Załącznik nr 1 do Systemu Zarządzania
Bezpieczeństwem Informacji w organizacji
o nazwie: **Urząd Miejski w Kuźni Raciborskiej**

Polityka

Bezpieczeństwa

Informacji

w organizacji o nazwie:

Urząd Miejski w Kuźni Raciborskiej

Wprowadzenie

1. Mając świadomość wymogów formalnoprawnych oraz technicznych w procesie przetwarzania danych, w tym danych osobowych, najwyższe kierownictwo zdecydowało o konieczności wprowadzenia do podmiotu procedur, które składają się na System Zarządzania Bezpieczeństwem Informacji.

2. 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 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) Ustawę z dnia 10 maja 2018 o ochronie danych osobowych;

3) Wytyczne Grupy Roboczej art. 29 / EROD;

4) Dyrektywę parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (Dyrektywa NIS 2);

5) Ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;

6) 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;

7) Ustawę z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne;

8) Narodowe Standardy Cyberbezpieczeństwa (NSC);

9) Normy:

a) PN-EN ISO/IEC 27001:2023 (Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji - Wymagania);

b) PN-EN ISO/IEC 27002:2023 (Technika Informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zabezpieczania informacji);

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

3. Bezpieczeństwo informacji podmiot rozumie jako zestaw narzędzi i procedur oraz zabezpieczeń, które szeroko chronią poufne informacje podmiotu przed nieautoryzowanym dostępem, zakłóceniami, incydentami oraz naruszeniami. Bezpieczeństwo informacji obejmuje aspekt fizyczny i środowiskowy, kontrolę dostępu oraz cyberbezpieczeństwo.

4. Celem wprowadzenia Systemu Zarządzania Bezpieczeństwem Informacji jest zharmonizowanie systemu ochrony danych osobowych w taki sposób, by zapewnić realizacje podstawowych praw i wolności osób fizycznych, których dane osobowe podmiot przetwarza w związku z realizacją swoich zadań. Celem jest także ciągłe edukowanie osób zaangażowanych w proces przetwarzania danych osobowych. System Zarządzania Bezpieczeństwem 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.

5. Najwyższe kierownictwo zobowiązuje się do spełnienia obowiązujących wymagań związanych z bezpieczeństwem informacji, a także do ciągłego doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji.

6. 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 podmiocie. Najwyższe kierownictwo dba o to, by odpowiedzialność za bezpieczeństwo informacji była z góry przypisana konkretnym właścicielom poszczególnych ryzyk, a role w procesie przetwarzania danych osobowych były zdefiniowane.

7. Najwyższe kierownictwo zatwierdza wszelkie zmiany w Systemie Zarządzania Bezpieczeństwem Informacji.

8. Zarządzanie bezpieczeństwem informacji opiera się na następujących procesach:

1) Zarządzania ryzykiem - strategicznym elementem zarządzania aktywami i bezpieczeństwem informacji jest przeprowadzanie okresowej analizy ryzyka oraz opracowania planów postępowania z ryzykiem. Analiza jej wyników stanowi podstawę podejmowania wszelkich działań w zakresie utrzymania i doskonalenia ochrony zasobów podmiotu. Szacowanie ryzyka bazuje na wytycznych normy PN-ISO/IEC 27005 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji).

2) Monitorowania i przeglądów Systemu Zarządzania Bezpieczeństwem Informacji – przeprowadzanie audytów z zakresu bezpieczeństwa informacji oraz cyklicznych przeglądów formalnych w zakresie dokumentacyjnym względem zmieniającego się otoczenia prawnego, faktycznego oraz organizacyjnego.

3) Utrzymania i doskonalenia Systemu Zarządzania Bezpieczeństwem Informacji - przeprowadzanie działań korygujących oraz ocena ich skuteczności; przeprowadzanie działań zapobiegawczych oraz ocena ich skuteczności; informowanie zainteresowanych stron o działaniach i udoskonaleniach.

4) Nadzoru nad dokumentacją - prowadzenie i nadzorowanie dokumentacji systemowej; prowadzenie i nadzorowanie zapisów systemowych.

