Instrukcja zarządzania systemem informatycznym

ZATWIERDZAM
BURMISTRZ
mgr Piotr Ćwikła
.....
podpis Burmistrza

Łobez 2018

METRYKA

Nazwa przedsiębiorstwa	Urząd Miejski Łobez		
Tytuł dokumentu	Instrukcja zarządzania systemem informatycznym		
Opis	W skład dokumentu wchodzą: Instrukcja zarządzania systemem informatycznym wraz z załącznikami		
Zastosowanie	Wszystkie komórki organizacyjne		
Plik	Instrukcja zarządzania systemem informatycznym		
Status	Dokument zatwierdzony, obowiązujący do stosowania od dnia ..... 2018 r.	Liczba stron	25

HISTORIA DOKUMENTU

Wersja	Data wersji	Akcja*	Rozdziały**	Autor / Autorzy	Zatwierdził
1.00	15.07.2018	utworzenie	wszystkie	Krzysztof Rychel	
2.00	15.10.2018	modyfikacja	wszystkie	Krzysztof Rychel	

* Np.: utworzenie nowego dokumentu, modyfikacja, weryfikacja, uzupełnienie.

** Wymienić rozdziały, w których dokonano zmian.

Spis treści

1. Cel instrukcji

Instrukcja określa sposób zarządzania systemem informatycznym wykorzystywanym do przetwarzania danych osobowych w stosunku, do których jednostka pełni funkcję administratora, współadministratora bądź przetwarzającego lub jest odbiorcą danych. Celem opisanych poniżej działań, jest zabezpieczenie danych osobowych przed zagrożeniami, w tym zwłaszcza przed ich udostępnieniem osobom nieupoważnionym, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.

Zasady opisane w niniejszym dokumencie są zgodne z obowiązującymi wymaganiami prawnymi, w szczególności odpowiadają wymogom *rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s.1)* i są zgodne z przyjętą w jednostce *Polityką ochrony danych osobowych*. Niniejszy dokument jest integralną częścią przyjętej Polityki ochrony danych osobowych w jednostce. Wszystkie użyte pojęcia, określenia osób, swoje zdefiniowanie znajdują w Rozdziale 2. Definicje Polityki ochrony danych osobowych.

Instrukcja zarządzania systemem informatycznym stanowi zbiór zasad postępowania w obszarze IT, związanym z przetwarzaniem danych osobowych, za wdrożenie i przestrzeganie, których odpowiada osoba sprawująca funkcję administratora systemu informatycznego (dalej: ASI), niezależnie od sposobu i formy jej zatrudnienia w jednostce.

2. Uprawnienia dostępu do systemów informatycznych, nadawanie i obieranie

2.1 Dostęp do systemu informatycznego służącego do przetwarzania danych osobowych, posiada wyłącznie ASI oraz osoba upoważniona do ich przetwarzania i zarejestrowana, jako użytkownik w systemie przez administratora systemu informatycznego.

2.2 Podstawą do nadania uprawnień przez administratora systemu informatycznego do przetwarzania danych osobowych w systemie informatycznym, jest upoważnienie do przetwarzania danych osobowych wydane przez administratora danych osobowych, na formularzu stanowiącym **załącznik nr 5** do *Polityki ochrony danych osobowych.* Przedmiotowy formularz winien określać systemy, do których udziela się użytkownikowi dostęp. Uprawnienia, o których mowa ASI może nadać po nadaniu upoważnienia użytkownikowi do czynności przetwarzania danych, przez administratora danych osobowych.

2.3 Osoby uprawnione do wnioskowania o nadanie uprawnień do systemów informatycznych, w tym do systemów, w których przetwarzane są dane osobowe określa *Polityka ochrony danych osobowych*.

2.4 ASI w związku z nadawaniem uprawnień dostępowych do systemu informatycznego zobowiązuje się do:

- ✓ określenia w formie pisemnej zasad tworzenia loginów do systemów informatycznych o ile twórca systemu lub administrator centralny systemu nie określił zasad ich tworzenia;
- ✓ w przypadku, gdy dana osoba na podstawie wydanego upoważnienia do przetwarzania danych osobowych, otrzymuje uprawnienia dostępowe do systemów informatycznych po raz pierwszy, informuje ją o zasadach bezpieczeństwa związanych z ich użytkowaniem;
- ✓ nadaje osobie upoważnionej, indywidualny login i hasło do pierwszego zalogowania się w systemie i instruuje osobę o konieczności zmiany hasła po zalogowaniu się do systemu, wskazując sposób wykonania tej czynności;
- ✓ powstrzymania się przed nadaniem uprawnień dostępowych w przypadku, jeżeli dana osoba nie posiada upoważnienia do przetwarzania danych osobowych w wymaganym zakresie zatwierdzonego przez ADO;
- ✓ nadania użytkownikowi unikalnego loginu w systemie informatycznym i nie może być to login, który w przeszłości był już stosowany w systemie informatycznym. Sprawdzenie unikalności loginu odbywa się na podstawie *Rejestru osób upoważnionych do systemów,* którego wzór stanowi **załącznik nr 1** do niniejszej instrukcji;
- ✓ prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych w systemach informatycznych w postaci *Rejestru osób upoważnionych do systemów*;
- ✓ skonfigurowania systemu operacyjnego na jednostce komputerowej użytkownika w sposób zapewniający wymuszenie na nim zmiany hasła okresowo co 30 dni;
- ✓ hasła administracyjne (używane przez ASI) mogą być w szczególnych sytuacjach stosowane dłużej niż zaznaczono to powyżej, jednak nie dłużej niż 6 miesięcy oraz każdorazowo po rozwiązaniu umowy z administratorem systemu informatycznego;
- ✓ skonfigurowania systemu, by hasło dostępu do systemu informatycznego spełniało poniższe warunki:
  - długość co najmniej 8 znaków,
  - zawierało małe i duże litery,
  - zawierało cyfry lub znaki specjalne,
  - w trakcie wpisywania, nie było widoczne na ekranie monitora,
  - nie było jednakowe z loginem użytkownika,

- nie było poprzednio stosowane przez użytkownika – do 4 razy wstecz.

2.5 Login i hasło użytkownika, stanowią podstawowe środki uwierzytelniania dostępu do systemu informatycznego, który służy do przetwarzania danych osobowych.

2.6 W przypadku konieczności odebrania uprawnień, czynność ta jest realizowana również w oparciu o formularz, który stanowi **załącznik nr 6** do *Polityki ochrony danych osobowych.*

2.7 Wyrejestrowanie użytkownika z systemu może mieć charakter stały lub czasowy.

2.8 Przyczyną trwałego wyrejestrowania użytkownika z systemu informatycznego jest rozwiązanie lub wygaśnięcie stosunku pracy lub innego stosunku prawnego w ramach, którego zatrudniony był użytkownik, zmiana indywidualnego zakresu czynności. Trwałe wyrejestrowanie użytkownika z systemu jest równoznaczne z wygaśnięciem lub odwołaniem wydanego upoważnienia do przetwarzania danych osobowych.

