

Załącznik nr 11 do Zarządzenia Nr 25/2025 Prezesa Agencji Restrukturyzacji i Modernizacji Rolnictwa zmieniającego zarządzenie w sprawie wprowadzenia Polityki bezpieczeństwa informacji w Agencji Restrukturyzacji i Modernizacji Rolnictwa

Załącznik nr 12 do Polityki bezpieczeństwa informacji w ARiMR

REGULAMIN EKSPLOATACJI SYSTEMÓW TELEINFORMATYCZNYCH (ICT)

Spis treści:

§ 1.....	3
Definicje.....	3
Rozdział 1. Podstawowe zasady eksploatacji systemów teleinformatycznych.....	4
Podział obowiązków w eksploatacji	4
Monitorowanie pojemności i wydajności systemów	4
Ochrona przed szkodliwym oprogramowaniem	5
Kontrola licencjonowanego oprogramowania	6
Zarządzanie kopiami zapasowymi i archiwalnymi	7
Zarządzanie poprawkami i podatnościami technicznymi	8
Rozdział 2. Zasady bezpieczeństwa sieci	9
Ogólne mechanizmy bezpieczeństwa sieci	9
Uwierzytelnianie węzłów.....	10
Ochrona urządzeń sieciowych.....	10
Bezpieczeństwo zdalnego dostępu do portów diagnostycznych i konfiguracyjnych.....	11
Bezpieczeństwo dostępu do sieci publicznych (Internet)	11
Rozdział 3. Bezpieczeństwo systemów operacyjnych.....	12
Ogólne mechanizmy bezpieczeństwa	12
Identyfikacja i uwierzytelnianie użytkowników	12
System zarządzania hasłami.....	13
Użycie programów narzędziowych.....	13
Ograniczenia czasowe sesji połączeniowej.....	14
Eksploatacja aplikacji w systemach teleinformatycznych Agencji.....	14
Świadczenie usług informatycznych przez Podmioty zewnętrzne.....	15
Rozdział 4. Zarządzanie zmianami w systemach teleinformatycznych Agencji	16
Odbiór systemu teleinformatycznego	16

Kontrola zmian w eksploatacji.....	16
Bezpieczeństwo dokumentacji systemu.....	18
Rozdział 5. Zarządzanie wymiennymi nośnikami komputerowymi.....	18
Użytkowanie nośników.....	18
Wycofanie z eksploatacji nośników komputerowych.....	19
Rozdział 6. Bezpieczeństwo wymiany danych	19
Bezpieczeństwo serwisów intranetowych i ekstranetowych.....	19
Bezpieczeństwo wymiany poczty elektronicznej wewnętrznej i zewnętrznej	19
Konserwacja i naprawa sprzętu.....	20
Zabezpieczenie sprzętu poza siedzibą.....	20
Rozdział 8. Zarządzanie dostępem do systemów teleinformatycznych.....	21
Rejestrowanie użytkowników i przypisanie praw dostępu	21
Zarządzanie przywilejami	21
Zarządzanie hasłami użytkowników	22
Zasady dostępu do plików i katalogów	23
Rozdział 9. Zasady monitorowania systemów i ich użycia	24
Mechanizmy monitorowania systemów.....	24
Dziennik pracy systemu	25
Synchronizacja zegarów.....	26
Bezpieczeństwo okablowania	26
Eksploatacja urządzeń zasilających	27
Rozdział 10.	28
Chmura.....	28
Cyber Threat Intelligence.....	29
Załącznik nr 1 do Regulaminu eksploatacji systemów teleinformatycznych - Rejestr kopii zapasowych.....	30
Załącznik nr 2 do Regulaminu eksploatacji systemów teleinformatycznych - Ewidencja bezpiecznych kopert.....	31
Załącznik nr 3 do Regulaminu eksploatacji systemów teleinformatycznych - Dziennik pracy systemu	32
Załącznik nr 4 do Regulaminu eksploatacji systemów teleinformatycznych - Wniosek dotyczący użytkowania programu narzędziowego.....	33

§ 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. identyfikatory, 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 (kopia bezpieczeństwa) – duplikat danych, przechowywany na innym niż macierzystym 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 zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi (ISO 7498-2: 1989);
- 12) spam – niepożądana przesyłka poczty elektronicznej kierowana do niezdefiniowanego adresata, generująca koszty po jego stronie;
- 13) uwierzytelnianie – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu (np. użytkownika lub innej aplikacji, systemu);
- 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 – uzgodniona i zaakceptowana wcześniej zmiana konfiguracji urządzeń lub sposobu/ zakresu świadczenia usług;
- 17) zmiana infrastruktury/ usługa awaryjna - zmiana podejmowana w trybie nagłym wynikająca z konieczności usunięcia awarii lub błędu w systemie;