5) Zarządzania dostępem do zasobów - zarządzanie dostępem do zasobów odbywa się w ramach procesu opartego na systemie obiegu karty uprawnień.

6) Zarządzania naruszeniem - prowadzone jest w ramach Procedury Zarządzania Naruszeniami.

9. W podmiocie stosuje się kodeks dobrych praktyk w zakresie przetwarzania danych, w tym danych osobowych, a są to zasady kierujące wszystkimi przedsięwzięciami w aspekcie bezpieczeństwa informacji. Wszelkiego rodzaju odstępstwa od ustalonych w podmiocie zasad bezpieczeństwa informacji mogą mieć swoje źródło jedynie w przepisach prawa, którymi podmiot jest związany (w myśl zasady „Lex specialis derogat legi generali).

Podstawa prawna:

- Zgodnie z art. 24 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r.
- Zgodnie z § 20 ust. 1 Rozporządzenia 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.

W oparciu o:

- W oparciu o normę PN-EN ISO/IEC 27001:2023 zał. A.1 pkt 5.1

§ 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 czynności branżowo-administracyjnych / zadań publicznych. 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.

W oparciu o:

- W oparciu o normę PN-EN ISO/IEC 27001:2023 zał. A.1 pkt 5.1

§ 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 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) Ustawę z dnia 10 maja 2018 o ochronie danych osobowych;

   3) Wytyczne Grupy Roboczej art. 29 / EROD;

   4) Dyrektywę parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (Dyrektywa NIS 2);

5) Ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;

6) 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;

7) Ustawę z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne;

8) Narodowe Standardy Cyberbezpieczeństwa (NSC);

9) Normy:

d) PN-EN ISO/IEC 27001:2023 (Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji - Wymagania);

e) PN-EN ISO/IEC 27002:2023 (Technika Informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zabezpieczania informacji);

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

§ 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: **Urząd Miejski w Kuźni Raciborskiej;**
2. **Administratorze** – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych tj. **Burmistrz Miasta Kuźnia Raciborska;**
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. **Prawie 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. **Analizie Ryzyka Ogólnego i Ocenie Skutków dla Przetwarzania danych (DPIA)** – rozumie się przez to dokumentację zawierającą opis metodologii, częstotliwości oraz zakresu przeprowadzanego procesu szacowanie ryzyka;

21. **Naruszeniu** – rozumie się przez to naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

22. **Incydencie** – rozumie się przez to zdarzenie, które co prawda ostatecznie nie prowadzi do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych, niemniej jednak może oznaczać podatność organizacji na zagrożenie lub może wywołać skutki innego rodzaju niż ryzyko dla podmiotów danych.

§ 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.

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.

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,
- technologiczne,
- konkurencyjne.

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 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. 1a"** stanowiący **załącznik nr 1a** do **Polityki Bezpieczeństwa Informacji** oraz **„Rejestr kategorii czynności przetwarzania"** – dokument nr: **„SZBI-PBI-Zał. 1b"** stanowiący **załącznik nr 1b** 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 powyżej określone zostały w **„Rejestrze czynności przetwarzania"** – dokumencie nr: **„SZBI-PBI-Zał. 1a"** stanowiącym **załącznik nr 1a** do **Polityki Bezpieczeństwa Informacji**.

9) Organizacja wdrożyła również procedurę **„Rejestru kategorii czynności przetwarzania"** – dokument nr: **„SZBI-PBI-Zał. 1b"** stanowiący **załącznik nr 1b** do **Polityki Bezpieczeństwa Informacji** (na wypadek, gdyby w procesie przetwarzania danych osobowych organizacja występowała w roli Podmiotu przetwarzającego).

W oparciu o:

- W oparciu o normę PN-EN ISO/IEC 27001:2023 zał. A.1 pkt 5.9

Podstawa prawna:

- Zgodnie z art. 30 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 danych jest niezbędne do ochrony interesu, który ma istotne znaczenie dla życia osoby, której dane dotyczą, lub innej osoby fizycznej,

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

6) prawnie uzasadnione interesy realizowane przez Administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

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. 5 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. 1a"** stanowiący **załącznik nr 1a** 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:

- Zgodnie z art. 38 ust. 1 – 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r.