2.9 Przyczynę czasowego wyrejestrowania użytkownika z systemu informatycznego może stanowić:

- ✓ jego nieobecność w pracy trwająca dłużej niż 31 dni kalendarzowych, o której winien poinformować ASI bezpośredni przełożony pracownika;
- ✓ zawieszenie w pełnieniu obowiązków służbowych, o którym administrator systemu informatycznego winien być poinformowany przez bezpośredniego przełożonego pracownika bądź przez komórkę ds. kadr.

3. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu informatycznego służącego do przetwarzania danych osobowych

3.1 Przed przystąpieniem do pracy w systemie informatycznym, użytkownik winien zapewnić sobie zorganizowanie stanowiska pracy z wykorzystaniem systemu informatycznego w sposób zgodny z przyjętymi poniżej zasadami bezpiecznego przetwarzania informacji.

3.2 Przed rozpoczęciem przetwarzania danych osobowych w systemach informatycznych użytkownik powinien sprawdzić, czy nie ma oznak fizycznego uszkodzenia sprzętu komputerowego. W przypadku wystąpienia jakichkolwiek nieprawidłowości, powiadamia bezpośredniego przełożonego i administratora systemu informatycznego.

3.3 Rozpoczęcie pracy na stacji roboczej następuje poprzez:

- ✓ uruchomienie komputera;
- ✓ wprowadzenie loginu i hasła lub samego hasła, w zależności od sposobu skonfigurowania jednostki;
- ✓ hasła są wprowadzane w sposób minimalizujący ryzyko podejrzenia ich przez osoby postronne;
- ✓ w przypadku problemów z rozpoczęciem pracy, spowodowanych odrzuceniem przez system wprowadzonego loginu i hasła, użytkownik natychmiast powiadamia o tym fakcie bezpośredniego przełożonego i administratora systemu informatycznego;
- ✓ w przypadku niestandardowego zachowania aplikacji przetwarzającej dane osobowe, pracownik natychmiast powiadamia o zaistniałym fakcie bezpośredniego przełożonego i administratora systemu informatycznego oraz powstrzymuje się przed dalszym korzystaniem z aplikacji.

3.4 Zabrania się wykonywania jakichkolwiek operacji w systemie informatycznym służącym do przetwarzania danych osobowych z wykorzystaniem loginu i hasła dostępu innego użytkownika.

3.5 W przypadku czasowego opuszczenia stanowiska pracy, użytkownik musi:

- ✓ dokonać zapisu wprowadzonych danych, wylogować się z systemu informatycznego służącego do przetwarzania danych osobowych lub,
- ✓ zablokować stację roboczą odpowiednią kombinacją klawiszy, przy czym odblokowanie może nastąpić dopiero po podaniu hasła [klawisze: windows+L lub klawisze: ctr+alt+delet].

3.6 W przypadku zakończenia pracy użytkownik musi:

- ✓ wylogować się z systemu informatycznego służącym do przetwarzania danych osobowych. Wylogowanie powinno być poprzedzone zapisem wprowadzonych danych, opcjonalnie sporządzeniem w miarę potrzeb kopii zapasowej danych oraz zabezpieczeniem przed nieuprawnionym dostępem nośników danych płyty CD, pendrive i innych, zawierających dane osobowe;
- ✓ zamknąć wszystkie aplikacje uruchomione na stacji roboczej;
- ✓ wyłączyć stację roboczą za pomocą odpowiednich poleceń, zawartych w zainstalowanym na niej systemie operacyjnym. Zabronione jest wyłączanie jednostki za pomocą przycisków „POWER" lub „RESET", (możliwe tylko i wyłącznie na wyraźne polecenie administratora systemu informatycznego);
- ✓ po wyłączeniu stacji roboczej, należy wyłączyć wszystkie pozostałe urządzenia z nią współpracujące, takie jak: monitor, drukarka, skaner, UPS, itp.;
- ✓ pozostawienie włączonych stacji roboczych poza godzinami pracy jednostki, możliwe jest po uzyskaniu zgody przełożonego i poinformowaniu o tym fakcie administratora systemu informatycznego;

- ✓ administrator systemu informatycznego prowadzi rejestr osób korzystających z systemów informatycznych poza godzinami pracy jednostki. Wzór rejestru stanowi **załącznik nr 2** do Instrukcji - *Rejestr osób korzystających z systemów informatycznych poza godzinami pracy jednostki.*

3.7 Powyżej wskazane zasady obowiązują przy przetwarzaniu danych osobowych również na komputerach przenośnych, w tym również poza siedzibą jednostki z wyjątkiem konieczności powiadamiania administratora systemu informatycznego o użytkowaniu urządzenia poza godzinami pracy jednostki.

3.8 Administrator systemu informatycznego prowadzi *Rejestr mobilnych jednostek komputerowych użytkowanych poza siedzibą jednostki* wg wzoru zamieszczonego w **załączniku nr 3** do niniejszej instrukcji. W rejestrze należy uwzględnić również tablety oraz smartfony.

3.9 Użytkownicy, którym zostały powierzone komputery przenośne powinni chronić je przed uszkodzeniem, kradzieżą i dostępem osób postronnych. Sposób użytkowania komputerów przenośnych określa *Regulamin użytkowania komputerów przenośnych* stanowiący **załącznik nr 4** do niniejszej instrukcji.

3.10 Pliki zawierające dane osobowe przechowywane na komputerach przenośnych muszą być zaszyfrowane i opatrzone hasłem dostępu.

3.11 Obowiązuje zakaz przetwarzania na komputerach przenośnych całych zbiorów danych nawet w postaci zaszyfrowanej.

3.12 Obowiązuje kategoryczny zakaz samodzielnej modernizacji, naprawy, aktualizowania jakiegokolwiek elementu wchodzącego w skład użytkowanego systemu informatycznego. Wszelkie zmiany, mogą być wykonane przez administratora systemu informatycznego lub w jego obecności przez podmiot serwisujący dany system informatyczny lub urządzenie.

4. Zasady tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

4.1 Do wykonywania kopii zapasowych całościowych baz danych, plików aplikacji oraz systemów wykorzystywanych do przetwarzania danych osobowych, upoważniony jest jedynie administrator systemu informatycznego.

4.2 Administrator systemu informatycznego prowadzi rejestr kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.

4.3 Dla każdego elementu wymienionego w pkt. 4.2 będącego przedmiotem wykonywania kopii zapasowych, administrator systemu informatycznego w porozumieniu z użytkownikiem (grupą użytkowników, komórką organizacyjną użytkującą elementy), określa częstotliwość wykonywania kopii zapasowych. Przedmiotowe ustalenia muszą zostać udokumentowane w postaci przyjętego harmonogramu wykonywania kopii zapasowych. Wzór *Harmonogramu wykonywania kopii zapasowych* stanowi **załącznik nr 5.**

4.4 Administrator systemu informatycznego w odniesieniu do każdego systemu, określi rodzaj wykonywanej kopii wybierając jej wariant z możliwych, o których mowa poniżej tj.