- 18) przywilej – specjalne uprawnienie wyższe od podstawowego prawa dostępu w systemie lub aplikacji (np. umożliwiające zarządzanie użytkownikami, rolami, itp.), stosowane jedynie dla wybranych pracowników, w szczególności uprawnienie administratora;
- 19) ICT – technologie informacyjno-komunikacyjne;
- 20) Chmura (cloud computing) - to technologia, która pozwala na przetwarzanie danych przez Internet. Dzięki niej można korzystać z zasobów, usług lub aplikacji bez konieczności instalowania ich na urządzeniach lokalnych;
- 21) Cyber Threat Intelligence – poddziedzina cyberbezpieczeństwa, która koncentruje się na zbieraniu, analizie danych dotyczących potencjalnych lub istniejących zagrożeń cybernetycznych oraz na zwalczaniu zagrożeń.

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 Procesu/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 tę 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 (ang. 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 domeny, 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. Sprzęt teleinformatyczny użytkowany w Agencji chroniony jest podczas pracy dedykowanymi systemami zabezpieczającymi, takimi jak np. systemy AV (antywirusowe, antyspamowe), systemy wykrywające i blokujące ataki IDS/IPS, zapory NGFW (ang. Next-generation firewall), serwery proxy, sondy filtrujące ruch sieciowy, itp.
2. Użytkowane poza systemem Agencji wymienne komputerowe nośniki danych, 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 i moduły behawioralne.
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 podlegają rejestrowaniu w dzienniku pracy systemu.

§ 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 ostrzeżenie 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 dyrektorowi komórki właściwej ds. bezpieczeństwa.

§ 6.

Zarządzanie kopiami zapasowymi i archiwalnymi

1. Kopie zapasowe systemów, aplikacji, baz danych i dokumentów w postaci cyfrowej 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.
7. Dla wskazanych dokumentów, systemów, baz danych i aplikacji podlegających tworzeniu kopii zapasowych:
 - 1) Administrator Systemu w porozumieniu z Właścicielem Procesu/Właścicielem Zasobu określa strategię tworzenia kopii uwzględniającą: częstotliwość tworzenia kopii, rodzaj kopii (przyrostowa, pełna, różnicowa), ilość kopii, miejsce, okres i sposób przechowywania kopii, rotację nośników,
 - 2) Administrator Systemu określa 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 Księżce Procedur KP-611-186-ARiMR.
10. Tworzenie kopii odbywa się zgodnie z procedurą tworzenia i odtwarzania kopii zapasowych i podlega rejestracji. Przykładowy 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/Właścicielem Ryzyka 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 niszczone 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.
20. W przypadku, gdy transportowane nośniki zawierają dane osobowe w postaci niezaszyfrowanej, przed realizacją usługi należy podpisać z Podmiotem zewnętrznym dodatkową umowę powierzenia przetwarzania danych osobowych.

§ 7.

Zarządzanie poprawkami i podatnościami technicznymi

1. Zarządzanie poprawkami i podatnościami 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 o:

- 1) wyniki testów bezpieczeństwa systemów i aplikacji teleinformatycznych przeprowadzonych przez departament właściwy ds. bezpieczeństwa,
 - 2) informacje uzyskane od producentów urządzeń sieciowych, systemów operacyjnych i aplikacji oraz od profesjonalnych organizacji zajmujących się tematyką bezpieczeństwa informacji i systemów teleinformatycznych,
 - 3) wyniki automatycznych skanerów podatności.
4. Poprawki techniczne, w zależności od ich krytyczności, o ile to możliwe są testowane w środowisku testowym zanim zostaną wprowadzone do środowiska produkcyjnego. Administrator Systemu prowadzi rejestr dokonywanych zmian.
 5. Wprowadzanie poprawek niekrytycznych bezpośrednio do środowiska produkcyjnego może być wykonane wyłącznie po uzyskaniu akceptacji Właściciela Procesu/Właściciela Zasobu/Właściciela Ryzyka. Wprowadzanie poprawek podlega dokumentowaniu w dzienniku pracy systemu,
 6. W przypadku poprawek krytycznych, Administrator Systemu wdraża niezwłocznie poprawkę informując o tym Właściciela Procesu/Właściciela Zasobu/Właściciela Ryzyka.