W oparciu o:

- W oparciu o normę PN-EN ISO/IEC 27001:2023 zał. A.1 pkt 5.2; 5.3; 5.4

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 i/lub potwierdza wyznaczenie 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:

- Zgodnie z art. 37 ust. 5 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r.

W oparciu o:

- W oparciu o normę PN-EN ISO/IEC 27001:2023 zał. A.1 pkt 5.2; 5.3; 5.4

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) organizowanie szkoleń dla pracowników organizacji zaangażowanych w proces przetwarzania danych osobowych;

f) przeprowadzanie sprawdzeń 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. Odpowiedzialność pracowników organizacji

1) Odpowiedzialność za bezpieczeństwo informacji w organizacji ponoszą wszyscy pracownicy zgodnie z posiadanymi zakresami obowiązków. Każdy pracownik obowiązany jest dbać o bezpieczeństwo powierzonych mu do przetwarzania, archiwizowania lub przechowywania informacji zgodnie z obowiązującymi w organizacji przepisami wewnętrznymi w tym m. in.:

a) Stosować zasady opisane w PBI oraz PBT, a także innych dokumentach wewnętrznych organizacji,

b) Chronić informacje podlegające ochronie przed dostępem do nich osób nieuprawnionych,

c) Chronić dane przed przypadkowym lub umyślnym zniszczeniem, utratą lub modyfikacją,

d) Chronić sprzęt, wydruki komputerowe i inne nośniki zawierające dane chronione,

e) Utrzymywać w tajemnicy powierzone hasła, częstotliwość ich zmiany oraz szczegóły technologiczne systemów także po ustaniu zatrudnienia w organizacji,

f) Stosować się do szczegółowych zaleceń w zakresie ochrony antywirusowej, a także do innych zaleceń wynikających z Systemu Zarządzania Bezpieczeństwem Informacji,

g) Powiadomić Administratora lub Inspektora Ochrony Danych lub bezpośredniego przełożonego o:

- ujawnieniu lub możliwości ujawnienia informacji chronionych osobom nieupoważnionym,
- nieautoryzowanej zmianie informacji chronionych lub możliwości wprowadzenia nieautoryzowanych zmian,
- zniszczeniu lub możliwości zniszczenia informacji chronionych,
- zablokowaniu lub możliwości zablokowania pracy systemu informatycznego przetwarzającego informacje chronione lub uniemożliwienia innego dostępu do informacji chronionych.

W oparciu o:

- W oparciu o normę PN-EN ISO/IEC 27001:2023 zał. A.1 pkt 5.2; 5.3; 5.4

4. 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) Zarządzanie bezpieczeństwem informacji opiera się na następujących procesach:

a) Zarządzania ryzykiem - strategicznym elementem zarządzania aktywami i bezpieczeństwem informacji w organizacji jest przeprowadzanie okresowej Analizy Ryzyka Ogólnego i Oceny Skutków dla Przetwarzania danych oraz opracowania planów postępowania z ryzykiem. Analiza jej wyników stanowi podstawę podejmowania wszelkich działań w zakresie utrzymania i doskonalenia ochrony zasobów organizacji. Analiza Ryzyka Ogólnego i Ocena Skutków dla Przetwarzania danych (DPIA) bazuje na wytycznych normy PN-ISO/IEC 27005:2014-01 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji – Wsparcie do Normy PN-EN ISO/IEC 27001:2017) oraz przyjętej przez organizację metodyce szacowania i analizy ryzyka dla bezpieczeństwa informacji opisanej w dokumencie Analizy Ryzyka Ogólnego i Oceny Skutków dla Przetwarzania danych (DPIA). Proces szacowania ryzyka jest wspierany poprzez wykorzystanie programu do szacowania ryzyka stanowiącego załącznik do dokumentu o nazwie: Analiza Ryzyka Ogólnego i Oceny Skutków dla Przetwarzania danych (DPIA).

b) Monitorowania i przeglądów SZBI – przeprowadzanie audytów z zakresu bezpieczeństwa informacji (nie rzadziej niż raz na rok) oraz cyklicznych przeglądów formalnych w zakresie dokumentacyjnym względem zmieniającego się otoczenia prawnego, faktycznego oraz organizacyjnego.

c) Utrzymania i doskonalenia SZBI - przeprowadzanie działań korygujących oraz ocena ich skuteczności; przeprowadzanie działań zapobiegawczych oraz ocena ich skuteczności; informowanie zainteresowanych stron o działaniach i udoskonaleniach.

