ZARZĄDZENIE NR 46/2018
WÓJTA GMINY MASŁOWICE

z dnia 31 lipca 2018 r.

w sprawie wdrożenia Systemu Zarządzania Bezpieczeństwa Informacji w organizacji o nazwie: Urząd Gminy Masłowice

Na podstawie art. 24 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) z 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 zarządza się co następuje:

§ 1. Wójt Gminy Masłowice wdraża System Zarządzania Bezpieczeństwem Informacji.

§ 2. Na System Zarządzania Bezpieczeństwem Informacji składa się Polityka Bezpieczeństwa Informacji, stanowiąca załącznik nr 1 do niniejszego zarządzenia oraz Polityka Bezpieczeństwa Teleinformatycznego stanowiąca załącznik nr 2 do niniejszego zarządzenia.

§ 3. Przetwarzanie danych osobowych w Urzędzie Gminy Masłowice:

1. Służy realizacji zadań wynikających z ustawy o samorządzie gminnym oraz innych ustaw szczególnych.

2. Dane osobowe przetwarza się wyłącznie dla określonych celów związanych z działalnością urzędu.

3. Przetwarzanie danych osobowych może odbywać się w systemie informatycznym, a także w kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych.

§ 4. Administratorem danych osobowych w Urzędzie Gminy Masłowice w rozumieniu ustawy o ochronie danych osobowych jest Wójt Gminy Masłowice.

§ 5. 1. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie, wydane przez Administratora danych osobowych.

2. Osoba dopuszczona do przetwarzania danych osobowych podpisuje oświadczenie, które dołącza się do jej akt osobowych.

§ 6. 1. Powołuje się Administratora systemów informatycznych w celu sprawowania nadzoru nad funkcjonowaniem systemów i programów informatycznych przetwarzających dane osobowe.

2. Funkcję Administratora systemów informatycznych powierza się Inspektorowi d/s informatyki w Urzędzie Gminy Masłowice – Pani Ewie Stypa – Wodo

§ 7. Traci moc zarządzenie Nr 30/2016 Wójta Gminy Masłowice z dania 05.05. 2016 r.

§ 8. Zarządzenie wchodzi w życie z dniem podpisania.

Wójt Gminy Masłowice

Bogusław Gontkowski

Załącznik Nr 1 do Zarządzenia Nr 46/2018
Wójta Gminy Masłowice
z dnia 31 lipca 2018 r.

Polityka Bezpieczeństwa Informacji *w organizacji o nazwie:* GMINA MASŁOWICE

Spis treści

Wprowadzenie

Mając świadomość zmian formalnoprawnych oraz technicznych w procesie przetwarzania danych osobowych, najwyższe kierownictwo zdecydowało o konieczności wprowadzenia do organizacji procedur, które uregulują System Zarządzania Bezpieczeństwem Informacji zarówno wewnątrz organizacji, jak i na zewnątrz, w postaci Polityki Bezpieczeństwa Informacji.

Najwyższe kierownictwo organizacji określiło w **„Deklaracji stosowania"** – dokumencie nr: **„SZBI-PBI-Zał. 0"** stanowiącym **załącznik nr 0** do **Polityki Bezpieczeństwa Informacji** jakie zabezpieczenia są wdrażane i stosowane, a także argumenty uzasadniające wybór konkretnych zabezpieczeń.

§ 1. Cele bezpieczeństwa informacji

1. Celem wprowadzenia Polityki Bezpieczeństwa Informacji do organizacji jest zharmonizowanie systemu ochrony danych osobowych w taki sposób, by zapewnić realizacje podstawowych praw i wolności osób fizycznych, których dane osobowe organizacja przetwarza w związku z realizacją zadań publicznych oraz czynności branżowo-administracyjnych. Celem wprowadzenia Polityki Bezpieczeństwa Informacji jest także ciągłe edukowanie osób zaangażowanych w proces przetwarzania danych osobowych. Polityka Bezpieczeństwa Informacji ma również na celu zapewnienie poufności oraz integralności danych osobowych, względem których zachodzi proces przetwarzania poprzez przypisanie odpowiedzialności i uprawnień względem osób upoważnionych do przetwarzania tych danych oraz użytkowników systemów teleinformatycznych.

2. Najwyższe kierownictwo dochowuje należytej staranności, by System Zarządzania Bezpieczeństwa Informacji był silnie zintegrowany z innymi systemami czy procesami, które warunkują osiągniecie celów strategicznych przez organizacje.

3. Najwyższe kierownictwo deklaruje, iż bezpieczeństwo informacji jest uwzględniane w ramach projektowania procesów czy systemów, które służą organizacji do osiągnięcia celów strategicznych.

4. Najwyższe kierownictwo, wdrażając Politykę Bezpieczeństwa Informacji wykazuje przywództwo i zaangażowanie w kontekście bezpieczeństwa przetwarzanych danych osobowych w związku z realizacją czynności branżowo-administracyjnych poprzez zapewnienie, iż wprowadzona Polityka Bezpieczeństwa Informacji:

1) jest zgodna z celami strategicznymi istnienia organizacji,

2) określa cele bezpieczeństwa informacji,

3) zobowiązuje najwyższe kierownictwo do ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji,

4) określa spełnienie wymagań zgodnie z obowiązującymi normami prawnymi,

5) jest zakomunikowana w organizacji,

6) jest dostępna jako udokumentowana i formalnoprawnie wdrożona procedura,

7) jest dostępna dla podmiotów zainteresowanych, o ile jest to uzasadnione względami formalnoprawnymi.

Podstawa prawna:
Zgodnie z wymogami normy PN-EN ISO/IEC 27001:2017 pkt 5.2; 6.2; 7.5

§ 2. Przepisy ogólne

1. Z racji tego, iż najwyższe kierownictwo w ramach realizacji praw podstawowych w zakresie ochrony danych osobowych, kieruje się zasadą legalności przetwarzania zgodnego z prawem, opiera System Zarządzania Bezpieczeństwem Informacji określony w niniejszej Polityce Bezpieczeństwa Informacji na następujących podstawach prawnych oraz normach ISO:

1) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. 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) Norma PN-EN ISO/IEC 27001:2017 (Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji - Wymagania);

3) Norma PN-EN ISO/IEC 27002:2017 (Technika Informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zabezpieczania informacji);

4) Norma PN-ISO/IEC 27005:2014-01 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji – Wsparcie do Normy PN-EN ISO/IEC 27001:2017);

5) Norma PN-ISO 31000:2012 (Zarządzanie ryzykiem – Zasady i wytyczne).

§ 3. Definicje legalne

Ilekroć w „Polityce Bezpieczeństwa Informacji" mówi się o:

1. **Organizacji** – rozumie się przez to osobę prawną, organ publiczny, jednostkę lub inny podmiot. Do celów niniejszej Polityki Bezpieczeństwa Informacji wprowadza się nazwę własną organizacji: **GMINA MASŁOWICE;**

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

3. **Najwyższym kierownictwie administratora (najwyższe kierownictwo)** – rozumie się przez to osoby, które reprezentują organizację, ustanawiają Politykę Bezpieczeństwa Informacji oraz inne polityki, a także określają role, odpowiedzialność i uprawnienia;

4. **Podmiocie przetwarzającym (procesorze)** – rozumie się przez to osobę fizyczną lub organizację, która przetwarza dane osobowe w imieniu administratora;

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

6. **Odbiorcy** – rozumie się przez to osobę fizyczną lub organizację, której ujawnia się dane osobowe bez względu na to, czy jest stroną trzecią;

7. **Stronie trzeciej** – rozumie się przez to osobę fizyczną lub organizację inną niż osoba, której dane dotyczą, inną niż administrator, podmiot przetwarzający czy osoby upoważnione do przetwarzania danych osobowych;

8. **Podmiocie zewnętrznym** – rozumie się przez to kontrahenta Administratora;

9. **Organie nadzorczym** – rozumie się przez to niezależny organ publiczny ustanowiony przez państwo członkowskie, który monitoruje stosowanie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w celu ochrony praw podstawowych osób fizycznych w związku z czynnościami przetwarzania;

10. **Rozporządzeniu ogólnym** – rozumie się przez to Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. 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);

11. **Prawo państwa członkowskiego** – z uwagi na fakt, iż organizacja nie przetwarza danych osobowych poza granicami państwa polskiego, rozumie się przez to prawo krajowe;

12. **Inspektorze Ochrony Danych (DPO)** – 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.

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

14. **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.

15. **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;

16. **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;

17. **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;

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

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

20. **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.

21. **Uchybieniu** – rozumie się przez to uświadomione lub nieuświadomione działanie zmierzające do naruszenia, które może doprowadzić do uszkodzenia bądź utraty danych osobowych.

22. **Naruszeniu** – rozumie się przez to uświadomione lub nieuświadomione działanie, które doprowadziło do uszkodzenia bądź utraty danych osobowych.

§ 4. Zakres Systemu Zarządzania Bezpieczeństwem Informacji

1. Określenie zakresu Systemu Zarządzania Bezpieczeństwem Informacji

1) Organizacja, określając zakres Systemu Zarządzania Bezpieczeństwem Informacji, rozważa jej kontekst wewnętrzny oraz zewnętrzny, identyfikuje strony zainteresowane, a także określa interfejsy i zależności między działaniami wykonywanymi wewnątrz organizacji, a także przez inne organizacje.