- ✓ standardowa – polega na skopiowaniu każdego wybranego pliku i wyczyszczeniu archiwa. Dzięki czemu przy tworzeniu kolejnej kopi zapiszą się pliki, w których zmieniło się archiwum. Tworzenie tego typu kopi trwa najdłużej. Zazwyczaj jest wykonywane przy tworzeniu pierwszej kopi;
- ✓ przyrostowa – wybór tego typu kopi zapasowej powoduje archiwizacje plików które zostały utworzone lub zmodyfikowane od momentu wykonania ostatniej kopi przyrostowej lub kopi normalnej. Proces odtwarzania danych polega na przywróceniu normalnej kopi zapasowej oraz kopi przyrostowych w kolejności tworzenia. Tworzenie kopi przyrostowej zajmuje mniej miejsca oraz mniej czasu niż w porównaniu z kopią normalną. Jednak odtwarzanie zajmuje więcej czasu;
- ✓ różnicowa – kopiuje tyle te pliki, które zmieniły się od czasu wykonania ostatniej kopii normalnej lub przyrostowej. Kopia różnicowa nie zmienia atrybuty archiwizacji plików. Aby przywrócić dane wystarczy kopia normalna i ostatnia kopia różnicowa. Kopia ta zajmuje więcej miejsca niż kopia przyrostowa, ale nie trzeba każdej wersji przechowywać na dysku, bo wystarczy najnowsza;
- ✓ codzienna – wykonuje kopie tylko tych plików które zostały utworzone lub zmienione w dni wykonania archiwizacji. Podczas wykonywania tej kopi nie jest czyszczony atrybut archiwizacji;
- ✓ kopia (backup) – polega na skopiowaniu zaznaczonych plików bez czyszczenia atrybutów archiwizacji. Opcja ta przydaje się dla osób, które wykonują kopie raz na jakiś czas i nie potrzebują regularnej archiwizacji lub chcą mieć dodatkową kopię pomiędzy cyklem archiwizacji.

4.4 Użytkownik może zapisywać i wykonywać kopie sporządzanych pism i innych dokumentów roboczych wyłącznie wtedy, gdy związane są z prowadzonymi przez niego sprawami i nie stanowią zbiorów danych osobowych lub częściowych wyciągów z nich.

4.5 Za dopuszczalne można uznać zapisywanie kopii, o których mowa w pkt. 4.4 na nośniku zewnętrznym pod warunkiem, że nośnik taki pod koniec każdego dnia pracy, będzie przekazywany do przechowania bezpośredniemu przełożonemu użytkownika.

4.6 Po upływie okresu użyteczności lub przechowywania, kopie zapasowe, a w szczególności zawierające dane osobowe powinny zostać skasowane lub zniszczone tak, aby nie było możliwe ich odczytanie.

4.7 Nośniki kopii zapasowych, które zostały wycofane z użycia, podlegają fizycznemu zniszczeniu z wykorzystaniem metod adekwatnych do typu nośnika w sposób uniemożliwiający odczytanie zapisanych na nich danych.

4.8 W przypadku likwidacji nośników informatycznych zawierających dane osobowe lub kopie zapasowe systemów informatycznych, służących do przetwarzania danych osobowych, należy przed ich likwidacją usunąć dane osobowe lub uszkodzić je w sposób uniemożliwiający ich odczyt. Z powyższych czynności likwidacji nośników należy sporządzić protokół.

5. Zasady postepowania z elektronicznymi nośnikami danych osobowych

5.1 Nie należy przechowywać zbędnych nośników zawierających dane osobowe oraz nieprzydatnych kopii zapasowych zawierających dane osobowe.

5.2 W jednostce dopuszcza się użytkowanie tylko i wyłącznie nośników wydanych przez administratora systemu informatycznego, który odpowiada za ich ewidencjonowanie. Ewidencja jest prowadzona wg wzoru stanowiącego **załącznik nr 7** do niniejszej instrukcji.

5.3 Elektroniczne nośniki informacji zawierające dane osobowe nie mogą być wynoszone poza pomieszczenia stanowiące obszar przetwarzania danych osobowych, określony w załączniku nr 10 do *Polityki ochrony danych osobowych.* Jedynym wyjątkiem jest sytuacja, gdzie kopie zapasowe ze względów bezpieczeństwa i zapewnienie możliwości przywrócenia lub odtworzenia działania są przechowywane poza siedzibą jednostki oraz sytuacje wymagające przeniesienia danych między różnymi lokalizacjami.

5.4 Elektroniczne nośniki informacji, a także wydruki i inne dokumenty zawierające dane osobowe przechowywane są w zamykanych szafach w pomieszczeniach stanowiących obszar przetwarzania danych osobowych, celem zabezpieczenia ich przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem i zniszczeniem.

5.5 Nośniki zawierające kopie zapasowe, których celem jest zapewnienie możliwości przywrócenia działania i odtworzenia danych po awarii lub innym zdarzeniu o charakterze katastroficznym, winny być przechowywane w innych lokalizacjach, niż lokalizacja jednostek komputerowych, z których dokonano kopii zapasowych, przy jednoczesnym spełnieniu wszystkich zasad bezpiecznego

przechowywania, dających gwarancję ich zabezpieczenia przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem i zniszczeniem oraz gwarancję pełnej dostępności na wypadek konieczności ich wykorzystania w celu przywrócenia lub odtworzenia działań jednostki.

5.6 Okres przechowywania nośników informacji zawierających kopie zapasowe dla poszczególnych systemów informatycznych służących przetwarzaniu danych osobowych określa **załącznik nr 5** do Instrukcji – *Harmonogram wykonywania kopii zapasowych.* Po upływie tego okresu nośniki danych są niszczone lub dane na nich zawarte trwale usuwane.

5.7 Dopuszcza się powierzenie niszczenia nośników (szczególnie papierowych) danych osobowych, wyspecjalizowanym podmiotom zewnętrznym, pod warunkiem:

- ✓ zawarcia umowy powierzenia danych osobowych do dalszego przetwarzania z tym podmiotem;
- ✓ zagwarantowania poufności danych przez usługodawcę;
- ✓ umożliwienia prowadzenia nadzoru nad procesem niszczenia nośników przez IOD lub upoważnionego przez niego pracownika jednostki;
- ✓ udokumentowania faktu przekazania nośników do zniszczenia protokołem.

5.8 W przypadku wycofania sprzętu komputerowego z użycia, dane osobowe na nim zapisane są kasowane przez administratora systemu informatycznego przy użyciu dedykowanego oprogramowania do bezpiecznego usuwania danych. W przypadku braku możliwości programowego usunięcia danych, dysk takiego urządzenia podlega fizycznemu zniszczeniu. Za zniszczenie danych odpowiada administrator systemu informatycznego. Zniszczenie nośnika potwierdzane jest protokołem przechowywanym przez administratora systemu informatycznego.

5.9 W przypadku przekazania sprzętu komputerowego do podmiotu zewnętrznego, celem jego naprawy, należy usunąć z niego wszystkie zapisy zawierające dane osobowe, jeżeli jest to niemożliwe naprawa/serwisowanie takiego sprzętu, może być realizowana jedynie w obecności administratora systemu informatycznego.

5.10 Przekazanie sprzętu komputerowego do podmiotu zewnętrznego musi być potwierdzone protokołem przekazania, a jego odbiór również winien być zaprotokołowany.

