Załącznik nr 2 do Systemu Zarządzania Bezpieczeństwem Informacji w organizacji o nazwie: **MIEJSKI OŚRODEK POMOCY SPOŁECZNEJ W LEŻAJSKU**

Polityka

Bezpieczeństwa

Teleinformatycznego

w organizacji o nazwie:

MIEJSKI OŚRODEK POMOCY SPOŁECZNEJ W LEŻAJSKU

SPIS TREŚCI

§ 1

Postanowienia ogólne

1. Cel instrukcji

1) Polityka Bezpieczeństwa Teleinformatycznego jest integralnym elementem Systemu Zarządzania Bezpieczeństwem Informacji.

2) Niniejsza Polityka Bezpieczeństwa Teleinformatycznego jest zbiorem zasad mających na celu właściwe zarządzanie systemami teleinformatycznymi służącymi do elektronicznego przetwarzania danych osobowych z uwzględnieniem warunków technicznych i organizacyjnych, jakim powinny odpowiadać wchodzące w jego skład urządzenia, odpowiednio do skali zagrożeń i kategorii danych objętych ochroną.

3) Stosowanie zasad bezpieczeństwa określonych w niniejszym dokumencie ma na celu zapewnienie prawidłowej ochrony danych osobowych przetwarzanych przez podmiot o nazwie: **MIEJSKI OŚRODEK POMOCY SPOŁECZNEJ W LEŻAJSKU** w systemach teleinformatycznych, jednocześnie przeciwdziałając zagrożeniom jakimi są:

a) udostępnianie danych osobom nieupoważnionym,

b) zmiana lub zabranie danych przez osobę nieuprawnioną,

c) przetwarzanie z naruszeniem przepisów,

d) utrata, uszkodzenie lub zniszczenie danych.

Podstawa prawna:

Zgodnie z wymogami normy PN-EN ISO/IEC 27001:2017 pkt 5.2; zał. A.5.1.1

2. Definicje legalne

Ilekroć w „Polityce Bezpieczeństwa Teleinformatycznego" mówi się o:

1) **Organizacji** – rozumie się przez to osobę prawną, organ publiczny, jednostkę lub inny podmiot. Do celów niniejszej Polityki Bezpieczeństwa Teleinformatycznego wprowadza się nazwę własną organizacji: **MIEJSKI OŚRODEK POMOCY SPOŁECZNEJ W LEŻAJSKU**;

2) **Administratorze** – rozumie się przez to osobę fizyczną lub organizację, która samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.

3) **Inspektorze Ochrony Danych** – rozumie się przez to osobę, której Administrator powierzył pełnienie obowiązków określonych w art. 39 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016.

4) **Administratorze Systemu Informatycznego** – rozumie się przez to osobę, której Administrator powierzył pełnienie obowiązków nadzoru nad przestrzeganiem zasad ochrony danych osobowych pod kątem zabezpieczeń teleinformatycznych;

5) **Danych osobowych** – rozumie się przez to dane oznaczające informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

6) **Przetwarzaniu** – rozumie się przez to operacje lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

7) **Sieci lokalnej** – rozumie się przez to sieć LAN (ang. Local Area Network) – sieć komputerową łączącą komputery na określonym obszarze (urząd, szkoła, laboratorium, biuro). Sieć LAN może być wydzielona zarówno fizycznie, jak i logicznie w ramach innej sieci. Główne różnice LAN, w porównaniu z WAN, to wyższy wskaźnik transferu danych i mniejszy obszar geograficzny;

8) **Sieci rozległej** – rozumie się przez to sieć WAN (ang. Wide Area Network) – sieć komputerową znajdującą się na obszarze wykraczającym poza miasto, kraj, kontynent;

9) **Sieci publicznej** – rozumie się przez to sieć telekomunikacyjną wykorzystywaną głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz.U.2017.1907 t.j.);

10) **Zbiorze danych** – rozumie się przez to uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

11) **Osobie upoważnionej** – rozumie się przez to osobę posiadającą formalne upoważnienie do przetwarzania danych osobowych wydane przez Administratora;

12) **Identyfikatorze użytkownika** – rozumie się przez to nazwę przypisaną określonemu użytkownikowi. Używany jest podczas logowania, umożliwia uprawniony dostęp do danego komputera, systemu bądź sieci. Identyfikator jest ciągiem znaków o ograniczonej długości, wybranych z określonego zestawu znaków. Do identyfikatora przypisane jest konto użytkownika oraz ściśle określone uprawnienia, jakie ma dany użytkownik. Główną cechą identyfikatora jest jego unikalność w ramach danego systemu informatycznego;

13) **Użytkowniku systemu** - rozumie się przez to osobę fizyczną posiadającą formalne upoważnienie do przetwarzania danych osobowych wydane przez Administratora, oraz nadane uprawnienia do przetwarzania w systemie teleinformatycznym;

14) **Systemie teleinformatycznym** – rozumie się przez to zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz.U.2017.1907 t.j.);

15) **Kryptografii** – rozumie się przez to gałąź wiedzy o utajnianiu wiadomości z dziedziny kryptologii - dziedziny wiedzy o przekazywaniu informacji w sposób zabezpieczony przed niepowołanym dostępem. Istotnym elementem technik kryptograficznych jest proces zamiany tekstu jawnego w szyfrogram (inaczej kryptogram); proces ten nazywany jest szyfrowaniem, a proces odwrotny, czyli zamiany tekstu zaszyfrowanego na powrót w możliwy do odczytania, deszyfrowaniem.

16) **Polityce Bezpieczeństwa Informacji (PBI)** – rozumie się przez to zestaw formalnych zasad, procedur oraz kodeksów dobrych praktyk odnoszących się do bezpieczeństwa przepływu informacji zbieżnych z celami istnienia organizacji;

17) **Polityce Bezpieczeństwa Teleinformatycznego (PBT)** – rozumie się przez to zestaw formalnych zasad i procedur odnoszących się do bezpieczeństwa przepływu informacji w systemie teleinformatycznym;

18) **Procedurze Zarządzania Incydentami (PZI)** – rozumie się przez to zestaw formalnych procedur odnoszących się do postępowania z naruszeniami w zakresie bezpieczeństwa ochrony danych osobowych;

19) **Polityce Audytu Wewnętrznego (PAW)** – rozumie się przez to dokumentację zawierającą opis metodologii, częstotliwości oraz zakresu prowadzonego audytu wewnętrznego w organizacji lub w ramach podmiotu przetwarzającego.