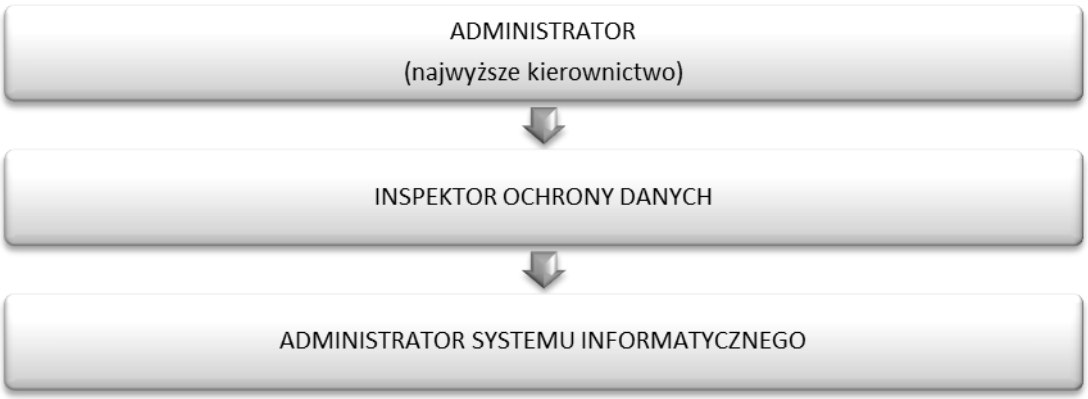
d) Nadzoru nad dokumentacją - prowadzenie i nadzorowanie dokumentacji systemowej; prowadzenie i nadzorowanie zapisów systemowych.

e) Zarządzania dostępem do zasobów - zarządzanie dostępem do zasobów odbywa się w ramach procesu opartego na systemie obiegu karty uprawnień.

f) Zarządzania incydentem - prowadzone jest w ramach Procedury Zarządzania Incydentami.

3) 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.

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



Podstawa prawna:

- Zgodnie z § 20 ust. 1 Rozporządzenia 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 poz. 2247)
- Zgodnie z § 20 ust. 2 pkt 1, 3, 14, Rozporządzenia 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 poz. 2247).

W oparciu o:

- W oparciu o normę PN-EN ISO/IEC 27001:2023 zał. A.1 pkt 5.2; 5.3; 5.4

5. Zarządzanie ciągłością działania

1) Organizacja dba o zapewnienie ciągłości funkcjonowania usług związanych z przetwarzaniem informacji. Dla poszczególnych obszarów i systemów krytycznych tworzone są plany postępowania w sytuacjach awaryjnych i kryzysowych. Celem takiego postępowania jest przeciwdziałanie przerwom w działalności organizacji oraz ochrona krytycznych procesów przed rozległymi awariami lub katastrofami.

2) Powyższe cele realizowane mogą być dzięki:

a) podziałowi odpowiedzialności związanemu z zarządzeniem ciągłością działania,

b) wdrożeniu planów ciągłości działania dla krytycznych systemów teleinformatycznych.

3) O konieczności tworzenia planu ciągłości działania dla konkretnego z systemu decyduje Administrator.

4) Za zapewnienie ciągłości działania, a zatem za tworzenie, przegląd, testowanie planów ciągłości działania odpowiada Administrator.

5) Procedura audytowania w zakresie bezpieczeństwa informacji (nie rzadziej niż na rok) stanowi potwierdzenie zarządzania ciągłością działania w organizacji.

6) W celu utrzymania ciągłości działania, Administrator w przypadkach uzasadnionych Analizą Ryzyka Ogólnego i Oceną Skutków dla przetwarzania danych ustanawia dodatkowe zabezpieczenia. Plan postępowania z ryzykiem wraz z wtórnym procesem szacowania ryzyka będący integralną częścią Analizy Ryzyka Ogólnego i Oceny Skutków, stanowi udokumentowaną procedurę, w ramach której Administrator wdraża dodatkowe zabezpieczenia (również w zakresie środowiska informatycznego).