6. Sposób zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego służącego do przetwarzania danych osobowych

6.1 W celu zabezpieczenia systemu informatycznego przed działaniem niebezpiecznego oprogramowania zabrania się:

- ✓ uruchamiania użytkownikowi jakiegokolwiek oprogramowania, które nie zostało zatwierdzone do użytku w jednostce;
- ✓ samowolnego korzystania z nośników przenośnych innych niż wydane przez administratora systemu informatycznego;
- ✓ otwierania poczty elektronicznej, której tytuł (temat) nie sugeruje związku z pełnionymi obowiązkami służbowymi lub adres nadawcy budzi obawy. W przypadkach wątpliwych należy skonsultować się z administratorem systemu informatycznego;
- ✓ korzystania z Internetu w celach nie związanych z pełnionymi obowiązkami służbowymi;
- ✓ podłączania komputerów do sieci zewnętrznych za pośrednictwem modemów.

6.2 W przypadku zauważenia objawów mogących wskazywać na obecność niebezpiecznego oprogramowania, użytkownik zobowiązany jest powiadomić swojego przełożonego i administratora systemu informatycznego. Do objawów powyższych można zaliczyć:

- ✓ istotne spowolnienie działania systemu informatycznego;
- ✓ nietypowe działanie aplikacji;
- ✓ nietypowe komunikaty;
- ✓ utratę danych lub modyfikację danych.

6.3 System informatyczny jest zabezpieczony przed działaniem niebezpiecznego oprogramowania poprzez:

- ✓ oprogramowanie antywirusowe;
- ✓ zaporę sieciową;
- ✓ wykorzystywanie wyłącznie oprogramowania systemowego posiadającego wsparcie techniczne;
- ✓ automatyczną aktualizację oprogramowania systemowego oraz antywirusowego;
- ✓ konfigurację oprogramowania, o którym mowa powyżej w sposób minimalizujący ryzyko naruszenia bezpieczeństwa (ciągła praca w tle i wykrywanie zagrożeń w czasie rzeczywistym);
- ✓ monitoring ruchu sieciowego;

- ✓ zainstalowanie ww. oprogramowania na każdej stacji roboczej i jednostce komputerowej.
- ✓ stałe blokowanie dostępu do stron internetowych sklasyfikowanych jako potencjalnie niebezpieczne (np.: portale randkowe i erotyczne),

6.4 Za nadzór nad powyższymi zabezpieczeniami jest odpowiedzialny administrator systemu informatycznego, a w szczególności za:

- ✓ weryfikację aktualności sygnatur systemu antywirusowego i podejmowanie ewentualnych działań korekcyjnych;
- ✓ weryfikację logów systemu antywirusowego i podejmowanie działań korekcyjnych;
- ✓ przegląd logów zapory sieciowej oraz podejmowanie działań mających na celu zablokowanie ataków sieciowych;
- ✓ weryfikację poprawności aktualizacji oprogramowania systemowego.

7. Wykonywanie przeglądów i konserwacji systemów informatycznych oraz urządzeń służących do ich funkcjonowania

7.1 Konserwacja sprzętu i urządzeń pracujących w systemach informatycznych jednostki ma na celu, zapewnienie nieprzerwanej i bezpiecznej pracy tych systemów, zapobieganie utraty, uszkodzeniu lub naruszenia bezpieczeństwa.

7.2 Przeglądy i konserwacje urządzeń wchodzących w skład użytkowanych systemów informatycznych, są dokonywane przez administratora systemu informatycznego, wyznaczone przez niego osoby lub przez podmioty zewnętrzne w oparciu o zawarte umowy serwisowe.

7.3 W odniesieniu do użytkowanej w jednostce infrastruktury informatycznej realizowane są okresowe czynności konserwacyjne w sposób zapewniający, iż każdy jej element (jednostki robocze, drukarki, skanery, monitory itd.), zostanie objęty czynnościami, o których mowa minimum raz w roku. Harmonogram prac z tym związanych sporządza administrator systemu informatycznego wg **załącznika nr 6** do niniejszej instrukcji – *Harmonogram przeglądów i konserwacji urządzeń*. Przy tworzeniu harmonogramu należy uwzględnić zalecenia producenta urządzenia.

7.4 Prace serwisowe wykonywane na terenie jednostki przez podmioty zewnętrzne podlegają bezpośredniemu nadzorowi administratora systemu informatycznego lub osoby przez niego wyznaczonej.

7.5 Wszelkie prace serwisowe oraz prace, o których mowa w pkt. 5.9 niniejszej instrukcji wymagają sporządzenia protokołu zawierającego co najmniej następujące informacje:

- ✓ wskazanie osoby przeprowadzającej prace serwisowe lub przyjmującej sprzęt do serwisowania oraz podmiotu, którego osoba ta jest pracownikiem;
- ✓ wskazanie osoby nadzorującej przebieg prac serwisowych (dotyczy sytuacji, gdy prace realizowane są w siedzibie jednostki);
- ✓ przedmiot prac serwisowych (w szczególności identyfikator sprzętu w przypadku prac serwisowych dotyczących sprzętu, w przypadku oprogramowania określenie systemu będącego przedmiotem serwisu);
- ✓ zakres prac serwisowych i ich wynik;
- ✓ czas przeprowadzania prac serwisowych.

7.6 Zabronione jest wykonywanie czynności związanych z konserwacją i naprawą urządzeń wchodzących w skład systemów informatycznych samodzielnie przez ich użytkowników.

7.7 Powierzenie sprzętu użytkownikowi, nieodłącznie wiąże się z przekazaniem jemu instrukcji obsługi opracowanej przez producenta lub innego dokumentu, zawierającego zasady bezpiecznego użytkowania powierzonego sprzętu.

8. Kontrola licencjonowanego oprogramowania

8.1 Administrator systemu informatycznego celem uzyskania zapewnienia, iż jednostka wykorzystuje jednie legalne oprogramowanie, prowadzi spis użytkowanych w jednostce systemów, programów i aplikacji zawierający:

- ✓ informację o nośniku instalacyjnym (jeżeli występuje) i miejscu jego przechowywania;
- ✓ określenie licencji (np.: wersja jedno, wielostanowiskowa, z ograniczeniami, bez ograniczeń itp.) ze wskazaniem okresu jej ważności;
- ✓ określenie miejsca zainstalowania (ze wskazaniem nr inwentarzowego jednostki komputerowej lub jej nazwy, komórki organizacyjnej, nr pomieszczenia),

8.2 IOD niezależnie od innych osób posiada prawo do kontroli spisu licencjonowanego oprogramowania ze względu na charakter realizowanych działań.

8.3 Kontrole IOD licencjonowanego oprogramowania mogą być przeprowadzane w trybie doraźnym po uprzednim poinformowaniu kierownika jednostki.

8.4 Do przesłanek uruchamiających proces kontroli doraźnej w szczególności można zaliczyć:

- ✓ informację o popełnieniu lub podejrzeniu popełnienia czynu niedozwolonego przez pracownika, na żądanie, jego przełożonego lub innej osoby posiadającej wiedzę o takim zdarzeniu;

- ✓ otrzymanie zgłoszenia lub innej informacji o pojawieniu się lub podejrzeniu pojawienia się w systemie informatycznym nieautoryzowanego oprogramowania, aplikacji,

8.5 Nie rzadziej niż raz na dwa lata ASI w porozumieniu z IOD przeprowadza planową kontrolę spisu użytkowanego w jednostce oprogramowania.