3. Źródła wymagań

Niniejsza Polityka Bezpieczeństwa Teleinformatycznego została opracowana w oparciu o:

1) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 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);

2) wytyczne Grupy Roboczej art. 29 ds. Ochrony Danych z dnia 13 grudnia 2016:

a) wytyczne dotyczące inspektorów ochrony danych ('DPO') (WP 243),

b) wytyczne dotyczące prawa do przenoszenia danych (WP 242),

c) wytyczne dotyczące ustalenia wiodącego organu nadzorczego właściwego dla administratora lub podmiotu przetwarzającego (WP 244),

d) wytyczne dotyczące oceny skutków dla ochrony danych (WP 248).

3) Ustawę z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U.2017.570 t.j.);

4) Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U.2017.2247 t.j.);

5) Normę:

a) PN-EN ISO/IEC 27001:2017 - Technika informatyczna - Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji – Wymagania;

b) PN-EN ISO/IEC 27002:2017 - Technika informatyczna - Techniki bezpieczeństwa – Praktyczne zasady zabezpieczania informacji;

c) PN-ISO/IEC 27005:2014 - Technika informatyczna - Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji;

d) PN-ISO 31000:2012 – Zarządzanie ryzykiem – Zasady i wytyczne.

Podstawa prawna:

Zgodnie z wymogami normy PN-EN ISO/IEC 27001:2017 zał. A.18.1

4. Obszar stosowania

Za obszar stosowania traktuje się pomieszczenia budynków, w których zachodzi proces przetwarzania danych osobowych, opisany w „**Ewidencji obszarów przetwarzania**" – dokument nr: **„SZBI-PBI-Zał. 7**" stanowiącym **załącznik nr 7** do **Polityki Bezpieczeństwa Informacji**.

Podstawa prawna:

Zgodnie z wymogami normy PN-EN ISO/IEC 27001:2017 pkt 4.3

5. Zakres stosowania

1) Na zakres Polityki Bezpieczeństwa Teleinformatycznego składa się:

a) odpowiedzialność Administratora, Inspektora Ochrony Danych, Administratora Systemu Informatycznego oraz użytkowników,

b) zarządzanie pracą użytkownika w systemach teleinformatycznych tj. nadawanie, modyfikacja i wycofywanie uprawnień oraz rozpoczęcie, zawieszenie/odwieszenie i zakończenie pracy użytkownika w systemie teleinformatycznym,

c) zarządzanie bezpieczeństwem w systemach teleinformatycznych,

d) zabezpieczenia kryptograficzne,

e) zarządzanie bezpieczeństwem i komunikacją w sieciach teleinformatycznych,

f) ochrona przed szkodliwym oprogramowaniem,

g) postępowanie z urządzeniami mobilnymi,

h) nadzór nad oprogramowaniem,

i) inwentaryzacja sprzętu,

j) kopie zapasowe,

k) postępowanie z nośnikami.

2) Polityka Bezpieczeństwa Teleinformatycznego obowiązuje wszystkie osoby upoważnione do:

a) przetwarzania danych osobowych,

b) przebywania w obszarze przetwarzania danych osobowych.

Podstawa prawna:

Zgodnie z wymogami normy PN-EN ISO/IEC 27001:2017 pkt 4.3

§ 2

Odpowiedzialność

1. Administrator

Do obowiązków Administratora należy zarządzanie bezpieczeństwem informacji, a w szczególności:

1) zapewnienie warunków aktualizacji wobec regulacji wewnętrznych w stosunku do zmieniającego się otoczenia,

2) zapewnienie aktualności inwentaryzacji sprzętu i oprogramowania co do rodzaju i konfiguracji,

3) umożliwienie/wykonanie okresowej analizy ryzyka wraz z adekwatnymi do wyniku działaniami minimalizującymi ryzyko,

4) podejmowanie działań zapewniających weryfikację stosownych uprawnień wobec osób uczestniczących w procesie przetwarzania danych,

5) zapewnienie warunków technicznych, organizacyjnych i fizycznych ze szczególnym naciskiem na:

a) szkolenia obejmujące tematykę zagrożeń, skutków naruszenia bezpieczeństwa informacji oraz zapewnienie bezpieczeństwa wraz z minimalizacją ryzyka błędów ludzkich,

b) ochrona przed kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami,

6) stosowanie umów powierzenia danych.

Podstawa prawna:

1. Zgodnie z Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U.2017.2247 t.j.)
2. Zgodnie z wymogami normy PN-EN ISO/IEC 27001:2017 pkt 5.3, zał. A.6.1

2. Inspektor Ochrony Danych

Do obowiązków Inspektora Ochrony Danych należy:

1) nadzór nad stosowaniem środków bezpieczeństwa w systemach teleinformatycznych,

2) nadzór nad przestrzeganiem procedur bezpieczeństwa przez Administratora oraz użytkowników,

3) proponowanie i uzgadnianie procedur w systemach teleinformatycznych z Administratorem oraz Administratorem Systemu Informatycznego,

4) zapewnienie punktu kontaktowego dla Administratora, użytkowników i organizacji współpracujących,

5) prowadzenie ewidencji użytkowników systemów teleinformatycznych, w których przetwarzane są dane osobowe, stanowiącej część ewidencji osób upoważnionych do przetwarzania danych osobowych oraz wszelkiej dokumentacji opisującej sposób realizacji i stopień ochrony danych osobowych w organizacji,

6) kontrolowanie nadanych w systemach teleinformatycznych uprawnień do przetwarzania danych osobowych pod kątem ich zgodności z wpisami umieszczonymi w ewidencji osób upoważnionych do przetwarzania danych osobowych.

Podstawa prawna:

1. Zgodnie z art. 39 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.
2. Zgodnie z wymogami normy PN-EN ISO/IEC 27001:2017 pkt 5.3, zał. A.6.1

3. Administrator Systemu Informatycznego

Do obowiązków Administratora Systemu Informatycznego należy:

1) opracowywanie i przestrzeganie procedur bezpieczeństwa systemów teleinformatycznych,

2) kontrola przepływu informacji pomiędzy systemem teleinformatycznym a siecią rozległą (z uwzględnieniem komunikacji poprzez sieć publiczną), oraz kontrola działań inicjowanych z sieci rozległej (z uwzględnieniem komunikacji poprzez sieć publiczną) a systemem teleinformatycznym,

3) zarządzanie stosowanymi w systemach teleinformatycznych środkami uwierzytelnienia, w tym rejestrowanie i wyrejestrowywanie użytkowników oraz dokonywanie zmiany uprawnień na podstawie uprzednio zaakceptowanego przez Administratora wniosku o udzielenie upoważnienia do przetwarzania danych osobowych,

4) utrzymanie systemu teleinformatycznego w należytej kondycji technicznej,

5) współtworzenie i doradztwo w zakresie Polityki Bezpieczeństwa Teleinformatycznego, służącej do określenia zasad elektronicznego przetwarzania danych osobowych,

6) regularne tworzenie kopii zapasowych elektronicznych zasobów danych osobowych, programów służących do ich przetwarzania, oraz okresowe sprawdzanie poprawności wykonania kopii zapasowych celem uzyskania ciągłości zarządzania,

7) wykonywanie lub nadzór nad wykonywaniem okresowych przeglądów i konserwacji sprzętu IT, systemów teleinformatycznych, aplikacji oraz elektronicznych nośników informacji, na których zapisane są dane osobowe.

