) kable komunikacyjne wyposażone są w zabezpieczenia odgromowe (jeżeli ma zastosowanie),
    7) prowadzi się kompletną i aktualną dokumentację połączeń fizycznych i logicznych w celu zmniejszenia prawdopodobieństwa błędów.
2. Pomieszczenia, w których znajdują się panele połączeniowe, węzły telekomunikacyjne i szafy dystrybucyjne objęte są systemem kontroli dostępu.
3. Niewykorzystywane segmenty sieci strukturalnej są odłączane od sieci teleinformatycznej.
4. W przypadku systemów wskazanych w procesie szacowania ryzyka jako kluczowe, są uwzględnione następujące zabezpieczenia obejmujące:
    1) stosowanie zapasowych (awaryjnych) dróg komunikacyjnych lub mediów transmisyjnych zapewniających odpowiedni poziom bezpieczeństwa,
    2) korzystanie z kabli światłowodowych.
5. Badanie właściwości transmisyjnych okablowania strukturalnego przeprowadzane jest przez Administratora Systemu nie rzadziej niż raz na 2 lata.

§ 37.

Eksploatacja urządzeń zasilających

1. Wszystkie urządzenia sieci teleinformatycznej są zasilane napięciem o parametrach zgodnych z wymaganiami producenta.
2. Urządzenia teleinformatyczne muszą być zasilane z wydzielonej instalacji elektrycznej.
3. Urządzenia sieci teleinformatycznej, od ciągłości pracy, których zależne jest realizowanie podstawowych zadań Agencji, muszą być zasilane z gwarantowanych źródeł.
4. Gwarantowane zasilanie uzyskiwane jest przez zastosowanie dywersyfikacji zewnętrznych źródeł energii elektrycznej z samoczynnym załączaniem rezerwy (SZR),

zastosowanie zasilaczy bezprzerwowych (UPS), zastosowanie awaryjnych agregatów prądotwórczych.

5. Konfiguracja zasilania gwarantowanego wynika z Planu Zapewnienia Ciągłości Działania Agencji.
6. Dobór urządzeń podtrzymujących zasilanie pod względem wydajności mocowej poprzedzane jest przeprowadzeniem udokumentowanego bilansu mocy.
7. Każde urządzenie sieci teleinformatycznej jest opatrzone tabliczką, z której wynika skąd dane urządzenie jest zasilane, zawierającą nazwę rozdzielnicy lub tablicy zabezpieczeń oraz nazwę pola w rozdzielnicy lub bezpiecznika na tablicy zabezpieczeń.
8. Stan zasilania zasobów sieci teleinformatycznej, którym nadano status zasobu kluczowego, jest na bieżąco monitorowany przez Administratora Systemu. Jakość zasilania pozostałych zasobów sieci teleinformatycznej musi być okresowo sprawdzana.
9. Zasilacze bezprzerwowe, zasilające kluczowe zasoby sieci teleinformatycznej, raportują stan swojej pracy (zasilanie z sieci, zasilanie z baterii) oraz parametry baterii (jej stopień naładowania i przewidziany czas pracy z baterii przy danym obciążeniu) systemom operacyjnym serwerów. W przypadku, gdy stopień naładowania baterii osiągnie w czasie pracy z baterii poziom, którego przekroczenie nie gwarantuje podtrzymania ciągłości pracy, system operacyjny wymusza automatyczne zamknięcie aplikacji i baz danych oraz kontrolowane wyłączenie serwera.
10. W przypadku, gdy automatyczne raportowanie nie jest technicznie możliwe Administrator Systemu dokonuje okresowych, raz na tydzień, oględzin polegających na sprawdzeniu wskazań paneli sterujących (według instrukcji techniczno-eksploatacyjnych). Oględziny muszą być odnotowywane w dzienniku pracy systemu.
11. Elementy systemu zasilania gwarantowanego podlegają okresowym przeglądom i konserwacjom w zakresie określonym przez producenta.
12. Akumulatory podlegają wymianie po okresach eksploatacji przewidzianych w instrukcjach użytkowania.
13. Serwisowanie urządzeń zasilających przeprowadzane jest wyłącznie przez autoryzowane podmioty zewnętrzne.
14. Przeglądy, konserwacje i serwisowanie podlega odnotowaniu w dzienniku pracy systemu.
15. Agregaty prądotwórcze są okresowo uruchamiane w okresach i zakresie przewidzianych przez ich producentów.