7) Administrator zgodnie z planem postepowania w procesie szacowania ryzyka przekazuje w formie elektronicznej bądź pisemnej treść zaleceń do osób odpowiedzialnych za ich wdrożenie z jednoczesnym uwzględnieniem terminu realizacji.

Podstawa prawna:

- Zgodnie z art. 32 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r.
- Zgodnie z § 20 ust. 2 pkt 3, 14, Rozporządzenia 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 poz. 2247).
- Zgodnie z § 20 ust. 4 Rozporządzenia 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 poz. 2247).

W oparciu o:

- W oparciu o normę PN-EN ISO/IEC 27001:2023 zał. A.1 pkt 5.7

6. Współpraca z organami państwowymi

1) Podmiot współpracuje z organami państwowymi w zakresie wynikającym z przepisów prawa, szczególnie w zakresie obsługi incydentów oraz naruszeń. Utrzymywanie kontaktów z organami państwowymi jest także przydatne z uwagi na konieczność śledzenia zmian w odpowiednich przepisach ustawowych lub wykonawczych, które mogą mieć wpływ na podmiot. Kontakty obejmują między innymi takie organy jak:

a) Urząd Ochrony Danych Osobowych,

b) Właściwy do załatwienia danej sprawy CSIRT,

c) przedsiębiorstwa użyteczności publicznej,

d) służby ratownicze,

e) dostawcy energii elektrycznej oraz BHP np. straż pożarna (w związku z ciągłością działania), dostawcy usług telekomunikacyjnych (w związku z routingiem i dostępnością linii) oraz dostawcy wody (w związku z urządzeniami chłodniczymi dla urządzeń).

Podstawa prawna:

- W oparciu o normę PN-EN ISO/IEC 27001:2023 zał. A.1 pkt 5.5

7. Interakcje z zainteresowanymi stronami

1) Najwyższe kierownictwo współpracuje z podmiotami zewnętrznymi w zakresie bezpieczeństwa informacji oraz innymi grupami, które w sposób profesjonalny zajmują się bezpieczeństwem informacji. Podmiot należy także do grona organizacji, które cyklicznie w ramach funkcji newsletter otrzymują materiał dydaktyczny z Urzędu Ochrony Danych Osobowych. Ponad to, Administrator dba o to, by Inspektor Ochrony Danych oraz Administrator Systemów Informatycznych mieli dostęp do szkoleń i materiałów merytorycznych z zakresu bezpieczeństwa informacji i mogli poszerzać swoją bazę wiedzy, umiejętności i kompetencji.

2) Dla zapewnienia aktualności branżowych informacji z zakresu cyberbezpieczeństwa oraz otrzymywania wczesnych alertów (oraz ich zgłaszania) z obszaru bezpieczeństwa informacji organizacja wdrożyła następujące rozwiązania:

a) aktualizacja wiedzy na temat bieżących praktyk w dziedzinie bezpieczeństwa oraz śledzenie najnowszych informacji z tego obszaru poprzez śledzenie branżowych portali cyberinformacyjnych w tym CERT Polska;

b) utrzymanie dogłębnego zrozumienia aktualnego stanu środowiska bezpieczeństwa informacji;

c) odbieranie wstępnych alertów dotyczących zagrożeń, wskazówek i poprawek zabezpieczeń poprzez rejestrację osób kontaktowych w adekwatnym dla organizacji CSiRT tj. CSiRT NASK z zapewnieniem elektronicznego kanału komunikacji (e-mail) oraz w ramach systemu „S46-react" (Naukowa i Akademicka Sieć Komputerowa – Państwowego Instytutu Badawczego);

d) dostęp do zaawansowanych konsultacji specjalistycznych w zakresie bezpieczeństwa informacji w ramach CSiRT oraz S46-react;

e) wymiana wiedzy na temat innowacji technologicznych, nowych produktów, usług, potencjalnych zagrożeń oraz identyfikacja słabych punktów;

f) zapewnienie odpowiednich ścieżek kontaktowych w przypadku incydentów bezpieczeństwa informacji poprzez CSiRT oraz system S46-react.