Podstawa prawna:
Zgodnie z wymogami normy PN-EN ISO/IEC 27001:2017 pkt 5.3, zał. A.6.1

4. Użytkownik systemu teleinformatycznego

Do obowiązków użytkownika systemu teleinformatycznego przy przetwarzaniu danych osobowych należy znajomość, zrozumienie i stosowanie w możliwie największym stopniu środków ochrony danych osobowych przy jednoczesnym uwzględnieniu przepisów prawa, oraz uniemożliwienie osobom nieuprawnionym dostępu do danych organizacji na swojej stacji roboczej. Dodatkowo użytkownik systemu teleinformatycznego zobligowany jest do:

1) współpracy przy ustaleniu przyczyn naruszenia ochrony danych osobowych, oraz usuwania skutków tych naruszeń, w tym zapobieganie ich ewentualnemu ponownemu wystąpieniu,

2) przestrzegania opracowanych dla systemu teleinformatycznego zasad przetwarzania danych osobowych oraz procedur i instrukcji,

3) informowania Inspektora Ochrony Danych o wszelkich naruszeniach, podejrzeniach naruszenia i nieprawidłowościach w sposobie przetwarzania i ochrony danych osobowych,

4) wykonywania bez zbędnej zwłoki poleceń Inspektora Ochrony Danych w zakresie ochrony danych osobowych jeśli są one zgodne z przepisami prawa powszechnie obowiązującego.

Podstawa prawna:
Zgodnie z wymogami normy PN-EN ISO/IEC 27001:2017 pkt 5.3, zał. A.6.1

§ 3

Zarządzanie pracą użytkownika w systemach teleinformatycznych

1. Nadawanie uprawnień do przetwarzania danych osobowych w systemie teleinformatycznym wraz z ich rejestracją

1) Przetwarzać dane, w tym dane osobowe w systemie teleinformatycznym może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych wydane przez Administratora.

2) Nadanie przez Administratora upoważnienia do przetwarzania danych osobowych w systemie teleinformatycznym oraz rejestracja użytkownika przetwarzającego dane osobowe w systemie teleinformatycznym następuje na wniosek przełożonego użytkownika lub koordynatora zadania, na rzecz którego będą wykonywane czynności związane z przetwarzaniem danych osobowych.

3) Aby nadać uprawnienia do przetwarzania danych osobowych w systemie teleinformatycznym, przełożony użytkownika lub koordynator zadania składa wniosek: „**Obiegowa Karta Uprawnień**" – dokument nr: „**SZBI-PBI-Zał. 3**" – stanowiący **załącznik nr 3** do **Polityki Bezpieczeństwa Informacji** - do Inspektora Ochrony Danych o wydanie upoważnienia do przetwarzania danych osobowych w systemie teleinformatycznym. Następnie Inspektor Ochrony Danych przekazuje wniosek do Administratora. W sytuacji nieobecności Inspektora Ochrony Danych w organizacji, przełożony użytkownika lub koordynator zadania składa wniosek bezpośrednio do Administratora.

4) Wniosek po rozpatrzeniu przez Administratora zostaje przekazany do przełożonego użytkownika lub koordynatora zadania bądź do Inspektora Ochrony Danych. Przełożony użytkownika lub koordynator zadania bądź Inspektor Danych Osobowych kieruje podpisany wniosek do Administratora Systemu Informatycznego o przydzielenie uprawnień do przetwarzania danych osobowych w systemie teleinformatycznym. W tym momencie następuje proces przyznawania uprawnień zgodnie z wytycznymi przełożonego użytkownika lub koordynatora zadania bądź Inspektora Ochrony Danych. Po nadaniu uprawnień, Administrator Systemu Informatycznego przekazuje wniosek do następujących osób z zachowaniem kopii dla siebie:

a) przełożony użytkownika lub koordynator zadania,

b) Inspektor Ochrony Danych.

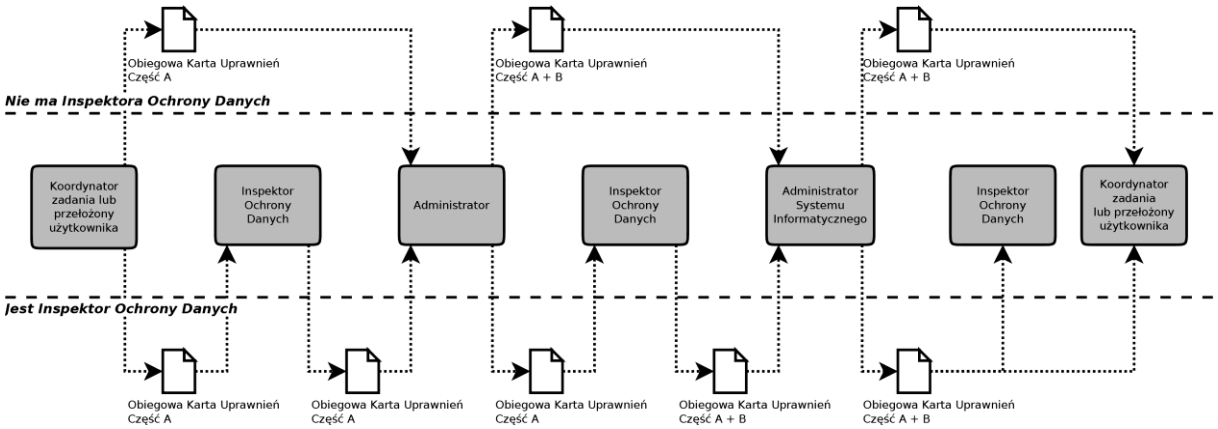
5) O okresie upoważnienia decyduje Administrator.

6) Identyfikator i hasło do systemu teleinformatycznego przetwarzającego dane osobowe jest przydzielany użytkownikowi tylko w przypadku, gdy posiada on pisemne upoważnienie do przetwarzania danych osobowych, wydane przez Administratora.

7) Identyfikator użytkownika jest unikalny i niezmienialny.

8) Zmiana hasła odbywa się co 30 dni kalendarzowych z uwzględnieniem niepowtarzalności hasła oraz budowy składającej się na minimum 8 znaków w tym minimum jedna mała, duża litera i znak specjalny.