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

2. Kontekst wewnętrzny

1) Organizacja określa kontekst wewnętrzny uwzględniając następujące czynniki:

   a) schemat organizacyjny będący odzwierciedleniem zależności pomiędzy komórkami funkcjonalnymi w kontekście przepływu danych osobowych oraz określający bezpośrednią podległość Inspektora Ochrony Danych,

   b) ład organizacyjny w rozumieniu zindywidualizowanych zasad zarządzania organizacją znajdujących swoje źródło we wdrożonych procedurach i normach,

   c) ustanowione przez najwyższe kierownictwo cele organizacji w rozumieniu celów strategicznych, ekonomicznych i pozaekonomicznych, taktycznych, operacyjnych (katalog otwarty),

   d) określoną przez najwyższe kierownictwo misję organizacji w rozumieniu zespołu wartości podkreślających rolę organizacji na rzecz otoczenia, w którym organizacja działa,

   e) aktywa organizacji w postaci zasobu ludzkiego - jego wiedzy, kompetencji, umiejętności oraz postaw,

   f) procesy podejmowania decyzji uwzględniając strukturę organizacyjną,

   g) kulturę organizacji,

   h) relacje do wewnątrz organizacji.

Podstawa prawna:
Zgodnie z wymogami normy PN-ISO 31000:2012 pkt 2.11

3. Kontekst zewnętrzny

1) Organizacja określa kontekst zewnętrzny uwzględniając następujące czynniki:

   a) relacje z zewnętrznymi podmiotami,

   b) środowisko zewnętrzne mające wpływ na cele organizacji:

      - prawne,

finansowe,

ekonomiczne.

Podstawa prawna:
Zgodnie z wymogami normy PN-ISO 31000:2012 pkt 2.10

4. **Określenie potrzeb stron zainteresowanych wraz z rejestrem czynności przetwarzania danych**

1) Określenie potrzeb stron zainteresowanych stanowi istotny element systemowego podejścia do zarządzania bezpieczeństwem informacji.

2) Organizacja określa kategorie osób oraz katalog podmiotów, które podlegają wpływom decyzji lub działań organizacji i przez to należy wziąć pod uwagę ich potrzeby:

a) pracownicy organizacji,

b) osoby fizyczne oraz podmioty gospodarcze obsługiwane przez organizację w ramach wykonywanych przez nią zadań,

c) podmioty publiczne,

d) organy kontrolne,

e) kontrahenci organizacji (dostawcy, podwykonawcy, usługodawcy),

f) organizacje pozarządowe, fundacje, stowarzyszenia,

g) inne strony zainteresowane nieokreślone powyżej.

3) Katalog stron zainteresowanych szczegółowo określa **„Rejestr czynności przetwarzania"** – dokument nr: **„SZBI-PBI-Zał. 1"** stanowiący **załącznik nr 1** do **Polityki Bezpieczeństwa Informacji**.

4) Po zidentyfikowaniu stron zainteresowanych, organizacja ma świadomość tych najistotniejszych dla niej. Organizacja określa strony zainteresowane najbardziej dla niej istotne w ten sposób, iż bada, które z organizacji sektora prywatnego czy publicznego mogą najsilniej oddziaływać na realizację głównego celu działalności organizacji.

5) Określenie potrzeb stron zainteresowanych jest istotne w punktu widzenia zrozumienia kontekstu organizacji, który z kolei w znacznej mierze rzutuje na formę systemu bezpieczeństwa informacji w organizacji.

6) Administrator prowadzi rejestr czynności przetwarzania danych osobowych, za które odpowiada. W przedmiotowym rejestrze podaje się następujące informacje:

a) imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie - przedstawiciela Administratora oraz Inspektora Ochrony Danych,

b) cel przetwarzania,

c) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych,

d) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych,

e) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej (nie dotyczy),

f) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych,

g) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

7) Administrator prowadzi rejestr czynności przetwarzania w wersji papierowej oraz elektronicznej.

8) Informacje, o których mowa w § 4 ust. 4 pkt 6 niniejszej PBI określone zostały w **„Rejestrze czynności przetwarzania"** – dokumencie nr: **„SZBI-PBI-Zał. 1"** stanowiącym **załącznik nr 1** do **Polityki Bezpieczeństwa Informacji**.

Podstawa prawna:
1.Zgodnie z wymogami normy PN-EN ISO/IEC 27001:2017 pkt 4.2 2.Zgodnie z art. 30 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r.

5. **Interfejsy i zależności między działaniami wykonywanymi przez organizację, a także przez inne organizacje**

1) Interfejsy i zależności między działaniami wykonywanymi przez organizację, a także przez inne organizacje wymagają analizy pod względem przepływu informacji.

2) Przepływ informacji, o którym mowa w § 4 ust. 5 pkt 1 niniejszej PBI, odbywa się w następujących kierunkach:

   a) wewnątrz organizacji: najwyższe kierownictwo à kierownictwo wyższego szczeblaà kierownictwo niższego szczebla à pracownicy merytoryczni à pracownicy gospodarczy;

   b) na zewnątrz organizacji: najwyższe kierownictwo organizacji à najwyższe kierownictwo innej organizacji à najwyższe kierownictwo organizacji;

3) w ramach przepływu danych Administrator w szczególności uwzględnia odpowiednie środki techniczne i organizacyjne zapewniające ochronę powierzanych danych osobowych przed ich nieuprawnionym przejęciem, utratą, uszkodzeniem czy zniszczeniem.

Podstawa prawna:
Zgodnie z art. 5 ust. 1 lit. f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r.

§ 5. Podstawy legalności przetwarzania danych osobowych

1. Organizacja przetwarza dane osobowe w oparciu o następujące przesłanki legalności:

1) udzielona zgoda na przetwarzanie danych osobowych w jednym lub w większej liczbie określonych celów,

2) umowa, której stroną jest osoba, której dane dotyczą, lub w celu podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy,

3) realizacja obowiązku prawnego, któremu podlega Administrator,

4) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi.

Podstawa prawna:
Zgodnie z motywem 40, 45, 46, 47 oraz art. 6 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r.

2. Organizacja w zakresie przetwarzania szczególnych kategorii danych osobowych bierze pod uwagę przesłanki legalności wynikające z art. 9 ust. 2 Rozporządzenia ogólnego. Należy zaznaczyć, iż organizacja niektóre przesłanki traktuje jako przeważające w procesie przetwarzania danych osobowych, inne natomiast zupełnie pomija lub wykorzystuje wspomagająco.

3. Organizacja w procesie przetwarzania danych osobowych uwzględnia następujące zasady:

1) legalność przetwarzania danych osobowych (zgodność z prawem),

2) rzetelność oraz przejrzystość,

3) przetwarzanie danych w ściśle określonym celu,

4) minimalizacja przetwarzanych danych osobowych,

5) prawidłowość przetwarzanych danych osobowych,

6) ograniczenie przechowywania danych osobowych,

7) integralność oraz poufność przetwarzanych danych osobowych.

Podstawa prawna:
Zgodnie z art. 9 ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r.

§ 6. Charakterystyka danych osobowych

1. Zasady ochrony danych w organizacji mają zastosowanie do wszystkich informacji, za pomocą których możliwe jest zidentyfikowanie konkretnej osoby fizycznej. Możliwości w zakresie identyfikacji należy rozpatrywać odnosząc się do wszelkich rozsądnych sposobów, za pomocą których organizacja ma możliwość bezpośredniego lub pośredniego dookreślenia osoby fizycznej. Sposoby, za pomocą których organizacja ma możliwość zidentyfikowania konkretnej osoby fizycznej, należy oceniać przez pryzmat takich czynników jak: czas, koszt, dostępną na dany moment technologię oraz postęp technologiczny.

Podstawa prawna:

Zgodnie z motywem 26 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r.

2. W celu kontroli rodzaju przetwarzanych identyfikatorów, o których mowa w art. 4 ust. 1 rozporządzenia ogólnego, organizacja prowadzi wykaz zbiorów danych osobowych wraz ze wskazaniem ich struktury w **„Rejestrze czynności przetwarzania"** – dokumencie nr: **„SZBI-PBI-Zał. 1"** stanowiący **załącznik nr 1** do **Polityki Bezpieczeństwa Informacji**.

Podstawa prawna:

Zgodnie z art. 9, 10 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r.

§ 7. Odpowiedzialność za bezpieczeństwo informacji

1. Odpowiedzialność Administratora

1) Najwyższe kierownictwo Administratora wykazuje przywództwo i zaangażowanie w proces bezpieczeństwa informacji.
2) Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z rozporządzeniem ogólnym.
3) Administrator wdraża odpowiednie polityki ochrony danych.
4) Administrator uwzględnia ochronę danych w fazie projektowania.
5) Administrator rejestruje czynności przetwarzania.
6) Administrator współpracuje z organem nadzorczym.
7) Administrator wprowadza procedury gwarantujące, iż osoby fizyczne działające z jego upoważnienia, które mają dostęp do danych osobowych, przetwarzają je wyłącznie na polecenie Administratora.
8) Administrator wdraża procedury zgłaszania naruszenia ochrony danych osobowych organowi nadzorczemu.
9) Administrator wdraża procedury zawiadamiania osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych.
10) Administrator wdraża procedury oceny skutków dla ochrony danych osobowych w przypadku, gdyby istniało wysokie prawdopodobieństwo, iż rodzaj przetwarzania może spowodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.
11) Administrator informuje osoby fizyczne o procesie przetwarzania ich danych osobowych kierując się zasadą przejrzystości poprzez formułowanie komunikatów jasnym i prostym językiem.
12) Administrator wyznacza Inspektora Ochrony Danych.

Podstawa prawna:

Zgodnie z art. 24 ust. 1 – 2, art. 25, 30, 32 ust. 4, art. 33 – 35, art. 37 oraz motywem nr 50 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r.

