POLITYKA BEZPIECZEŃSTWA OCHRONY DANYCH OSOBOWYCH

Zespół Szkół Zawodowych im. gen. Stanisława Maczka
86-010 Koronowo ul. Dworcowa 53

SPIS TREŚCI

I. WSTĘP.

Niniejszy dokument jest zgodny z następującymi aktami prawnymi:

1. Rozporządzeniem 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 (dalej: RODO);
2. Ustawa z dnia 7 września 1991 r. o Systemie Oświaty;
3. Ustawa z dnia 26 stycznia 1982 r. - Karta Nauczyciela;

4. Rozporządzenie MINISTRA EDUKACJI NARODOWEJ z dnia 29 sierpnia 2014 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji;
5. Ustawą o ochronie danych osobowych

Administratorem Danych Osobowych jest
Zespół Szkół Zawodowych im. gen. Stanisława Maczka
reprezentowany przez Dyrektora

Wprowadzenie „Polityki Bezpieczeństwa" ochrony danych osobowych reguluje zasady przetwarzania danych osobowych w Jednostce. Wszystkie informacje gromadzone podczas wykonywania standardowych działań w tym dane osobowe, są niezbędne do funkcjonowania jednostki organizacyjnej i z tego powodu zaleca się ich odpowiednią ochronę. W coraz większym stopniu organizacje w toku przetwarzania danych są wspomagane systemami informatycznymi i sieci informatyczne stają w obliczu zagrożeń pochodzących z rozmaitych źródeł, takich jak oszustwa dokonywane za pomocą komputerów, komunikatorów, urządzeń mobilnych oraz sieci. Odpowiednie zabezpieczenia, ochrona przetwarzanych danych, niezawodność funkcjonowania oraz systematyczna i wielowątkowa edukacja użytkowników, stają się podstawowymi wymogami stawianymi systemom informatycznym, a informacja oraz wspierające ją procesy, systemy i sieci są ważnymi aktywami działalności jednostki organizacyjnej.

Realizacja ustawowych zadań związanych z **„Rozporządzeniem 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"** (**dalej: RODO)** a także krajowej ustawy o ochronie danych osobowych wymaga, między innymi, efektywnego dostępu do informacji zawierających dane osobowe oraz zapewnienia odpowiedniego poziomu bezpieczeństwa tych danych.

Utrata **poufności, integralności, dostępności, autentyczności lub niezawodności** może mieć negatywny wpływ na bieżącą działalność lub wizerunek jednostki. Bezpieczeństwo danych osobowych oznacza jej ochronę przed szerokim spektrum zagrożeń w celu zachowania poufności, integralności i dostępności informacji, a także minimalizacji ryzyka oraz zapewnienia ciągłości działania jednostki i realizacji jej zadań statutowych na odpowiednim poziomie.

Bezpieczeństwo informacji można osiągnąć w jednostce, wdrażając odpowiedni zestaw zabezpieczeń organizacyjnych poprzez opracowanie **Polityki Bezpieczeństwa** oraz zabezpieczenie oprogramowania i sprzętu.

Polityka Bezpieczeństwa jest zbiorem zasad i procedur, którym muszą podporządkować się wszystkie osoby posiadające dostęp do przetwarzania danych osobowych bez względu na status zatrudnienia w jednostce (umowa o pracę, umowa cywilno-prawna, stażyści, praktykanci). Dokument zwraca uwagę na konsekwencje, jakie mogą ponosić osoby, przekraczające określone granice oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń. Opracowany dokument deklaruje zaangażowanie kierownictwa jednostki i wyznacza procesowe podejście pracowników jednostki do zarządzania bezpieczeństwem danych osobowych.

Należy zaznaczyć, że niektóre zabezpieczenia opisane w niniejszym dokumencie są traktowane, jako zasady przewodnie w zarządzaniu bezpieczeństwem informacji, możliwe do zastosowania i zapewniające odpowiedni punkt wyjścia dla procesu wdrażania bezpieczeństwa informacji.

II. SŁOWNIK POJĘĆ I SKRÓTÓW.

1. **System teleinformatyczny** - zespół współpracujących ze sobą według określonych reguł urządzeń, oprogramowania, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
2. **System Zarządzania Bezpieczeństwem Informacji (SZBI)** - część całościowego systemu zarządzania, odnosząca się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa danych osobowych;
3. **Dostępność** - właściwość bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu (na podstawie PN-ISO/IEC 27001);
4. **Poufność** - właściwość polegająca na tym, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom (na podstawie PN-ISO/IEC 27001);
5. **Ryzyko** - prawdopodobieństwo, że określone zagrożenie w połączeniu z podatnością doprowadzi do utraty lub zniszczenia zasobów;
6. **Integralność** - właściwość polegająca na zapewnieniu dokładności i kompletności aktywów (na podstawie PN-ISO/IEC 27001);
7. **Rozliczalność** - właściwość pozwalająca przypisać określone działanie do określonego podmiotu (osoby fizycznej, procesu, systemu) oraz umiejscowić je w czasie;
8. **Autentyczność** - właściwość zapewniająca, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana (autentyczność dotyczy użytkowników, procesów, systemów i informacji);
9. **Niezawodność** - właściwość oznaczająca spójne, zamierzone zachowanie i skutki;
10. **Niezaprzeczalność** - właściwość oznaczająca niemożność wyparcia się swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów;
11. **Dane osobowe** - oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"). 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;
12. **Przetwarzanie** - oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką 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, które można podzielić na dwie grupy:
13. **Ograniczenie przetwarzania** - oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
14. **Profilowanie** - oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
15. **Pseudonimizacja** - oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są

objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

16. **Zbiór danych** - oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
17. **Administrator Danych (AD)** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;
18. **Inspektor Ochrony Danych (IOD)** – osoba powołana przez administratora na podstawie kwalifikacji i doświadczenia odpowiadająca za przestrzeganie procedur w zakresie danych osobowych i zgłoszona do Urzędu Ochrony Danych;
19. **Administrator Systemu Informatycznego (ASI) / Informatyk** - wyznaczony pracownik lub firma zewnętrzna realizująca obsługę IT jednostki, odpowiedzialny za realizację zadań związanych z zarządzaniem systemem informatycznym, w tym za zabezpieczenie sieci komputerowej tzn. wdrażanie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów infrastruktury informatycznej oraz ochrony danych przed nieuprawnioną modyfikacją, zniszczeniem, dostępem i ujawnieniem, a także ich utratą;
20. **Podmiot przetwarzający** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
21. **Zgoda osoby, której dane dotyczą** - oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;
22. **Naruszenie ochrony danych osobowych** - oznacza 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;
23. **Dane genetyczne** - oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej;
24. **Dane biometryczne** - oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;
25. **Dane dotyczące zdrowia** - oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia;
26. **Przedsiębiorca** - oznacza osobę fizyczną lub prawną prowadzącą działalność gospodarczą, niezależnie od formy prawnej, w tym spółki osobowe lub zrzeszenia prowadzące regularną działalność gospodarczą;
27. **Grupa przedsiębiorstw** - oznacza przedsiębiorstwo sprawujące kontrolę oraz przedsiębiorstwa przez nie kontrolowane.

III. CEL POLITYKI BEZPIECZEŃSTWA INFORMACJI.

1. Celem wprowadzenia niniejszej Polityki Bezpieczeństwa jest:
   1) Ochrona danych osobowych przetwarzanych i gromadzonych w jednostce (**bez względu na formę – forma tradycyjna „papierowa" czy forma zapisu informatycznego**) dotycząca:
      a. zabezpieczenia przed dostępem do danych osób nieupoważnionych, na każdym etapie ich przetwarzania tj. wprowadzania, aktualizacji lub usuwania, wyświetlania lub drukowania zestawień i raportów, przemieszczania danych w sieci lokalnej pomiędzy programami i osobami je przetwarzającymi;
      b. metod archiwizacji oraz ochrony danych zarchiwizowanych na nośnikach zewnętrznych i wydrukach;
      c. procedur niszczenia niepotrzebnych wydruków lub nośników z danymi;
      d. ustalenia i wdrożenia zabezpieczeń przed dostępem osób niepowołanych do pomieszczeń, w których są eksploatowane urządzenia gromadzące i przetwarzające dane;
      e. określenia polityki i sposobów dostępu do tych pomieszczeń przez pracowników, personel pomocniczy oraz serwis zewnętrzny.
   2) Zmniejszenie ryzyka utraty informacji;
   3) Określenia zakresu obowiązków pracowników – w części dotyczącej bezpieczeństwa danych;
   4) Podnoszenie świadomości pracowników i ich pełne zaangażowanie w ochronę przetwarzanych danych.
2. W związku z opracowaną Polityką Bezpieczeństwa zostały sformułowane poszczególne cele w zakresie bezpieczeństwa informacji, które są realizowane poprzez odpowiednie procedury, obejmujące w szczególności:
   a. zapewnienie kwalifikacji i świadomości pracowników w zakresie bezpieczeństwa informacji;
   b. zapewnienie ciągłości działania jednostki;
   c. zakomunikowanie pracownikom konsekwencji, w tym dyscyplinarnych, w przypadku naruszenia bezpieczeństwa informacji;
   d. raportowanie incydentów związanych z bezpieczeństwem informacji w tym do Urzędu Ochrony Danych.
3. W jednostce dokonano szacowania ryzyka zgodnie z przyjętą metodą i kryteriami akceptacji ryzyka, opisanymi w załączniku Polityki Bezpieczeństwa, a następnie zaimplementowano w stosunku do zidentyfikowanego ryzyka stosowne zabezpieczenia. Szacowanie ryzyka będzie stałym elementem działania.
4. Obowiązkiem wszystkich osób przetwarzających dane osobowe jest przestrzeganie szczegółowych zasad postępowania udokumentowanych w Polityce Bezpieczeństwa oraz wszystkich procedur funkcjonujących w jednostce, składających się na System Zarządzania Bezpieczeństwem Danych Osobowych.

IV. ZAKRES OBOWIĄZYWANIA POLITYKI BEZPIECZEŃSTWA INFORMACJI.

1. Dokument ten dotyczy wszystkich pracowników, a także innych osób mających dostęp do danych osobowych (np. pracowników firm zewnętrznych realizujących prace w jednostce).

2. Dokument ma zastosowanie do wszystkich informacji zawierających dane osobowe niezależnie od formy, w jakiej są przechowywane (papierowej, elektronicznej i innej) z wyjątkiem informacji niejawnych.
3. Dokument ten dotyczy również wszystkich systemów informatycznych zlokalizowanych w budynkach jednostki oraz systemów mobilnych będących własnością jednostki.
4. Niniejsza polityka jest dokumentem ogólnym w stosunku do dokumentów szczególnych, mających na celu ochronę danych osobowych, do których stosuje się procedury im przypisane.

V. ORGANIZACJA BEZPIECZEŃSTWA INFORMACJI.

1. Za organizację systemu ochrony danych osobowych odpowiada Administrator Danych, który wdrożył na podstawie analizy ryzyka naruszenia przepisów o ochronie danych osobowych i naruszenia praw i wolności osób fizycznych, których dane przetwarza odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z prawem.
2. Administrator Danych (oraz podmiot przetwarzający) **wyznacza Inspektora Ochrony Danych** (IOD), zawsze, gdy:
   a. przetwarzania dokonują organ lub podmiot publiczny;
   b. główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę;
   c. główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę danych wrażliwych (szczególnych kategorii), oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa.
3. Inspektor Ochrony Danych jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań. Inspektor Ochrony Danych:
   a. może być członkiem personelu administratora (nie może nadzorować obszaru przetwarzania danych osobowych).
   b. może wykonywać zadania na podstawie umowy o świadczenie usług.
4. Administrator (podmiot przetwarzający) publikują dane kontaktowe IOD i zawiadamiają o nich organ nadzorczy – Prezesa Urzędu Ochrony Danych osobowych.

VI. ZAKRES OBOWIĄZKÓW OSÓB ODPOWIEDZIALNYCH ZA BEZPIECZEŃSTWO DANYCH OSOBOWYCH.

<u>Administrator Danych (AD).</u>

Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane w szczególności:

   a. opracowuje i wdraża Politykę Bezpieczeństwa ochrony danych osobowych;
   b. wyznacza Inspektora Ochrony Danych osobowych;

c. zatwierdza raport z analizy ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania;
d. wdraża odpowiednie środki techniczne i organizacyjne, takie jak:
   - organizacja systemu ochrony danych osobowych
   - pseudonimizacja, zaprojektowana w celu skutecznej realizacji zasad ochrony danych oraz minimalizacja danych tak by spełnić wymogi prawa w zakresie ochrony danych osobowych oraz chronić prawa osób, których dane dotyczą;
   - prowadzenie rejestru czynności przetwarzania danych osobowych.

Inspektor Ochrony Danych (IOD).

Inspektor Ochrony Danych podlega bezpośrednio Administratorowi Danych. IOD ma następujące zadania:

1. informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich zgodnie z prawem oraz zatwierdzoną polityką bezpieczeństwa danych osobowych i doradzanie im w tej sprawie;
2. monitorowanie przestrzegania przepisów prawa oraz polityki w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
3. udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania;
4. współpraca z organem nadzorczym;
5. pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem.

Ponadto

1. nadzoruje za pośrednictwem Administratora Systemu Informatycznego przestrzeganie zasad ochrony danych osobowych w systemie teleinformatycznym, w tym właściwego i bezpiecznego obiegu dokumentów oraz elektronicznych nośników informacji zawierających dane osobowe;
2. wydaje w imieniu i z upoważnienia Administratora Danych upoważnienia do przetwarzania danych osobowych na wniosek przełożonego osoby, która będzie przetwarzała dane osobowe;
3. prowadzi „Ewidencję Wydanych Upoważnień" dostępu do danych osobowych;
4. monitoruje oraz aktualizuje Rejestr czynności przetwarzania danych osobowych – Załącznik nr 4;
5. nadzoruje za pośrednictwem osób funkcyjnych zapewnienie bezpieczeństwa fizycznego obszaru przetwarzania danych osobowych;
6. nadzoruje za pośrednictwem ASI zapewnienie dostępu do systemu TI przetwarzającego dane osobowe wyłącznie upoważnionym osobom, posiadającym odpowiednie upoważnienie dostępu do danych osobowych nadane uprawnienia do pracy w systemie TI;
7. uczestniczy w opracowywaniu projektów dokumentów normatywnych regulujących w jednostce organizacyjnej problematykę ochrony danych osobowych.

Administrator Systemu Informatycznego (ASI).

ASI – jest to osoba lub firma wyznaczona przez Administratora Danych Osobowych do pełnienia obowiązków Administratora Systemu Informatycznego. Podlega Administratorowi Danych i współpracuje w zakresie przestrzegania procedur w zakresie przetwarzania danych osobowych w systemach teleinformatycznych. Realizuje zadania w zakresie zapewnienia funkcjonowania oraz przestrzegania zasad bezpieczeństwa systemu TI przetwarzającego dane osobowe, a w szczególności odpowiada za:

1. obsługę techniczną systemu przetwarzającego dane osobowe;
2. opracowanie specyfikacji zakupu, wdrożenie oprogramowania, nadzór nad jego eksploatacją, tak aby zapewnić skuteczną ochronę tych danych w obszarach: poufności, integralności i rozliczalności;
3. konfigurację systemu operacyjnego zainstalowanego na komputerach zgodnie z zaleceniami niniejszej PB;
4. aktualizację oprogramowania antywirusowego;
5. nadawanie uprawnień do dostępu do zbiorów danych przetwarzanych w systemie na podstawie wniosku o nadanie dostępu;
6. nadzór pracy uprawnionych użytkowników przetwarzających dane osobowe w systemie TI;
7. uczestniczy w opracowywaniu projektów wymagań bezpieczeństwa dla systemów przetwarzających dane osobowe oraz nadzoruje przestrzeganie wymagań przez uprawnionych użytkowników;
8. informowanie IOD o stwierdzonych naruszeniach bezpieczeństwa systemu teleinformatycznego oraz wykrytych wirusach;
9. proponowanie zmian mających na celu poprawę bezpieczeństwa systemu teleinformatycznego;

Ponadto:

10. utrzymuje i aktualizuje listę autoryzowanych użytkowników systemu do przetwarzania danych osobowych i nadanymi indywidualnymi identyfikatorami dostępu do systemu
11. upewnia się, czy cały personel posiadający dostęp do systemu TI posiada stosowne upoważnienia dostępu do przetwarzania danych osobowych;
12. prowadzi osobiście profilaktykę antywirusową systemu TI;
13. dokonuje wraz z IOD analizy zgłoszonych przypadków incydentów infekcji wirusowych lub innych, wskazujących na nieautoryzowane próby ingerencji w systemie bezpieczeństwa oraz w zależności od stopnia zagrożenia funkcjonowania systemu bezpieczeństwa, podejmuje odpowiednie kroki zaradcze zapewnienie strategii, uregulowań i procedur bezpieczeństwa;
14. prowadzi szkolenie dla użytkowników z zakresu bezpieczeństwa teleinformatycznego i przestrzegania wymagań bezpieczeństwa;
15. wykonuje archiwizację danych systemu, zgodnie z obowiązującymi procedurami;
16. uczestniczy w analizie ryzyka i informuje inspektora ochrony danych o wszelkich lukach naruszeniach i zagrożeniach;
17. analizuje rejestr zdarzeń (logi systemowe).