9) Za przydzielenie i wygenerowanie identyfikatora oraz hasła użytkownikowi, który pierwszy raz będzie korzystał z systemu teleinformatycznego, odpowiada Administrator Systemu Informatycznego (czynności te wykonuje na podstawie zatwierdzonej „**Obiegowej Karty Uprawnień**" – dokument nr: „**SZBI-PBI-Zał. 3**" – stanowiącej **załącznik nr 3** do **Polityki Bezpieczeństwa Informacji**). Identyfikator użytkownika zostaje wpisany do „**Obiegowej karty uprawnień**" – dokument nr **„SZBI-PBI-Zał. 3**" - stanowiącej **załącznik nr 3** do **Polityki Bezpieczeństwa Informacji**.



Podstawa prawna:

Zgodnie z wymogami normy PN/ISO/IEC 27001:2017 zał. A.9.2

2. Modyfikacja uprawnień do przetwarzania danych osobowych w systemie teleinformatycznym

1) Modyfikacja uprawnień użytkownika do przetwarzania danych osobowych w systemie teleinformatycznym następuje na wniosek przełożonego użytkownika lub koordynatora zadania lub Inspektora Ochrony Danych w następujących przypadkach:

a) modyfikacja uprawnień użytkownika do przetwarzania danych osobowych w systemie teleinformatycznym z powodu zmiany zakresu czynności,

2) Zgłoszenie modyfikacji uprawnień użytkownika do przetwarzania danych osobowych w systemie teleinformatycznym zgłasza się poprzez „**Obiegową Kartę Uprawnień**" – dokument nr: „**SZBI-PBI-Zał. 3**" – stanowiącą **załącznik nr 3** do **Polityki Bezpieczeństwa Informacji**.

3) Pisemny wniosek o modyfikację uprawnień użytkownika do przetwarzania danych osobowych w systemie teleinformatycznym składa się do Inspektora Ochrony Danych poprzez wniosek: „**Obiegowa Karta Uprawnień**" – dokument nr: „**SZBI-PBI-Zał. 3**" – stanowiący **załącznik nr 3** do **Polityki Bezpieczeństwa Informacji**. Następnie Inspektor Ochrony Danych przekazuje wniosek do Administratora Systemu Informatycznego. W sytuacji nieobecności Inspektora Ochrony Danych w organizacji, przełożony użytkownika lub koordynator zadania składa wniosek bezpośrednio do Administratora. Wniosek po rozpatrzeniu przez Administratora zostaje przekazany do Administratora Systemu Informatycznego.

4) Po modyfikacji uprawnień użytkownika do przetwarzania danych osobowych w systemie teleinformatycznym, Administrator Systemu Informatycznego przekazuje wniosek do następujących osób z zachowaniem kopii dla siebie:

a) przełożony użytkownika lub koordynator zadania,

b) Inspektor Ochrony Danych.

Podstawa prawna:

Zgodnie z wymogami normy PN-EN ISO/IEC 27001:2017 zał. A.9.2

3. Wycofywanie uprawnień do przetwarzania danych osobowych w systemie teleinformatycznym

1) Wycofanie uprawnień użytkownika do przetwarzania danych osobowych w systemie teleinformatycznym może nastąpić na wniosek przełożonego użytkownika lub koordynatora zadania lub Inspektora Ochrony Danych w następujących przypadkach:

a) wycofanie uprawnień użytkownika z powodu zakończenia przetwarzania danych osobowych w obrębie systemu teleinformatycznego,

b) wycofanie uprawnień użytkownika z powodu ustania stosunku pracy.

2) Zgłoszenie wycofania uprawnień użytkownika do przetwarzania danych osobowych w systemie teleinformatycznym zgłasza się poprzez „**Obiegową Kartę Uprawnień**" – dokument nr: „**SZBI-PBI-Zał. 3**" – stanowiącą **załącznik nr 3** do **Polityki Bezpieczeństwa Informacji**.

3) Pisemny wniosek o wycofanie uprawnień użytkownika do przetwarzania danych osobowych w systemie teleinformatycznym należy złożyć do Inspektora Ochrony Danych poprzez wniosek: „**Obiegowa Karta Uprawnień**" – dokument nr: „**SZBI-PBI-Zał. 3**" – stanowiący **załącznik nr 3** do **Polityki Bezpieczeństwa Informacji**. Następnie Inspektor Ochrony Danych przekazuje wniosek do Administratora Systemu Informatycznego. W sytuacji nieobecności Inspektora Ochrony Danych w organizacji, przełożony użytkownika lub koordynator zadania składa wniosek bezpośrednio do Administratora. Wniosek po rozpatrzeniu przez Administratora zostaje przekazany do Administratora Systemu Informatycznego.

4) Po wycofaniu uprawnień użytkownika do przetwarzania danych osobowych w systemie teleinformatycznym, Administrator Systemu Informatycznego przekazuje wniosek do następujących osób z zachowaniem kopii dla siebie:

a) przełożony użytkownika lub koordynator zadania,

b) Inspektor Ochrony Danych.

5) Po wycofaniu uprawnień do przetwarzania danych osobowych w systemie teleinformatycznym, Administrator Systemu Informatycznego dokonuje zablokowania identyfikatora użytkownika celem uniemożliwienia przydzielenia innemu użytkownikowi.

Podstawa prawna:
Zgodnie z wymogami normy PN-EN ISO/IEC 27001:2017 zał. A.9.2

4. Rozpoczęcie pracy przez użytkownika w systemie teleinformatycznym

1) Przed przystąpieniem do pracy w systemie teleinformatycznym użytkownik zobowiązany jest sprawdzić urządzenie komputerowe i stanowisko pracy zwracając uwagę, czy nie zaszły okoliczności wskazujące na naruszenie danych osobowych. W przypadku stwierdzenia naruszenia danych osobowych użytkownik zobowiązany jest do niezwłocznego powiadomienia Administratora Systemu Informatycznego oraz Inspektora Ochrony Danych.

2) Użytkownik uruchamia komputer.

3) Celem zalogowania się do systemu teleinformatycznego użytkownik wpisuje swój identyfikator i hasło. Jeżeli jest to pierwsze logowanie użytkownika od momentu nadania uprawnień do przetwarzania w sieci teleinformatycznej, użytkownik jest zobligowany do zmiany hasła, chyba, że konfiguracja systemu teleinformatycznego samoczynnie wymusza takową zmianę.

4) Zmiana hasła odbywa się co 30 dni kalendarzowych z uwzględnieniem niepowtarzalności hasła oraz budowy składającej się na minimum 8 znaków w tym minimum jedna mała, duża litera i znak specjalny.

5) Wpisywanie hasła lub jego modyfikacja nie może się odbywać w obecności innych osób.

6) Hasło nie może być zapisywane lub przechowywane w miejscu dostępnym dla osób nieuprawnionych.

7) W przypadku zagubienia hasła, użytkownik musi się skontaktować z Administratorem Systemu Informatycznego, który o zaistniałym zdarzeniu informuje Inspektora Ochrony Danych.