13) Najwyższe kierownictwo zapewnia, by Inspektor Ochrony Danych był angażowany we wszystkie sprawy związane z problematyką przetwarzania danych osobowych.
14) Najwyższe kierownictwo wspiera Inspektora Ochrony Danych poprzez dostarczenie mu zasobów pozwalających na należyte wykonywanie zadań oraz pielęgnowanie jego wiedzy fachowej.
15) Najwyższe kierownictwo przeprowadza cyklicznie (nie rzadziej, niż raz na rok) wraz z Inspektorem Ochrony Danych przegląd zarządzania bezpieczeństwem informacji w celu zapewnienia jego przydatności do aktualnych warunków formalnych oraz faktycznych, skuteczności, a także adekwatności.
16) Najwyższe kierownictwo wraz z Inspektorem Ochrony Danych ciągle doskonali System Zarządzania Bezpieczeństwem Informacji.

Podstawa prawna:

1.Zgodnie z art. 38 ust. 1 – 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r.
2.Zgodnie z wymogami normy PN-EN ISO/IEC 27001:2017 pkt 5.1; 9.3; 10.2; zał. A.6.1.1, A.6.1.2

2. Wyznaczenie Inspektora wraz z określeniem jego odpowiedzialności

1) Celem przestrzegania procedur ustanowionych w ramach Polityki Bezpieczeństwa Informacji, Administrator wyznacza Inspektora Ochrony Danych.

2) Administrator wyznacza Inspektora Ochrony Danych na mocy **„Procedury wyznaczenia DPO oraz zakres jego obowiązków"** – dokumentu nr: **„SZBI-PBI-Zał. 2"** stanowiącego **załącznik nr 2** do **Polityki Bezpieczeństwa Informacji**.

3) Inspektor Ochrony Danych sprawuje swoje obowiązki z zachowaniem należytej staranności uwzględniając ryzyko związane z procesem przetwarzania danych osobowych mając jednocześnie na uwadze: zakres przetwarzania, jego charakter, kontekst wewnętrzny i zewnętrzny organizacji oraz cele przetwarzania.

Podstawa prawna:

Zgodnie z art. 39 ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r.

4) Inspektor Ochrony Danych wyznaczony został na podstawie kwalifikacji zawodowych, a także w oparciu o jego wiedzę prawną w zakresie ochrony danych osobowych oraz przepisów branżowych, zgodnie z którymi działa organizacja.

Podstawa prawna:

1.Zgodnie z art. 37 ust. 5 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r.
2.Zgodnie z wymogami normy PN-EN ISO/IEC 27001:2017 pkt 7.2

5) Inspektor Ochrony Danych działa niezależnie – nie mogą go spotkać negatywne konsekwencje w związku z tym, iż wykonuje swoje zadania.

Podstawa prawna:

Zgodnie z art. 38 ust. 3 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r.

6) Zadania Inspektora Ochrony Danych:

a) uświadamianie Administratora, podmiotu przetwarzającego i pracowników organizacji w kontekście ich obowiązków względem rozporządzenia ogólnego, innych przepisów unijnych oraz przepisów państw członkowskich o ochronie danych oraz prowadzenie polityki doradczej w tym zakresie;

b) monitorowanie przestrzegania przez organizację zapisów rozporządzenia ogólnego, innych przepisów unijnych oraz przepisów państw członkowskich o ochronie danych;

c) monitorowanie przestrzegania przez podmiot przetwarzający zapisów rozporządzenia ogólnego, innych przepisów unijnych oraz przepisów państw członkowskich o ochronie danych;

d) prowadzenie działań zwiększających świadomość organizacji oraz podmiotu przetwarzającego;

e) szkolenia pracowników organizacji zaangażowanych w proces przetwarzania danych osobowych;

f) przeprowadzanie audytów wewnętrznych w organizacji lub w strukturach podmiotu przetwarzającego;

g) przedstawianie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie procesu dostosowywania się do zaleceń;

h) współpracowanie z organem nadzorczym;

i) sprawowanie funkcji punktu kontaktowego dla organu nadzorczego.

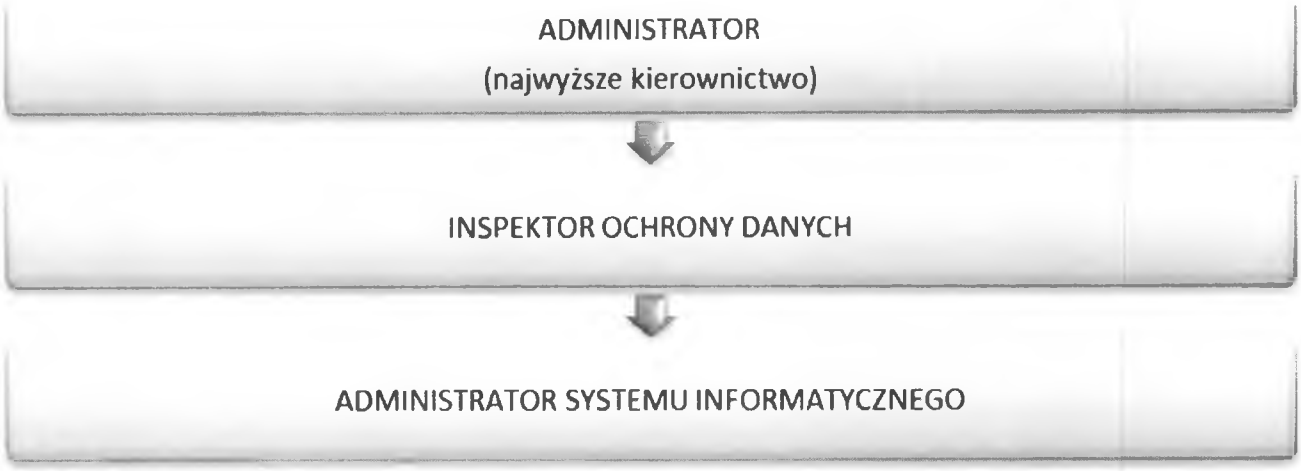
Podstawa prawna:

Zgodnie z art. 39 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r.

3. **Struktura zarządzania bezpieczeństwem informacji**

1) Poprzez to, iż najwyższe kierownictwo wykazuje przywództwo i zaangażowanie w stosunku do zarządzania bezpieczeństwem informacji i ma świadomość, iż odpowiedzialność za bezpieczeństwo informacji powinna być określona i przypisana, ustanawia strukturę zarządzania tak, aby można było nadzorować wdrażanie oraz eksploatację bezpieczeństwa informacji w organizacji.

2) Struktura zarządzania bezpieczeństwem informacji w organizacji przedstawia się następująco:



Podstawa prawna:
Zgodnie z wymogami normy PN-EN ISO/IEC 27001:2017 pkt 5.3 zał. A.6.1.1

§ 8. Bezpieczeństwo osobowe

1. **Procedura nadawania, zmiany oraz ustania upoważnienia do przetwarzania danych osobowych oraz odpowiedzialność osób przetwarzających dane osobowe w organizacji**

1) Najwyższe kierownictwo zapewnia, by pracownicy rozumieli zakres swojej odpowiedzialności w ramach bezpieczeństwa informacji.

2) Najwyższe kierownictwo wymaga, aby wszyscy pracownicy organizacji stosowali zasady bezpieczeństwa informacji zgodnie z niniejszą PBI.

3) Najwyższe kierownictwo zapewnia warunki formalne w formie upoważnienia do przetwarzania danych osobowych dla osób przetwarzających dane osobowe w organizacji z uwagi na fakt, iż przetwarzać dane może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych wydane przez Administratora.

Podstawa prawna:
Zgodnie z wymogami normy PN-EN ISO/IEC 27001:2017 pkt 5.1 zał. nr A.7.2

4) Nadanie przez Administratora upoważnienia do przetwarzania danych osobowych następuje na wniosek przełożonego osoby upoważnianej do przetwarzania danych lub koordynatora zadania, na rzecz którego będą wykonywane czynności związane z przetwarzaniem danych osobowych.

5) Aby nadać upoważnienie do przetwarzania danych osobowych, przełożony osoby upoważnianej do przetwarzania danych osobowych lub koordynator zadania składa wniosek: **„Obiegowa Karta Uprawnień"** – dokumentu nr: **„SZBI-PBI-Zał. 3"** stanowiącego **załącznik nr 3** do **Polityki Bezpieczeństwa Informacji** - do Inspektora Ochrony Danych o wydanie upoważnienia do przetwarzania danych osobowych. Z racji tego, że **„Obiegowa Karta Uprawnień"** jest współdzielona z PBT, jeśli nie planuje się upoważnić osoby, w sprawie której składany jest wniosek, do przetwarzania danych osobowych w systemach teleinformatycznych, wypełniana jest tylko i wyłącznie **część A „Obiegowej Karty Uprawnień"**. Kolejno Inspektor Ochrony Danych przekazuje wniosek do Administratora. W sytuacji nieobecności Inspektora Ochrony Danych w organizacji przełożony osoby upoważnianej do przetwarzania danych osobowych lub koordynator zadania składa wniosek bezpośrednio do Administratora.

6) Wniosek po rozpatrzeniu przez Administratora zostaje przekazany do przełożonego osoby upoważnianej do przetwarzania danych osobowych lub koordynatora zadania oraz do Inspektora Ochrony Danych.