Użytkownik systemu przetwarzania danych osobowych - każdy pracownik, który wykonując czynności służbowe, przetwarza dane osobowe, tzn. wykonuje na nich operacje takie jak:

zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, usuwanie niezależnie czy odbywa się to w zbiorach tradycyjnych czy systemie TI.

Użytkownicy systemu są odpowiedzialni za zapewnienie bezpieczeństwa systemu ochrony danych osobowych, w tym przetwarzanych w systemie TI, a w szczególności są zobowiązani do:

1. Zapoznania się z „Polityką Bezpieczeństwa" i przestrzeganie jej procedur;
2. Utrzymania poufności swoich haseł dostępu do systemu teleinformatycznego oraz przestrzegania ustalonych reguł złożoności przy zmianie hasła;
3. Zgłaszania IOD lub ASI faktów potencjalnych incydentów w obszarze ochrony danych osobowych;
4. Przeprowadzania kontroli antywirusowej wykorzystywanych elektronicznych nośników informacji;
5. Sporządzanie kopii zapasowych zbiorów danych, za których administrowanie są odpowiedzialni.

VII. UTRZYMANIE ODPOWIEDNIEGO POZIOMU BEZPIECZEŃSTWA INFORMACJI.

1. Standardową procedurą po wdrożeniu mechanizmów ochrony danych osobowych jest monitorowanie zagrożeń i zabezpieczeń, systematyczna weryfikacja i aktualizacja dokumentów Polityki Bezpieczeństwa i stosowanych zabezpieczeń.
2. Nakłady ponoszone na zabezpieczenia muszą być poprzedzone analizą ryzyka i kosztów, adekwatnie do potencjalnych strat spowodowanych naruszeniem bezpieczeństwa.
3. Zadaniem Polityki Bezpieczeństwa jest zminimalizowanie ryzyka płynącego z zagrożeń do akceptowalnego poziomu, to znaczy zapobieganie przypadkom naruszenia bezpieczeństwa danych osobowych przetwarzanych przez jednostkę po przez:
   a. zminimalizowanie możliwości takiego naruszenia bezpieczeństwa,
   b. umożliwienie wczesnego jego wykrycia,
   c. zminimalizowanie strat związanych z takim naruszeniem oraz sprawne usunięcie jego skutków.
4. System Zarządzania Bezpieczeństwem Informacji wprowadzony w jednostce uwzględnia procesy utrzymania odpowiedniego poziomu bezpieczeństwa, w tym:
   a. zarządzania ryzykiem;
   b. zarządzania dostępem do zasobów;
   c. monitorowania poziomu bezpieczeństwa;
   d. zarządzania incydentem.
   e. nadzoru nad dokumentacją systemu zarządzania bezpieczeństwem danych osobowych.
5. Dla utrzymania odpowiedniego poziomu bezpieczeństwa danych osobowych istotne jest:
   a. systematyczne szkolenie osób uprawnionych do przetwarzania danych osobowych oraz podnoszenie kwalifikacji zawodowych pracowników (w szczególności dotyczy to osób odpowiedzialnych za bezpieczeństwo danych osobowych: IOD; ASI);
   b. uczestniczenie przez pracowników w szkoleniach doskonalących praktyczne umiejętności z zakresu bezpieczeństwa danych (np. ochrona antywirusowa);
   c. przeprowadzanie audytów bezpieczeństwa danych osobowych.

VIII. ELEMENTY DOKUMENTACJI POLITYKI BEZPIECZEŃSTWA INFORMACJI.

1. Na Politykę Bezpieczeństwa danych osobowych składają się:

- „Polityka Bezpieczeństwa Ochrony Danych Osobowych – Zasady ogólne oraz procedury";
- „Polityka Bezpieczeństwa Ochrony Danych Osobowych – Raport z szacowania ryzyka i doboru środków bezpieczeństwa".

2. Procedury, instrukcje i regulaminy zawarte w/w dokumentach regulują szczegółowo zasady korzystania z zasobów informacyjnych – danych osobowych, w tym także użytkowania systemów informatycznych.

IX. ZASADY OGÓLNE OCHRONY DANYCH OSOBOWYCH.

1. Skuteczna ochrona zasobów informacyjnych – danych osobowych w jednostce wymaga wspólnego działania i zaangażowania wszystkich pracowników.
2. Zarówno kierownictwo jak i wszyscy pracownicy są zobowiązani, odpowiednio do swoich obowiązków i zajmowanych stanowisk, do przestrzegania Polityki Bezpieczeństwa, a zwłaszcza zasad zawartych w procedurach, instrukcjach i innych dokumentach PB.
3. Pracownicy w szczególności zobowiązani są do przestrzegania procedur opisujących zasady korzystania z haseł, procedur ochrony antywirusowej oraz procedur eksploatacji systemów informatycznych, a także do przestrzegania zakazu udostępniania hasła do swojego komputera, zakazu korzystania z nielegalnego oprogramowania oraz zakazu instalowania jakiegokolwiek oprogramowania bez zgody administratora systemu informatycznego (ASI). Pracownicy są zobowiązani do używania zasobów informacyjnych – danych osobowych jednostki wyłącznie do celów służbowych.
4. Ponadto wszyscy pracownicy są zobowiązani do przestrzegania zasad ochrony danych osobowych.
5. W przypadku osób, z którymi jednostka zawiera umowy cywilno-prawne, z których wynika, że będą przetwarzali dane osobowe, których AD jest jednostka należy w zawieranej umowie wprowadzić klauzulę dot. obowiązku przestrzegania postanowień Polityki Bezpieczeństwa. Wówczas:
   a. należy w zawieranej umowie wprowadzić klauzulę dot. obowiązku przestrzegania postanowień Polityki Bezpieczeństwa;
   b. dostęp do zasobów informatycznych i pomieszczeń jednostki jest możliwy po wcześniejszym otrzymaniu stosownego upoważnienia i zapoznaniu się z Polityką Bezpieczeństwa;
   c. dostęp do danych osobowych jest ograniczony do okresu zdefiniowanego w umowie;
   d. w uzasadnionych przypadkach należy przeprowadzić szkolenie w zakresie PB obowiązującej w jednostce.
6. Odpowiedzialność za bezpieczeństwo danych osobowych obejmuje nie tylko siedzibę jednostki, ale także wszelkie sytuacje, w których dane osobowe są przetwarzane poza jej siedzibą. (szczególności zdalny dostęp do sieci komputerowej jednostki).
7. Jeżeli przetwarzanie ma być dokonywane w imieniu administratora, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszej polityki i przepisów prawa i chroniło prawa osób, których dane dotyczą.
8. Podmiot przetwarzający nie może korzystać z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody administratora. W przypadku ogólnej pisemnej zgody podmiot przetwarzający informuje administratora o wszelkich zamierzonych

zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian.

9. Przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy, określającej przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora.
10. Umowa określa w szczególności, że podmiot przetwarzający:
    a. przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora;
    b. zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania poufności przetwarzanych danych;
    c. podejmuje wszelkie środki bezpieczeństwa przetwarzania wymagane na mocy RODO;
    d. po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie;
    e. udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków prawnych oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.

- WZÓR -

Umowa powierzenia przetwarzania danych osobowych

zawarta dnia _____ pomiędzy:

_____ *(*dane podmiotu, który umowę zawiera)*

zwanym w dalszej części umowy **„Podmiotem przetwarzającym”**
reprezentowana przez:

_____

a

_____ (*dane podmiotu, który umowę zawiera)*

zwanym w dalszej części umowy **„Administratorem Danych” lub „Administratorem”**
reprezentowana przez:

_____

zwane w treści umowy łącznie również Stronami, o następującej treści:

§ 1

Definicje

1. „**Dane osobowe**” - oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”) zebrane w celu ……. Zgodnie z obowiązującymi przepisami prawa UE i prawa polskiego *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.
2. „**Dane dotyczące danej branży (dane budowlane, medyczne itp. – definicja danych specyficznych dla danej branży – fakultatywnie)**
3. „**Państwo trzecie**” – państwo nienależące do Unii Europejskiej.
4. „**Podmiot trzeci**” - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe.
5. **„Przetwarzanie**” oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką 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.
6. **„Rozporządzenie” -** Rozporządzenia 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,

7. **„Dyrektywa" -** Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych.

§ 2

Powierzenie przetwarzania danych osobowych

1. Administrator Danych, który samodzielnie ustala cele i sposoby przetwarzania danych osobowych powierza Podmiotowi przetwarzającemu, w trybie art. 28 rozporządzenia, dane osobowe do przetwarzania, na zasadach i w celu określonym w niniejszej Umowie. W celu uniknięcia wątpliwości Strony oświadczają, że przetwarzanie danych osobowych przez Podmiot przetwarzający nie pozbawia Administratora Danych decydowania o celu i sposobie przetwarzania danych osobowych.
2. Administrator Danych oświadcza i potwierdza, że posiada podstawę prawną do przetwarzania danych osobowych powierzonych do przetwarzania Podmiotowi przetwarzającemu i zobowiązuje się, na żądanie tego Podmiotu, wskazać na jakiej podstawie prawnej powierza mu dane osobowe oraz przekazać, kopie zgód na przetwarzanie danych osobowych (jeśli dotyczy) oraz udzielić wszelkich żądanych w tym zakresie wyjaśnień.
3. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą umową, Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
4. Podmiot przetwarzający oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi Rozporządzenia.

§3

Zakres i cel przetwarzania danych

1. Podmiot przetwarzający będzie przetwarzał, powierzone na podstawie umowy dane …… (**należy podać rodzaj danych*) *np. dane zwykłe oraz dane szczególnych kategorii ……. (*należy podać kategorię osób, których dane dotyczą*) *np. pracowników administratora, klientów administratora itd. w postaci …….. np. imion i nazwisk, adresu zamieszkania, nr PESEL itd*.
2. Powierzone przez Administratora dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu ……. (**należy podać cel przetwarzania danych przez podmiot przetwarzający*) *np. realizacji umowy z dnia …… nr …… w przedmiocie …….*
3. Na mocy Umowy Podmiot przetwarzający jest upoważniony do wykonywania wszelkich operacji na przekazanych jej na mocy Umowy Danych osobowych, zgodnych z zakresem i celem przetwarzania wskazanym w Umowie, w szczególności takich jak: zbieranie, utrwalanie, przechowywanie, pobieranie, przeglądanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a także tych, które wykonuje się w systemach informatycznych.
4. Dane osobowe mogą być przekazywane Podmiotowi przetwarzającemu bezpośrednio przez Administratora Danych lub za pośrednictwem podmiotu przez niego wyznaczonego

§4

Obowiązki Administratora Danych

1. Administrator Danych jest zobowiązany przestrzegać obowiązujące przepisy prawa dotyczące przetwarzania danych osobowych w tym w szczególności przepisów krajowych oraz przepisów Unii Europejskiej, w tym w szczególności Dyrektywy 95/46/WE Parlamentu

Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych *(w par. 1 - „Dyrektywa")*, a po dacie 25 maja 2018 r. także Rozporządzenia 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 (*w par. 1 - „Rozporządzenie")* i realizować obowiązki tam wskazane.

2. Administrator Danych jest zobowiązany spełnić obowiązek informacyjny, wobec osób których dotyczą Dane osobowe objęte niniejszą Umową, w sposób umożliwiający wykazanie zrealizowania tego obowiązku, oraz uzyskać zgodę podmiotu którego Dane osobowe dotyczą (jeżeli jest to wymagane).
3. Administrator Danych jest zobowiązany udzielać Podmiotowi przetwarzającemu wszelkich informacji niezbędnych do prawidłowego przetwarzania powierzonych danych osobowych.

§5

Obowiązki podmiotu przetwarzającego

1. Podmiot przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, o których mowa w art. 32 Rozporządzenia.
2. Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
3. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej umowy.
4. Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy**,** (o której mowa w art. 28 ust 3 pkt b Rozporządzenia) przetwarzane dane przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej umowy, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu.
5. Podmiot przetwarzający**,** po zakończeniu świadczenia usług związanych z przetwarzaniem usuwa / zwraca Administratorowi wszelkie dane osobowe (*należy wybrać czy podmiot przetwarzający ma usunąć czy zwrócić dane*) oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.
6. W miarę możliwości Podmiot przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 Rozporządzenia.
7. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je Administratorowi Danych w ciągu ….. (**można wskazać np. w ciągu 24 h*).

§6

Prawo kontroli

1. Administrator Danych zgodnie z art. 28 ust. 3 pkt h. Rozporządzenia ma prawo kontroli, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia umowy.

2. Administrator Danych ma prawo realizować prawo kontroli, o którym mowa w ust. 1 par.6, tylko w siedzibie Podmiotu przetwarzającego lub innym miejscu, w którym przetwarzane są dane osobowe powierzone na podstawie niniejszej Umowy i tylko w godzinach pracy Podmiotu przetwarzającego, po ustaleniu terminu kontroli, z co najmniej z trzydziestodniowym (30) wyprzedzeniem.
3. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora Danych nie dłuższym niż 7 dni (**administrator termin może określić dowolnie*).
4. Podmiot przetwarzający udostępnia Administratorowi Danych wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.
5. W celu uniknięcia wątpliwości Strony oświadczają, że Podmiot przetwarzający nie jest Inspektorem Danych Osobowych w rozumieniu Rozporządzenia ani też nie pełni funkcji administratora bezpieczeństwa informacji w rozumieniu ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz.U. z 2016 r. poz. 922) ani też nie pełni innej analogicznej roli znanej w przepisach krajowych Administratora Danych.

§7

Dalsze powierzenie danych do przetwarzania

1. Podmiot przetwarzający może powierzyć dane osobowe objęte niniejszą umową do dalszego przetwarzania podwykonawcom jedynie w celu wykonania umowy po uzyskaniu uprzedniej pisemnej zgody Administratora Danych.
2. Przekazanie powierzonych danych do państwa trzeciego może nastąpić jedynie na pisemne polecenie Administratora Danych, chyba że obowiązek taki nakłada na Podmiot przetwarzający prawo Unii lub prawo państwa członkowskiego, któremu podlega Podmiot przetwarzający. W takim przypadku przed rozpoczęciem przetwarzania Podmiot przetwarzający informuje Administratora Danych o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
3. Podwykonawca, o którym mowa w §3 ust. 2 Umowy winien spełniać te same gwarancje i obowiązki jakie zostały nałożone na Podmiot przetwarzający w niniejszej Umowie.
4. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za niewywiązanie się ze spoczywających na podwykonawcy obowiązków ochrony danych.

§ 8

Odpowiedzialność Podmiotu przetwarzającego

1. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią umowy, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.
2. Podmiot przetwarzający zobowiązuje się do niezwłocznego poinformowania Administratora Danych o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający danych osobowych określonych w umowie, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Podmiotu przetwarzającego, a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania w Podmiocie przetwarzającym tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez Generalnego Inspektora Ochrony

Danych Osobowych. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora Danych.