8) Niedopuszczalne jest uwierzytelnianie się poprzez identyfikator i hasło innego użytkownika, lub praca w systemie teleinformatycznym na koncie innego użytkownika.

Podstawa prawna:
Zgodnie z wymogami normy PN-EN ISO/IEC 27001:2017 zał. A.9.3

5. Zawieszenie / odwieszenie pracy przez użytkownika w systemie teleinformatycznym

1) W celu zawieszenia pracy w systemie teleinformatycznym służącym do przetwarzania danych osobowych użytkownik zobowiązany jest się „wylogować" się lub jednoczesne wcisnąć kombinację klawiszy „⊞ + L", celem zablokowania ekranu z opcją ponownego logowania po podaniu hasła.

2) Celem ponownego zalogowania się w systemie teleinformatycznym użytkownik podaje hasło i rozpoczyna pracę z uwzględnieniem zasad rozpoczęcia pracy użytkownika w systemie teleinformatycznym zawartych w §3 ust. 4 niniejszej Polityki Bezpieczeństwa Teleinformatycznego.

3) Zabrania się pozostawienia stanowiska komputerowego z uruchomionym systemem bez uprzedniej aktywacji blokady ekranu poprzez kombinację klawiszy „⊞ + L".

Podstawa prawna:
Zgodnie z wymogami normy PN-EN ISO/IEC 27001:2017 zał. A.9.3

6. Zakończenie pracy przez użytkownika w systemie teleinformatycznym

1) Celem zakończenia pracy w systemie teleinformatycznym, użytkownik zamyka wszystkie aktywne programy.

2) Użytkownik wylogowuje się, zamyka system operacyjny i wyłącza komputer (przeważnie wszystkie trzy opcje są ze sobą powiązane).

3) Po zakończeniu pracy użytkownik sprawdza swoje stanowisko pracy i zabezpiecza wszelakie nośniki danych takie jak dokumenty, pendrive, dyski przenośne, płyty CD/DVD zawierające dane osobowe, przed dostępem osób nieupoważnionych.

4) W przypadku wystąpienia nieprawidłowości podczas procesu wylogowywania się, zamknięcia systemu lub fizycznego wyłączenia komputera, użytkownik musi powiadomić Administratora Systemu Informatycznego.

Podstawa prawna:

Zgodnie z wymogami normy PN-EN ISO/IEC 27001:2017 zał. A.9.3

§ 4

Zarządzanie bezpieczeństwem w systemach teleinformatycznych

1. Zabezpieczenia kryptograficzne

1) Za bezpieczeństwo informacji w organizacji odpowiada Inspektor Ochrony Danych.

2) Za bezpieczeństwo informacji w systemach teleinformatycznych odpowiada Administrator Systemu Informatycznego, przy jednoczesnym uwzględnieniu wymagań związanych z kompatybilnością mechanizmu kryptograficznego.

3) Wprowadzenie zabezpieczenia kryptograficznego wykonywane jest przez Administratora Systemu Informatycznego na zlecenie Inspektora Ochrony Danych o uprzedniej z nim konsultacji co do następujących warunków:

a) adekwatność zabezpieczenia kryptograficznego wobec przetwarzanych danych osobowych,

b) poziom ryzyka utraty poufności danych,

c) rodzaj usługi kryptograficznej (szyfrowanie symetryczne, asymetryczne, podpis cyfrowy, znakowanie czasem itp.).

d) odpowiednia moc mechanizmów kryptograficznych (zastosowane algorytmy, długości kluczy),

e) sposób zarządzania kluczami kryptograficznymi,

f) wydajność mechanizmu kryptograficznego,

g) kompatybilność z istniejącą infrastrukturą teleinformatyczną organizacji,

h) rodzaj zabezpieczanych danych (dane przechowywane na nośniku, przesyłane przez sieci lokalne, transmitowane w sieciach rozległych lub publicznych),

i) wymagania dotyczące certyfikacji produktu (o ile występują),

j) wymagania dotyczące zgodności z normami branżowymi i wykorzystanie standardowych protokołów dla mechanizmów kryptograficznych (o ile występują),

k) łatwość wdrożenia mechanizmu i integracji z systemem teleinformatycznym organizacji,

l) odporność na próby kompromitacji mechanizmu kryptograficznego,

m) wymagany stopień interakcji z użytkownikiem.

4) Wprowadzenie zabezpieczenia kryptograficznego odnotowywane jest w ewidencji zabezpieczeń kryptograficznych prowadzonej przez Administratora Systemu Informatycznego, która zawiera udokumentowane procesy opisujące generowanie, rozprowadzanie, używanie, przechowywanie, aktywację, zastępowanie oraz niszczenie wszystkich kluczy szyfrujących.

5) Ewidencja zabezpieczeń kryptograficznych znajduje się na terenie organizacji w zamkniętej szafie, oraz zamkniętym pomieszczeniu jako niezależny dokument spoza dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji w skład której wchodzi Polityka Bezpieczeństwa Teleinformatycznego.

6) Prawa dostępu do ewidencji zabezpieczeń kryptograficznych jakimi są wgląd, wprowadzanie, modyfikacja, usuwanie i archiwizacja, mają następujące osoby:

a) osoba reprezentująca Administratora organizacji na szczeblu najwyższego kierownictwa;

b) Inspektor Ochrony Danych;

c) Administrator Systemu Informatycznego.

7) Mając na uwadze rozwiązania określone w §4 ust. 1 pkt 6 niniejszej Polityki Bezpieczeństwa Teleinformatycznego organizacja jednocześnie wprowadza procedurę opartą o praktyczne zastosowanie praw dostępu z uwagi na utrzymywanie wysokiego stopnia poufności, rozliczalności i integralności a mianowicie:

a) Administrator posiada bezwzględne prawo wglądu do ewidencji zabezpieczeń kryptograficznych. Prawo wprowadzania, modyfikacji, usuwania i archiwizacji spełnione jest wyłącznie w asyście Inspektora Ochrony Danych oraz/lub Administratora Systemu Informatycznego,

b) Inspektor Ochrony Danych posiada bezwzględne prawo wglądu do ewidencji zabezpieczeń kryptograficznych. Prawo wprowadzania, modyfikacji, usuwania i archiwizacji spełnione jest wyłącznie w asyście Administratora Systemu Informatycznego,

c) Administrator Systemu Informatycznego posiada bezwzględne prawo wglądu do ewidencji zabezpieczeń kryptograficznych. Prawo wprowadzania, modyfikacji, usuwania i archiwizacji spełnione jest wyłącznie po uprzedniej konsultacji z Inspektorem Ochrony Danych oraz/lub Administratorem.