Podstawa prawna:

- W oparciu o normę PN-EN ISO/IEC 27001:2023 zał. A.1 pkt 5.6

8. Bezpieczeństwo informacji w ramach projektów

1) Organizacja stosuje zasadę, iż zasady bezpieczeństwa w ramach projektów realizowanych w organizacji są tożsame z wewnętrznymi regulacjami niniejszej polityki. Niemniej jednak elementy bezpieczeństwa, na które wpływ ma przykładowo zewnętrzny realizator usługi zawierane są w ramach umowy głównej i regulują obszary takie jak:

a) komunikacja elektroniczna pomiędzy stronami projektu w postaci poczty elektronicznej winna być szyfrowana z zastosowaniem aktualnego certyfikatu SSL/TLS minimum w wersji 1.2;

b) dostęp do infrastruktury wewnętrznej za pomocą połączenia zdalnego może być realizowany tylko za pomocą bezpiecznego połączenia VPN (z wykluczeniem standardu PPTP) gdzie certyfikat służący autoryzacji użytkownika jest indywidualnie przypisany wobec jednej osoby oraz połączenie jest ograniczane czasowo.

c) dostęp do infrastruktury wewnętrznej za pomocą połączenia lokalnego może być realizowany tylko po uprzedniej autoryzacji działu IT bądź administratora danych.

d) sfinalizowanie projektu jest równoznaczne z odjęciem uprawnień dostępowych do wewnętrznej infrastruktury organizacji (dla strony zewnętrznej projektu).

e) zabezpieczenie poufności, dostępności i integralności danych przechowywanych przez zewnętrzną stronę projektu regulowane jest w ramach umowy.

Podstawa prawna:

- W oparciu o normę PN-EN ISO/IEC 27001:2023 zał. A.1 pkt 5.8

§ 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.

W oparciu o:

- W oparciu o normę PN-EN ISO/IEC 27001:2023 zał. A.1 pkt 5.15 – 5.18

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 Administratora 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”**.

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

7) O ile zachodzi konieczność upoważniania osoby do przetwarzania danych osobowych w systemie teleinformatycznym, przełożony osoby upoważnianej do przetwarzania danych osobowych lub koordynator zadania kieruje podpisany wniosek do Administratora 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 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. 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. Wycofanie upoważnienia do przetwarzania danych osobowych może nastąpić na wniosek przełożonego osoby upoważnionej do przetwarzania danych lub koordynatora zadania 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. Wniosek o wycofanie upoważnienia po rozpatrzeniu przez Administratora zostaje przekazany do przełożonego osoby upoważnianej do przetwarzania danych osobowych lub koordynatora zadania. Wycofanie uprawnień do przetwarzania danych osobowych w systemie teleinformatycznym odbywa się zgodnie z procedurą przewidzianą w PBT.

11) Inspektor Ochrony Danych w ramach podejmowanych czynności audytowych sprawuje nadzór nad drogą nadawania, modyfikowania oraz odbierania upoważnień oraz uprawnień.

12) 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**.

13) Pracownik naruszający zasady bezpieczeństwa informacji może zostać pociągnięty do odpowiedzialności w trybie art. 52 ustawy z dnia 26 czerwca 1974 r. kodeks pracy.

14) 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.

15) 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 (również w przypadku innej formy zatrudnienia np. umowy cywilnoprawnej). 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.

16) 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.

17) 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.

18) 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.

19) 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.

20) 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 (zgodnie z przyjętymi rozwiązaniami wewnętrznymi).

Podstawa prawna:

- Zgodnie z § 20 ust. 2 pkt 4, 5, 11 Rozporządzenia 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

W oparciu o:

- W oparciu o normę PN-EN ISO/IEC 27001:2023 zał. A.1 pkt 5.15 – 5.18

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

1) W przypadku osób, które są zatrudnione w organizacji, 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.

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**.