3. Podmiot przetwarzający odpowiada wyłącznie za szkody powstałe z jego winy spowodowane przetwarzaniem powierzonych mu Danych osobowych w sposób niezgody z Umową lub powszechnie obowiązującym prawem.
4. Administrator Danych ponosi odpowiedzialność za przetwarzanie Danych osobowych przekazanych Podmiotowi przetwarzającemu wobec których nie posiada podstawy prawnej do ich przetwarzania.
5. W przypadku, o którym mowa w ust. 4 par. 8 Administrator Danych jest zobowiązany niezwłocznie zwrócić Podmiotowi przetwarzającemu równowartość wszelkich kosztów jakie w związku z tym zostały przez niego poniesione, w szczególności kar lub grzywien nałożonych na Podmiot przetwarzający przez właściwe organy państwowe oraz organy Unii Europejskiej, odszkodowań, zadośćuczynienia lub zlikwidowanych szkód finansowych.
6. Jeśli Podmiot trzeci lub osoba, której dane dotyczą podejmie działania prawne przeciwko choćby jednej ze Stron w związku z naruszeniem zasad przetwarzania Danych osobowych, każda ze Stron jest zobowiązana wobec drugiej Strony podjąć współpracę w celu podjęcia odpowiednich działań prawnych mających na celu odparcia zarzutów, zawarcia ugody lub innych środków prawnych.

§9

Czas obowiązywania umowy

1. Niniejsza umowa obowiązuje od dnia jej zawarcia przez czas *nieokreślony/określony* od …. do … .*
2. Każda ze stron może wypowiedzieć niniejszą umowę z zachowaniem …… * okresu wypowiedzenia.

§10

Rozwiązanie umowy

1. Administrator Danych może rozwiązać niniejszą umowę ze skutkiem natychmiastowym, gdy Podmiot przetwarzający:
   a) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;
   b) przetwarza dane osobowe w sposób niezgodny z umową;
   c) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora Danych;

§11

Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora Danych i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej („dane poufne").
2. Podmiot przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora Danych w innym celu niż wykonanie Umowy, chyba że konieczność ujawnienia posiadanych informacji wynika z obowiązujących przepisów prawa lub Umowy.

3. Strony zobowiązują się do dołożenia należytej staranności w celu zapewnienia, aby środki łączności wykorzystywane do odbioru, przekazywania oraz przechowywania Danych poufnych gwarantowały odpowiednie zabezpieczenie tych danych, przed dostępem osób nieuprawnionych,
4. Strony są zobowiązane także do zachowania w poufności wszelkich danych, informacji, materiałów i dokumentów zawierających informacje lub dane uzyskane w związku z zawarciem lub realizacją Umowy. Informacje Poufne stanowią wszystkie w szczególności techniczne, technologiczne i administracyjne informacje oraz inne informacje o charakterze tajemnicy przedsiębiorstwa, przekazywane przez **Strony**, zarówno ustnie, jak i pisemnie, w tym drogą elektroniczną (dalej: „Informacje poufne"). O poufności Informacji Poufnych decyduje ich charakter, a nie sposób ich przekazania.

§12
Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach dla każdej ze stron.
2. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego oraz Rozporządzenia.
3. W przypadku, gdyby którekolwiek z postanowień Umowy uznane zostało za nieważne lub prawnie wadliwe, pozostałe postanowienia Umowy pozostają w mocy w najszerszym zakresie dopuszczalnym przez obowiązujące przepisy prawa.
4. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej umowy będzie sąd właściwy dla Administratora Danych (**lub Podmiotu przetwarzającego w zależności od postanowień stron*).
5. Oświadczenia wysłane do Strony w formie wiadomości elektronicznej e-mail, dla swojej skuteczności, wymagają doręczenia co najmniej do następujących osób na następujące adresy poczty elektronicznej e-mail:

a) oświadczenia kierowane do Administratora Danych:
- [_____];
- [_____];

b) oświadczenia kierowane do Podmiotu Przetwarzającego:
- [_____];
- [_____]

6. Zmiana osób i adresów e-mail wskazanych w ust. 1 powyżej nie stanowi zmiany Umowy i jest skuteczna od chwili doręczenia drugiej Stronie w formie pisemnej lub e-mail, informacji o nowych osobach oraz adresach e-mail

_____ _____

Administrator Danych Podmiot przetwarzający

X. WARUNKI WYRAŻENIA ZGODY NA PRZETWARZANIE DANYCH OSOBOWYCH.

1. Jeżeli przetwarzanie odbywa się na podstawie zgody, administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych.
2. Jeżeli osoba, której dane dotyczą, wyrażą zgodę w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.
3. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody musi być równie łatwe jak jej wyrażenie.
4. Oceniając, czy zgodę wyrażono dobrowolnie, w jak największym stopniu uwzględnia się, czy między innymi od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, w tym świadczenie usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy.

Klauzula zgody jednorazowej (np. rekrutacja)

Treść klauzuli	**Sposób wprowadzenia**
Zgodnie z art. 6 ust 1 pkt a w zw. z art. 8 Rozporządzenia 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 (RODO) wyrażam zgodę na przetwarzanie moich danych osobowych do **celów rekrutacyjnych**	• checkbox na formularzu rejestracyjnym na stronie www • pole do zaznaczenia na formularzu papierowym • dodatkowa informacja na CV

Klauzula zgody dla większej ilości celów

Treść klauzuli	**Sposób wprowadzenia**
Zgodnie z art. 6 ust 1 pkt a w zw. z art. 8 Rozporządzenia 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 (RODO) wyrażam zgodę na przetwarzanie moich danych osobowych do **(*)**: • Aktualnego procesu rekrutacyjnego i przyszłych procesów rekrutacyjnych • Przekazania innym podmiotom • Uczestnictwa w konkursie, olimpiadzie, zawodach <nazwa> **(*) przykłady, wskazać właściwe**	• checkbox na formularzu rejestracyjnym na stronie www • pole do zaznaczenia na formularzu papierowym • dodatkowa informacja na CV <u>Uwaga:</u> zgoda musi być wyrażona przed przetwarzaniem danych osobowych

XI. OBOWIĄZKI INFORMACYJNE ADMINISTRATORA DANYCH.

Informacje o przetwarzaniu danych osobowych:

1. Administrator podejmuje odpowiednie środki, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem udzielić osobie, której dane dotyczą, wszelkich informacji o przetwarzaniu danych osobowych. Informacji udziela się na piśmie lub w inny sposób, w tym w stosownych przypadkach – elektronicznie.
2. Administrator bez zbędnej zwłoki – a w każdym razie w terminie miesiąca od otrzymania żądania – udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku z prawem dostępu do danych osobowych. W razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań.
3. Jeżeli administrator nie podejmuje działań w związku z żądaniem osoby, której dane dotyczą, to niezwłocznie – najpóźniej w terminie miesiąca od otrzymania żądania – informuje osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.
4. Jeżeli administrator ma uzasadnione wątpliwości co do tożsamości osoby fizycznej składającej żądanie dotyczące przetwarzania jej danych osobowych, może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą.

Informacje podawane w przypadku zbierania danych od osoby, której dane dotyczą:

1. Jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, AD podaje jej wszystkie następujące informacje:
   a. swoją tożsamość i dane kontaktowe;
   b. gdy ma to zastosowanie – dane kontaktowe inspektora ochrony danych;
   c. cele przetwarzania danych osobowych oraz podstawę prawną przetwarzania;
   d. prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią – o ile ma zastosowanie;
   e. informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
   f. gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej.
   g. okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
   h. informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
   i. Informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
   j. informacje o prawie wniesienia skargi do organu nadzorczego;
   k. informacje czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
   l. informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu.
2. Powyższe zasady informacyjne nie mają zastosowania, gdy – i w zakresie, w jakim – osoba, której dane dotyczą, dysponuje już tymi informacjami.

Informacje podawane w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą:

1. Jeżeli danych osobowych nie pozyskano od osoby, której dane dotyczą, administrator podaje osobie, której dane dotyczą informacje jak powyżej oraz źródło pozyskania tych danych., następujące informacje:
2. Informacje powyższe, administrator podaje:
   a. w rozsądnym terminie po pozyskaniu danych osobowych – najpóźniej w ciągu miesiąca – mając na uwadze konkretne okoliczności przetwarzania danych osobowych;
   b. jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą – najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą; lub
   c. jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu.

Przykładowe klauzule informacyjne

Klauzula informacyjna dla pracownika

Treść klauzuli	Sposób wprowadzenia
Zgodnie z art. 13 Rozporządzenia 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 (RODO), informuje Pana/Panią, że: 1. Administratorem przetwarzanych Pana/ Pani danych osobowych jest: **Zespół Szkół Zawodowych** **im. gen. Stanisława Maczka** **86-010 Koronowo ul. Dworcowa 53** 2. Dane osobowe przetwarzane są na podstawie art. 6 ust. 1 pkt c Rozporządzenia 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 (RODO) celem **spełnienia wymogów prawnych.** 3. Obowiązek podania danych wynika z Ustawy Kodeks pracy z dnia 26 czerwca 1974 r. (tj. z dnia 8 września 2016 r. (Dz. U. z 2016 r. poz. 1666), niepodania danych osobowych sprawia pozostawienie sprawy – procesu zatrudnienia bez rozpatrzenia; 4. Dane osobowe przetwarzane będą przez okres wskazany w Kodeksie pracy. 5. Dane osobowe nie będą przekazane za granicę ani użyte do profilowania. 6. Posiada Pan/ Pani prawo do: a. żądania dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania;	• na kwestionariuszu osobowym w stopce • dodatkowa informacja do kwestionariusza innego dokumentu związanego z zatrudnieniem UWAGA: osoby informowane podpisują klauzule informacyjne, że zostały z nimi zapoznane

b. wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych; c. wniesienia skargi do Urzędu Ochrony Danych; 7. Inspektorem Ochrony Danych w jednostce jest: **Arnold Paszta** arnold.partner@gmail.com	

Klauzula informacyjna dla umów – zleceń, umów o dzieło oraz z osobami fizycznymi prowadzącymi własną działalność gospodarczą.

Treść klauzuli	Sposób wprowadzenia
Zgodnie z art. 13 Rozporządzenia 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 (RODO), informuje Pana/Panią, że: 1. Administratorem przetwarzanych Pana/ Pani danych osobowych jest: **Zespół Szkół Zawodowych** **im. gen. Stanisława Maczka** **86-010 Koronowo ul. Dworcowa 53** 2. Dane osobowe przetwarzane są na podstawie art. 6 ust. 1 pkt b Rozporządzenia 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 (RODO) celem **zawarcia umowy cywilno - prawnej.** 3. Brak podania danych osobowych powoduje brak możliwości zawarcia umowy; 4. Dane osobowe przetwarzane będą przez okres niezbędny przewidziany dla realizacji umowy i ustawy o archiwizacji. 5. Dane osobowe nie będą przekazane za granicę ani użyte do profilowania. 6. Posiada Pan/ Pani prawo do: a. żądania dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania; b. wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych; c. prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem; d. wniesienia skargi do Urzędu Ochrony Danych; 7. Inspektorem Ochrony Danych w jednostce jest: **Arnold Paszta** arnold.partner@gmail.com	• w treści umowy • w postaci stopki na fakturze • załącznik do umowy • w stopce poczty służbowej

Klauzula informacyjna na ogłoszeniach o pracę.

Treść klauzuli	Sposób wprowadzenia
Zgodnie z art. 13 Rozporządzenia 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 (RODO), informuje Pana/Panią, że: 1. Administratorem przetwarzanych Pana/ Pani danych osobowych jest: **Zespół Szkół Zawodowych** **im. gen. Stanisława Maczka** **86-010 Koronowo ul. Dworcowa 53** 2. Dane osobowe przetwarzane są na podstawie art. 6 ust. 1 pkt a Rozporządzenia 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 (RODO) celem realizacji procesu rekrutacyjnego/ potrzeb aktualnej i przyszłych rekrutacji **(*).** 3. Podanie danych nie jest obowiązkowe, brak podania danych osobowych powoduje wstrzymanie procesu rekrutacyjnego/ potrzeb aktualnej i przyszłych rekrutacji **(*)**; 4. Dane osobowe przetwarzane będą przez okres niezbędny związany z rekrutacji. 5. Dane osobowe nie będą przekazane za granicę ani użyte do profilowania. 6. Posiada Pan/ Pani prawo do: a. żądania dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania; b. wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych; c. prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem; d. wniesienia skargi do Urzędu Ochrony Danych; 7. Inspektorem Ochrony Danych w jednostce jest: **Arnold Paszta** arnold.partner@gmail.com ***niepotrzebne skreślić**	• w ogłoszeniu prasowym lub na portalach pracy • mailem po przyjęciu CV • w stopce poczty służbowej

Klauzula informacyjna dla klientów/ petentów

Treść klauzuli	Sposób wprowadzenia
Zgodnie z art. 13 Rozporządzenia 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 (RODO), informuje Pana/Panią, że: 1. Administratorem przetwarzanych Pana/ Pani danych osobowych jest: **Zespół Szkół Zawodowych** **im. gen. Stanisława Maczka** **86-010 Koronowo ul. Dworcowa 53** 2. Dane osobowe przetwarzane są na podstawie art. 6 ust. 1 pkt a lub c Rozporządzenia 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 (RODO) celem np. zakwalifikowania do placówki oświatowej. 3. Podanie danych osobowych nie jest wymogiem ustawowym, niepodania danych osobowych uniemożliwia zakwalifikowanie dziecka do Jednostki oświatowej; 4. Dane osobowe nie będą przekazywane za granicę ani użyte do profilowania 5. Dane osobowe przetwarzane będą przez okres niezbędny przewidziany dla danej sprawy. 6. Posiada Pan/ Pani prawo do: a. żądania dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania; b. wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych; c. prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem; d. wniesienia skargi do Urzędu Ochrony Danych; 7. Inspektorem Ochrony Danych w jednostce jest: **Arnold Paszta** arnold.partner@gmail.com	• w postaci wywieszki na tablicy ogłoszeń • w Sekretariacie • na stronie internetowej • w stopce poczty służbowej

XII. DOBÓR ZABEZPIECZEŃ.

1. Jednostka dobiera cele stosowania zabezpieczeń i zabezpieczenia odpowiednio do wymagań prawnych i wyników analizy ryzyka dla bezpieczeństwa danych osobowych.
2. Zabezpieczenia fizyczne, techniczne i organizacyjne powinny uzupełniać się wzajemnie zapewniając wspólnie wymagany poziom bezpieczeństwa informacji.
3. Podstawowe zasady mające wpływ na bezpieczeństwo danych osobowych:
    a. **zasada przywilejów koniecznych** - każdy pracownik posiada prawa dostępu do danych osobowych ograniczone wyłącznie do tych, które są konieczne do wykonywania powierzonych mu zakresów obowiązków. Dostęp do pomieszczeń posiadają tylko osoby upoważnione;
    b. **zasada wiedzy koniecznej** - pracownicy posiadają wiedzę o danych osobowych ograniczoną wyłącznie do zagadnień, które są konieczne do realizacji powierzonych im zadań;
    c. **zasada asekuracji zabezpieczeń** - ochrona danych osobowych winna opierać się na co najmniej dwóch mechanizmach zabezpieczenia;
    d. **zasada rozliczalności** - jednostka dąży do zapewnienia jednoznacznej odpowiedzialności pracowników za powierzone im dane osobowe; wszyscy użytkownicy danych osobowych ponoszą odpowiedzialność za zaniedbanie swoich obowiązków w zakresie bezpieczeństwa danych osobowych. Niedopuszczalne jest pozostawianie w pomieszczeniach bez nadzoru osób nieupoważnionych;
    e. **zasada czystego biurka** - należy unikać pozostawiania dokumentów zawierających dane osobowe na biurku bez opieki. Dokumenty i nośniki zawierające dane osobowe, przechowuje się zamknięte na klucz (np. w szafie, szufladzie);
    f. **zasada czystego ekranu** - zamykanie sesji lub blokowanie komputera pozostawionego bez opieki lub czasowo nieużywanego (za pomocą mechanizmu blokowania ekranu i klawiatury, kontrolowanego hasłem). Po zakończonym dniu pracy komputer musi (po za uzasadnionymi przypadkami i zgłoszonymi do Administratora Systemu Informatycznego) zostać wyłączony;
    g. **zasada niszczenia nośników informacji (np. papier, płyty CD) -** niszczenie nieużytecznych (po ustaniu ich przydatności i niepodlegających archiwizacji) nośników zawierających dane osobowe w odpowiednich niszczarkach lub w sposób uniemożliwiający odczytanie zawartych w nich danych.