7) O ile zachodzi konieczność upoważniania osoby do przetwarzania danych osobowych w systemie teleinformatycznym, przełożony osoby upoważnianej do przetwarzania danych osobowych lub koordynator zadania bądź Inspektor Danych Osobowych kieruje podpisany wniosek do Administratora Systemu Informatycznego o przydzielenie uprawnień do przetwarzania danych osobowych w systemie teleinformatycznym. Proces przyznawania uprawnień odbywa się zgodnie z procedurą przewidzianą w PBT.

8) O okresie upoważnienia decyduje Administrator.

9) W przypadku zmiany stanowiska pracy lub zakresu czynności, przełożony osoby upoważnianej do przetwarzania danych osobowych lub koordynator zadania bądź Inspektor Danych Osobowych składają

pisemny wniosek do Administratora za pomocą **część A „Obiegowej Karty Uprawnień"** – dokumentu nr: **„SZBI-PBI-Zał. 3"** stanowiącego **załącznik nr 3** do **Polityki Bezpieczeństwa Informacji**. Wniosek po rozpatrzeniu przez Administratora zostaje przekazany do przełożonego osoby upoważnianej do przetwarzania danych osobowych lub koordynatora zadania oraz do Inspektora Ochrony Danych. Jeśli w ślad za zmianą stanowiska pracy lub zakresu czynności idzie zmiana uprawnień w systemie teleinformatycznym, proces zmiany uprawnień odbywa się zgodnie z procedurą przewidzianą w PBT.

10) Z racji tego, że upoważnienie do przetwarzania danych osobowych wydawane jest na czas określony tj. do zakończenia stosunku pracy, wycofanie upoważnienia następuje automatycznie po faktycznym zakończeniu pracy w organizacji osoby do tej pory upoważnionej do przetwarzania danych. W szczególnych przypadkach wycofanie upoważnienia do przetwarzania danych osobowych może nastąpić na wniosek przełożonego osoby upoważnionej do przetwarzania danych lub koordynatora zadania lub Inspektora Ochrony Danych bądź z inicjatywy samego Administratora. Wniosek: **„Obiegowa Karta Uprawnień"** o wycofanie upoważnienia do przetwarzania danych osobowych składa do Administratora przełożony osoby upoważnianej do przetwarzania danych osobowych lub koordynator zadania bądź Inspektor Danych Osobowych. Wniosek o wycofanie upoważnienia po rozpatrzeniu przez Administratora zostaje przekazany do przełożonego osoby upoważnianej do przetwarzania danych osobowych lub koordynatora zadania oraz do Inspektora Ochrony Danych. Wycofanie uprawnień do przetwarzania danych osobowych w systemie teleinformatycznym odbywa się zgodnie z procedurą przewidzianą w PBT.

11) Inspektor Ochrony Danych lub Administrator prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych zawierającą: imię, nazwisko, stanowisko, datę wydania upoważnienia, data ustania upoważnienia oraz zakres upoważnienia. **„Ewidencja osób upoważnionych do przetwarzania danych osobowych"** stanowi dokument nr: **„SZBI-PBI-Zał. 4"** tj. **załącznik nr 4** do **Polityki Bezpieczeństwa Informacji**.

12) Wobec pracownika naruszającego zasady bezpieczeństwa informacji może być prowadzone postępowanie dyscyplinarne w trybie art. 52 ustawy z dnia 26 czerwca 1974r. kodeks pracy (Dz.U.2016.1666 t.j.).

13) Osoba przetwarzająca dane osobowe w organizacji jest zobowiązana do zachowania wszelkiego rodzaju powziętych informacji co do danych osobowych osób fizycznych, których dane dotyczą, w tajemnicy.

14) Klauzula poufności informacji obowiązuje pracownika przetwarzającego dane osobowe w organizacji przez okres trwania umowy o pracę, a także bezwzględnie po jej zakończeniu przez okres nieoznaczony. Najwyższe kierownictwo jest zobowiązane przedstawić osobie przetwarzającej dane osobowe w organizacji odpowiedzialność oraz obowiązki w zakresie bezpieczeństwa informacji, którymi dana osoba będzie związana po ustaniu stosunku pracy lub zmianie zatrudnienia.

15) Osoba przetwarzająca dane osobowe w organizacji ma świadomość, iż przetwarzane dane może wykorzystywać tylko i wyłącznie w celu wykonywania powierzonych jej zadań w ramach stosunku pracy.

16) Osoba przetwarzająca dane osobowe w organizacji ma bezwzględny zakaz przekazywania informacji powziętych co do danych osobowych przetwarzanych w organizacji osobom fizycznym lub podmiotom nieuprawnionym do pozyskiwania takich informacji.

17) Osoba przetwarzająca dane osobowe w organizacji ma świadomość, iż ochrona osób fizycznych w związku z przetwarzaniem danych osobowych jest jednym z praw podstawowych oraz że każda osoba ma prawo do ochrony danych osobowych jej dotyczących.

18) Mając powyższe na uwadze, osoba przetwarzająca dane osobowe w organizacji powinna mieć szczególnie na względzie prawa przysługujące osobie, której dane osobowe są przetwarzane w organizacji oraz mieć świadomość zagrożeń związanych z procesem przetwarzania tych danych za pomocą systemu teleinformatycznego oraz tradycyjnego sposobu przetwarzania.

19) Osoba przetwarzająca dane osobowe w organizacji ma bezwzględny obowiązek postępowania według obowiązujących w organizacji kodeksów postępowania, które zakładają między innymi (*wyliczenie ma charakter otwarty*):

a) zakaz używania prywatnych nośników pamięci,

b) zakaz przechowywania danych osobowych na prywatnych stacjach roboczych,

c) zakaz używania nieswojego loginu i hasła do systemu teleinformatycznego,

d) zakaz przekazywania treści przetwarzanych danych osobom nieuprawnionym,

e) zakaz pozostawiania otwartego pomieszczenia bez nadzoru,

f) zakaz pozostawiania osoby nieupoważnionej do przetwarzania danych osobowych w pomieszczeniu bez nadzoru,

g) konieczność stosowania się do zasady czystego biurka (*po zakończonej pracy, osoba przetwarzająca dane osobowe jest w obowiązku schowania ich w szafie zamykanej przeznaczonej do przechowywania dokumentacji papierowej*),

h) konieczność stosowania się do zasady czystego monitora (*zakaz przechowywania loginu i hasła do systemu teleinformatycznego w miejscu powszechnie dostępnym, szczególnie blisko stacji roboczej, do której loguje się osoba przetwarzająca dane osobowe*),

i) konieczność sprawdzenia przed wyjściem z pomieszczenia, w których zachodzi proces przetwarzania danych osobowych czy wszystkie okna są zamknięte,

j) konieczność pilnego strzeżenia akt, nośników, wszelkiego rodzaju urządzeń mobilnych szczególnie podczas podróży służbowej,

k) konieczność niszczenia zbędnej dokumentacji (nie podlegającej konieczności archiwizacji np. błędnie wydrukowanej) w niszczarce przeznaczonej do tego (*zakaz wyrzucania błędnie wydrukowanych dokumentów do kosza na śmieci*),

l) konieczność stosowania się do zarządzonej przez Administratora polityce kluczy.

Podstawa prawna:
Zgodnie z wymogami normy PN-EN ISO/IEC 27001:2017 pkt 5.3 zał. A.7.1 - A.7.3

2. **Procedura wydania zgody na przebywanie w obszarze przetwarzania danych osobowych**

1) W przypadku osób, które są zatrudnione w organizacji zgodnie z kodeksem pracy, ale z racji zajmowanego stanowiska pracy nie mogą przetwarzać danych osobowych, co nie zmienia faktu, że istnieje uzasadniona konieczność by przebywały w obszarach przetwarzania danych osobowych, Administrator wydaje **„Upoważnienie do przebywania w obszarze przetwarzania danych"** stanowiącą dokument nr: **„SZBI-PBI-Zał. 5"** tj. **załącznik nr 5** do **Polityki Bezpieczeństwa Informacji.**

2) Procedura zgody na przebywanie w obszarze przetwarzania zawiera zobowiązanie osoby, której dotyczy, do zachowania wszelkiego rodzaju powziętych informacji o osobach, których dane osobowe organizacja przetwarza, w poufności.

3) Administrator zaznacza, iż względem każdej osoby zatrudnionej w organizacji, która narusza zasady bezpieczeństwa informacji, również względem osoby, która nie jest upoważniona do przetwarzania danych osobowych, a tylko uzyskała od Administratora zgodę na przebywanie w obszarze przetwarzania danych osobowych, może być prowadzone postępowanie dyscyplinarne w trybie art. 52 ustawy z dnia 26 czerwca 1974r. kodeks pracy (Dz.U.2016.1666 t.j.)

4) Administrator prowadzi ewidencję osób, względem których wydano zgodę na przebywanie w obszarze przetwarzania zawierającą imię i nazwisko, stanowisko oraz datę wydania zgody. **„Ewidencja osób upoważnionych do przebywania w obszarze przetwarzania danych"** stanowi dokument nr**: „SZBI-PBI-Zał. 6"** tj. **załącznik nr 6** do **Polityki Bezpieczeństwa Informacji**.

Podstawa prawna:
Zgodnie z wymogami normy PN-EN ISO/IEC 27001:2017 pkt 5.3 zał. A.7.1 - A.7.3

3. **Prawa przysługujące osobie, której dane dotyczą**

1) Administrator zapewnia przejrzystość komunikatu kierowanego do osoby, której dane osobowe są przetwarzane w sprawie przetwarzania.