8.6 Okresowo, nie rzadziej niż raz w roku, wszystkie komputery przenośne użytkowane poza lokalizacjami jednostki są sprawdzane przez administratora systemu informatycznego pod kątem obecności nieautoryzowanego oprogramowania.

8.7 W terminie do 20 stycznia każdego roku obrachunkowego celem zatwierdzenia, administrator systemu informatycznego przedstawia kierownikowi jednostki aktualne zestawienie przenośnych jednostek komputerowych, o których mowa w pkt. 8.6 wraz z harmonogramem ich przeglądu.

8.8 Do przeprowadzenia kontroli zgodności zainstalowanego oprogramowania z posiadanymi licencjami, a także zgodności z konfiguracją standardową, mogą zostać zastosowane narzędzia programistyczne umożliwiające m.in.:

- ✓ automatyczne sprawdzanie stacji roboczych i serwerów,
- ✓ centralne zarządzanie spisem licencjonowanego oprogramowania,
- ✓ automatyczne ostrzeganie przed przekroczeniem liczby licencji.

8.9 Administrator systemu informatycznego odpowiada za niezwłoczne usunięcie nielicencjonowanego oprogramowania, a informacja o przypadkach używania nieautoryzowanego oprogramowania jest przedstawiana kierownikowi jednostki.

9. Zarządzanie poprawkami technicznymi

9.1 Zarządzanie poprawkami ma na celu eliminowanie lub ograniczanie zidentyfikowanych podatności systemów informatycznych, programów.

9.2 Administrator systemu informatycznego zobowiązany jest do bieżącego i ciągłego monitorowania pojawiania się poprawek do poszczególnych usług sieciowych, systemów operacyjnych, programów i aplikacji wykorzystywanych w jednostce.

9.3 Administrator systemu informatycznego obowiązany jest do wprowadzania poprawek w oparciu o informacje uzyskane od producentów urządzeń sieciowych, systemów operacyjnych, programów i aplikacji oraz od profesjonalnych organizacji zajmujących się tematyką bezpieczeństwa informacji i systemów teleinformatycznych.

9.4 Poprawki techniczne, w zależności od ich krytyczności i istotności są testowane w środowisku

testowym, zanim zostaną wprowadzone do środowiska produkcyjnego. Administrator bezpieczeństwa informacji prowadzi rejestr dokonywanych zmian. Nie dotyczy to systemów, które samodzielnie rejestrują wprowadzone poprawki techniczne.

9.5 Wprowadzanie krytycznych i istotnych poprawek bezpośrednio do środowiska produkcyjnego przez ASI, może być wykonane wyłącznie po skonsultowaniu takiego stanu rzeczy z użytkownikami zasobu obsługiwanego przez system, program, aplikację, którego dotyczy poprawka.

10. Bezpieczeństwo systemów operacyjnych

10.1 W jednostce stosuje się następujące mechanizmy bezpieczeństwa systemów operacyjnych:

- ✓ uwierzytelnianie użytkowników, zgodnie z przyjętymi zasadami kontroli dostępu;
- ✓ rejestrowanie nieudanych prób dostępu do systemu;
- ✓ rejestrowanie użytkowników systemów operacyjnych;
- ✓ generowanie alarmów w przypadku naruszenia reguł bezpieczeństwa systemu;
- ✓ blokowanie dostępu po 10 minutach braku aktywności w sesji.

10.2 Systemy operacyjne użytkowane w jednostce muszą mieć włączone mechanizmy bezpiecznego logowania zapewniające (w zależności od możliwości technicznych):

- ✓ ujawnianie minimum informacji o systemie;
- ✓ wyświetlanie ostrzeżenia, że dostęp do systemu jest dozwolony jedynie dla uprawnionych użytkowników;
- ✓ unikanie wyświetlania komunikatów pomocniczych, które mogłyby pomóc nieuprawnionemu użytkownikowi przy nieautoryzowanych próbach dostępu;
- ✓ unikanie wskazywania, która część danych jest poprawna lub niepoprawna w przypadku wystąpienia błędu podczas logowania;
- ✓ ograniczenie liczby nieudanych prób logowania się do systemu do 3, a następnie blokowanie konta po 3 następujących po sobie nieudanych próbach logowania;
- ✓ wykonywanie zapisu każdego nieudanego logowania w logach zdarzeń;
- ✓ ograniczenie możliwości zalogowania się do systemu w określonych przedziałach czasowych („oknach logowania") w godzinach np. 6-18;
- ✓ blokowanie wyświetlania hasła w trakcie jego wprowadzania;
- ✓ szyfrowanie przesyłanych haseł.

10.3 Wszyscy użytkownicy systemów muszą posiadać unikalne identyfikatory użytkownika (loginy, identyfikatory ID użytkownika) do swojego wyłącznego użytku.

10.4 Dostęp do systemu dla użytkownika, który trzykrotnie pod rząd podał błędne hasło jest blokowany. Odblokowania dokonuje ręcznie administrator systemu informatycznego na pisemny wniosek bezpośredniego przełożonego pracownika.

11. Zarządzanie zmianami w systemach informatycznych

11.1 Kryteria odbioru systemu informatycznego obejmują dostarczenie przez dostawcę:

- ✓ w przypadku oprogramowania - dokumentacji technicznej, instrukcji dla administratora i użytkownika;
- ✓ w przypadku infrastruktury – dokumentacji powykonawczej obejmującej w szczególności schemat połączeń fizycznych i logicznych elementów infrastruktury;

11.2 Ponadto, kryteria odbioru obejmują:

- ✓ sprawdzenie wymagań wydajnościowych i pojemnościowych systemu informatycznego,
- ✓ dokumenty potwierdzające, że instalacja nowych systemów nie będzie miała negatywnego wpływu na istniejące systemy, szczególnie w chwilach największego obciążenia;
- ✓ dokumenty potwierdzające, że wpływ nowych systemów na bezpieczeństwo informacji, a w szczególności przetwarzanych danych osobowych został uwzględniony;
- ✓ szkolenia z zakresu posługiwania się i działania nowych systemów;

11.3 Odbiór nowo instalowanych systemów informatycznych lub oprogramowania systemowego obejmuje następujące główne elementy:

- ✓ wykonanie instalacji oprogramowania;
- ✓ wykonanie testowania systemu zakończone stosownym dokumentem potwierdzającym prawidłowość testów;
- ✓ odbiór oprogramowania potwierdzony stosownym dokumentem;
- ✓ odrzucenie oprogramowania potwierdzone stosownym dokumentem w przypadku negatywnych wyników testów;
- ✓ w przypadku wystąpienia jakichkolwiek rozbieżności, co do jakości produktu, może zostać zlecony zewnętrzny audyt mający na celu wyjaśnienie przyczyn rozbieżności.