XIII. SANKCJE ZA NARUSZENIE ZASAD BEZPIECZEŃSTWA INFORMACJI.

1. Nieprzestrzeganie zasad zawartych w dokumentach Polityki Bezpieczeństwa, jest naruszeniem obowiązków pracowniczych wynikających w szczególności z Kodeksu Pracy i może pociągnąć za sobą skutki dyscyplinarne oraz spowodować pociągnięcie do odpowiedzialności wynikającej z przepisów prawa lub umów.
2. Naruszenie zasad ochrony danych osobowych może spowodować pociągnięcie do odpowiedzialności karnej wynikającej z przepisów:
    a. ustawy o ochronie danych osobowych;
    b. RODO;
    c. kodeksu karnego dot. przestępstw przeciwko ochronie informacji;
    d. przepisów chroniących tajemnice zawodowe.

3. Odpowiedzialność dyscyplinarna lub karna nie zwalnia od dochodzenia roszczeń cywilno – prawnych wynikających z RODO, ustawy o ochronie danych osobowych oraz kodeksu cywilnego

XIV. ZASADY ROZPOWSZECHNIANIA DOKUMENTU ORAZ TRYB WPROWADZANIA ZMIAN.

1. Do zapoznania się i stosowanie niniejszej Polityki Bezpieczeństwa oraz dokumentów z nią związanych, zobligowani są wszyscy pracownicy.
2. Niniejszy dokument winien być udostępniony również uprawnionym podmiotom zewnętrznym w celu zapoznania się i stosowania w przypadku zaistnienia takiej potrzeby.
3. Komórka organizacyjna odpowiedzialna za sprawy kadrowe przekazuje, do zapoznania się, nowo zatrudnionym pracownikom oraz stażystom i praktykantom Politykę Bezpieczeństwa wraz z dokumentami związanymi.
4. Nowo zatrudniony pracownik oraz stażysta czy praktykant jest zobowiązany zapoznać się i złożyć pisemne oświadczenie potwierdzające znajomość zasad, reguł i postanowień zawartych w/w dokumentach.
5. Dokumentacja PB powinna być przeglądana i weryfikowana:
   - na polecenie AD;
   - w przypadku wystąpienia poważnych incydentów związanych z bezpieczeństwem informacji;
   - w celu realizacji zaleceń wynikających z przeprowadzonych audytów i kontroli;
   - w przypadku wejścia w życie nowych przepisów dotyczących ochrony danych osobowych;
   - w przypadku poważnych modyfikacji infrastruktury teleinformatycznej;
   - w przypadku zawarcia umów, z których wynikają zobowiązania związane z bezpieczeństwem danych osobowych;
   - okresowo, nie rzadziej niż raz w roku.
6. Za aktualizację dokumentacji bezpieczeństwa odpowiada Inspektor Ochrony Danych.
7. Zmieniony dokument zatwierdza i wprowadza w drodze zarządzenia AD.

Załącznik nr 1 do PB

P_01	**PROCEDURA KONTOLI DOSTĘPU DO INFORMACJI.**	Wydanie: 01
		Data: 25.05.2018 r.

I. Definicje stosowanych pojęć w dokumencie:

1. **Inspektor Ochrony Danych (IOD)** – osoba powołana przez administratora na podstawie kwalifikacji i doświadczenia odpowiadająca za przestrzeganie procedur w zakresie danych osobowych i zgłoszona do Urzędu Ochrony Danych.
2. **Administrator Systemu Informatycznego (ASI) / Informatyk** - wyznaczony pracownik lub firma zewnętrzna realizująca obsługę IT jednostki, odpowiedzialny za realizację zadań związanych z zarządzaniem systemem informatycznym, w tym za zabezpieczenie sieci komputerowej tzn. wdrażanie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów infrastruktury informatycznej oraz ochrony danych przed nieuprawnioną modyfikacją, zniszczeniem, dostępem i ujawnieniem, a także ich utratą.
3. **Stanowisko** - pojedynczy komputer osobisty lub terminal przeznaczony do określonych zadań związanych między innymi z dostępem do sieci komputerowej jednostki.
4. **System informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
5. **Zasoby informatyczne** - ogół systemów informatycznych wykorzystywanych przez jednostkę.
6. **Konto** - to zbiór zasobów i uprawnień mający unikalny identyfikator w systemie informatycznym lub sieci komputerowej.
7. **Użytkownik** - to byt (osoba lub inny system) korzystający z systemu komputerowego. Użytkownicy mogą być identyfikowani w celach zliczania czasu pracy, bezpieczeństwa, czy też zarządzania danymi osobowymi. Aby użytkownik został zidentyfikowany, musi posiadać konto (konto użytkownika), do którego przypisana jest nazwa (nazwa użytkownika) i hasło (lub inny sposób uwierzytelnienia - np. informacje biometryczne). Użytkownicy uzyskują dostęp do systemów przez interfejs użytkownika, a sam proces uwierzytelniania nazywany jest logowaniem.

II. Cel procedury

1. Celem tej procedury jest określenie zasad udzielania dostępu użytkowników do danych zgromadzonych w sieci komputerowej oraz uniemożliwienie dostępu osobom nieupoważnionym.
2. Dostęp do określonych zasobów informatycznych (danych osobowych) jest przydzielany na podstawie udokumentowanych potrzeb użytkowników.

III. Zakres stosowania.

1. Działania opisane w niniejszej procedurze obowiązują, we wszystkich działaniach jednostki.
2. Niniejsza procedura jest elementem Polityki Bezpieczeństwa ustanowionej w jednostce.

IV. Odpowiedzialność.

1. Wszyscy użytkownicy uzyskujący dostęp do danych osobowych przetwarzanych w sieci komputerowej jak również użytkownicy stanowisk nie podłączonych do sieci, ale zainstalowanych na terenie jednostki, odpowiedzialni są za przestrzeganie zasad opisanych w procedurze w zakresie ochrony haseł.
2. Administrator systemu odpowiedzialny jest za:
    a. zakładanie i usuwanie kont w systemie,
    b. generowanie użytkownikom pierwszych haseł dostępowych,
    c. przydzielanie i odbieranie dostępu do zasobów użytkownikom stanowisk.
3. Kierownicy komórek organizacyjnych, korzystający z sieci komputerowej, odpowiedzialni są za analizę celowości uruchomienia stanowiska, za przygotowanie i przekazanie wniosków o skonfigurowanie stanowiska oraz przydzielenie lub zlikwidowanie konta użytkownikowi, a także zapoznanie podległych im pracowników z treścią zawartą w tej polityce.

V. Procedura udzielenia dostępu do danych osobowych przetwarzanych w systemie informatycznym.

1. Utworzenie konta:
    a. Wniosek o założenie / zmianę konta AD wydaje poprzez IOD - wzór wniosku stanowi **Załącznik nr 1** do niniejszej procedury.
    b. Następnie wniosek po weryfikacji jest przekazywany Administratorowi Systemu Informatycznego / Informatykowi, który ustanawia parametry konta.
    c. AD poprzez ASI ma prawo zablokować dostęp do funkcji i zasobów systemu w przypadku stwierdzenia niewłaściwego, niezgodnego z treścią wniosku wykorzystywania stanowiska roboczego.

2. Zmiany na koncie:
    a. W przypadku zmiany danych podanych we wniosku osoba bezpośrednio zainteresowana jest zobowiązana złożyć nowy wniosek do AD niezwłocznie od wystąpienia zdarzenia powodującego zmianę.
    b. AD poprzez ASI / IDO informuje o potrzebie likwidacji konta niezwłocznie od wystąpienia zdarzenia powodującego likwidację konta.
    c. Wzór wniosku stanowi **Załącznik nr 2** do niniejszej procedury.
    d. Inspektor Ochrony Danych przekazuje wniosek AD.
    e. Wniosek umieszczany jest w aktach osobowych lub dokumentacji bezpieczeństwa danych osobowych.
    f. Administrator Systemu Informatycznego na podstawie wniosku zakłada konto lub zmienia parametry konta i przekazuje użytkownikowi wszystkie dane niezbędne do korzystania z niego, w tym hasło do pierwszego zalogowania.
    g. W przypadku likwidacji konta, Administrator Systemu Informatycznego blokuje konto

niezwłocznie lub w terminie podanym we wniosku.

h. Ostateczne usunięcie konta może nastąpić nie wcześniej niż 12 m-cy po zablokowaniu konta.
i. Administrator Systemu Informatycznego dokonuje końcowej konfiguracji poczty elektronicznej na komputerze użytkownika (jeżeli wniosek tego dotyczy) i innych niezbędnych elementów potrzebnych użytkownikowi do wykonywania zadań.
j. Administrator Systemu Informatycznego ma prawo zablokować konto, w przypadku stwierdzenia niewłaściwego, niezgodnego z treścią wniosku wykorzystywania konta.

VI. Określenie sposobu przydziału haseł dla użytkowników i częstotliwość ich zmiany oraz wskazanie osoby/osób odpowiedzialnej/odpowiedzialnych za te czynności.

1. Użytkownicy stanowisk roboczych są zobowiązani zapoznać się z „Polityką Bezpieczeństwa" oraz chronić przed nieuprawnionym wykorzystaniem wszelkie znane im lub będące w ich posiadaniu dane umożliwiające dostęp do danych osobowych przetwarzanych w sieci informatycznej.
2. Oznacza to m.in. zakaz ujawniania haseł umożliwiających dostęp do kont lub innych zasobów, np. do plików zawierających hasła, klucze szyfrujące, itp.
3. Po otrzymaniu od Administratora Systemu Informatycznego haseł umożliwiających dostęp do konta użytkownik powinien niezwłocznie zmienić te hasła na inne, znane tylko sobie.
4. Hasła powinny spełniać następujące wymagania:
   a. minimalna długość hasła powinna wynosić 8 znaków;
   b. hasło powinno zawierać duże i małe litery, znaki specjalne oraz cyfry;
   c. nie należy używać wyrazów występujących we wszelkiego rodzaju słownikach, nawet jeśli zostaną uzupełnione innymi znakami;
   d. nie należy też używać żadnych wyrazów lub liczb występujących w danych personalnych użytkownika;
   e. nie należy używać haseł wynikających z układu klawiatury (np.: qwerty);
   f. hasło nie może się powtarzać.
5. Hasła nie wolno udostępniać.
6. Nie dopuszcza się zmiany loginu.
7. Niedopuszczalne jest zapisywanie haseł na kartkach przyklejonych do monitora, klawiatury czy biurka.
8. Hasło należy zmieniać co najmniej raz na trzy miesiące o ile nie zastosowano metod autentyfikacji biometrycznej.
9. Posługiwanie się danymi identyfikującymi lub uwierzytelniającymi należącymi do innego użytkownika w celu dostępu do zasobów sieci komputerowej na jego konto lub podejmowania jakichkolwiek innych działań w jego imieniu jest zabronione.
10. Hasła do kont awaryjnych (o wysokich uprawnieniach) są przechowywane w zaklejonych kopertach przez AD. Na każdej kopercie powinna być informacja o przeznaczeniu konta oraz data umieszczenia hasła w kopercie.

VII. Zasady postępowania dotyczące dostępu pracowników do systemów informatycznych udostępnianych do celów służbowych przez zewnętrzne instytucje, poprzez sieć Internet lub inną sieć rozległą.

1. W przypadku, gdy pracownicy używają w pracy systemu informatycznego udostępnianego przez zewnętrzną instytucję (np.: ministerstwo) ochronie podlegają jedynie dane i programy umożliwiające uwierzytelnienie i dostęp do ww. systemu (np.: loginy, hasła, certyfikaty).
2. Należy wtedy oprócz stosowania się do zasad opisanych w niniejszej procedurze stosować się do zaleceń i polityki bezpieczeństwa instytucji udostępniającej system.
3. Pracownicy korzystają z systemu udostępnionego przez zewnętrzne instytucje wyłącznie w siedzibie jednostki i w godzinach pracy Jednostki, na sprzęcie komputerowym przeznaczonym do celów służbowych, chyba, że ustalenia z instytucją udostępniającą system stanowią inaczej lub specyfika pracy wymaga odstąpienia od tej zasady.

VIII. Kontrola dostępu do sieci komputerowej.

1. Każda stacja (i konto) użytkownika podłączona do sieci ma z góry określoną politykę dostępu do Internetu i pozostałych sieci.
2. Zaleca się, aby każda droga połączenia z Internetem przechodziła przez zaporę urządzenia UTM, które filtruje ruch sieciowy.
3. Dla systemów zawierających dane wrażliwe zaleca się stworzenie wydzielonej sieci.
4. Użytkownicy powinni mieć bezpośredni dostęp tylko do danych osobowych określonych we wniosku.

IX. Zasady postępowania dotyczące pracy na odległość oraz urządzeń przenośnych i nośników danych wynoszonych poza siedzibę Jednostki.

1. Zdalny dostęp do systemów informatycznych realizowany jest przez szyfrowane połączenie VPN tylko i wyłącznie po poprawnej identyfikacji i uwierzytelnieniu zdalnego użytkownika.
2. Zdalny dostęp do sieci jednostki poprzez VPN, ograniczony jest tylko do tych użytkowników, którym ten dostęp jest niezbędny do realizacji powierzonych zadań.
3. Podstawą do uzyskania zdalnego dostępu jest wniosek złożony do AD lub osoby działającej w jego imieniu oraz zapis w umowie, jeśli sprawa dotyczy podmiotu zewnętrznego.
4. Zgoda wyrażana jest przez AD, po uzyskaniu pozytywnej opinii Administratora Systemu Informatycznego oraz Inspektora Ochrony Danych.
5. AD/ASI prowadzą rejestr użytkowników zdalnych.
6. Wynoszenie urządzeń przenośnych będących własnością jednostki poza jego siedzibę może występować wyłącznie w ramach wykonywania obowiązków służbowych po wyrażeniu zgody przez AD i po wpisaniu ich do rejestru.
7. W przypadku utraty urządzenia należy niezwłocznie powiadomić przełożonego.
8. AD/ASI prowadzi ewidencję urządzeń, które mogą być wynoszone poza siedzibę jednostki.

X. Kontrola dostępu do pomieszczeń serwerowni i pomieszczeń technicznych.

1. Wydziela się strefę bezpieczeństwa w pomieszczeniach serwerowni i pomieszczeniach technicznych jednostki.
2. Znajdują się tam wszystkie serwery, które przechowują zasoby informatyczne oraz urządzenia sieciowe.
3. Dostęp do tych pomieszczeń mają tylko uprawnieni pracownicy jednostki.
4. Inne osoby mogą przebywać w tych pomieszczeniach tylko w obecności osób uprawnionych.
5. W strefie wydzielonej należy stosować następujące mechanizmy bezpieczeństwa:
   a. drzwi i okna antywłamaniowe;
   b. czujniki włamaniowe - alarm;
   c. monitoring warunków klimatycznych;
   d. monitoring wizyjny;
   e. zarządzanie kluczami zapasowymi.
6. Strefa bezpieczeństwa jest obszarem ograniczonego dostępu nie przeznaczonym do ciągłej pracy ludzi. Zabrania się przechowywania tam innych sprzętów lub rzeczy nie związanych z wykonywaniem zadań.

XI. Procedura przeglądu uprawnień do systemów.

1. W celu utrzymania efektywnej kontroli nad dostępem do danych i systemów informatycznych Administrator Systemu Informatycznego dokonuje przeglądu praw użytkowników do systemów.
2. Przegląd uprawnień do systemów jest wykonywany przynajmniej raz w roku oraz w przypadku dużych zmian kadrowych, a także w dowolnym czasie na wniosek Inspektora ochrony danych.
3. Przegląd musi obejmować zarówno konta zwykłych użytkowników, jak i konta o uprawnieniach administracyjnych i awaryjnych.
4. Danymi wejściowymi są informacje o zmianach kadrowych.
5. Wynikiem przeglądu jest aktualizacja danych o uprawnieniach potwierdzona sporządzeniem notatki przez Administratora Systemu Informatycznego.

Załącznik nr 1
Procedury Kontroli Dostępu

WNIOSEK
O ZAŁOŻENIE / ZMIANĘ KONTA* W SIECI KOMPUTEROWEJ.

1. **Wnioskodawca:**

Imię i nazwisko: ……

Stanowisko służbowe: ……

2. **Główny użytkownik stanowiska:**

Imię i nazwisko: ……

Stanowisko służbowe: ……

3. Lokalizacja stanowiska (budynek, piętro, pokój):
   ……
4. Przeznaczenie stanowiska (należy podać wszystkie zasoby sieci komputerowej, do których stanowisko ma mieć dostęp).