2) Od otrzymania żądania (zapytania o swoje dane osobowe) od osoby, której dane dotyczą, Administrator udziela informacji tej osobie w terminie miesiąca. Termin ten może zostać przedłużony o kolejne dwa miesiące, jeśli żądanie będzie miało skomplikowany charakter lub liczba żądań będzie znaczna. Bez względu na okoliczności, Administrator jest w obowiązku w terminie miesiąca jeśli nie udzielić przedmiotowych informacji, to przynajmniej poinformować o przyczynie zastosowania terminu dłuższego niż miesiąc licząc od dnia skutecznego złożenia żądania (zapytania).

3) Jeśli Administrator stwierdzi, iż na podstawie udzielonych informacji w żądaniu (zapytaniu) nie ma pewności co do tego, iż żądanie składa uprawniona osoba, może zażądać dodatkowych informacji niezbędnych do ustalenia tożsamości osoby fizycznej.

4) Podczas pozyskiwania, Administrator udziela osobie, której dane dotyczą w przypadku, kiedy dane osobowe pobierane są bezpośrednio od tej osoby, informacje o następującej treści:

a) dane kontaktowe,

b) dane kontaktowe Inspektora Ochrony Danych,

c) cel przetwarzania danych oraz podstawę prawną,

d) prawnie uzasadnione interesy Administratora (*o ile dane osobowe przetwarzane są na podstawie tej przesłanki*),

e) informacje o odbiorcach lub kategoriach odbiorów danych osobowych,

f) zamiar przekazania danych do państwa trzeciego lub organizacji międzynarodowej (*o ile dotyczy*),

g) okres, przez który dane osobowe będą przetwarzane,

h) zapewnienie o realizacji praw: żądanie dostępu do swoich danych, sprostowania danych, usunięcia lub ograniczenia przetwarzania, złożenia sprzeciwu, przenoszenia danych,

i) możliwość cofnięcia udzielonej zgody na przetwarzanie danych osobowych (*o ile dane osobowe były przetwarzane na podstawie przesłanki zgody i była to przesłanka wiodąca*),

j) prawo do wniesienia skargi do organu nadzorczego,

k) informacje, czy podanie danych wiążę się z wymogiem ustawowym, umownym, warunkiem zawarcia umowy wraz z informacją, czy osoba jest zobowiązana do podania swoich danych osobowych o konkretnej strukturze, a także poinformowanie o ewentualnych konsekwencjach niepodania danych,

l) informacje o profilowaniu (*o ile za pomocą tego sposobu Administrator przetwarza dane*).

5) W przypadku pozyskiwania danych osobowych w inny sposób, niż bezpośrednio od osoby, której dane dotyczą, Administrator udziela następujących informacji:

a) dane kontaktowe,

b) dane kontaktowe Inspektora Ochrony Danych,

c) cel przetwarzania danych oraz podstawę prawną,

d) kategorie danych osobowych,

e) informacje o odbiorcach lub kategoriach odbiorów danych osobowych,

f) zamiar przekazania danych do państwa trzeciego lub organizacji międzynarodowej (*o ile dotyczy*),

g) okres, przez który dane osobowe będą przetwarzane,

h) prawnie uzasadnione interesy Administratora (*o ile dane osobowe przetwarzane są na podstawie tej przesłanki*),

i) zapewnienie o realizacji praw: żądanie dostępu do swoich danych, sprostowania danych, usunięcia lub ograniczenia przetwarzania, złożenia sprzeciwu, przenoszenia danych,

j) możliwość cofnięcia udzielonej zgody na przetwarzanie danych osobowych (*o ile dane osobowe były przetwarzane na podstawie przesłanki zgody i była to przesłanka wiodąca*),

k) prawo do wniesienia skargi do organu nadzorczego,

l) źródło pochodzenia danych osobowych (*czy pochodzą one ze źródeł publicznie dostępnych*),

m) informacje o profilowaniu (*o ile za pomocą tego sposobu Administrator przetwarza dane*).

6) Informacje, o których mowa w § 8 ust. 3 pkt 5 niniejszej PBI Administrator podaje w terminie :

a) miesiąca po pozyskaniu danych osobowych,

b) jeśli dane mają być wykorzystane do komunikacji z osobą, której dane dotyczą, to najpóźniej przy pierwszej takiej komunikacji,

c) jeżeli dane będą ujawniane innemu odbiorcy, to najpóźniej przy pierwszym ich ujawnieniu.

7) Zakres wskazany w § 8 ust. 3 pkt 5 – 6 niniejszej PBI nie ma zastosowania jeśli:

a) osoba, które dane dotyczą jest już w posiadaniu informacji, o których mowa w § 8 ust. 3 pkt 5 – 6 niniejszej PBI,

b) udzielenie takich informacji jest niemożliwe lub wymaga niewspółmiernie dużego wysiłku (*np. cel archiwalny w interesie publicznym, badania naukowe lub historyczne, statystyka*). W takim przypadku Administrator udostępnia informacje publicznie (nie w kontekście konkretnej osoby fizycznej, której dane dotyczą, ale w ogóle informuje o zakresie treści obowiązku informacyjnego),

c) pozyskiwanie danych jest wyraźnie uregulowane prawem Unii lub prawem państwa członkowskiego, któremu podlega Administrator,

d) dane osobowe muszą pozostać poufne (*tajemnica zawodowa, ustawowy obowiązek zachowania tajemnicy*).

8) Każdej osobie fizycznej, której dane dotyczą przysługuje prawo do uzyskania od Administratora informacji co do swoich danych osobowych, a mianowicie:

a) cel przetwarzania,

b) kategorie danych osobowych,

c) informacje o odbiorcach lub kategoriach odbiorców danych osobowych,

d) okres, przez który dane osobowe będą przetwarzane,

e) zapewnienie o realizacji praw: sprostowania danych, usunięcia lub ograniczenia przetwarzania, złożenia sprzeciwu,

f) prawo do wniesienia skargi do organy nadzorczego,

g) źródło pozyskania danych (*chyba, że pochodzą od osoby, której dane dotyczą*),

h) informacje o profilowaniu (*o ile za pomocą tego sposobu Administrator przetwarza dane*),

i) jeśli dane są przekazywane do organizacji międzynarodowej lub państwa trzeciego, należy poinformować osobę o zabezpieczeniach względem tych danych,

j) kopii danych osobowych podlegających przetwarzaniu.

9) Osoba, której dane dotyczą ma prawo żądania sprostowania jej danych osobowych.

Podstawa prawna:
Zgodnie z art. 12 - 16 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r.

4. **Procedura przechowywania dokumentów aplikacyjnych**

1) W zakresie przetwarzania danych osobowych złożonych przez osoby aplikujące do pracy w organizacji, Administrator kieruje się w szczególności zasadą ograniczonego celu, ograniczonego przechowywania oraz poufności.

2) Administrator przechowuje dane osobowe osób składających dokumentację aplikacyjną w trybie ogłoszonego do informacji publicznej konkursu przez okres wskazany w jednolitym rzeczowym wykazie akt, stanowiącym załącznik do obowiązujących organizację normatywów kancelaryjnych.

3) Administrator zapewnia, żeby dane osobowe osób składających aplikacje były przetwarzane w sposób zapewniający ich bezpieczeństwo oraz stosowną poufność. Dostęp do tego zakresu danych osobowych mogą mieć tylko i wyłącznie pracownicy organizacji upoważnieni do przetwarzania takich danych z racji zajmowanego stanowiska pracy lub miejsca w strukturze organizacji.

4) Administrator zapewnia ochronę przed nieuprawnionym dostępem do tych danych osobowych, a jednocześnie do sprzętu, który służy do przetwarzania takich danych.

5) Administrator zapewnia przetwarzanie danych osobowych zawartych w aplikacjach tylko i wyłącznie w ściśle określonym celu, dla którego osoby składające przedmiotowe dokumenty, wyraziły zgodę (np. tylko i wyłącznie do postępowania konkursowego o konkretnej sygnaturze).

6) Przetwarzanie do innych celów niż cele, w których dane osobowe zostały pierwotnie zebrane, mimo wszystko i tak powinno odbywać się tylko i wyłącznie w przypadkach, gdy przetwarzanie w innym celu jest

zgodne z celem pierwotnym i owa zgodność nie budzi żadnych wątpliwości tzn. Administrator w dalszym ciągu przetwarza te dane osobowe bezwzględnie w oparciu o zasadę legalności przetwarzania danych. Aby to ustalić, Administrator uwzględnia: powiązania pomiędzy pierwotnym celem, a dalszym celem, kontekst, w ramach którego dane zostały zebrane, rodzaj danych osobowych, konsekwencje dalszego przetwarzania względem osób, których dane dotyczą oraz środki, które miałyby zapewnić poufność.

Podstawa prawna:
Zgodnie z motywem 39 i 50 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r.