11.4 Każdorazowo, w odniesieniu do systemów operacyjnych oraz użytkowanych aplikacji, wszelkie

ich zmiany na nowsze wersje administrator systemu informatycznego winien odnotować odrębnym dokumentem sporządzonym w dowolnej formie (notatka, protokół):

- ✓ wykaz dokonanych zmian w systemie (oprogramowaniu) w stosunku do poprzedniej wersji wraz z ich opisem;
- ✓ uaktualnienie dokumentacji opisującej system (oprogramowanie) uwzględniające zmiany dokonane.

11.5 Mechanizmy opisane w pkt. od 11.1 do 11.4 mają na celu zapewnianie poprawnego i bezpiecznego działania systemów informatycznych pracujących w jednostce.

11.6 Zarządzanie zmianami polega na koordynacji, nadawaniu priorytetów, zatwierdzaniu, planowaniu zasobów i oceną ryzyka w związku ze zmianami dokonywanymi w systemach informatycznych jednostki.

11.7 Każda zmiana w systemie informatycznym dotycząca jego kluczowych elementów musi być udokumentowana.

11.8 Zasady wskazane w niniejszym rozdziale odnoszą się do:

- ✓ zmian infrastruktury technicznej systemu informatycznego, sprowadzających się do wprowadzenia nowego elementu infrastruktury, zmodyfikowania lub usunięcia istniejącego elementu infrastruktury, poprawiania błędu w infrastrukturze, przy czym:

  - zmiana infrastruktury regularna – oznacza zmianę, która nie wymaga natychmiastowego wdrożenia,

  - zmiana infrastruktury awaryjna - stosowana w sytuacjach awaryjnych, gdzie czas implementacji zmiany jest krytyczny, z pominięciem lub uproszczeniem niektórych etapów (np. testów) przy założonym ryzyku,

  - zmiana infrastruktury rutynowa - zaakceptowane wcześniej działanie związane z relatywnie prostymi czynnościami np. wymiana drukarki lub monitora.

- ✓ zmian aplikacyjnych będących poprawkami (w tym usuwanie błędów) albo modyfikacjami, zmiany aplikacyjne są klasyfikowane, jako:

  - zmiany aplikacyjne regularne – oznaczają zmiany, które nie wymagają natychmiastowego wdrożenia,

  - zmiany aplikacyjne awaryjne – wprowadzane w stanie pilnej konieczności z powodu zagrożenia działania, aplikacji,

11.9 Za proces zarządzania zmianami odpowiedzialny jest administrator systemu informatycznego i kierownik komórki organizacyjnej, w której dokonuje się zmian.

11.10 Każda zmiana regularna jest poprzedzona udokumentowanym:

- ✓ opisem zmiany;
- ✓ opisem przyczyny zmiany wraz z podaniem aktów prawnych uzasadniających zmianę;
- ✓ opisem rodzaju wymaganych działań;
- ✓ szacowaniem ryzyka potencjalnego wpływu zmian;
- ✓ wykonaniem kopii zapasowej z możliwością odtworzenia stanu poprzedniego na wypadek nieprzewidzianych zdarzeń;
- ✓ przetestowaniem zmian.

11.11 Za realizację działań wskazanych w pkt. 11.10 odpowiada kierownik komórki organizacyjnej, w której realizowane są zmiany wspólnie z administratorem systemu informatycznego

11.12 Jeżeli zmiana ma charakter awaryjny, dokumentacja, o której mowa w pkt. 11.10 może być opracowana najpóźniej w przeciągu 7 dni od dokonania zmiany.

11.13 Zmiana mająca charakter awaryjny, którą trzeba wprowadzić bezzwłocznie w celu ograniczenia ryzyka poważnego zakłócenia działalności jednostki, wymaga zgody kierownika jednostki.

12. Bezpieczeństwo dokumentacji systemu

12.1 Dokumentacja powykonawcza infrastruktury oraz dokumentacja techniczna systemów podlegają ochronie i nie powinna stanowić informacji o charakterze publicznym.

12.2 Osobą odpowiedzialną za aktualność i kompletność dokumentacji, o której mowa w niniejszym rozdziale jest administrator systemu informatycznego.

11.3 Nieograniczony dostęp do przedmiotowej dokumentacji posiada administrator systemu informatycznego, pozostałym osobom (użytkownikom) jest ona udostępniana na zasadzie „wiedzy koniecznej".

13. Bezpieczeństwo wymiany poczty elektronicznej wewnętrznej i zewnętrznej

13.1 System bezpieczeństwa poczty elektronicznej winien zapewniać:

ochronę przed szkodliwym oprogramowaniem rozpowszechnianym za pomocą poczty elektronicznej,

- ✓ ochronę antywirusową załączników przesyłanych w poczcie elektronicznej;

- ✓ ochronę antyspamową;
- ✓ możliwość użycia dostępnych technik kryptograficznych do ochrony poufności i integralności wiadomości poczty elektronicznej;
- ✓ monitorowanie i rejestrowanie poczty elektronicznej.

13.2 Zasoby poczty elektronicznej podlegają sporządzaniu kopii zapasowej. Kopia zapasowa sporządzana jest zgodnie z harmonogramem dla właściwego serwera pocztowego.

13.3 System poczty elektronicznej nakłada ograniczenia, co do rozmiaru pojedynczej skrzynki pocztowej oraz wielkości przesyłanej wiadomości.

13.4 Ruch HTTP między klientem poczty w Internecie, a serwerem poczty powinien być zabezpieczony za pomocą protokołu szyfrującego SSL.

13.5 Uwierzytelnienie dostępu użytkownika do poczty internetowej realizowane jest za pomocą certyfikatu lub identyfikatora i hasła.

13.6 Administrator systemu informatycznego jest odpowiedzialny za ochronę kluczy w trakcie ich użytkowania, a w szczególności za ochronę klucza prywatnego przed ujawnieniem lub nieautoryzowanym użyciem. W przypadku zaistnienia faktu (lub uzasadnionego podejrzenia), naruszenia ochrony klucza prywatnego, należy niezwłocznie przeprowadzić proces unieważniania certyfikatu.

13.7 Odnowienie certyfikatu klucza publicznego musi nastąpić przed końcem okresu jego ważności.

13.8 Po zakończeniu użytkowania certyfikatu klucza publicznego, w przypadku stosowania go wyłącznie do zabezpieczenia komunikacji w protokole SSL, należy parę kluczy zniszczyć w sposób nieodwracalny.

14. Zasady przechowywania haseł przez administratora systemu informatycznego

14.1 Administrator systemu informatycznego zobowiązany jest do zachowania wszystkich haseł dostępu wykorzystywanych przy administrowaniu systemem informatycznym jednostki.

14.2 Utrzymywanie w poufności przedmiotowych haseł, przez administratora systemu informatycznego nie może stanowić samo w sobie zagrożenia w sytuacji zaistnienia nagłej konieczności ich użycia w trakcie czasowej lub trwałej jego nieobecności.

14.3 W celu zapewnienia ciągłości działania jednostki na wypadek nieprzewidzianych zdarzeń o charakterze losowym wprowadza się zasady postępowania w odniesieniu do haseł dostępowych użytkowanych przez osobę lub podmiot pełniący funkcję administratora systemu informatycznego w odniesieniu do wszystkich elementów infrastruktury informatycznej jednostki.