   ……
   ……
5. Miejsca korzystania z konta:

LP	LOKALIZACJA STANOWISKA ROBOCZEGO (BUDYNEK, PIĘTRO, POKÓJ)

…… ……

Data Pieczątka i podpis Wnioskodawcy

* - niepotrzebne skreślić

Załącznik nr 2
Procedury Kontroli Dostępu

WNIOSEK
O ZAŁOŻENIE / ZMIANĘ / LIKWIDACJĘ* KONTA W ZASOBACH INFORMATYCZNYCH

1. **Dane wnioskodawcy:**

Imię i nazwisko: ……
Stanowisko służbowe: ……

2. **Dane osoby, która jest/będzie użytkownikiem konta:**

Imię i nazwisko: ……
Stanowisko służbowe: ……
Nazwa konta: ……

3. **Przeznaczenie konta wpisać słowo „TAK" lub" NIE''):**
4. Poczta elektroniczna (email): ……
5. Dostęp do zasobów Internetu: ……
6. Inne usługi (podać jakie wraz z uzasadnieniem celowości):

……
……

7. Termin likwidacji konta (w przypadku konta czasowego lub wniosku o likwidację konta):

……

…… ……
Data Pieczątka i podpis Wnioskodawcy

* - niepotrzebne skreślić

Załącznik nr 2 do PB

P_02	**PROCEDURA TWORZENIA KOPII ZAPASOWYCH.**	Wydanie: 01
		Data: 25.05.2018 r.

I. Definicje pojęć stosowanych w dokumencie:

1. **Administrator Systemu Informatycznego (ASI) / Informatyk** - wyznaczony pracownik lub firma zewnętrzna realizująca obsługę IT jednostki, odpowiedzialny za realizację zadań związanych z zarządzaniem systemem informatycznym, w tym za zabezpieczenie sieci komputerowej tzn. wdrażanie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów infrastruktury informatycznej oraz ochrony danych przed nieuprawnioną modyfikacją, zniszczeniem, dostępem i ujawnieniem, a także ich utratą.
2. **Stanowisko** - pojedynczy komputer osobisty przeznaczony do określonych zadań związanych między innymi z dostępem do sieci komputerowej jednostki.
3. **System informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
4. **Zasoby informatyczne** - ogół systemów informatycznych wykorzystywanych przez daną organizację
5. **Kopia zapasowa** - kopia danych lub oprogramowania. Celem jej wykonywania jest odtworzenie systemu po awarii.

II. Cel procedury.

Procedura Tworzenia Kopii Zapasowych określa zasady tworzenia, przechowywania i testowania kopii zapasowych oraz odzyskiwania z nich danych i systemów informatycznych, w celu zapewnienia integralności i dostępności informacji oraz środków przetwarzania informacji.

III. Zakres stosowania.

1. Działania opisane w niniejszej procedurze obowiązują, we wszystkich działaniach jednostki.
2. Niniejsza procedura jest elementem Polityki Bezpieczeństwa ustanowionej w jednostce.

IV. Wykonywanie kopii systemów informatycznych.

1. Na potrzeby zachowania ciągłości działania systemów informatycznych i utrzymania integralności danych, wykonuje się następujące kopie zapasowe:
    a. Bazy danych na stacji roboczej;
    b. Pliki i katalogi na stacji roboczej;
2. Zaleca się, aby wykonywanie kopii zapasowych realizowane było codziennie w dni robocze.
3. Kopie tworzone są całościowo, następnie przyrostowo, tzn. kopiowane są pliki nowe i te których zawartość uległa zmianie.
4. Kopie zapasowe sporządza się również w następujących przypadkach:
    a. przed dokonaniem istotnej zmiany konfiguracyjnej (np. aktualizacji oprogramowania, ustawień systemowych);
    b. po przeprowadzeniu zmiany konfiguracyjnej (np. aktualizacji oprogramowania, ustawień systemowych, zmianie praw dostępu).
5. Kopie zapasowe, wykonane w danym dniu przechowywane są przez okres 2 miesięcy.

6. Po ustaniu użyteczności kopii zapasowej jest ona niezwłocznie usuwana.
7. Kopie zapasowe konfiguracji systemów operacyjnych serwerów wykowywane są za pomocą dedykowanego oprogramowania.
8. Miejscem przechowywania kopii zapasowych jest wydzielona macierz lub nośnik zewnętrzny, zlokalizowane w innym miejscu (budynku) niż są wykonywane.
9. Za prawidłowość tworzenia kopii zapasowych odpowiada Administrator Systemu Informatycznego lub osoba wskazana przez AD legitymująca się odpowiednią wiedzą techniczną.

V. Odzyskiwanie danych i systemów informatycznych z kopii zapasowych.

1. Odzyskiwanie danych z kopii zapasowych jest wykonywane w następujących przypadkach:
   - utraty całości lub części danych na stacji roboczej;
   - na wniosek organu kontrolnego (np.: Urzędu Ochrony Danych);
   - przy przenoszeniu danych na nową stację roboczą.
2. Odzyskiwanie całego systemu informatycznego jest wykonywane w wypadku awarii sprzętowej lub systemowej nośników danych, na których jest on zlokalizowany, uniemożliwiającej korzystanie z danego systemu.
3. Za odzyskiwanie danych z kopii zapasowych odpowiedzialny jest Administrator Systemu Informatycznego lub osoba wskazana przez AD legitymująca się odpowiednią wiedzą techniczną.

Załącznik nr 3 do PB

P_03	**PROCEDURA ZARZĄDZANIA RYZYKIEM W BEZPIECZEŃSTWIE INFORMACJI**	Wydanie: 01
		Data: 25.05.2018 r.

I. Definicje pojęć i skrótów stosowanych w procedurze:

- **Zasoby** – wszystko, co stanowi wartość, aktywa jednostki;
- **Zagrożenie** - zdarzenie, które może wywołać negatywne skutki, czynnik ryzyka;
- **Podatność** - aspekty, które mogą być wykorzystane przez/ sprzyjać powstaniu zagrożenia, słabość, przyczyna, słaby punkt;
- **Skutek** - efekt wystąpienia zagrożenia, następstwo;
- **Zmaterializowanie się ryzyka** - sytuacja, w której ryzyko zaistniało, wystąpienie ryzyka;
- **Zabezpieczenia** - rozwiązania, które zmniejszają ryzyko, mechanizmy kontroli, środki kontroli;
- **Ryzyko rezydualne** - ryzyko uwzględniające zabezpieczenia i ich skuteczność, ryzyko szczątkowe;
- **Ryzyko nieodłączne** - ryzyko nieuwzględniające zabezpieczeń;
- **STI** - system teleinformatyczny;
- **KZ** - krytyczne zasoby;
- **PB** – Polityka Bezpieczeństwa.
- **Postępowanie z ryzykiem** - to działania podejmowane w następstwie oceny ryzyka.

II. Cel ustanowienia procedury.

Celem Procedury Zarządzania Ryzykiem w bezpieczeństwie informacji jest wsparcie PB, w zakresie ograniczania do minimum ryzyka dla bezpieczeństwa danych osobowych w jednostce, a w szczególności określenie metodyki i zasad zarządzania ryzykiem.

III. Metodyka zarządzania ryzykiem.

1. Zgodnie z powszechnie stosowanymi metodykami i systemami zarządzania bezpieczeństwem, w tym bezpieczeństwem teleinformatycznym dla zaplanowania i realizowania adekwatnych działań zapewniających bezpieczeństwo teleinformatyczne niezbędne jest:
   - dokonanie inwentaryzacji zasobów;
   - określenie zasobów kluczowych;
   - przeprowadzenie oceny ryzyka;
   - podjęcie działań będących następstwem oceny ryzyka.
2. Ocena ryzyka obejmuje:
   - identyfikację ryzyka;
   - analizę ryzyka;
   - ewaluację ryzyka.
3. Zarządzanie ryzykiem obejmuje m.in. ocenę ryzyka i postępowanie z ryzykiem.

IV. Założenia do działań związanych z zarządzaniem ryzykiem oraz sprawozdawczością wynikającą z Polityki Bezpieczeństwa.

1. Przez STI rozumie się całość zasobów, w tym sprzęt i oprogramowanie niezbędne do prawidłowego świadczenia usługi lub usług, dla których stosuje się STI.
2. STI może mieć zastosowanie do realizacji procesów wewnętrznych i zewnętrznych.
3. Oceną ryzyka, jak również sprawozdawczością nie są objęte STI wykorzystywane przez jednostkę, których administratorem jest podmiot udostępniający system/usługę.
4. W celu efektywnego wykorzystania sił i środków szczegółowej ocenie ryzyka i sprawozdawczości będą poddane KZ.
5. Ocena ryzyka oraz działania z niej wynikające nie ograniczają się jedynie do zagrożeń natury technicznej i uwzględniają również zagrożenia generowane przez użytkowników STI oraz inne strony zainteresowane.
6. Na potrzeby oceny ryzyka i przygotowania sprawozdania zidentyfikowane ryzyka dzieli się na:
   - ryzyko wewnętrzne - ryzyko, które jest związane z wystąpieniem zagrożenia wewnętrznego lub takiego, na które jednostka ma wpływ (działanie albo zaniechanie pracownika, dostawcy, awaria urządzenia spowodowana złą eksploatacją itp.);
   - ryzyko zewnętrzne - ryzyko, które jest związane z wystąpieniem zagrożenia zewnętrznego (działanie cyberprzestępcy, działanie sił przyrody itp.).

V. Odpowiedzialność.

1. Odpowiedzialność za przeprowadzenie oceny ryzyka i przygotowanie sprawozdania podsumowującego wyniki oceny ryzyka ponosi Inspektor Ochrony Danych lub inna osoba wskazana przez Administratora Danych.
2. Odpowiedzialność za podejmowanie określonych działań w stosunku do zidentyfikowanego ryzyka ponoszą odpowiednio AD / ASI / IOD i osoby którym przypisano podjęcie odpowiedniego przeciwdziałania ryzyku.

VI. Sposób przeprowadzania oceny ryzyka.

1. Identyfikacja zbiorów, kategorii przetwarzanych danych oraz systemów teleinformatycznych służących do przetwarzania danych osobowych.
2. Wybór **Krytycznych Zasobów** (KZ) teleinformatycznych oraz zbiorów przetwarzanych w formie nieelektronicznej.
3. Podział zidentyfikowanych zasobów na: krytyczne i pozostałe.
4. Uwzględniane takich czynników jak:
   a. prawdopodobieństwo naruszenia praw lub wolności osób fizycznych, których dane przetwarzane są przez jednostkę;
   b. ciągłość działania oraz realizowania zadań jednostki, które na dzień obecny byłby niemożliwe do realizacji bez STI;
   c. możliwość realizowania konstytucyjnych praw i obowiązków obywatela;
   d. zaufanie i ocena jednostki.

VII. Identyfikacja ryzyka.

1. Identyfikacja zagrożeń związanych z KZ.

1.1. Dla każdego z KZ należy zidentyfikować związane z nim zagrożenia, które mogą spowodować m.in.;
   a. niedostępność usług;
   b. nieuprawniony dostęp do danych / kradzież danych;
   c. nieuprawnioną modyfikację danych;
   d. zniszczenie danych.

1.2. Na etapie identyfikacji zagrożeń sporządzana jest lista zidentyfikowanych zagrożeń. Identyfikacja zagrożeń dokonywana jest z zastosowaniem m.in. pracy zespołowej (z wykorzystaniem burzy mózgów i innych narzędzi wspomagających pracę zespołową), lub kwestionariuszy i ankiet. Przy Identyfikacji zagrożeń wykorzystywane są m.in.:
   a. prowadzony rejestr incydentów;
   b. wyniki audytów i kontroli;
   c. fachowa literatura;
   d. specjalistyczne fora internetowe.
   e. informacje udostępniane przez producentów oprogramowania i sprzętu.

1.3. Przykładowe zagrożenia dotyczące bezpieczeństwa teleinformatycznego wymieniono w załączniku nr 1 do niniejszej Procedury.

2. Wybór kluczowych zagrożeń.

2.1. W celu skoncentrowania oraz efektywnego wykorzystania sił i środków wybierane są w jednostce zagrożenia kluczowe, których liczba waha się od kilku do kilkunastu.

2.2. Dokonanie selekcji zagrożeń odbywa się przez podjęcie arbitralnej decyzji osoby odpowiedzialnej za KZ.

2.3. Dopuszcza się również dokonanie wyboru zespołowo, stosując np. głosowanie, ocenę punktową.

2.4. Przeanalizowanie zagrożeń pod względem ich skutków i prawdopodobieństwa wystąpienia.

2.5. Analiza skutków zagrożeń uwzględnia:
   a. skutki - związane z naruszenia praw lub wolności osób fizycznych;
   b. skutki - finansowe dla jednostki;
   c. skutki - związane z nierealizowaniem zadań jednostki;
   d. skutki - związane z zaufaniem i opinią na rynku.

2.6. Analiza prawdopodobieństwa wystąpienia zagrożeń, tam, gdzie ma to zastosowanie, uwzględnia:
   a. dane historyczne (informacje o zmaterializowaniu ryzyka w jednostce i otoczeniu);
   b. zabezpieczenia i ich skuteczność (w tym przeciwdziałające, detekcyjne, dające możliwość skutecznej reakcji po wykryciu);
   c. podatności (występujące słabości);
   d. ekspozycję (czas dostępności, liczba użytkowników, liczba operacji, dostępność przez Internet);
   e. atrakcyjność zasobu (m.in. korzyść materialna, prestiż, korzyść polityczna dla potencjalnego cyberprzestępcy związana z naruszeniem bezpieczeństwa);
   f. potencjalny agresor, jego wiedza, motywacja i zasoby.

VIII. Analiza ryzyka.

1. Ocena skutków zagrożeń i prawdopodobieństwa ich wystąpienia.

1.1. Zgromadzone dane na temat skutków i prawdopodobieństwa, oceniane są z zastosowaniem poniższej skali punktowej:

- **Skala oceny skutków** - poniżej znajduje się macierz, która ma ułatwić ocenę skutku na właściwym poziomie. Każde zagrożenie analizowane jest pod kątem skutków w czterech aspektach (naruszenie praw i wolności osób, finanse, funkcje i zadania jednostki, zaufanie i opinia jednostki).

  W celu ułatwienia i zapewnienia obiektywnej i wyważonej oceny skutków, dla poszczególnych aspektów przyjęto charakterystyki przypisane do odpowiednich poziomów punktowych. Ocena punktowa skutku wyrażana jest jako jedna wartość w przedziale od 1 do 5, co oznacza odpowiednio skutek oceniony jako nieznaczny (1) do bardzo duży (5).

  Możliwe jest wystąpienie zagrożenia, które nie będzie oddziaływało na wszystkie cztery aspekty, przykładowo nie będzie oddziaływało na aspekt finansowy, ale jego wpływ np. na naruszenie praw i wolności osób spowoduje wysoką (4 albo 5 punktów) ocenę skutków. Może również wystąpić sytuacja, w której dane zagrożenie będzie niosło za sobą skutki, dla których opis trzech aspektów będzie wskazywał na ocenę na poziomie 1 (np. straty poniżej 100 000, krótkie i nieznaczne zakłócenia w realizacji funkcji i zadań jednostki, nieznaczna utrata zaufania), natomiast bardzo wysoka ocena w jednym aspekcie (np. naruszenie praw i wolności osób) spowoduje całościową ocenę skutków na poziomie 4 czy nawet 5 punktów.

  Ocenę skutków można przeprowadzić stosując metody matematyczne np. dokonanie oceny punktowej w poszczególnych aspektach i wyliczenia średniej. Jednakże wyrażona punktowo ocena jest wynikiem analizy, zaś poniższa macierz ma charakter jedynie wspomagający. Określając wartość skutku, zakładany jest możliwy, ale najbardziej negatywny scenariusz wystąpienia zagrożenia.

Ocena	Poziom (S)	Skutki związane z naruszeniem praw i wolności osób, których dane są przetwarzane	Skutki finansowe dla jednostki	Skutki związane z nierealizowaniem funkcji i zadań jednostki	Skutki związane z zaufaniem i opinią dot. jednostki
1	NIEZNACZNY	Nieznaczne naruszenie	Straty nieznacznie wpływające na działanie jednostki.	Krótkotrwałe i nieznaczne zakłócenia w realizacji funkcji i zadań	Nieznaczna utrata zaufania i opinii
2	MAŁY	Niewielkie naruszenie	Straty mające mały wpływ na działanie jednostki.	Niewielkie zakłócenia w realizacji funkcji i zadań	Niewielka utrata zaufania i opinii
3	ŚREDNIE	Poważne naruszenie	Straty średnio wpływające na działanie jednostki.	Poważne zakłócenia w realizacji funkcji i zadań	Poważna utrata zaufania i opinii
4	DUŻY	Poważne i trwałe naruszenie	Straty mające duży wpływające na działanie jednostki.	Poważne i trwałe zakłócenia w realizacji funkcji i zadań	Poważna i trwała utrata zaufania i opinii
5	BARDZO DUŻY	Bardzo poważne naruszenie praw i wolności	Straty paraliżujące działalność jednostki.	Poważny i długotrwały brak realizacji funkcji i zadań	Poważna i długotrwała utrata zaufania i opinii

Przy ocenie skutków uwzględniane są zabezpieczenia, które mają zastosowanie do zmniejszenia skutków.