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) właściwe (z punktu widzenia bezpieczeństwa informacji) skonfigurowanie aplikacji, usług lub systemów operacyjnych,
 - 7) aktualizowanie aplikacji, systemów operacyjnych oraz usług sieciowych do aktualnych, bezpiecznych i stabilnych wersji, posiadających wsparcie techniczne producenta,
 - 8) fizycznych zabezpieczeń dostępu do systemów,
 - 9) rozdzielania środowisk produkcyjnych od testowych i developerskich.
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 routingu 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).
8. W agencji stosuje się:
 - 1) Segmentację sieci, która oddziela sieć użytkowników od sieci serwerowej,
 - 2) Systemowe filtrowanie stron WWW.

§ 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 itp.).
2. Za zgodą Komitetu, sieć teleinformatyczna Agencji może być połączona z innymi sieciami zewnętrznymi. Warunki takiego połączenia określone są przez reguły filtrowania zapór sieciowych ustalone 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, systemy antymalwerowe).
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 wyłączonego 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 z rzędu podał błędne hasło jest blokowany; odblokowania dokonuje Administrator Systemu 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 hasel,
 - 2) wybór i zmianę hasel przez użytkowników,
 - 3) potwierdzanie zmiany hasel dla uniknięcia błędów podczas ich wprowadzania,
 - 4) wymuszenie wyboru hasel o odpowiedniej jakości, tj.: składających się co najmniej z 12 znaków, zawierających małe i wielkie litery oraz cyfry i znaki specjalne,
 - 5) wymuszenie zmiany hasel z ustaloną częstotliwością, w przypadku systemów przetwarzających dane osobowe zmiana hasła następuje nie rzadziej niż co 90 dni,
 - 6) wymuszenie zmiany hasel tymczasowych przy pierwszym rejestracji się w systemie, przy czym hasła te muszą być generowane indywidualnie,
 - 7) pamiętanie hasel przez system w celu zapobiegania ponownemu ich użyciu, minimalna liczba hasel pamiętanych przez system wynosi 5,
 - 8) domyślne informacje uwierzytelniające w postaci predefiniowanej lub przekazanej przez dostawców zostają zmienione bezpośrednio po instalacji systemów lub oprogramowania.
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/Właściciela Ryzyka, którego wzór zamieszczono w załączniku nr 4 do niniejszego Regulaminu.
2. Poziom uprawnień umożliwiający uruchamianie programów narzędziowych jest udokumentowany.
3. Administrator Systemu rejestruje 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/Właściciel Ryzyka 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/Właściciel Ryzyka 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/Właściciel Ryzyka w Centrali oraz w razie potrzeby, dyrektor oddziału regionalnego (zgodnie z §6 ust. 4 Polityki), który jest także Właścicielem Ryzyka w określonym terytorialnie zakresie zarządzania, dla użytkowników w oddziale regionalnym i przynależnych biurach powiatowych.
2. Uprawnienia administratora są nadawane ograniczonej liczbie użytkowników.
3. Mechanizm dziedziczenia uprawnień administratora aplikacji na podstawie uprawnień administratora nadanych w systemie operacyjnym lub na platformie bazodanowej jest zablokowany.
4. Właściciel Procesu/Właściciel Zasobu/Właściciel Ryzyka 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.
5. Systemy operacyjne pracujące w Agencji, służące do przetwarzania danych osobowych powinny zapewnić funkcjonalność maskowania danych.

§ 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/Właściciel Ryzyka na podstawie informacji dostarczonych przez Administratora Systemu.
3. W szczególności, Właściciel Procesu/Właściciel Zasobu/Właściciel Ryzyka 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/Właściciel Ryzyka, 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 informacji 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 jakiegokolwiek 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 oszacowany i że zastosowano odpowiednie środki techniczne i organizacyjne, zapewniające poziom bezpieczeństwa zgodny z polityką oraz przepisami prawa,
 - 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 błędów 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/Właściciel Ryzyka, zaś za wykonywanie 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.
- 6a. Administrator Systemu ustanawia konfiguracje sprzętu, oprogramowania, usług oraz sieci i przedstawia je do formalnego zatwierdzenia przez KSBI.
- 6b. Administrator Systemu zobowiązany jest do zarządzania oraz okresowego monitorowania konfiguracji.
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/Właściciela Ryzyka.
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 podlegają 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 szafach zlokalizowanych w strefie administracyjnej.
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. Za zapewnienie bezpieczeństwa informacjom wrażliwym przewożonym pomiędzy lokalizacjami odpowiada pracownik przewożący.