Załącznik nr 1 do Regulaminu eksploatacji systemów teleinformatycznych - Rejestr kopii zapasowych

L.p.	Nazwa systemu lub aplikacji	Lokalizacja jednostki danych	Nazwa serwera	Typ danych (system operacyj-ny, baza danych, pliki, poczta, inne)	Typ backupu (pełny, przyrostowy, różnicowy)	Wolumen [GB]
1						
2						
3						
4						
5						
6						
7						

cd.:

L.p.	Nazwa systemu lub aplikacji	Częstotliwość wykonywania backupu	Ilość kopii zapasowych	Sposób wykonywania kopii	Okres przechowywania	Miejsce przecho-wywania kopii zapasowych	Okno czasowe backupu
1							
2							
3							
4							
5							
6							
7							

Załącznik nr 2 do Regulaminu eksploatacji systemów teleinformatycznych - Ewidencja bezpiecznych kopert

1. Ewidencja bezpiecznych kopert prowadzona jest w książce ewidencji haseł, która zawiera:
    1) Numer ewidencyjny,
    2) Oznaczenie przynależności hasła zawartego w kopercie (nazwa systemu, zasobu, komputera, elementu aktywnego, itp.),
    3) Imię i nazwisko, pełnioną funkcję oraz podpis osoby składającej kopertę (właściciela hasła),
    4) Datę złożenia koperty z hasłem,
    5) Podpis osoby przyjmującej kopertę na przechowanie,
    6) Datę wygaśnięcia ważności hasła zawartego w kopercie,
    7) Adnotację o wydaniu koperty z hasłem (użyciu awaryjnym).

Wzór etykiety na kopercie:

Właściciel hasła	**Imię i nazwisko**
Nazwa systemu, zasobu lub komputera, do którego przynależy hasło	Nazwa
Numer kolejny hasła	01, 02, ...
Daty początku i końca okresu ważności hasła	dd-mm-rr - dd-mm-rr
Data złożenia	dd-mm-rrrr

Załącznik nr 3 do Regulaminu eksploatacji systemów teleinformatycznych - Dziennik pracy systemu

Lp.	Rodzaj zdarzenia	Opis zdarzenia	Rozpoczęcie pracy [data, godzina]	Zakończenie pracy [data, godzina]	Nazwisko i imię osoby dokonującej wpisu	Konto, które zostało użyte do obsługi zdarzenia	Podjęte działania naprawcze
1	2	3	4	5	6	7	8

Załącznik nr 4 do Regulaminu eksploatacji systemów teleinformatycznych - Wniosek dotyczący użytkowania programu narzędziowego

Część I

(Wypełnia kierownik komórki/jednostki organizacyjnej/Właściciel Zasobu)

1) Komórka organizacyjna:

.....

2) Nazwa programu narzędziowego, wersja i krótki opis

.....

Program wewnętrzny (część systemu lub aplikacji)		☐
Program zewnętrzny		☐
Wymagane uprawnienia w systemie (zwykły użytkownik, administrator, supervisor itp.) – opcjonalnie, jeśli Wypełniający dysponuje taką wiedzą	.....	
Szczegółowe informacje techniczne i dostępność (np. URL producenta, dostawcy)	.....	
Okres użytkowania programu:	Regularnie, z częstotliwością <....>, bezterminowo	☐
	Regularnie, z częstotliwością <....> do: (data)	☐
	Jednorazowo	☐

3) Imiona i nazwiska użytkowników:

.....

.....

4) Uzasadnienie wniosku:

.....

.....

.....

(data i podpis kierownika komórki/jednostki organizacyjnej/Właściciela Zasobu)

Część II Ocena zasadności wniosku (w aspekcie bezpieczeństwa informacji i systemów teleinformatycznych)

(wypełnia dyrektor komórki właściwej ds. bezpieczeństwa informacji)

Decyzja pozytywna	□	Decyzja negatywna	□

Uzasadnienie:

.....

.....

……

(data i podpis dyrektora komórki właściwej ds. bezpieczeństwa informacji)

Część III Informacje o realizacji wniosku

(Wypełnia Administrator Systemu)

Identyfikator wniosku: .....

.....

.....

.....

Nadany(e) identyfikator(y) (ID) użytkownika(ów) .....

.....

Poziom uprawnień (przywilejów) .....

…….

(data i podpis Administratora Systemu)