- **Skala oceny prawdopodobieństwa -** przy ocenie prawdopodobieństwa, analizowane jest zagrożenie, uwzględniające charakterystyki umieszczone w kolumnie „Opis wspomagający". W przypadku wystąpienia sytuacji, w której poszczególne charakterystyki występują w różnych przedziałach punktowych, ocena oparta jest na osądzie oceniających prawdopodobieństwo. W przypadku oceny danych historycznych, uwzględniane są dane posiadane w jednostce, jak również informacje z otoczenia. Analiza podatności uwzględnia znane i występujące w rzeczywistości podatności. W sytuacji, w której jedna albo więcej charakterystyk nie ma miała zastosowania nie jest uwzględniana, np. zagrożenie może nie być wywołane celowym działaniem pracownika lub innej strony zainteresowanej (nie ma zastosowania charakterystyka - cyberprzestępca).

OCENA	POZIOM (P)	OPIS WSPOMAGAJĄCY
1	BARDZO MAŁO PRAWDOPODOBNE	Dane historyczne: Nie występuje Zabezpieczenia: Liczne i bardzo skuteczne Podatności: Brak Atrakcyjność: Bardzo mała Ekspozycja: Nieistotna Cyberprzestępca: Przypadkowy
2	MAŁO PRAWDOPODOBNE	Dane historyczne: Bardzo nieliczne wystąpienia Zabezpieczenia: Liczne i skuteczne Podatności: Bardzo nieliczne Atrakcyjność: Mała Ekspozycja: Bardzo małe znaczenie Cyberprzestępca: Nieprofesjonalny, mający małą wiedzę
3	PRAWDOPODOBNE	Dane historyczne: Nieliczne wystąpienia Zabezpieczenia: Liczne i częściowo skuteczne Podatności: Nieliczne Atrakcyjność: Średnia Ekspozycja: Małe znaczenie Cyberprzestępca: Profesjonalny, mający odpowiednią wiedzę
4	BARDZO PRAWDOPODOBNE	Dane historyczne: Wystąpienia Zabezpieczenia: Nieliczne i mało skuteczne Podatności: Liczne Atrakcyjność: Duża Ekspozycja: Duże znaczenie Cyberprzestępca: Profesjonalny, mający odpowiednią wiedzę i zmotywowany
5	PEWNE	Dane historyczne: Liczne wystąpienia Zabezpieczenia: Brak albo nieliczne i nieskuteczne Podatności: Bardzo liczne Atrakcyjność: Bardzo duża Ekspozycja: Bardzo duże znaczenie Cyberprzestępca: Profesjonalny, mający odpowiednią wiedzę, zmotywowany i wyposażony w niezbędne zasoby, w tym finansowe

2. Ustalenie poziomu ryzyka.

Poziom ryzyka (PR) jest obliczany jako iloczyn skutków (S) i prawdopodobieństwa (P), tj. PR= S x P

3. **Ewaluacja ryzyka dokonywana jest według poniższej tabeli.**

KRYTERIA		EWALUACJA RYZYKA
WARTOŚĆ PUNKTOWA PR	**POZIOM RYZYKA**	
1 - 5	**Małe**	Akceptowalne
6 - 9	**Średnie**	Akceptowalne, wymagające decyzji AD i Inspektora ochrony danych
10 - 16 oraz 5 gdzie: P = 1, a S = 5	**Duże**	Nieakceptowalne, wymagające decyzji AD i Inspektora ochrony danych w zakresie dalszego postępowania z ryzykiem
18 - 25	**Bardzo Duże**	Nieakceptowalne, wymagające decyzji Administratora Danych w zakresie dalszego postępowania z ryzykiem

IX. Podjęcie decyzji dotyczącej postępowania z ryzykiem.

1. W stosunku do ryzyka podejmowane są następujące decyzje:

- zapobieganie, czyli działania polegające na zmniejszeniu poziomu ryzyka;
- przeniesienie ryzyka na inną jednostkę (przenosząc ryzyko, należy pamiętać, że jego przeniesienie najczęściej nie zmniejsza odpowiedzialności za jego wystąpienie, co ma istotne znaczenie z punktu widzenia działania jednostki);
- unikanie, czyli m.in. zaprzestanie działań powodujących ryzyko;
- tolerowanie (akceptowanie) ryzyka w przypadku, gdy istnieją określone trudności w przeciwdziałaniu ryzykom lub gdy koszty planowanych działań doskonalących mogą przekroczyć przewidywane korzyści.

X. Monitorowanie ryzyka.

2. Podstawowym celem monitorowania ryzyka jest uzyskanie potwierdzenia, że wdrożona procedura jest skuteczna.
3. Równie ważne jest wykrywanie sytuacji, gdy środki ochrony są niewystarczające bądź funkcjonowanie procedury jest poniżej przyjętych standardów.
4. W obu przypadkach konieczne jest podejmowanie zdecydowanych działań doskonalących.
5. Proces monitorowania ryzyka składa się z następujących elementów:
    a. Wejście: wszystkie uzyskane informacje z systemu zarządzania ryzykiem,
    b. Działanie: obserwacja ryzyka i czynników ryzyka,
    c. Wyjście: ciągłe dostrajanie systemu zarządzania ryzykiem.
6. Proces monitorowania ryzyka ma charakter ciągły.
7. Podczas etapu monitorowania powinny być zbierane również informacje o tym, jak zmieniają się ryzyka:
    - Czy zmieniły się zagrożenia?
    - Czy zmieniły się podatności?
    - Czy zmieniło się prawdopodobieństwo wystąpienia ryzyka?
    - Czy zmienił się wpływ skutków zaistniałego ryzyka?
    - Czy działania dla złagodzenia ryzyka są nadal odpowiednie?

XI. Informowanie o ryzyku.

1. Komunikowanie ryzyka polega na wzajemnej wymianie informacji dotyczących ryzyka, między odpowiedzialnymi za zarządzanie ryzykiem, a zainteresowanymi stronami.
2. Powinno prowadzić do wzrostu świadomości ryzyka wśród pracowników jednostki, co może wspierać naturalne mechanizmy kontroli wewnętrznej.

XII. Działania związane z zarządzaniem ryzykiem.

1. Na podstawie przedstawionej powyżej metodyki przynajmniej raz w roku podczas przeglądu PB oraz po każdej istotnej zmianie w jednostce mogącej mieć wpływ na ryzyko, dokonuje się identyfikacji i oceny ryzyka oraz określa metody przeciwdziałania ryzyku.
2. Wykonywany jest także przegląd procesu zarzadzania ryzykiem w celu jego usprawnienia.
3. Na podstawie wyników powyższych działań sporządza się arkusz sprawozdania podsumowującego wyniki analizy ryzyka zgodnie z wzorem stanowiącym Załącznik nr 2 do niniejszej Procedury.
4. Jednocześnie stale realizowany jest proces monitorowania ryzyka.
5. Podstawowym źródłem danych do monitorowania ryzyka jest proces zarządzania incydentami związanymi z bezpieczeństwem informacji.

Załącznik nr 1
do Procedury Zarządzania Ryzykiem

PRZYKŁADOWE ZAGROŻENIA DOTYCZĄCE BEZPIECZEŃSTWA INFORMACJI.

1. Zainstalowanie złośliwego oprogramowania (m.in. wirusy, robaki, bomby logiczne, konie trojańskie) przez korespondencję elektroniczną.
2. Zainstalowanie złośliwego oprogramowania (m.in. wirusy, robaki, bomby logiczne, konie trojańskie) przez stronę www.
3. Zainstalowanie złośliwego oprogramowania (m.in. wirusy, robaki, bomby logiczne, konie trojańskie) przez nośniki zewnętrzne.
4. Zainstalowanie złośliwego oprogramowania (m.in. wirusy, robaki, bomby logiczne, konie trojańskie) w instalowanym oprogramowaniu.
5. Zainstalowanie złośliwego oprogramowania (m.in. wirusy, robaki, bomby logiczne, konie trojańskie) w trakcie naprawy lub serwisu.
6. Wykorzystanie luk w systemach urządzeń mobilnych.
7. Atak zewnętrzny ograniczający dostęp typu DDoS.
8. Przejęcie informacji przesyłanych pocztą elektroniczną.
9. Podsłuchanie informacji przesyłanych siecią radiową (informatyczną)
10. Podsłuchanie informacji przesyłanych siecią tradycyjną.
11. Włamanie do STI.
12. Atak socjotechniczny w celu przejęcia danych (phishing).
13. Przekierowanie – pharming.
14. Nieuprawniony fizyczny dostęp do urządzeń.
15. Nieuprawniony dostęp do nośników danych (m.in. optycznych, magnetycznych).
16. Brak zasilania energetycznego.
17. Zalanie wodą lub innymi substancjami z instalacji wewnętrznych.
18. Pożar.
19. Powódź.
20. Przegrzanie sprzętu.
21. Awaria sprzętu.
22. Zły stan techniczny sprzętu.
23. Niewydolne urządzenia (zbyt wolne, nieodpowiadające wymaganiom programowym).
24. Niestabilność łącza w usłudze dostępu do internetu.
25. Niewystarczająca przepustowość łącza w usłudze dostępu do internetu.
26. Używanie oprogramowania niemającego wsparcia producenta.
27. Kradzież sprzętu z siedziby jednostki.
28. Kradzież sprzętu mobilnego.

29. Podejrzenie informacji w siedzibie jednostki.
30. Podejrzenie informacji przetwarzanej na sprzęcie mobilnym.
31. Błędy uprawnionych użytkowników - niezapisanie danych.
32. Błędy uprawnionego użytkownika - skasowanie danych.
33. Błąd uprawnionego użytkownika - wysłanie informacji pocztą elektroniczną do nieuprawnionej osoby.
34. Błąd uprawnionego użytkownika - administratora - błędna konfiguracja dająca nadmierne uprawnienia.
35. Celowe działanie uprawnionych użytkowników - zniszczenie informacji.
36. Celowe działanie uprawnionych użytkowników - sprzedaż informacji.
37. Celowe działanie uprawnionych użytkowników – sabotaż.
38. Celowe działanie uprawnionych użytkowników - nadużycie uprawnień.
39. Celowe działanie - zniszczenie sprzętu.
40. Brak świadomości użytkowników STI na temat ryzyk (zagrożeń, podatności, skutków).
41. Brak znajomości zasad i procedur bezpieczeństwa.
42. Zbyt rzadko zmieniane hasła.
43. Zbyt słabe hasła.
44. Zbyt często zmieniane hasła.
45. Nieprzestrzeganie przez użytkowników STI zasad i procedur bezpieczeństwa.
46. Nieprawidłowe zarządzanie uprawnieniami użytkowników - nadanie nadmiernych uprawnień.
47. Nieprawidłowe zarządzanie uprawnieniami użytkowników (brak cofnięcia albo zbyt późne cofnięcie uprawnień).
48. Źle skonfigurowane, w tym otwarte porty.
49. Źle skonfigurowane systemy operacyjne.
50. Brak zabezpieczeń protokołów komunikacyjnych.
51. Kradzież zbiorów danych „szczególnych”.
52. Kradzież zbiorów danych „zwykłych”.
53. Zniszczenie zbiorów danych „szczególnych”.
54. Zniszczenie zbiorów danych „zwykłych”.
55. Udostępnienie zbiorów danych przetwarzanych w formie papierowej osobom nieuprawnionym.

Załącznik nr 2
do Procedury Zarządzania Ryzykiem

RAPORT Z OCENY RYZYKA I DOBORU ŚRODKÓW BEZPIECZEŃSTWA

KZ	Identyfikacja ryzyka			Analiza ryzyka			Ewaluacja ryzyka	Sposób postępowania z ryzykiem przyjętym w jednostce
	Rodzaj ryzyka	Zdarzenie (dodatkowo można krótko opisać jego skutki i prawdopodobieństwo)	Podatność	Ocena (S)	Ocena (P)	Poziom ryzyka = S x P		

1. **Proponowane działania zmniejszające ryzyko.**

……

2. **Informacje dodatkowe o środkach bezpieczeństwa TI oraz fizycznego stosowanych w Jednostce.**

……

……

Administrator Danych

Załącznik nr 4 do PB

P_04	**PROCEDURA** **ZARZĄDZANIA INCYDENTAMI ZWIĄZANYMI Z BEZPIECZEŃSTWEM DANYCH OSOBOWYCH.**	Wydanie: 01 Data: 25.05.2018 r.

I. Definicje pojęć stosowanych w procedurze.

1. **Administrator Systemu Informatycznego (ASI) / Informatyk** - wyznaczony pracownik lub firma zewnętrzna realizująca obsługę IT jednostki, odpowiedzialny za realizację zadań związanych z zarządzaniem systemem informatycznym, w tym za zabezpieczenie sieci komputerowej tzn. wdrażanie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów infrastruktury informatycznej oraz ochrony danych przed nieuprawnioną modyfikacją, zniszczeniem, dostępem i ujawnieniem, a także ich utratą.
2. **Inspektor Ochrony Danych** – osoba powołana przez administratora na podstawie kwalifikacji i doświadczenia odpowiadająca za przestrzeganie procedur w zakresie danych osobowych i zgłoszona do Urzędu Ochrony Danych.
3. **Stanowisko** - pojedynczy komputer osobisty lub terminal przeznaczony do określonych zadań związanych między innymi z dostępem do sieci komputerowej jednostki.
4. **System informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
5. **Zasoby informatyczne** - ogół systemów informatycznych wykorzystywanych przez daną organizację.
6. **Incydent związany z bezpieczeństwem informacji** - pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań statutowych organizacji i zagrażają bezpieczeństwu informacji.
7. **Podatność** - słabość systemu informatycznego, która może być wykorzystana przez co najmniej jedno zagrożenie.

II. Cel procedury.

Celem Procedury Zarządzania Incydentami Związanymi z Bezpieczeństwem danych osobowych jest zapewnienie, że zdarzenia związane z bezpieczeństwem informacji oraz słabości systemów informacyjnych, są zgłaszane w sposób umożliwiający szybkie podjęcie działań korygujących.

III. Zakres stosowania.

Działania opisane w niniejszej procedurze obowiązują, we wszystkich komórkach organizacyjnych jednostki.

IV. Odpowiedzialność.

1. Odpowiedzialność za prawidłowe zgłoszenie incydentów dotyczących bezpieczeństwa infrastruktury informatycznej spoczywa na pracownikach dokonujących zgłoszeń.

2. Każdy pracownik odpowiedzialny za rozwiązanie problemu lub zapobieżenie incydentowi działa zgodnie z niniejszą procedurą.
3. **Inspektor Ochrony Danych/ ASI są odpowiedzialni za:**
   a. Niezwłoczne reagowanie na incydenty naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób;
   b. Ocenę istniejących i potencjalnych zagrożeń w zakresie bezpieczeństwa danych osobowych.
   c. Ocenę przyczyn i skutków incydentów naruszenia bezpieczeństwa danych osobowych w tym gromadzenie materiału dowodowego;
   d. Przygotowywanie propozycji działań korygujących i naprawczych oraz nadzór nad ich wprowadzaniem;
   e. Dokonywanie okresowego przeglądu i aktualizacji Polityki Bezpieczeństwa.
   f. Prowadzenie działań zmierzających do wzrostu świadomości w zakresie zapewnienia bezpieczeństwa danych osobowych;
   g. Zarządzanie ryzykiem zgodnie z procedurą stanowiącą załącznik nr 3 do Polityki Bezpieczeństwa.