§ 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/Właściciela Ryzyka.
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/ Właściciela Ryzyka.
2. Pracownik wyznaczony przez Właściciela Procesu/Właściciela Zasobu/Właściciela Ryzyka 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 Księżce 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 Administrator Systemu udostępnia na żądanie Właściciela Procesów/Właściciela Zasobów/Właściciela Ryzyka. Na podstawie przekazanego rejestru Właściciele Procesów/Właściciele Zasobów/Właściciele Ryzyka przeprowadzają przegląd uprawnień 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/Właściciela Ryzyka. 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/Właścicieli Ryzyka.
9. Konta domenowe użytkowników nieużywane przez okres 30 dni są blokowane.
10. Konta techniczne podlegają niezależnemu bieżącemu nadzorowi.

§ 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 Księżce 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 na danym 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 przechowywane są w postaci zaszyfrowanej. Dopuszcza się przechowywanie haseł w wersji elektronicznej poprzez zastosowanie oprogramowania typu „password manager” z bazą szyfrowaną minimum algorytmem AES lub Twofish.
 9. Do przechowywania hasła awaryjnego 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 przechowywane są 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/Właściciela Ryzyka 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/Właściciela Ryzyka 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/Właściciela Ryzyka 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.
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 informacji wyznaczony zespół w komórce właściwej ds. bezpieczeństwa, a także zespół Administratora 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, 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 mogą być prowadzone w oparciu o logi systemowe oraz inne rejestry zapewniające informacje o których mowa w ust. 1-4.
 7. Dzienniki prowadzone są przez administratora odpowiedzialnego za dany serwer, urządzenie sieciowe, aplikację.
 8. Dzienniki systemowe lub ich części prowadzone są w formie elektronicznej lub papierowej (dziennik może być prowadzony wg wzoru określonego w załączniku nr 3).
 9. 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 jest na bieżąco monitorowany przez Administratora Systemu.
9. Zasilacze bezprzerwowe, 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 podlegają odnotowaniu w dzienniku pracy systemu.
15. Agregaty prądotwórcze są okresowo uruchamiane w okresach i zakresie przewidzianych przez ich producentów.

Rozdział 10.

§ 38.

Chmura

1. Dokumenty wrażliwe, w tym zawierające dane osobowe udostępniane podmiotom zewnętrznym należy zabezpieczyć zgodnie z wymogami regulaminu danych osobowych.
2. Pracownik odpowiada za przydział uprawnień do plików zamieszczonych przez niego w przydzielonym zasobie chmurowym, w szczególności uwzględniając zasadę minimalnych przywilejów, wiedzy koniecznej, czasu dostępu.
3. Przegląd uprawnień do chmury odbywa się zgodnie z regulaminem nadzoru.
4. Operator chmury gwarantuje, że dane osobowe przetwarzane w chmurze nie opuszczają terenu unii europejskiej.
5. Chmura podlega polityce Backupu przyjętej przez Administratora Systemu.
6. W przypadku zmiany operatora chmury wymagane jest przeprowadzenie analizy ryzyka, strategii wyjścia dla usług w chmurze. Opracowane dokumenty podlegają akceptacji KSBI.
7. Przy wyborze zewnętrznego dostawcy usług chmurowych należy wziąć pod uwagę zapisy normy ISO/IEC 27002 dotyczących bezpieczeństwa usług chmurowych.
8. Za bezpieczeństwo chmury odpowiada Administrator Systemu.

§ 39.

Cyber Threat Intelligence

1. W organizacji gromadzi się i analizuje informacje dotyczące cyberbezpieczeństwa informacji w celu stworzenia rozpoznania zagrożeń.
2. Rozpoznawanie zagrożeń realizowane jest w trzech kategoriach:
 - 1) Strategiczne
 - 2) Taktyczne
 - 3) Operacyjne
3. Na podstawie zebranych informacji podejmowane są działania mające na celu minimalizację zagrożeń.

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 operacyjny, 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 przechowywania 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)		Y
Program zewnętrzny		Y
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	Y
	Regularnie, z częstotliwością <....> do: (data)	Y
	Jednorazowo	Y

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	Y	Decyzja negatywna	Y
-------------------	---	-------------------	---

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)