8) Procedura dystrybucji kluczy powinna zapewnić, by w czasie przesyłania klucz nie był czytelny w całości. Gdy używane są klucze zabezpieczające hasła (tak jak w przypadku plików samo rozszyfrowujących się), hasło powinno być przesłane osobno, a nie razem z plikiem zaszyfrowanym drogą e-mail. Jeśli to tylko możliwe, hasło powinno być przesyłane przy użyciu innego kanału dystrybucji (np. telefon komórkowy).

Podstawa prawna:

1. Zgodnie z art. 32 pkt 1 lit. a) oraz motywem nr 83 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.
2. Zgodnie z wymogami normy PN-EN ISO/IEC 27001:2017 zał. A.10

2. Zarządzanie bezpieczeństwem i komunikacją w sieciach teleinformatycznych

1) Bezpieczeństwo sieci

a) Za zarządzanie infrastrukturą teleinformatyczną odpowiedzialny jest Administrator Systemu Informatycznego, którego zakres obowiązków ma na celu zapewnienie właściwej ochrony, adekwatnie do zagrożeń mogących powodować utratę bezpieczeństwa przetwarzania danych osobowych.

b) Administrator Systemu Informatycznego zapewnia bezpieczeństwo teleinformatyczne względem zagrożeń pochodzących z sieci publicznej poprzez wdrożenie logicznych zabezpieczeń takich jak programy

antywirusowe (stacje robocze i serwer/y) oraz środka kontroli przepływu informacji na poziomie bramy sieciowej.

c) Wewnętrzna pula adresów IP organizacji nie jest udostępniana osobom nieupoważnionym za wyjątkiem sytuacji, w której Inspektor Ochrony Danych zleca Administratorowi Systemu Informatycznego takowe udostępnienie.

d) Podłączanie we własnym zakresie wszelakich urządzeń sieciowych takich jak modemy, karty sieciowe, urządzenia wzmacniające, koncentratory, mosty, przełączniki, punkty dostępowe, routery, bramy sieciowe, bramki VoIP, zapory sieciowe do infrastruktury teleinformatycznej organizacji jest surowo zabronione.

e) Podłączanie nieautoryzowanych stacji roboczych do sieci publicznej poprzez wewnętrzna sieć LAN organizacji jest surowo zabronione.

f) Sieci bezprzewodowe uwierzytelniane są zabezpieczeniem kryptograficznym w postaci klucza WPA2-PSK z opcją 256 bitowego hasła (standard AES).

g) Użytkownicy używają połączenia z siecią publiczną wyłącznie w celach służbowych.

h) Użytkownicy nie mogą ściągać za pośrednictwem sieci LAN, WAN, oprogramowania do wymiany plików p2p (np. BitTorrent, µTorrent itp…) żadnego oprogramowania, utworów muzycznych, filmów które mogą być niezgodne z prawem.

2) Bezpieczeństwo komunikacji

Organizacja w przypadku przesyłania informacji z użyciem środków komunikacji uwzględnia i stosuje następujące elementy:

a) brak stosowania środków kryptograficznych podczas komunikacji wewnętrznej,

b) ochrona przesyłanej informacji przed przechwyceniem, kopiowaniem, modyfikacją, błędnym routingiem i zniszczeniem za pomocą oprogramowania antywirusowego oraz bramy sieciowej,

c) wykrywanie i ochrona przed szkodliwym kodem, który może być przesyłany za pomocą środków komunikacji elektronicznej,

d) ochrona wrażliwych informacji elektronicznych przekazywanych w formie załączników do poczty e-mail,

e) zalecenia określające akceptowalny sposób korzystania z elektronicznych urządzeń komunikacyjnych opisanych w wytycznych co do rozpoczęcia, zawieszenia/odwieszenia, zakończenia pracy przez użytkownika w systemie teleinformatycznym wyszczególnionych w §3 ust. 4, 5 i 6 niniejszej Polityki Bezpieczeństwa Teleinformatycznego,

f) zobowiązanie personelu, podmiotów zewnętrznych i wszystkich innych użytkowników do nieprowadzenia działań na szkodę organizacji, np. poprzez zniesławienie, nękanie, podszywanie się, przesyłanie listów systemem łańcuszkowym, nieautoryzowane zakupy itp.,

g) korzystanie z technik kryptograficznych, np. do ochrony poufności, integralności i autentyczności informacji opisanych w § 4 ust. 1 niniejszej Polityki Bezpieczeństwa Teleinformatycznego,

h) zabezpieczenia i ograniczenia związane z możliwościami stosowania środków komunikacji, np. automatyczne przekazywanie poczty elektronicznej na zewnątrz,

i) doradzanie pracownikom w kwestii stosowania odpowiednich środków ostrożności, aby nie ujawniali informacji poufnych,

j) niepozostawianie wiadomości zawierających poufne informacje w automatycznych sekretarkach, gdyż mogą zostać odsłuchane przez nieupoważnione osoby, zapisane w publicznych systemach lub zapisane niewłaściwie w wyniku pomyłki w wybieraniu numeru.

Podstawa prawna:

1. Zgodnie z art. 32 pkt 1 lit. b) oraz motywem nr 83 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.
2. Zgodnie z wymogami normy PN-EN ISO/IEC 27001:2017 zał. A.13

3. Ochrona przed szkodliwym oprogramowaniem

Organizacja wprowadziła i stosuje następujące środki bezpieczeństwa przed szkodliwym oprogramowaniem:

1) zakaz korzystania z nieautoryzowanego oprogramowania na terenie całej organizacji;

2) zabezpieczenia wykrywające lub zapobiegające użyciu nieautoryzowanego oprogramowania (np. białe listy aplikacji),

3) zabezpieczenia wykrywające lub zapobiegające użyciu znanych szkodliwych stron webowych lub podejrzewanych o to (np. czarne listy),

4) zabezpieczenia przed ryzykami związanymi z otrzymywaniem złośliwego oprogramowania malware z sieci zewnętrznych albo za pośrednictwem innych mediów w postaci wymiennych nośników danych typu pendrive. Na oprogramowanie malware składają się: wirusy (w tym wirusy pasożytnicze, wirusy wieloczęściowe, wirusy towarzyszące, makrowirusy), robaki, wabbit, konie trojańskie, backdoory, programowanie szpiegujące (w tym scumware, stealware/parasiteware, oprogramowanie reklamowe, elementy typu hijacker), exploit, rootkit, rejestratory klawiszy, dialery, oprogramowanie szantażujące,

5) przeprowadzanie regularnych przeglądów oprogramowania i danych zawartych w systemach obsługujących krytyczne procesy organizacji,

6) instalacja i regularna aktualizacja oprogramowania do wykrywania oraz usuwania szkodliwego oprogramowania poprzez skanowanie komputerów i nośników informacji, jako zabezpieczenie prewencyjne lub na bieżąco. Skanowanie obejmuje:

a) skanowanie wszystkich plików odbieranych poprzez sieci lub na innych nośnikach pamięci pod kątem obecności szkodliwego oprogramowania,

b) skanowanie załączników poczty elektronicznej oraz ściąganych danych pod kątem obecności szkodliwego oprogramowania,

c) sprawdzanie stron internetowych pod kątem obecności szkodliwego oprogramowania,