V. Klasyfikacja incydentów.

1. Podział zdarzeń:
   a. Zdarzenia losowe zewnętrzne (np.: klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej, ciągłość pracy systemów zostaje zakłócona, nie dochodzi do naruszenia poufności danych.
   b. Zdarzenia losowe wewnętrzne (np.: niezamierzone pomyłki operatorów, administratorów, awarie sprzętowe, błędy w oprogramowaniu), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych.
   c. Zdarzenia zamierzone, świadome i celowe - stanowią najpoważniejsze zagrożenie naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zdarzenia te możemy podzielić na:
      - nieuprawniony dostęp do danych z zewnątrz (włamanie do systemu);
      - nieuprawniony dostęp do danych z sieci wewnętrznej;
      - nieuprawniony transfer danych;
      - pogorszenie funkcjonowania sprzętu i oprogramowania (np.: działanie wirusów);
      - bezpośrednie zagrożenie materialnych składników systemu (np.: kradzież sprzętu).
2. Przykłady zdarzeń które mogą być zakwalifikowane jako uzasadnione podejrzenie naruszenia bezpieczeństwa informacji:
   a. Sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na infrastrukturę teleinformatyczną jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.
   b. Niewłaściwe parametry środowiska jak zbyt wysoka temperatura lub nadmierna wilgotność (w szczególności dotyczy to serwerowni).

c. Awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie systemu, w tym sam fakt pozostawienia serwisantów bez nadzoru.
d. Pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu.
e. Jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikacje w systemie.
f. Naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie.
g. Stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji).
h. Nastąpiła niedopuszczalna manipulacja danymi w systemie.
i. Ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą elementy systemu zabezpieczeń.
j. Praca w systemie lub w sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych, np.: praca w systemie lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.
k. Ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. „bocznej furtki", itp.
l. Podmieniono lub zniszczono nośniki z danymi bez odpowiedniego upoważnienia lub w niedozwolony sposób skasowano lub kopiowano dane osobowe.
m. Rażąco naruszono dyscyplinę pracy w zakresie przestrzegania PBI (niewylogowanie się, pozostawienie włączonego komputera po zakończeniu pracy, nie zamknięcie pokoju z komputerem, niewykonywanie w ustalonych terminach kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.)
n. Stwierdzenie nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych, w tym także osobowych (otwarte szafy, regały, biurka).

VI. Zgłaszanie incydentów.

1. Pracownicy mają obowiązek zgłaszać zauważone przez siebie incydenty oraz notować wszystkie szczegóły związane z incydentem.
2. Zgłoszenie musi zawierać:
   - imię i nazwisko zgłaszającego,
   - miejsce i datę wystąpienia incydentu,
   - opis zdarzenia.
3. Zgłaszający incydent nie powinien podejmować żadnych działań na własną rękę jednak w miarę możliwości powinien zabezpieczyć materiał dowodowy, np.: robiąc zdjęcie ekranu komputera co do którego zaistniało podejrzenie, że jego działanie odbiega od normy. W przypadku podejrzenia istnienia wirusa komputerowego należy postępować zgodnie z Instrukcją w zakresie profilaktyki antywirusowej - załącznik nr 6 do Polityki Bezpieczeństwa.
4. Inspektor Ochrony Danych ocenia poziom istotności incydentu dla jednostki kierując się następującymi kryteriami:

- wpływ incydentu na ciągłość działania jednostki i wypełnianie jego zadań statutowych;
- krytyczność systemów dotkniętych skutkami incydentu naruszenia bezpieczeństwa;
- wrażliwość informacji, których poufność, integralność czy dostępność naruszono (np. czy naruszono bezpieczeństwo informacji prawnie chronionej - np.: danych osobowych, informacji niejawnych);
- rozległość wpływu incydentu na działanie systemów (np. nie działa jeden komputer, cała sieć itp.);
- rozmiar szkód będących skutkiem incydentu;
- prawdopodobieństwo naruszenia praw i wolności osób, których dane są przetwarzane
- koszt usunięcia i naprawy skutków incydentu naruszenia bezpieczeństwa;
- szacowany czas przywrócenia ciągłości działania dotkniętego incydentem bezpieczeństwa systemu;
- zasoby wymagane do przywrócenia ciągłości działania systemu (personel, wsparcie firm zewnętrznych, wymagane dodatkowe czy zamienne urządzenia oraz oprogramowanie, czas odtwarzania systemów z kopii zapasowych itp.);

VII. Postępowanie z incydentami.

1. Obsługa incydentu rozpoczyna się od jego dokładnego rozpoznania - ustalenia oznak naruszenia bezpieczeństwa, identyfikacji rodzaju incydentu, identyfikacji i zabezpieczenia dowodów oraz poinformowania o zdarzeniu odpowiednich osób:
2. Pracownik powiadamia niezwłocznie ASI lub IOD fakcie i treści incydentu.
3. Po analizie zdarzenia i okoliczności z nim związanych IOD wprowadza dane o incydencie do rejestru incydentów oraz zabezpiecza materiał dowodowy.
4. Inspektor Ochrony Danych dokonuje analizy materiału dowodowego i podejmuje decyzję o sposobie dalszego postępowania, o powyższym powiadamia Administratora Danych.
5. Gromadzenie materiału dowodowego:
   - dla dokumentów papierowych: oryginał jest bezpiecznie przechowywany wraz z informacją, kto znalazł dokument, gdzie, kiedy i kto by był świadkiem tego zdarzenia; każde śledztwo może wykazać, że oryginał nie został naruszony;
   - dla dokumentów na nośnikach komputerowych zaleca się: utworzenie obrazu lub kopii (zależnie od stosownych wymagań) wszelkich nośników wymiennych; zaleca się zapisanie informacji znajdujących się na dyskach twardych lub w pamięci komputera, aby zapewnić ich dostępność, zaleca się zachowanie zapisów wszelkich działań podczas procesu kopiowania oraz aby proces ten odbywał się w obecności świadków; zaleca się przechowywanie;
   - oryginalnego nośnika i dziennika zdarzeń w sposób bezpieczny i nienaruszony (jeśli to niemożliwe, to co najmniej jeden obraz lustrzany lub kopię).
6. W przypadku stwierdzenia działań umyślnych i ustaleniu sprawcy incydentu Inspektor Ochrony Danych przekazuje wyniki analizy wraz z zabezpieczonym materiałem dowodowym AD w celu wyciągnięcia konsekwencji dyscyplinarnych wobec sprawcy lub podjęcia kroków prawnych wobec osób trzecich.

7. Inspektor Ochrony Danych wyciąga wnioski z każdego incydentu i określa, jeśli to możliwe działania korygujące i zapobiegawcze w celu uniknięcia ponownego wystąpienia incydentu.
8. Administrator Danych bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je do Urzędu Ochrony Danych, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.
9. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

VIII. Szkolenia.

1. Brak wiedzy i umiejętności poprawnego rozpoznania i klasyfikacji oraz oceny poziomu istotności incydentu po stronie zgłaszającego nie może być przyczyną zaniechania powiadomienia IOD / ASI o zaistniałym incydencie lub podejrzeniu jego wystąpienia.
2. Dlatego w miarę posiadanych zasobów, należy przeprowadzać okresowe szkolenia pracowników w zakresie zarządzania incydentami.
3. Niezależnie od prowadzonych szkoleń wskazane jest przeprowadzanie szkolenia każdego nowozatrudnionego pracownika celem zapewnienia znajomości zasad prawidłowego zgłaszania incydentów.

Załącznik nr 5 do PB

P_05	**PROCEDURA PROFILAKTYKI ANTYWIRUSOWEJ.**	Wydanie: 01
		Data: 25.05.2018 r.

Profilaktyka antywirusowa w systemach informatycznych użytkowanych w sieci komputerowej jednostki.

1. Osobą prowadzącą działania profilaktyczne mające na celu ochronę zasobów sieci komputerowej przed atakami wirusów komputerowych jest Administrator Systemu Informatycznego.
2. Administrator Systemu Informatycznego wykorzystuje następujące funkcje systemowe:
   a. Rejestracja i śledzenie informacji o dostępach lub próbach dostępu do zasobów i usług danego systemu;
   b. Rejestracja i śledzenie komunikatów o błędach w pracy systemu;
   c. Szyfrowanie i uwierzytelnianie informacji przesyłanych w sieci;
   d. Wykrywanie obecności fałszywego oprogramowania w danych wpływających do systemu z sieci;
   e. Kontrola integralności oprogramowania zainstalowanego w systemie.
3. Ochrona antywirusowa zasobów informatycznych jest realizowana przez system antywirusowy posiadający następujące funkcje:
   a. Zabezpieczenie zasobów informatycznych przed wirusami komputerowymi za pomocą modułu rezydentnego, skanującego na bieżąco wszystkie zasoby komputera;
   b. Aktualizację baz sygnatur wirusów na bieżąco;
   c. Możliwość automatycznego podejmowania działań w przypadku pojawienia się nowych, nieznanych wirusów (np.: zablokowanie komunikacji z zawirusowanym komputerem).
4. Aktualizacja baz sygnatur wirusów:
   a. Bazy sygnatur wirusów dla serwera są aktualizowane bezpośrednio z serwera producenta systemu antywirusowego;
   b. Bazy sygnatur wirusów dla stanowisk roboczych są aktualizowane bezpośrednio z serwera producenta systemu antywirusowego;
   c. Aktualizacja baz sygnatur wirusów odbywa się nie rzadziej niż jeden raz każdego dnia roboczego.
5. Kontrola antywirusowa.
   a. Zasoby informatyczne są skanowane na bieżąco za pomocą modułu rezydentnego;
   b. Kontroli podlegają wszystkie pliki (odczytywane i zapisywane) w tym poczta elektroniczna;
   c. System antywirusowy jest zaprogramowany do wykonywania okresowych kontroli antywirusowych całego systemu plików;
   d. Kontrole te są wykonywane przez program automatycznie nie rzadziej niż jeden raz w tygodniu;
   e. Zabrania się korzystania ze stanowiska bez aktywnego programu antywirusowego.

Zasady ogólne ochrony przed szkodliwym oprogramowaniem.

1. Zidentyfikowanymi obszarami systemu informatycznego jednostki narażonymi na ingerencję wirusów oraz innego szkodliwego oprogramowania są dyski twarde lub karty pamięci urządzeń, pamięć RAM oraz nośniki informacji.
2. Drogą przedostania się wirusów lub szkodliwego oprogramowania może być sieć publiczna, wewnętrzna sieć teleinformatyczna lub elektroniczne nośniki informacji.
3. Stacje robocze, sprzęt mobilny oraz serwery objęte są ochroną w czasie rzeczywistym za pomocą oprogramowania antywirusowego oraz zapory firewall, zapewniających integralność zasobów przechowywanych i przetwarzanych w placówce.
4. Oprogramowanie antywirusowe uruchamiane jest przy starcie systemu, a użytkownik nie posiada uprawnień do jego wyłączenia.
5. Oprogramowanie antywirusowe musi być skonfigurowane w sposób wymuszający automatyczną aktualizację baz (wzorce wirusów) oraz nowych wersji programu antywirusowego.
6. Oprogramowanie antywirusowe musi być zainstalowane tak, aby użytkownik nie miał możliwości pominięcia etapu skanowania.
7. Każde oprogramowanie nie może być użyte bez wcześniejszego sprawdzenia przy pomocy odpowiedniego oprogramowania antywirusowego.
8. Nośniki nie mogą być użyte bez wcześniejszego sprawdzenia przy pomocy odpowiedniego programu antywirusowego.
9. W przypadku wykrycia wirusa komputerowego, użytkownik powinien zaprzestać wykonywania jakichkolwiek działań na urządzeniu oraz niezwłoczni powiadomić wydział odpowiedzialny za bezpieczeństwo i utrzymanie systemu informatycznego jednostki, który samodzielnie lub we współpracy z użytkownikiem podejmą działania w celu likwidacji zagrożenia.
10. Konfiguracja programu antywirusowego zapewnia ciągle monitorowanie otrzymanych i wysianych, a także uruchamianych plików pod katem występowania oprogramowania złośliwego.
11. W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy, ASI podejmuje działania zmierzające do usunięcia zagrożenia. W szczególności działania te mogą obejmować:
    a. Usunięcie zainfekowanych plików, o ile jest to akceptowalne ze względu na prawidłowe funkcjonowanie systemu informatycznego jednostki;
    b. Odtworzenie plików z kopii zapasowych, po uprzednim sprawdzeniu, czy informacje zapisane na kopiach zapasowych nie są zainfekowane;
    c. Samodzielną ingerencję w zawartość pliku - w zależności od posiadanych kwalifikacji lub konsultacje z odpowiednim serwisem.
12. Za instalację oraz aktualizację oprogramowania antywirusowego odpowiada ASI odpowiedzialny za bezpieczeństwo i utrzymanie systemu informatycznego jednostki. Za nadzór nad zapewnieniem ciągłości ochrony antywirusowej odpowiada ASI.
13. W przypadku sytuacji związanych z niezidentyfikowanym zagrożeniem należy bezwzględnie dostosować się do zaleceń ASI odpowiedzialnego za utrzymanie i bezpieczeństwo systemu informatycznego jednostki.

Zalecenia dla użytkowników stacji roboczych:

1. Zabrania się umieszczania w urządzeniach odczytujących dane na stanowisku (czytniki CD - ROM, DVD, porty USB itp.) nośników rozprowadzanych z różnego rodzaju czasopismami, materiałami reklamowymi itp.
2. Zabrania się bez zgody ASI używania na stanowisku pracy urządzeń do gromadzenia i przenoszenia danych, takich jak pamięci „flash" dołączane przez porty USB, karty radiowe, urządzenia „bluetooth", dyski wymienne, modemy nie będących własnością placówki.
3. Zabrania się wykorzystywania do celów służbowych bez zgody AD lub osoby przez niego upoważnionej innych, niż dopuszczone Polityce Bezpieczeństwa, systemów poczty elektronicznej.
4. Z uwagi na próby ataków na systemy użytkowników poprzez zainfekowanie poczty elektronicznej zaleca się zachowanie szczególnej ostrożności przy otwieraniu otrzymanych tą drogą załączników.
5. W przypadku otrzymania nieoczekiwanej przesyłki pocztowej, która zawiera załącznik lub odsyła do treści bezpośrednio do strony www zabrania się otwieranie załącznika oraz korzystanie bezpośrednio z przesłanych odnośników.
6. Zaleca się wyłączenie opcji auto podglądu załącznika w programie pocztowym Outlook.
7. Korzystając z programów MS Office (Word, Excel itp.) i podobnych należy, jeśli to możliwe, uaktywnić ich wewnętrzny system ochrony przed wirusami MAKRO.
8. Każdy nośnik danych, używany do przenoszenia danych pomiędzy stanowiskami komputerowymi, przed odczytaniem danych należy sprawdzić programem antywirusowym.

Postępowanie w przypadku ujawnienia lub podejrzenia istnienia wirusa:

1. Gdy zachowanie systemu komputerowego odbiega od normy (komunikaty o błędach, nieoczekiwane zniknięcie lub pojawienie się plików lub katalogów, spowolniona praca systemu, dziwne lub niezrozumiałe informacje pojawiające się na ekranie itp.) należy również przeprowadzić kontrolę antywirusową systemu.
2. Jeśli program antywirusowy stwierdził istnienie wirusa na nośniku danych, taki nośnik należy natychmiast wyjąć z czytnika (stacji dyskietek, czytnika DVD - ROM, USB itp.), wyraźnie oznaczyć i przekazać nośnik Administratorowi Systemu Informatycznego.
3. Po stwierdzeniu obecności wirusa w systemie przez program antywirusowy należy niezwłocznie zgłosić ten fakt do AD lub ASI.
4. Następnie ASI przeprowadza kontrolę antywirusową całego systemu.
5. Zabrania się samodzielnego usuwania zainfekowanych plików.
6. Użytkownik ma obowiązek zgłaszania do AD lub ASI wszelkich zauważonych niestandardowych zachowań systemu operacyjnego.

Załącznik nr 6 do PB

P_06	**REGULAMIN KORZYSTANIA Z KOMPUTERÓW SŁUŻBOWYCH.**	Wydanie: 01 Data: 25.05.2018 r.

Postanowienia ogólne

§ 1

Niniejszy regulamin ustala zasady:

1. Korzystania z komputerów służbowych;
2. Monitorowania pracy pracowników przy wykorzystaniu komputerów służbowych;
3. Wysyłania służbowej poczty elektronicznej;
4. Drukowania dokumentów;
5. Komunikacji w sieciach informatycznych.

§ 2

Celem wdrożenia regulaminu jest zachowanie równowagi pomiędzy uzasadnionym interesem pracownika / dziecka / rodzica do ochrony jego prywatności, a prawem do ochrony informacji prawnie chronionych przetwarzanych przez jednostkę, a w szczególności:

1. Poprawa jakości i zgodności z procedurami obowiązującymi w jednostce, wykonywania pracy przez pracowników;
2. Zabezpieczenie uzasadnionych interesów jednostki;
3. Zabezpieczenie danych oraz mienia jednostki.