5. **Procedura szkolenia pracowników**

1) Wszystkie osoby upoważnione do przetwarzania danych osobowych w organizacji są cyklicznie szkolone w zakresie bezpieczeństwa informacji.
2) Osoby przetwarzające dane osobowe w organizacji mają znaczący wkład w skuteczność Systemu Zarządzania Bezpieczeństwem Informacji.
3) Osoby przetwarzające dane osobowe w organizacji mają świadomość konsekwencji wynikających z niezgodności z wymaganiami Systemu Zarządzania Bezpieczeństwem Informacji.
4) Za politykę szkoleniową odpowiada Inspektor Ochrony Danych, a jeśli Administrator nie wyznaczył Inspektora Ochrony Danych, za szkolenia w tematyce bezpieczeństwa informacji odpowiada najwyższe kierownictwo.
5) Organizacja zastrzega sobie możliwość zlecenia przeprowadzenia szkolenia z zakresu bezpieczeństwa informacji osobie fizycznej lub podmiotowi spoza organizacji. Najwyższe kierownictwo wybiera osobę fizyczną lub podmiot spoza organizacji kierując się jednocześnie zasadą konieczności zbadania kompetencji zleceniobiorcy lub osoby oddelegowanej do wykonania zadania przez zleceniobiorcę.
6) Inspektor Ochrony Danych w ramach czynności audytowych oraz polityki informacyjnej, o której mowa w rozporządzeniu ogólnym, opracowuje agendę oraz zakres tematyczny szkoleń w zakresie bezpieczeństwa informacji. Inspektor Ochrony Danych, po uprzedniej konsultacji z najwyższym kierownictwem może zlecić przeprowadzenie szkolenia z zakresu bezpieczeństwa informacji osobie fizycznej lub podmiotowi spoza organizacji. Wtedy Inspektor Ochrony Danych wybiera osobę fizyczną lub podmiot spoza organizacji kierując się jednocześnie zasadą konieczności zbadania kompetencji zleceniobiorcy lub osoby oddelegowanej do wykonania zadania przez zleceniobiorcę.
7) Agenda oraz zakres tematyczny szkolenia stanowią udokumentowane informacje będące dowodem na ciągłe doskonalenie organizacji w zakresie bezpieczeństwa informacji.
8) Agenda oraz zakres tematyczny szkolenia jest przez Inspektora Ochrony Danych lub najwyższe kierownictwo skutecznie komunikowane pracownikom w organizacji poprzez udostępnienie tej informacji drogą tradycyjną (papierową) lub za pomocą środków teletransmisji (poczta elektroniczna, elektroniczny obieg dokumentacji) z rozsądnym wyprzedzeniem, tak, aby osoby przetwarzające dane osobowe w organizacji mogły przygotować problematyczne zagadnienia związane z przepływem danych osobowych, które będą bezwzględnie omawiane na każdym szkoleniu z zakresu bezpieczeństwa informacji.
9) Osoby przetwarzające dane osobowe w organizacji, w wyniku sprawnie działającej polityki szkoleniowej, mają świadomość pozycji Inspektora Ochrony Danych i jego umocowania w strukturze organizacyjnej.
10) Należy zaznaczyć, iż przeprowadzany audyt w zakresie bezpieczeństwa informacji przez Inspektora Ochrony Danych ma charakter edukacyjny, a zatem nieformalne spotkania Inspektora Ochrony Danych z personelem również stanowią element polityki szkoleniowej organizacji.

Podstawa prawna:
1.Zgodnie z art. 39 ust. 1 lit. b) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. 2.Zgodnie z wymogami normy PN-EN ISO/IEC 27001:2017 pkt 7.1 – 7.3

6. **Procedura zastosowania monitoringu w organizacji**

1) Administrator podejmuje wszelkie działania z poszanowaniem obowiązujących przepisów prawa zgodnie z zasadą legalizmu w kontekście przetwarzanych danych osobowych. Należy zaznaczyć, iż Administrator ma prawnie usprawiedliwiony cel, by stosować takiego rodzaju zabezpieczenie.
2) Zanim Administrator zastosował monitoring w organizacji, dokonał analizy czy wprowadzenie wideonadzoru nie może być zastąpione innym środkiem bezpieczeństwa, aczkolwiek ostatecznie, mając na

uwadze obowiązujące przepisy prawa, które chronią osoby, których dane osobowe są zbierane, podjął decyzję o zastosowaniu tego rodzaju zabezpieczenia.

3) Administrator cyklicznie przeprowadza przegląd stanu bezpieczeństwa w związku ze stosowaniem monitoringu między innymi w celu podjęcia decyzji co do dalszego stosowania tego zabezpieczenia.

4) Administrator ma świadomość, iż zapis z monitoringu utrwalony i przechowywany stanowi nie tylko zabezpieczenie, ale również zbiór danych osobowych, które powinny być przetwarzane mając na uwadze fakt, iż ochrona osób fizycznych w związku z przetwarzaniem danych osobowych jest jednym z praw podstawowych.

5) Administrator stosuje monitoring wizyjny w oparciu o zasadę adekwatności. Administrator, stosując tego rodzaju zabezpieczenie, ma na celu ochronę osób przebywających na terenie organizacji oraz ochronę mienia organizacji.

6) Administrator przechowuje zapis z monitoringu na czasookres optymalny stosując się jednocześnie do zasady ograniczenia czasowego przetwarzanych danych osobowych.

7) Administrator przetwarza dane osobowe pozyskane za pomocą wideonadzoru tylko i wyłącznie w celu, dla którego dane te zostały zebrane.

8) Przed dopuszczeniem pracownika do pracy, Administrator informuje pracownika o stosowanym monitoringu na terenie zakładu pracy.

9) Administrator nie stosuje monitoringu w celu nadzorowania efektywności czy wydajności wykonywanej pracy przez pracownika organizacji.

10) Monitoring obejmuje wewnętrzne pomieszczenia budynku organizacji, drzwi główne wejściowe oraz miejsce parkingowe.

11) Monitoring nie obejmuje pomieszczeń, które z racji swojego założenia, nie są przeznaczone do wykonywania pracy tj.: toalet, stołówek, szatni czy palarni.

12) Z racji tego, że monitoringiem mogą być objęte osoby spoza organizacji, Administrator jest w obowiązku poinformować te osoby o wideonadzorze. Administrator powinien w widocznym miejscu budynku organizacji umieścić piktogram kamery oraz informację, iż „obszar jest objęty monitoringiem". Dodatkowo Administrator umieszcza tablicę z zawartością obowiązku informacyjnego, o którym mowa w § 8 ust. 3 pkt 5 niniejszej PBI. Tablice, o których mowa powyżej, są proporcjonalne do miejsca, gdzie zostały umieszczone. Administrator ma świadomość, iż każdej osobie przysługuje oprócz prawa do informacji, również prawo do ochrony swojego wizerunku (chyba, że przepisy szczególne stanowią inaczej).

13) Administrator ma świadomość, iż instalowanie atrap, które wprowadzają w mylne poczucie bezpieczeństwa, powinno być zakazane, dlatego też kategorycznie ich nie stosuje.

Podstawa prawna:
Zgodnie z wytycznymi Urzędu Ochrony Danych Osobowych dotyczącymi wykorzystania monitoringu

§ 9. Bezpieczeństwo fizyczne

1. Zasady zarządzania bezpieczeństwem fizycznym

1) Administrator określił obszary bezpieczne po to, by zapobiec nieuprawnionemu fizycznemu dostępowi, w związku z tym powstałym szkodom oraz zakłóceniom w procesie przekazywania informacji.

2) Administrator określił granice bezpieczeństwa i wykorzystał je w ramach zabezpieczenia obszarów wrażliwych lub krytycznych.

3) Administrator zaprojektował i stosuje fizyczne zabezpieczenia biur, pomieszczeń oraz innych obiektów, które do administratora należą w zakresie zapewnienia zabezpieczeń fizycznej ochrony danych.

4) Administrator oprócz tego, że zabezpieczył pomieszczenia przed nieuprawnionym dostępem, również zaprojektował i stosuje fizyczne zabezpieczenia ewentualnymi katastrofami naturalnymi, wrogim atakiem czy wypadkami, które, gdy wystąpią, mogą mieć znaczny wpływ na system zarządzania bezpieczeństwem informacji w obszarach.

5) Administrator korzysta z profesjonalnego doradztwa w zakresie tego, jak uniknąć zniszczeń z tytułu wystąpienia katastrof naturalnych lub spowodowanych czynnikiem ludzkim (pożar, zalanie, trzęsienie ziemi, wybuch).

6) By zapobiec nieuprawnionemu dostępowi, Administrator odizolował pomieszczenia, w których zachodzi proces przetwarzania danych osobowych od pomieszczeń, które służą powszechnemu dostępowi osób z zewnątrz organizacji.

7) Decyzja najwyższego kierownictwa w zakresie fizycznej ochrony informacji przetwarzanych w organizacji, oparta jest na wynikach analizy szacowania ryzyka w odniesieniu do aktywów, jakimi organizacja zarządza.

8) Najwyższe kierownictwo zobowiązuje osoby przetwarzające dane osobowe w organizacji do bezwzględnego stosowania aktywów w zakresie zabezpieczeń, jakimi organizacja dysponuje np. drzwi zamykane na klucz, szafy zamykane na klucz, niszczarka do dokumentacji.

9) Administrator stosuje wiele barier fizycznych, co znacznie podwyższa poziom ochrony.

10) Zakres obszarów przetwarzania danych określa **„Ewidencja obszarów przetwarzania"** – dokument nr: **„SZBI-PBI-Zał. 7"** stanowiący **załącznik nr 7** do **Polityki Bezpieczeństwa Informacji**.

Podstawa prawna:

1.Zgodnie z wymogami normy PN-EN ISO/IEC 27001:2017 zał. A.11
2.Zgodnie z wymogami normy PN-EN ISO/IEC 27002:2017 zał. A.11.1

§ 10. Bezpieczeństwo informacji w relacjach z innymi podmiotami

1. Procedura powierzenia danych osobowych.

1) Administrator może zlecić wykonanie zadania podmiotowi zewnętrznemu, aczkolwiek jeśli w ślad za prawidłowym wykonaniem zadania idzie konieczność przekazania danych osobowych, Administrator jest w obowiązku podpisać umowę powierzenia danych osobowych z podmiotem przetwarzającym z zastrzeżeniem § 10 ust. 1 pkt 2.