7) plan ciągłości działania w celu odtwarzania po ataku szkodliwego oprogramowania, będący procedurą wykonywania kopii zapasowych danych elektronicznych opisaną w §4 ust.7 niniejszej Polityki Bezpieczeństwa Teleinformatycznego,

8) Administrator zapewnia środki organizacyjne celem wdrożenia procedur dostępu do informacji związanych ze szkodliwym oprogramowaniem i zapewnienia, że biuletyny informacyjne są dokładnym i użytecznym źródłem informacji. Najwyższe kierownictwo zapewnia korzystanie ze źródeł informacji o potwierdzonej jakości, np. renomowanych czasopism, rzetelnych stron internetowych lub stron producentów oprogramowania antywirusowego tak, aby odróżnić prawdziwie szkodliwe oprogramowanie od spreparowanych fałszywych informacji,

9) izolowanie środowisk, dla których skutki działania szkodliwego oprogramowania mogą być katastrofalne.

Podstawa prawna:

1. Zgodnie z art. 32 pkt 1 lit. b) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.
2. Zgodnie z wymogami normy PN-EN ISO/IEC 27001:2017 zał. A.12.2

4. Postępowanie z urządzeniami mobilnymi

1) Organizacja wprowadza wewnętrzny podział urządzeń mobilnych na:

a) mobilna stacja robocza typu notebook/ultrabook/netbook itp…,

b) smartfon - przenośne urządzenie telefoniczne łączące w sobie funkcje telefonu komórkowego i komputera kieszonkowego.

2) Wobec urządzeń mobilnych będących własnością organizacji stosuje się następujące środki bezpieczeństwa:

a) rejestracja urządzeń mobilnych objętych „**Ewidencją urządzeń elektronicznych przetwarzających dane osobowe**" – dokument nr: „**SZBI-PBT-Zał. 3**" stanowiącej **załącznik nr 3** do **Polityki Bezpieczeństwa Teleinformatycznego**.

b) wydającym sprzęt mobilny w imieniu Administratora jest wymiennie: Administrator, Inspektor Ochrony Danych, Administrator Systemu Informatycznego, osoba upoważniona, co potwierdza dokumentem o nazwie: „**Umowa powierzenia mienia pracownikowi**" – dokument nr: „**SZBI-PBT-Zał. 2**" stanowiący **załącznik nr 2** do **Polityki Bezpieczeństwa Teleinformatycznego**.

c) ograniczenie instalacji oprogramowania oraz kontrola dostępu w postaci konta użytkownika i administratora w przypadku mobilnej stacji roboczej lub aplikacji ograniczającej dostęp na smartfonie;

d) automatyczna aktualizacja oprogramowania z uwzględnieniem możliwości zarządzania czasookresem aktualizacji (momentem rozpoczęcia i zakończenia) przez Administratora Systemu Informatycznego,

e) ograniczenia w połączeniach do usług informacyjnych,

f) zabezpieczenia kryptograficzne o ile są wymagane w ocenie Administratora Systemu Informatycznego, opisane w §4 ust. 1 niniejszej Polityki Bezpieczeństwa Teleinformatycznego,

g) ochrona przed szkodliwym oprogramowaniem w postaci oprogramowania antywirusowego,

h) zdalne wyłączanie, usuwanie danych lub blokowanie będące integralną częścią oprogramowania antywirusowego,

i) kopie zapasowe opisane w §4 ust. 7 niniejszej Polityki Bezpieczeństwa Teleinformatycznego.

Podstawa prawna:

1. Zgodnie z art. 32 pkt 1 lit. b) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.
2. Zgodnie z wymogami normy PN-EN ISO/IEC 27001:2017 zał. A.6.2.1

5. Nadzór nad oprogramowaniem

1) Ilość i rodzaj oprogramowania instalowanego na stanowiskach roboczych oraz serwerze/ach jest nadzorowany przez Administratora Systemu Informatycznego.

2) Elementami składowymi nadzoru nad oprogramowaniem są:

a) modyfikacje oprogramowania/systemu wynikające z bieżących potrzeb,

b) parametryzacje i konfiguracje,

c) instalacje nowych wersji oprogramowania oraz aktualizacji,

d) konsultacje i szkolenia użytkowników,

e) usuwanie błędów i awarii oprogramowania/systemu,

f) opieka zdalna, z wykorzystaniem narzędzi zdalnego dostępu do danych.

Podstawa prawna:

1. Zgodnie z art. 32 pkt 1 lit. b) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.
2. Zgodnie z wymogami normy PN-EN ISO/IEC 27001:2017 zał. A.12.5

6. Inwentaryzacja sprzętu

1) Proces inwentaryzacji sprzętu ma zapobiec utracie, uszkodzeniu, kradzieży lub utracie integralności aktywów oraz zakłóceniom w działaniu organizacji.

2) Wyniki kontroli i inwentaryzacji sprzętu zawierają się w „**Ewidencji urządzeń elektronicznych przetwarzających dane osobowe**" – dokument nr: „**SZBI-PBT-Zał. 3**" stanowiącej **załącznik nr 3** do niniejszej **Polityki Bezpieczeństwa Teleinformatycznego**.

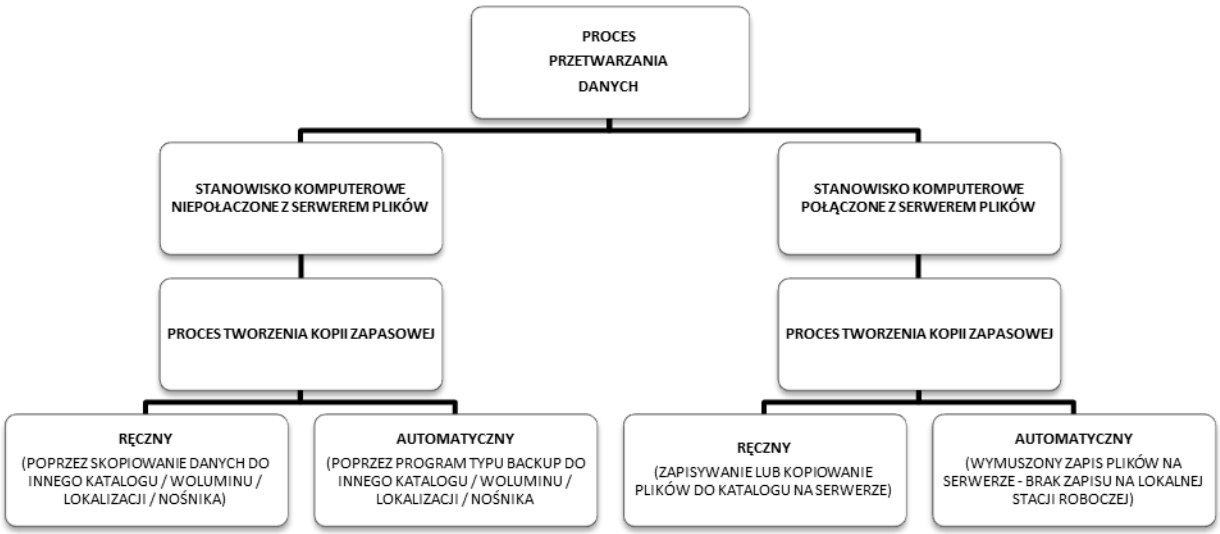
Podstawa prawna:

1. Zgodnie z art. 32 pkt 1 lit. d) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.
2. Zgodnie z wymogami normy PN-EN ISO/IEC 27001:2017 zał. A.11.2

7. Kopie zapasowe

1) Dane, w tym dane osobowe przetwarzane w systemach teleinformatycznych podlegają zabezpieczeniu poprzez tworzenie kopii zapasowych. Za proces tworzenia kopii zapasowych odpowiada Administrator Systemu Informatycznego lub osoba specjalnie do tego celu wyznaczona.

2) Kopie zapasowe informacji przechowywanych w systemie teleinformatycznym przetwarzającym dane osobowe tworzone są wg poniższego schematu:



3) Każdorazowo oraz okresowo po wykonaniu kopii bezpieczeństwa baz danych Administrator Systemu Informatycznego weryfikuje poprawność jej wykonania w sposób wymienny tj.:

a) w przypadku serwera / programu archiwizacyjnego: oprogramowanie archiwizujące wykonuje automatyczną analizę poprawności wykonania i odczytu kopii po wykonaniu kopii,

b) w przypadku samodzielnych stacji roboczych poprzez „ręczne" sprawdzenie poprawności wykonania kopii,

c) sposób oraz poprawność wykonania kopii potwierdzana jest w dokumencie „**Ewidencja kopii zapasowych**" – dokument nr: „**SZBI-PBT-Zał. 1**" – stanowiącym **załącznik nr 1** do niniejszej **Polityki Bezpieczeństwa Teleinformatycznego**.

4) Nośniki kopii zapasowych, które zostały wycofane z użycia pozbawiane są zapisanych danych za pomocą specjalnego oprogramowania do bezpiecznego usuwania zapisanych danych. W przeciwnym wypadku podlegają fizycznemu zniszczeniu z wykorzystaniem metod adekwatnych do typu nośnika, w sposób uniemożliwiający odczytanie zapisanych na nich danych.

5) Ponadto:

a) Zbiory danych przechowywane są na serwerze obsługującym system teleinformatyczny. Wszelkie dane przetwarzane w pamięci poszczególnych stacji roboczych oraz komputerów przenośnych są niezwłocznie umieszczane w odpowiednich, przydzielonych dla danego użytkownika przez Administratora Systemu Informatycznego miejscach na serwerze lub innych wskazanych i określonych lokalizacjach.

b) Zakazuje się zapisywania danych chronionych, w tym danych osobowych na zewnętrznych nośnikach magnetycznych, optycznych, półprzewodnikowych i innych bez zaszyfrowania.

c) Kopie zapasowe programów i aktualizowane kopie systemu teleinformatycznego przechowywane są w szafie zamykanej na klucz, stojącej w innym pomieszczeniu niż serwery.

d) Po wygaśnięciu okresu przydatności kopii zapasowych (zastąpieniu ich przez aktualne wersje lub zakończeniu okresu trwałości), są one trwale kasowane lub nośniki je przechowujące niszczone są mechanicznie zgodnie z §4 ust. 8 niniejszej Polityki Bezpieczeństwa Teleinformatycznego.

Podstawa prawna:

1. Zgodnie z art. 32 pkt 1 lit. c) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.
2. Zgodnie z wymogami normy PN-EN ISO/IEC 27001:2017 zał. A.12.3

8. Postępowanie z nośnikami

1) Organizacja stosuje oraz dopuszcza wedle zapotrzebowania nośniki danych takie jak:

a) nośnik magnetyczny: napęd taśmowy (streamer) oraz dysk twardy (HDD),

b) nośnik optyczny: CD oraz DVD z podziałem na ($ROM^{(tylko\ odczyt)}$ / $R^{(jednokrotny\ zapis)}$ / $RW^{(wielokrotny\ zapis)}$),

c) nośnik półprzewodnikowy: dysk SSD, pendrive oraz karta pamięci FLASH.

2) W przypadku posługiwania się nośnikiem danych pochodzącym od organizacji zewnętrznej, obligatoryjnym jest sprawdzenie go programem antywirusowym przez przynajmniej jedną osobę spośród wymienionych:

a) Administrator,

b) Inspektor Ochrony Danych,

c) Administrator Systemu Informatycznego,

d) użytkownik.

3) Nośniki danych mogą być używane tylko i wyłącznie na terenie organizacji lub na terenie organizacji, której to powierzono przetwarzanie danych poprzez stosowną umowę w trybach dostępu zależnych od rodzaju nośnika danych tj:

a) nośnik magnetyczny – tryb dostępu: zapis, odczyt, edycja, usuwanie,

b) nośnik optyczny – tryb dostępu: zapis, odczyt, usuwanie,

c) nośnik półprzewodnikowy – tryb dostępu: zapis, odczyt, edycja, usuwanie.

4) Nośniki magnetyczne i półprzewodnikowe raz użyte do przetwarzania danych osobowych mogą być wykorzystywane do innych celów, tylko po nadpisaniu danych w trybie kasowania formatującego przy zastosowaniu specjalistycznego oprogramowania lub demagnetyzacji. Nośniki na których nie można powtórnie zapisać informacji, powinny być niszczone poprzez zniszczenie mechaniczne (pocięcie, zgniecenie, spopielenie itp.).

5) Nośniki optyczne, których okres archiwizacji lub przydatności do przetwarzania zakończył się, niszczone są w sposób mechaniczny (pocięcie, zgniecenie, spopielenie itp.).

6) Zaszyfrowane nośniki półprzewodnikowe (dyski SSD, pendrive oraz karty pamięci FLASH) z jednostkowymi danymi osobowymi są – na czas ich użyteczności, przechowywane w zamkniętych na klucz szafach, a po wykorzystaniu dane na nich zawarte trwale usuwane, lub nośniki są niszczone w sposób mechaniczny (pocięcie, zgniecenie, spopielenie itp.).

Podstawa prawna:

1. Zgodnie z art. 32 pkt 1 lit. c) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.
2. Zgodnie z wymogami normy PN-EN ISO/IEC 27001:2017 zał. A.8.3