- ✓ administrator systemu informatycznego jest zobowiązany do prowadzenia tzw. wykazu haseł w systemie kopertowym;
- ✓ każde hasło użytkowane przez administratora systemu informatycznego musi zostać zapisane i umieszczone w zaklejonej kopercie z opisem czego dotyczy;
- ✓ koperty zawierające hasła winny być przechowywane przez administratora danych osobowych w sposób gwarantujący wyłącznie jemu dostęp do zarchiwizowanych haseł;
- ✓ w przypadku nagłej konieczności ADO może udostępnić hasło osobie zastępującej administratora systemu informatycznego, która po wykorzystaniu hasła nadaje nowe, które również zapisuje i w zaklejonej kopercie powierza administratorowi systemu informatycznego;
- ✓ każdy przypadek wykorzystania „systemu kopert" winien być zgłoszony przez osobę wykorzystującą hasło z koperty wraz z uzasadnieniem IOD.

15. Pozostałe zasady ochrony systemu informatycznego służącego przetwarzaniu danych osobowych

15.1 Administrator danych osobowych, administrator bezpieczeństwa informacji oraz inspektor ochrony danych osobowych mają prawo do kontroli stanu zabezpieczeń oraz przestrzegania zasad ochrony danych osobowych w dowolnym terminie.

15.2 Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się przed dopuszczeniem do przetwarzania danych z niniejszą instrukcją.

15.3 Naruszenie obowiązków wynikających z niniejszej instrukcji oraz przepisów o ochronie danych osobowych będzie uznane za ciężkie naruszenie obowiązków pracowniczych, podlegające sankcjom dyscyplinarnym oraz sankcjom karnym.

15.4 Wraz z niniejszą instrukcją przyjmuje się nw. standardy do stosowania:

- standard bezpiecznego przetwarzania danych osobowych,
- standard bezpiecznego rozmieszczenia urządzeń infrastruktury informatycznej,
- standard bezpiecznego okablowania.

16. Standard bezpiecznego przetwarzania danych osobowych

Standard bezpiecznego przetwarzania informacji wynika z przestrzegania niżej wymienionych zasad:

16.1 Zasada przywilejów koniecznych – polegająca na tym, że każdy użytkownik systemu informatycznego, posiada prawa dostępu do danych ograniczone wyłącznie do tych, które są konieczne do wykonywania powierzonych zadań i wynikających z otrzymanego upoważnienia.

16.2 Zasada wiedzy koniecznej – polegająca na tym, że poszczególni pracownicy mają dostęp do danych ograniczony wyłącznie do tych, których znajomość jest konieczna do realizacji powierzonych im zadań.

16.3 Zasada usług koniecznych – polegająca na tym, że zakres dostępnych użytkownikowi usług systemu informatycznego jest ograniczony tylko do tych usług, które są konieczne do prawidłowego realizowania obowiązków służbowych.

16.4 Zasada asekuracji zabezpieczeń – polegająca na tym, że wszyscy użytkownicy systemu informatycznego są świadomi konieczności ochrony wykorzystywanych zasobów.

16.5 Zasada indywidualnej odpowiedzialności – polegająca na tym, że za utrzymywanie właściwego poziomu bezpieczeństwa poszczególnych elementów systemu informatycznego, odpowiadają konkretne osoby, które mają świadomość tego, za co są odpowiedzialne i jakie konsekwencje poniosą, jeżeli zaniedbają swoje obowiązki.

16.6 Zasada obecności koniecznej – polegająca na tym, że prawo przebywania w określonych pomieszczeniach mają wyłącznie osoby, które są do tego upoważnione.

16.7 Zasada najsłabszego ogniwa łańcucha – polegająca na tym, że poziom bezpieczeństwa systemu informatycznego wyznacza najsłabszy element tego systemu (najczęściej jest to człowiek).

16.8 Zasada separacji obowiązków – polegająca na tym, że zadania krytyczne z punktu widzenia bezpieczeństwa systemu informatycznego nie mogą być realizowane przez jedną osobę.

16.9 Zasada wykorzystywania udostępnionego przez pracownikowi sprzętu, aplikacji programowych, konta poczty elektronicznej tylko i wyłącznie dla realizacji obowiązków służbowych. W praktyce oznacza to całkowity zakaz wykorzystywania powierzonych urządzeń i konta poczty elektronicznej dla potrzeb prywatnych.

16.10 Zasada niepozostawiania danych o charakterze poufnym na automatycznych sekretarkach oraz przesyłania drogą faksową.

16.11 Zasada czystego biurka dla dokumentów papierowych oraz zasada czystego ekranu.

17. Standard bezpiecznego rozmieszczenia i ochrony sprzętu

Sprzęt wykorzystywany do przetwarzania danych osobowych (jednostki komputerowe, monitory, klawiatury, drukarki, skanery itp.) powinien być tak rozlokowany i tak chroniony, aby redukować ryzyko wynikające z zagrożeń środowiskowych (zalanie przez nieszczelne okno, kradzież) oraz nieautoryzowanego dostępu. W tym celu należy przestrzegać nw. reguł;

17.1 Każdy sprzęt musi posiadać nr inwentarzowy i być przypisany do konkretnego użytkownika odpowiedzialnego materialnie za jego stan.

17.2 Sprzęt należy rozmieszczać w sposób zapewniający sprawowanie nad nim nadzoru przez osobę materialnie odpowiedzialną za jego stan.

17.3 W miejscu lokalizacji sprzętu winna się znajdować instrukcja jego obsługi opracowana przez producenta.

17.4 Niedopuszczalne jest usytuowanie sprzętu poza obszarami przetwarzania tj.: korytarze i inne ciągi komunikacyjne oraz pomieszczenia lub ich części, do których mają nieograniczony dostęp klienci jednostki.

17.5 Celem zapobieżenia uszkodzeniu urządzeń na skutek zalania pomieszczenia, ułatwienia czynności sprzątania pomieszczenia, nie należy umieszczać jego bezpośrednio na podłodze, lecz na stabilnych podstawach (biurko, półki, stoliki itp.),

17.6 Ponadto przy rozmieszczaniu sprzętu należy przestrzegać następujących zasad:

- ✓ nie należy umieszczać sprzętów w bezpośrednim sąsiedztwie źródeł ciepła (grzejniki, inne urządzenia grzewcze) oraz na parapetach okiennych;
- ✓ w pomieszczeniach na niskich kondygnacjach sprzęt nie powinien być rozmieszczany w bezpośrednim sąsiedztwie okien;
- ✓ urządzenia wchodzące w skład systemu informatycznego winny być podpięte do sieci elektrycznej za pośrednictwem listew antyprzepięciowych, które po zakończeniu pracy są wyłączane;
- ✓ niedopuszczalne jest podpinanie do listew antyprzepięciowych dodatkowo jakichkolwiek innych urządzeń elektrycznych nie będących częścią systemu informatycznego.

17.7 W bezpośrednim sąsiedztwie urządzeń wchodzących w skład systemu informatycznego obowiązuje kategoryczny zakaz spożywania posiłków, napojów i palenia tytoniu.

17.8 Wszystkie pomieszczenia wchodzące w skład obszarów przetwarzania winny posiadać instalację alarmową i znajdować się w budynku wyposażonym w instalację odgromową.