2) Administrator podpisuje odrębną od umowy macierzystej umowę powierzenia danych osobowych lub zastrzega sobie warunki formalne powierzenia danych osobowych w ramach wyodrębnionego rozdziału macierzystej umowy o współpracy.

3) Umowa powierzenia danych osobowych określa:

a) przedmiot i czas trwania przetwarzania,

b) charakter oraz cel przetwarzania,

c) rodzaj przetwarzanych danych osobowych,

d) kategorie osób, których powierzenie dotyczy,

e) prawa i obowiązki Administratora,

f) prawa i obowiązki podmiotu przetwarzającego.

4) Administrator korzysta tylko i wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, tak by maksymalnie chronić prawa osób, których dane dotyczą.

5) Zaplanowanie konieczności zapewnienia warunków formalnoprawnych wiążących Administratora oraz podmiot przetwarzający jest dowodem na ciągłe wdrażanie przez organizację planu w zakresie Systemu Zarządzania Bezpieczeństwem Informacji.

6) Warunki umowy powierzenia danych osobowych określa **„Umowa powierzenia danych"** – dokument nr: **„SZBI-PBI-Zał. 8"** stanowiący **załącznik nr 8** do **Polityki Bezpieczeństwa Informacji**.

7) Administrator prowadzi **„Ewidencję zawartych umów powierzenia danych"** – dokument nr: **„SZBI-PBI-Zał. 9"** stanowiący **załącznik nr 9** do **Polityki Bezpieczeństwa Informacji** zawierający datę zawarcia umowy wraz z sygnaturą umowy macierzystej, oznaczenie podmiotu przetwarzającego oraz imię i nazwisko osoby odpowiedzialnej po stronie podmiotu przetwarzającego.

Podstawa prawna:

1.Zgodnie z art. 28 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r.
2.Zgodnie z wymogami normy PN-EN ISO/IEC 27001:2017 pkt 6.1.1; 7.5; zał. A.18.1.1

2. **Klauzula poufności**

1) W przypadku, kiedy Administrator zleca podmiotowi zewnętrznemu wykonanie usługi, która pociąga za sobą konieczność, by najwyższe kierownictwo lub pracownicy podmiotu zewnętrznego mieli wgląd do pomieszczeń, w ramach których dochodzi do przetwarzania danych osobowych (np. w celach serwisowych urządzeń, sprzątających), Administrator podpisuje z podmiotem zewnętrznym tzw. klauzulę poufności, w której podmiot zewnętrzny obliguje się do przeszkolenia swojego personelu oraz zobowiązania go do zachowania bezwzględnej poufności co do danych osobowych przetwarzanych w organizacji, jakie osoby mogłyby zdobyć na etapie realizacji zadań w imieniu swoim (*najwyższe kierownictwo podmiotu zewnętrznego*) lub swojego pracodawcy (*pracownik podmiotu zewnętrznego*) na rzecz Administratora.

2) Klauzula poufności, o której mowa powyżej, nie ma zastosowania, w przypadku, gdy ze względu na charakter realizowanej usługi, uzasadnione będzie powierzenie danych osobowych w drodze stosownej udokumentowanej procedury.

3) Zapisy klauzuli poufności mogą stanowić element umowy macierzystej o współpracy lub zostać podpisane w formie odrębnego zobowiązania.

4) Warunki klauzuli poufności określa **„Klauzula poufności"** – dokument nr: **„SZBI-PBI-Zał. 10"** stanowiący **załącznik nr 10** do **Polityki Bezpieczeństwa Informacji**.

5) Administrator prowadzi ewidencję podmiotów zewnętrznych, których obowiązuje klauzula poufności zawierającą datę zawarcia postanowień o poufności wraz z sygnaturą macierzystej umowy, oznaczenie podmiotu zewnętrznego oraz imię i nazwisko osoby odpowiedzialnej po stronie podmiotu zewnętrznego, w ramach **„Ewidencji zawartych klauzul poufności"** – dokumentu nr: **„SZBI-PBI-Zał. 11"** stanowiący **załącznik nr 11** do **Polityki Bezpieczeństwa Informacji**.

Podstawa prawna:
Zgodnie z wymogami normy PN-EN ISO/IEC 27001:2017 zał. A.18.1.1, A.18.1.3

3. **Procedura szkolenia kontrahentów**

1) Administrator, jeśli uzna to za konieczne, szczególnie jeśli wnioski z wykonanej analizy szacowania ryzyka wskazują na taką konieczność, może przeszkolić kontrahenta z zakresu bezpieczeństwa informacji.

2) Administrator jest w obowiązku przedstawić kontrahentowi jego obowiązki oraz odpowiedzialność w zakresie bezpieczeństwa informacji, które będą podmiot zewnętrzny obligować w trakcie współpracy, a także bezpośrednio po jej zakończeniu.

3) Administrator, o ile podejmie decyzję o konieczności przeszkolenia swojego kontrahenta, powinien przedstawić podmiotowi zewnętrznemu odpowiednio wcześnie agendę wraz z zakresem tematycznym szkolenia.

4) Inspektor Ochrony Danych również może przedstawić najwyższemu kierownictwu Administratora zapotrzebowanie w kontekście przeszkolenia kontrahenta (oraz jego personelu) i sam takie szkolenie przeprowadzić.

Podstawa prawna:
1.Zgodnie z art. 39 ust. 1 lit. b) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. 2.Zgodnie z wymogami normy PN-EN ISO/IEC 27001:2017 zał. A.7.2.2; A7.3.1

§ 11. Procedura Zarządzania Incydentami

1. **Cel i zakres stosowania Procedury Zarządzania Incydentami**

1) Procedura Zarządzania Incydentami określa procedurę identyfikacji naruszenia lub uchybienia, które spowodowało bądź mogło spowodować ingerencję w prawa podstawowe osób fizycznych w związku z przetwarzaniem ich danych osobowych.

2) PZI jest stworzona w celu monitorowania procesów związanych z koniecznością zapewnienia bezpieczeństwa informacji.

3) Aby metoda monitorowania Systemu Zarządzania Bezpieczeństwem Informacji poprzez notyfikację incydentów była skuteczna, należy określić: kiedy należy monitorować, kto powinien to robić, kiedy należy analizować zidentyfikowane naruszenia lub uchybienia oraz kto powinien to analizować.

4) PZI prowadzi wyznaczony przez Administratora, Inspektor Ochrony Danych. Inspektor Ochrony Danych prowadzi PZI w ten sposób, iż:

a) Na bieżąco monitoruje, czy w organizacji doszło do uchybienia lub naruszenia i podejmuje w związku z tym określone stosownymi procedurami czynności,

b) Cyklicznie, jednak nie rzadziej niż raz na rok, Inspektor Ochrony Danych analizuje zidentyfikowane naruszenia bądź uchybienia, ocenia je pod względem istotności w zakresie bezpieczeństwa informacji, wyciąga wnioski, a także podejmuje działania naprawcze względem zidentyfikowanych incydentów,

c) przeprowadza audyt doraźny, jeśli uzna to za stosowne,

d) podejmuje decyzje w zakresie kwalifikacji incydentu jako zdarzenia, którego wystąpienie skutkuje koniecznością zgłoszenia tego faktu do organu nadzorczego lub jako zdarzenia, którego wystąpienie nie spowoduje konieczności zgłoszenia do organu nadzorczego,

e) podejmuje decyzje w zakresie kwalifikacji incydentu jako zdarzenia, którego wystąpienie skutkuje koniecznością zawiadomienia osób, których dane dotyczą o fakcie ich naruszenia lub jako zdarzenia, które takich skutków nie wywoła,

f) każdej kwalifikacji incydentu, o której mowa w § 11 ust. 1 pkt 4 lit. d, e niniejszej PBI Inspektor Ochrony Danych zawiadamia Administratora, a także Informuje Administratora na bieżąco w zakresie prowadzonej przez siebie PZI.

5) Zakres PZI opiewa o procedurę:

a) reagowania na incydenty,

b) zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu,

c) zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych.

6) Każdy pracownik, bez względu na to, czy zostało mu wydane upoważnienie do przetwarzania danych osobowych, czy tylko i wyłącznie zgoda na przebywanie w obszarze przetwarzania, jest zobowiązany do zgłoszenia swojego podejrzenia Inspektorowi Ochrony Danych, w przypadku jego braku, najwyższemu kierownictwu.

7) Względem pracownika, który nie podejmuje czynności, o których mowa w § 11 ust. 1 pkt 6 niniejszej PBI i bagatelizuje zdarzenie, co do którego można mieć podejrzenie, iż wystąpił incydent naruszenia danych osobowych, może zostać zastosowane postępowanie dyscyplinarne w trybie art. 52 ustawy z dnia 26 czerwca 1974r. kodeks pracy (Dz.U.2016.1666 t.j.).

8) W celu udokumentowania notyfikacji incydentów, które mogą przybrać formę uchybienia bądź naruszenia, Administrator wespół z Inspektorem Ochrony Danych prowadzi **„Ewidencję incydentów"** – dokument nr: **„SZBI-PBI-Zał. 12"** stanowiący **załącznik nr 12** do **Polityki Bezpieczeństwa Informacji** zawierający opis hipotetycznych incydentów, procedurę postępowania w przypadku notyfikacji uchybienia bądź naruszenia oraz katalog działań naprawczym z zastrzeżeniem, iż przyjęte w załączniku katalogi mają charakter otwarty.