W oparciu o:

- W oparciu o normę PN-EN ISO/IEC 27001:2023 zał. A.1 pkt 5.15 – 5.18

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 na podstawie **„Wniosku podmiotu danych o realizację praw"** dokumentu nr **„SZBI-PBI-Zał. 16"** tj. **załącznik nr 16** do **Polityki Bezpieczeństwa Informacji** (zapytania o swoje dane osobowe) od osoby, której dane dotyczą, Administrator udziela informacji tej osobie w terminie miesiąca. 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.

3) 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*).

4) 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*).

5) Informacje, o których mowa powyżej 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.

6) Zakres wskazany powyżej nie ma zastosowania jeśli:

a) osoba, które dane dotyczą jest już w posiadaniu ww. informacji,

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*).

7) 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.

8) 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 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 Administrator.

5) 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.

6) Agenda oraz zakres tematyczny szkolenia stanowią udokumentowane informacje będące dowodem na ciągłe doskonalenie organizacji w zakresie bezpieczeństwa informacji.

7) Zakres merytoryczny szkolenia szczególnie opiewa o zagadnienia takie jak: zagrożenia bezpieczeństwa informacji, skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna, stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich.

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 spotkania Inspektora Ochrony Danych z personelem również stanowią element polityki szkoleniowej organizacji.

11) Każdy pracownik, który przeszedł szkolenie wstępne stanowiskowe lub cykliczne stanowiskowe w kontekście przetwarzania danych osobowych oraz bezpieczeństwa informacji podpisuje **„Oświadczenie o przeszkoleniu"** stanowiące dokument nr **„SZBI-PBI-Zał. 17"** tj. **załącznik nr 17** do **Polityki Bezpieczeństwa Informacji.** Zastrzega się jednocześnie, że ww. dokument nie stanowi wyłącznego dowodu na realizowany proces szkoleniowy w organizacji. Dowodem równorzędnym na przeszkolenie jest przykładowo lista obecności, certyfikat/zaświadczenie poświadczające uczestnictwo w szkoleniu.

Podstawa prawna:

- Zgodnie z art. 39 ust. 1 lit. b) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r.
- Zgodnie z § 20 ust. 2 pkt 6 Rozporządzenia 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 poz. 2247).

W oparciu o:

- W oparciu o normę PN-EN ISO/IEC 27001:2023 zał. A.1 pkt 6.2 – 6.4

§ 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 (np. punkt kancelaryjny, sekretariat, recepcja, rejestracja).

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:

- Zgodnie z § 20 ust. 2 pkt 7, 9, 11, Rozporządzenia 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 poz. 2247).

W oparciu o:

- W oparciu o normę PN-EN ISO/IEC 27001:2023 zał. A.1 pkt 7.1 – 7.8

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

   5) 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. Podmioty przetwarzające na wezwanie Administratora przedstawiają ankietę, w której deklarują stosowanie w swoich organizacjach odpowiednich środków technicznych i organizacyjnych, by zapewnić bezpieczeństwo przetwarzanych danych osobowych. Wzór ankiety, którą może stosować Administrator znajduje odzwierciedlenie w **„Deklaracji stosowania środków technicznych i organizacyjnych przez podmiot przetwarzający”** – dokumencie nr: **„SZBI-PBI-Zał. 8a”** stanowiący **załącznik nr 8a** do **Polityki Bezpieczeństwa Informacji.**

   6) Warunki umowy powierzenia danych osobowych określa **„Umowa powierzenia danych”** – dokument nr: **„SZBI-PBI-Zał. 8b”** stanowiący **załącznik nr 8b** 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:

- Zgodnie z art. 28 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r.
- Zgodnie z § 20 ust. 2 pkt 10 Rozporządzenia 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 poz. 2247).

W oparciu o:

- W oparciu o normę PN-EN ISO/IEC 27001:2023 zał. A.1 pkt 5.19 – 5.21

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 § 20 ust. 2 pkt 10 Rozporządzenia 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

W oparciu o:

- W oparciu o normę PN-EN ISO/IEC 27001:2023 zał. A.1 pkt 6.6

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:

- Zgodnie z art. 39 ust. 1 lit. b) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r.
- Zgodnie z § 20 ust. 2 pkt 10 Rozporządzenia 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 poz. 2247).