18.Standard bezpiecznego okablowania

Okablowanie zasilające i telekomunikacyjne służące do przesyłania danych lub wspomagające usługi informacyjne powinno być chronione przed przejęciem (wykorzystaniem do nieautoryzowanego przetwarzania danych) lub uszkodzeniem. W odniesieniu do bezpieczeństwa okablowania należy przestrzegać następujących zasad:

18.1 Tam, gdzie to możliwe, linie zasilające i telekomunikacyjne należy prowadzić pod ziemią, tynkiem lub zabezpieczyć je w inny stosowny sposób adekwatny do zagrożeń.

18.2 Należy chronić okablowanie sieciowe przed nieautoryzowanym dostępem i przejęciem za pomocą rur, korytek kablowych unikając w mirę możliwości ich prowadzenia przez obszary wchodzące w skład strefy publicznej (ogólnodostępnej dla klientów jednostki).

18.3 Należy oddzielać okablowanie zasilające od okablowania komunikacyjnego celem uniknięcia zjawiska interferencji.

18.4 Należy używać jednoznacznego oznakowania umożliwiającego identyfikację kabli i sprzętu w celu zmniejszenia ryzyka takich błędów, jak nieumyślne połączenie nieodpowiedniego kabla sieciowego.

18.5 Niedopuszczalne jest prowadzenie przewodów zasilających i komunikacyjnych w sposób narażający je na deptanie, rozjeżdżanie fotelami i tym podobne zagrożenia.

18.6 Należy prowadzić dokumentację połączeń elektrycznych i komunikacyjnych w celu zmniejszenia prawdopodobieństwa błędów.

18.7 W odniesieniu do części systemów o znaczeniu krytycznym lub wrażliwym dodatkowo należy wprowadzić zabezpieczenia w postaci:

- ✓ zbrojonych rur lub koryt kablowych, zamknięć pomieszczeń w miejscach zakończeń sieci i instalacji o podwyższonym standardzie bezpieczeństwa;
- ✓ alternatywnego systemu zasilania (UPS) i transmisji (sieć bezprzewodowa) zapewniającego ciągłość działalności;
- ✓ ekranów elektromagnetycznych do ochrony kabli;

- ✓ systemu kontroli dostępu do pomieszczeń, jeżeli znajdują się w nich panele połączeniowe lub inna infrastruktura techniczna o podobnym znaczeniu;
- ✓ systematycznych przeglądów pod kątem możliwości podłączenia nieautoryzowanych urządzeń.

Załączniki:

Załącznik nr 1 - Rejestr osób upoważnionych do systemów

Załącznik nr 2 – Rejestr osób korzystających z systemów informatycznych poza godzinami pracy jednostki

Załącznik nr 3 – Rejestr mobilnych jednostek komputerowych użytkowanych poza siedzibą

Załącznik nr 4 – Regulamin użytkowania komputerów przenośnych

Załącznik nr 5 – Harmonogram wykonywania kopii zapasowych

Załącznik nr 6 – Harmonogram przeglądów i konserwacji urządzeń

Załącznik nr 7 – Rejestr wydanych nośników pamięci

Rejestr osób upoważnionych do systemów

L.p.	Nazwisko	Imię	Login	Data nadania	Obsługiwane systemy informatyczne ze wskazaniem dostępu lub jego braku do poczty zewnętrznej	Data odebrania

Rejestr osób korzystających z systemów informatycznych poza godzinami pracy jednostki

L.p.	Nazwisko	Imię	Login	Przedział czasowy wykorzystywania systemów informatycznych ze wskazaniem dni i godzin	Wykorzystywane systemy informatyczne

Rejestr mobilnych jednostek komputerowych użytkowanych poza siedzibą jednostki

L.p.	Określenie jednostki komputerowej (nazwa nr seryjny, nr inwentarzowy)	Imię i nazwisko użytkownika	Nazwa komórki organizacyjnej	Podpis osoby przyjmującej urządzenie do użytkowania	Data wydania urządzenia do użytkowania	Data zwrotu urządzenia	Podpis osoby przyjmującej zwrot urządzenia

Regulamin użytkowania komputerów przenośnych

1. Pracownicy upoważnieni do przetwarzania danych osobowych i pracujący na komputerach przenośnych muszą zapoznać się z Regulaminem użytkowania komputera przenośnego i zobowiązują do jego przestrzegania.

2. Dane osobowe lub dane poufne muszą zostać zaszyfrowane na dysku i zabezpieczone co najmniej 8-znakowym hasłem (duże, małe litery i cyfry).

3. Komputery przenośne są wykorzystywane do prac służbowych. W przypadku konieczności korzystania z komputera przenośnego w innym celu wszystkie dane osobowe muszą być zabezpieczone hasłem.

4. W przypadku kradzieży/zgubienia lub naruszenia ochrony danych osobowych osoba upoważniona zobowiązana jest zgłosić zdarzenie/problem przełożonemu i administratorowi systemu informatycznego.

5. Osoba upoważniona zobowiązana jest do zabezpieczenia komputera przenośnego w czasie transportu, a przede wszystkim:

   - ✓ zaleca się przenoszenie komputera przenośnego w przeznaczonej do tego celu torbie;
   - ✓ zabrania się pozostawiania komputera przenośnego w samochodzie podczas nieobecności osoby upoważnionej;
   - ✓ zabrania się pozostawiania komputera przenośnego w miejscach typu przechowalnie bagażu,

6. Użytkownik komputera przenośnego jest zobowiązany do regularnego tworzenia kopii bezpieczeństwa danych w sposób uzgodniony z administratorem systemu informatycznego.

7. Pracując na komputerze przenośnym w miejscach publicznych i środkach transportu, osoba upoważniona zobowiązana jest do chronienia wyświetlanych danych osobowych na monitorze przed wglądem osób nieupoważnionych oraz powstrzymania się od korzystania z internetu z wykorzystaniem publicznej sieci wi-fi.

8. Użytkownik komputera przenośnego zobowiązuje się do nie udostępniania jego innym osobą w jakimkolwiek celu.

9. Użytkownik komputera przenośnego nie może dokonywać samodzielnie jakichkolwiek jego napraw, modernizacji i innych czynności związanych z ingerencją w parametry konfiguracyjne jednostki.

Harmonogram wykonywania kopii zapasowych

L.p.	Określenie zasobów informacyjnych podlegających kopiowaniu	Określenie częstotliwości wykonywania kopii	Określenie metody wykonywania kopii	Określenie miejsca przechowywania nośników kopii	Określenie terminu przechowywania nośników kopii

Harmonogram przeglądów i konserwacji urządzeń

L.p.	Określenie urządzenia stanowiącego element systemu informatycznego	Miejsce użytkowania	Opis działań związanych z wykonywanymi czynnościami konserwacji lub przeglądu	Częstotliwość wykonywania przeglądów lub konserwacji	Określenie podmiotu wykonującego przegląd lub konserwację

Rejestr wydanych nośników pamięci

L.p.	Określenie nośnika	Data przyjęcia do użytkowania	Określenie pracownika korzystającego z nośnika	Data udostępnienia nośnika pracownikowi	Data zwrotu nośnika przez pracownika