9) W przypadku zidentyfikowania w organizacji incydentu w formie uchybienia bądź naruszenia, Inspektor Ochrony Danych sporządza **„Protokół uchybienia/naruszenia"** – dokument nr: **„SZBI-PBI-Zał. 13"** stanowiący **załącznik nr 13** do **Polityki Bezpieczeństwa Informacji.**

Podstawa prawna:
Zgodnie z wymogami normy PN-EN ISO/IEC 27001:2017 pkt 9.1

2. **Procedura zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu**

1) Jeśli w organizacji zostanie zidentyfikowane zdarzenie, które spowoduje naruszenie ochrony danych osobowych, Administrator jest w obowiązku zgłosić ten fakt organowi nadzorczemu w terminie 72 godzin, chyba, że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

2) Termin, o którym mowa w § 11 ust. 2 pkt 1 niniejszej PBI może ulec przedłużeniu, aczkolwiek Administrator ów fakt stosownie przed organem nadzorczym motywuje podając przyczyny opóźnienia.

3) Zgłoszenie, o którym mowa w § 11 ust. 2 pkt 1 niniejszej PBI zawiera:

a) opis charakteru naruszenia,

b) kategorie osób, których dane dotyczą,

c) przybliżoną liczbę osób, których dane dotyczą,

d) oznaczenie Administratora uwzględniając dane kontaktowe,

e) opis konsekwencji, jakie naruszenie mogło spowodować,

f) działania zaradcze, jakie Administrator podejmie w związku z incydentem.

4) Administrator oraz Inspektor Ochrony Danych jest w obowiązku dokumentować cały przebieg podejmowanych czynności począwszy od notyfikacji naruszenia po zgłoszenie tego faktu do organu nadzorczego.

5) W celu zgłoszenia naruszenia w trybie 72 godzin, Administrator korzysta ze wzoru udostępnionego przez Urząd Ochrony danych Osobowych tj.: **„Zgłoszenie naruszenia ochrony danych osobowych"** – dokumentu nr: **„SZBI-PBI-Zał. 14"** stanowiący **załącznik nr 14** do **Polityki Bezpieczeństwa Informacji.**

Podstawa prawna:
Zgodnie z art. 33 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r.

3. **Zawiadomienie osoby, której dane dotyczą o naruszeniu ochrony danych osobowych**

1) Jeżeli w organizacji dojdzie do naruszenia ochrony danych osobowych i zdarzenie to może spowodować wysokie ryzyko naruszenia praw lub wolności osób, których dane dotyczą, Administrator powiadamia o tym fakcie te osoby.

2) Administrator informuje osoby fizyczne, których naruszenie dotyczy mając jednocześnie na uwadze zasadę przejrzystości – komunikat powinien być jasny, prosty, zrozumiały dla jego odbiorców.

3) Komunikat, o którym mowa w § 11 ust. 3 pkt 1 niniejszej PBI zawiera:

a) oznaczenie Administratora uwzględniając dane kontaktowe,

b) opis konsekwencji, jakie naruszenie mogło spowodować,

c) działania zaradcze, jakie Administrator podejmie w związku z incydentem.

4) W celu zawiadomienia osób fizycznych, których naruszenie dotyczy, Administrator korzysta ze wzoru **„Zgłoszenie naruszenia osobie, której dane dotyczą"** – dokumentu nr: **„SZBI-PBI-Zał. 15"** stanowiący **załącznik nr 15** do **Polityki Bezpieczeństwa Informacji.**

5) Komunikat, o którym mowa w § 11 ust. 3 pkt 1 niniejszej PBI nie będzie konieczny jeśli:

a) Administrator wdrożył i zastosował takie środki techniczne i organizacyjne względem danych osobowych, których dotyczy naruszenie, że dostęp osób nieuprawnionych jest niemożliwy np.: szyfrowanie,

b) Administrator zastosował również środki eliminujące prawdopodobieństwo wystąpienia wysokiego ryzyka naruszenia praw lub wolności osób, których dane dotyczą,

c) Wymaga niewspółmiernie dużego wysiłku po stronie Administratora – wtedy Administrator wydaje komunikat publiczny lub stosuje inny równie skuteczny środek, za pomocą którego osoby zostaną w sposób skuteczny poinformowane o fakcie zaistnienia incydentu.

Podstawa prawna:
Zgodnie z art. 34 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r.

Wójt Gminy Masłowice

Bogusław Gontkowski

Wójt Gminy
Bogusław Gontkowski

Załącznik Nr 2 do Zarządzenia Nr 46/2018
Wójta Gminy Masłowice
z dnia 31 lipca 2018 r.

Polityka Bezpieczeństwa Teleinformatycznego *w organizacji o nazwie:* GMINA MASŁOWICE

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: **GMINA MASŁOWICE** 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: **GMINA MASŁOWICE;**

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.

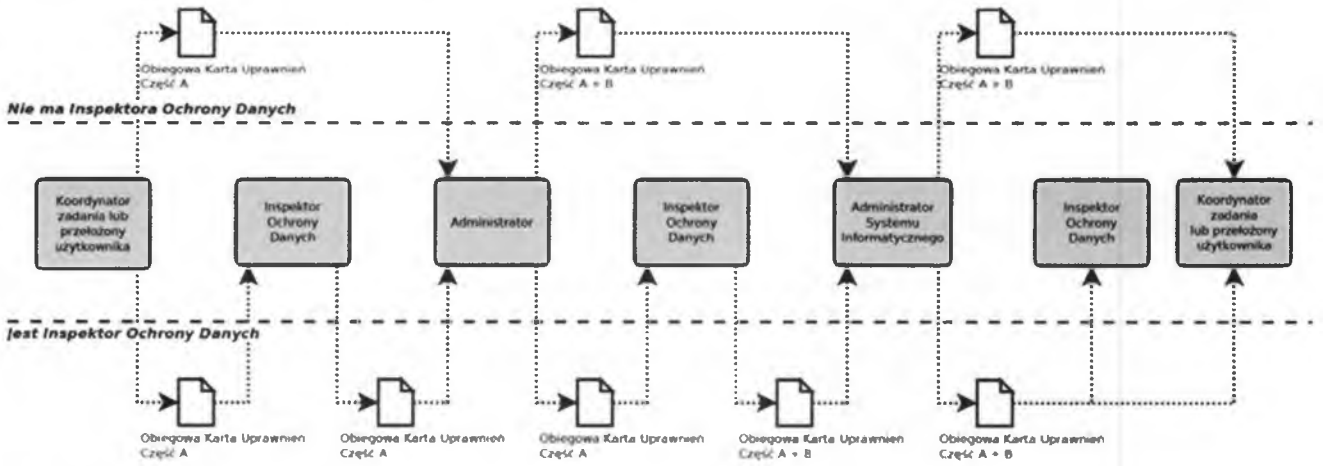
5) O okresie upoważnienia decyduje Administrator.

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 „ÿ + 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 „ŷ + 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.

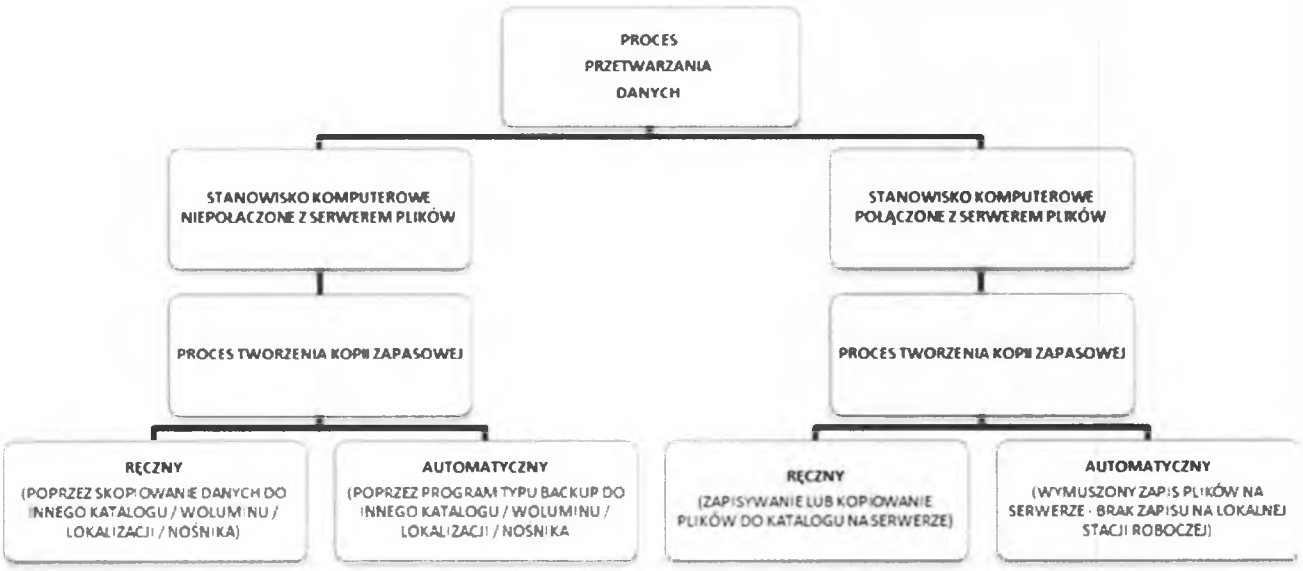
2) Wyniki kontroli i inwentaryzacji sprzętu zawierają się w „**Ewidencji urządzeń elektronicznych przetwarzających dane osobowe**" – dokument nr: „**SZBI-PBT-Zał. 3**" stanowiącej **załącznik nr 3** do niniejszej **Polityki Bezpieczeństwa Teleinformatycznego**.

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

Wójt Gminy Masłowice

Bogusław Gontkowski

Wójt Gminy
Bogusław Gontkowski