W oparciu o:

- W oparciu o normę PN-EN ISO/IEC 27001:2023 zał. A.1 pkt 6.2 – 6.4

§ 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.

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.

8) Administrator wdraża procedurę postępowania w przypadku notyfikacji uchybienia bądź naruszenia na danych osobowych poprzez wskazanie przykładowego katalogu incydentów w **„Wykazie przykładowych incydentów”** –

dokument nr: **„SZBI-PBI-Zał. 12”** stanowiący **załącznik nr 12** do **Polityki Bezpieczeństwa Informacji** zawierający opis przykładowych 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 incydentu/naruszenia”** – dokument nr: **„SZBI-PBI-Zał. 13”** stanowiący **załącznik nr 13** do **Polityki Bezpieczeństwa Informacji.**

Podstawa prawna:

- Zgodnie z § 20 ust. 2 pkt 13 Rozporządzenia 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

W oparciu o:

- W oparciu o normę PN-EN ISO/IEC 27001:2023 zał. A.1 pkt 5.24 – 5.31

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 opisuje co najmniej: charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazanie kategorii i przybliżonej liczby osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie; imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji; możliwe konsekwencje naruszenia ochrony danych osobowych; środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

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.

4. Zarządzanie incydentami w poziomu cyberbezpieczeństwa

1) Proces zarządzania incydentami w obszarze cyberbezpieczeństwa opracowano w ramach **„Procedury zarządzania incydentami związanymi z bezpieczeństwem informacji i cyberbezpieczeństwem”** – dokumencie nr: **„SZBI-PBI-Zał. 18”** stanowiący **załącznik nr 18** do **Polityki Bezpieczeństwa Informacji.**

§ 12

Procedura przeglądu polityk ochrony danych

1. Zasady stosowania

1) Przeglądu dokumentacji bezpieczeństwa dokonuje się zawsze po:

a) zmianie aktów prawnych, mających wpływ na stosowanie dokumentów,

b) wprowadzeniu nowych lub aktualizacji istniejących organizacyjnych systemów zabezpieczeń,

c) wprowadzeniu nowych lub aktualizacji istniejących technologicznych systemów zabezpieczeń,

d) po wystąpieniu incydentu, który wskazuje na konieczność modyfikacji dokumentów,

e) wystąpieniu takiej konieczności – np. na wniosek Inspektora Ochrony Danych.

2) Zaleca się przegląd dokumentacji bezpieczeństwa minimum raz w roku. Danymi do przeprowadzenia przeglądu są m.in. zarejestrowane podatności i incydenty oraz podjęte działania w kierunku ich naprawienia, wyniki audytów, okresowych raportów i doraźnych kontroli.

2. Odpowiedzialność

1) Za poprawne przestrzeganie niniejszej procedury odpowiedzialny jest Administrator.

3. Zasady przeprowadzania przeglądów

1) Przeglądy SZBI przeprowadza co do zasady Inspektor Ochrony Danych.

2) Administrator może wyznaczyć zespół odpowiedzialny za dokonanie przeglądów SZBI.

3) Zespół wykonuje przegląd określonych przez Inspektora Ochrony Danych dokumentów oraz w zależności od potrzeb przeprowadza audyt wśród osób przetwarzających danych osobowych.

4) Jeżeli przeglądu dokonuje podmiot zewnętrzny, koordynatorem prac jest Inspektor Ochrony Danych.

5) Zespół oddelegowany przez Inspektora Ochrony Danych może:

a) przeprowadzać rozmowy z kierownikami wydziałów oraz użytkownikami,

b) przeglądać dostępne zapisy i dokumenty,

c) dokonywać i utrwalać własne spostrzeżenia.

6) Po przeprowadzeniu przeglądu Inspektor Ochrony Danych wykonuje raport z przeprowadzonego przeglądu.

7) Inspektor Ochrony Danych opracowuje i przedstawia Administratorowi raport z wykonanego przeglądu.

W oparciu o:

- W oparciu o normę PN-EN ISO/IEC 27001:2023 zał. A.1 pkt 5.35 – 5.36

podpis i pieczęć Administratora