Korzystanie z komputerów służbowych

§ 3

Zabronione jest wykorzystywanie przez pracownika komputera służbowego do celów prywatnych. W szczególności zabronione jest instalowanie i wykorzystywanie jakiegokolwiek oprogramowania bez wiedzy i udziału osób odpowiedzialnych za tego rodzaju czynności w jednostce.

§ 4

Działania Administratora Danych, zmierzają do poprawy jakości pracy z komputerem polegające w szczególności na eliminowaniu możliwości pobierania określonych danych z Internetu, odciążeniu sieci informatycznej poprzez ograniczenie możliwości transferu danych z lub do komputera pracownika, usuwaniu nielegalnego oprogramowania, blokowania dostępu do nielegalnej treści oraz kontroli antywirusowej nie wymagają zgody pracownika.

Ogólne zasady monitorowania

§ 5

Monitorowanie pracy pracowników przy wykorzystaniu komputerów służbowych jest dopuszczalne, o ile nie jest sprzeczne z przepisami prawa, w szczególności przepisami o ochronie danych osobowych i prawem pracowników do poszanowania ich dóbr osobistych.

§ 6

1. Nie jest dopuszczalne ukryte monitorowanie komputerów pracowników.
2. Kontrola jakościowa i ilościowa pracy przy komputerze może być wykonywana po poinformowaniu o tym pracownika.

Służbowa poczta elektroniczna

§ 7

1. Pracownik zabezpiecza dostęp do służbowej poczty elektronicznej (służbowego adresu e-mail) poprzez nadanie jej indywidualnego hasła ochronnego.
2. Pierwsze hasło jest nadawane pracownikowi przez ASI. Pracownik jest zobowiązany do zmiany hasła podczas pierwszego logowania się do służbowej poczty elektronicznej.
3. Pracownik ma obowiązek chronić hasło przed dostępem osób trzecich. W każdym przypadku, gdy hasło zostało ujawnione innej osobie, pracownik jest zobowiązany do jego zmiany.

§ 8

1. Pracownik może wykorzystywać służbową pocztę elektroniczną (służbowy adres email) wyłącznie do czynności związanych z wykonywaną pracą.
2. Nie jest dopuszczalne wykorzystywanie służbowej poczty elektronicznej (służbowego adresu e-mail) do celów prywatnych.
3. Zabronione jest wykorzystywanie prywatnej poczty elektronicznej (prywatnego adresu email) do celów służbowych.

§ 9

1. W celu kontroli treści służbowej korespondencji elektronicznej pracownika, Pracodawca może wprowadzić monitoring służbowej skrzynki poczty elektronicznej.
2. Może być dokonywana kontrola treści służbowej korespondencji elektronicznej pracownika.

§ 10

1. Drukarki nie mogą być pozostawione bez kontroli, jeśli są lub wkrótce będą drukowane na nich dane osobowe lub informacje z systemu informatycznego jednostki, o ile dostęp osób postronnych do tych drukarek nie jest odpowiednio ograniczony.
2. Drukowanie na drukarkach jest dopuszczalne o ile otoczenie drukarki jest chronione przed fizycznym dostępem osób nieupoważnionych.
3. Za przechowywanie wydruku zawierającego dane osobowe lub informacje z systemu informatycznego jednostki odpowiada wykonawca danego wydruku.
4. Wykonawca może przekazać wydruk oraz odpowiedzialność za jego przechowywanie innej osobie tylko wtedy, gdy jest ona upoważniona do dostępu do danych osobowych lub informacji zawartych na danym wydruku.
5. Wydruki zawierające dane osobowe z systemu informatycznego jednostki po zakończeniu pracy powinny być przechowywane w zamkniętych szafach.
6. Ogranicza się do niezbędnego minimum ilość wytwarzanych kopii i wydruków.
7. Zbędne wydruki, notatki, kopie dokumentów, itp., jeśli zawierają dane osobowe muszą być bezwzględnie niszczone w sposób uniemożliwiający odtworzenie ich treści.

§ 11

Komunikacja w sieciach komputerowych

1. Zabrania się przesyłania danych osobowych z systemu informatycznego jednostki osobom nieupoważnionym do dostępu do danych osobowych.
2. Wszystkie połączenia zewnętrzne do systemu informatycznego jednostki powinny być monitorowane.

§ 12

Bezpieczeństwo nośników i sprzętu mobilnego poza siedzibą jednostki (telefony i tablety służbowe)

1. Przemieszczanie nośników lub sprzętu mobilnego zawierających dane osobowe poza pomieszczenia, w których są one przetwarzane, wymaga stosowania środków ochrony gwarantujących ich zabezpieczenie przed nieuprawnionym dostępem i ich ujawnianiem.
2. Na użytkowniku nośnika lub sprzętu mobilnego użytkowanego poza siedzibą jednostki spoczywa obowiązek jego ochrony. W szczególności zabrania się pozostawiania bez opieki sprzętu mobilnego i nośników w miejscach, gdzie użytkownik nie ma możliwości sprawowania nad nimi skutecznego nadzoru.
3. Za utratę lub zniszczenie nośnika lub sprzętu mobilnego powierzonego do pracy odpowiada dany użytkownik, któremu sprzęt został powierzony. Zaistnienie takiego zdarzenia użytkownik zgłasza do bezpośredniego przełożonego.
4. W przypadku, gdy na sprzęcie mobilnym lub nośniku przetwarzane są dane osobowe należy dodatkowo poinformować ASI / IOD.
5. W zawiadomieniu użytkownik, poza informacjami ogólnymi, podaje okoliczności utraty sprzętu mobilnego lub nośnika oraz zakres utraconych danych osobowych lub informacji wraz
   z podaniem ich znaczenia dla jednostki.
6. Sprzęt mobilny podlega szczególnej ochronie. Jego używanie poza siedzibą jednostki musi mieć uzasadnienie w realizowanych przez użytkownika zadaniach.
7. Zgodę na użytkowanie sprzętu mobilnego poza siedzibą jednostki wydaje AD na pisemny wniosek przełożonego pracownika użytkującego sprzęt mobilny po zaopiniowaniu wniosku przez ASI.
8. ASI dookreśla okres na jaki sprzęt jest wynoszony oraz odpowiada za jego zwrot w określonym terminie.
9. W przypadku sprzętu mobilnego, w którym przetwarza się dane osobowe dodatkowo potrzebna jest zgoda IOD.
10. Wszelkie dane osobowe przechowywane w sprzęcie mobilnym lub nośniku, które pracują poza siedzibą jednostki muszą być zaszyfrowane.
11. Każdy użytkownik, któremu powierzono urządzenie przenośne, przed rozpoczęciem użytkowania go poza siedzibą jednostki, obowiązany jest do wystąpienia do wydziału odpowiedzialnego za utrzymanie i bezpieczeństwo systemu informatycznego z wnioskiem o zapewnienie środków techniczno - organizacyjnych gwarantujących poufność i integralność przetwarzanych informacji. Do środków tych zalicza się w szczególności ochronę antywirusową.
12. Używanie sprzętu komputerowego poza siedzibą jednostki obliguje użytkownika do stosowania odpowiednich zabezpieczeń, takich jak np. zamykanie szafki, polityka czystego biurka i ekranu, zabezpieczenia dostępu do komputera.

Postanowienia końcowe

§ 11

1. Każdemu pracownikowi umożliwia się zapoznanie z niniejszym regulaminem.

Załącznik nr 7 do PB

P_07	**PROCEDURA NADAWANIA UPRAWNIEŃ DO DOSTĘPU DO DANYCH OSOBOWYCH.**	Wydanie: 01
		Data: 25.05.2018 r.

1. Celem tej procedury jest określenie zasad udzielania dostępu użytkownikom do danych osobowych przetwarzanych w sieci komputerowej Urzędu oraz innych zbiorach danych oraz uniemożliwienie dostępu osobom nieupoważnionym.
2. Dostęp do określonych danych osobowych jest przydzielany na podstawie udokumentowanych potrzeb użytkowników związanych ze stanowiskiem pracy.

NADAWANIE UPRAWNIEŃ DOSTĘPU DO DANYCH OSOBOWYCH.

1. **Bezpośredni przełożony przed wypełnieniem wniosku:**
   „UPOWAŻNIENIE DO PRZETWARZANIA DANCYH OSOBOWYCH" - Załącznik nr 4 zobowiązany jest do:
   a. Przeprowadzenia szkolenia podstawowego z ochrony danych osobowych w porozumieniu z IOD celem zapoznania z przepisami i uzyskaniem zaświadczenia o odbyciu szkolenia - Załącznik nr 1.
   b. Przyjęciem oświadczenia w formie pisemnej od pracownika o zachowaniu poufności - Załącznik nr 2.
   c. Przygotowanie wniosku o nadanie dostępu do zbiorów danych osobowych - Załącznik nr 3.
   d. Przygotowanie niezbędnych danych dla IOD celem wystawienia upoważnienia do przetwarzania danych osobowych.
   e. Przekazanie w/w dokumentów do kadr.
2. **Inspektor Ochrony Danych odpowiada za:**
   a. Wydanie upoważnienia;
   b. Wpisanie upoważnienia do ewidencji osób upoważnionych do przetwarzania danych osobowych;
   c. Skierowanie przygotowanego przez AD wniosku w formie ogólnie przyjętej (email) do ASI o utworzenie konta i nadanie stosownych uprawnień - Załącznik nr 3.
   d. Zorganizowanie szkolenia z zakresu ochrony danych osobowych (szkolenie osobiste, zapoznanie się szkolonego z przepisami na podstawie dostarczonych materiałów w ramach samokształcenia lub szkolenie w formie przekazu audio-wideo);
   e. Przekazywanie upoważnienia pocztą elektroniczną lub osobiście.
3. Wszyscy użytkownicy uzyskujący dostęp do danych osobowych odpowiedzialni są za przestrzeganie Polityki Bezpieczeństwa oraz zasad opisanych w procedurze. Każdy pracownik w obecności bezpośredniego przełożonego składa oświadczenie o przestrzeganiu przepisów o ochronie danych osobowych i zachowaniu w poufności przetwarzanych danych.
4. Odebranie uprawnień dostępu do zbiorów danych osobowych pracownikowi odbywa się na podstawie informacji skierowanej przez AD do IOD oraz ASI w formie pisemnej lub wiadomości e-mail (Załącznik nr 5) a w skrajnych sytuacjach wymagających szybkiego działania w formie rozmowy telefonicznej lub korespondencji e-mail z w/w osobami funkcyjnymi.

5. W sytuacji zawarcia umowy cywilno - prawnej z podmiotem lub osobą realizującą zadania dla AD wymagające dostępu do danych osobowych oraz innych informacji obligatoryjne jest podpisanie zobowiązania do zachowania tajemnicy - Załącznik nr 6.
6. **ASI odpowiedzialny jest za:**
    a. Zakładanie i usuwanie kont w systemie z zadanym poziomem dostępu do danych osobowych, przydzielanie indywidualnego Identyfikatora dostępu do systemu informatycznego przetwarzającego dane osobowe;
    b. Szkolenie użytkowników z zakresu bezpieczeństwa teleinformatycznego;
    c. Generowanie użytkownikom pierwszych haseł dostępowych;
    d. Przydzielanie i odbieranie dostępu do zasobów użytkownikom stanowisk;
    e. Prowadzenie ewidencji wydanych identyfikatorów.

AKTYWACJA KONT W SYSTEMIE INFORMATYCZNYM JEDNOSTKI.

1. Dostęp do systemu informatycznego jednostki nadawany jest w zakresie:
    a. **PODSTAWOWYM** - konto w domenie, konto poczty elektronicznej, konto w komunikatorze, dostęp do zasobów sieciowych.
    b. **DODATKOWYM** - konta i zakresy uprawnień w aplikacjach.
2. Za nadawanie, modyfikację i wyłączanie uprawnień użytkowników w poszczególnych aplikacjach odpowiedzialny jest AD lub osoba wyznaczona przez AD pełniąca funkcję ASI.
3. Z wnioskiem o przyznanie dostępu do systemu informatycznego przetwarzającego dane osobowe jednostki występuje AD do IOD oraz ASI.
4. AD informuje IOD / ASI o konieczności wyłączenia dostępu dla osoby posiadającej uprawnienia do aplikacji, w przypadku jej zwolnienia z pracy (dotyczy pracownika) lub zaprzestania współpracy.
5. O prawo dostępu do systemu informatycznego jednostki, mogą ubiegać się wyłącznie osoby posiadające odpowiednie upoważnienie do przetwarzania danych osobowych.
6. ASI lub upoważnieni pracownicy mogą w uzasadnionych przypadkach zastrzec prawo do korzystania z systemu informatycznego jednostki każdemu użytkownikowi.
7. W przypadku konieczności zastrzeżenia prawa do korzystania z systemu informatycznego jednostki dla danego użytkownika, natychmiast cofane są wszelkie prawa dostępu do systemu informatycznego jednostki dla tego użytkownika, a w uzasadnionych przypadkach następuje wymiana identyfikatorów i haseł dostępu dla wszystkich lub określonych grup użytkowników.

Załącznik nr 1
do Procedury nadawania uprawnień do dostępu do danych osobowych.

..... dnia ……
(miejscowość)

.....
(pieczęć)

ZAŚWIADCZENIE

stwierdzające odbycie szkolenia
w zakresie ochrony danych osobowych

Stwierdza się, że Pani (Pan):

.....
(imię i nazwisko)

odbyła (odbył) szkolenie podstawowe - przeznaczone dla pracowników przetwarzających dane osobowe

na podstawie przepisów 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 oraz Ustawy o ochronie danych osobowych.

……
(nazwa i adres siedziby jednostki organizacyjnej)

……..……
(Inspektor Ochrony Danych)

Załącznik nr 2
do Procedury nadawania uprawnień do dostępu do danych osobowych.

OŚWIADCZENIE

Jako pracownik upoważniony do wykonywania czynności związanych z przetwarzaniem danych osobowych gromadzonych przez pracodawcę – Administratora Danych

oświadczam, że:

1. Zostałem przeszkolony i znane mi są przepisy RODO oraz ustawy o ochronie danych osobowych oraz obowiązujące w podmiocie Polityki Bezpieczeństwa danych osobowych, w tym w szczególności procedury w sytuacji naruszenia ochrony danych osobowych.
2. Zobowiązuję się do ich przestrzegania, a w szczególności do zachowania w tajemnicy wszelkich informacji (w tym danych osobowych), do których uzyskam dostęp w związku wykonywaniem powierzonych mi czynności (oraz sposobów ich zabezpieczenia) w trakcie wykonywania prac w jednostce.
3. Zobowiązanie powyższe dotyczy również okresu po ustaniu zatrudnienia (zakończeniu trwania umowy cywilno-prawnej) w jednostce.

Równocześnie potwierdzam, iż mam świadomość, że za naruszenie przepisów RODO, ustawy ODO grożą sankcje wskazane w RODO i ustawie o ochronie danych osobowych i sankcje pracownicze z Kodeksu Pracy (w przypadku zatrudnienia w oparciu o Kodeks pracy), które mogą być zastosowane również w wypadku naruszenia Polityki Bezpieczeństwa danych osobowych, jak również ewentualne roszczenia odszkodowawcze określone w prawie cywilnym.

.....
Czytelny podpis składającego oświadczenie

....., dnia .....

Załącznik nr 3
do Procedury nadawania uprawnień do dostępu do danych osobowych.

WNIOSEK

o nadanie dostępu do zbioru danych osobowych

w związku z zatrudnieniem

Pani/Pana* ……

na stanowisku/odbywającą / cego* staż ……

z przypisanym identyfikatorem .....

proszę o wpisanie do ewidencji osób biorących udział przy przetwarzaniu danych osobowych oraz nadanie dostępu do zbioru danych osobowych:

……

……

z poziomem dostępu: edycja/zapis*

w ramach określonych czynności zawodowych

(w tym udział przy przetwarzaniu danych osobowych)

……
(podpis bezpośredniego przełożonego)

....., dnia ……
(miejscowość)

* - *niepotrzebne skreślić*

Załącznik nr 4
do Procedury nadawania uprawnień do dostępu do danych osobowych.

Data nadania upoważnienia: **……..**

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

NR……

Zgodnie Rozporządzeniem 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 oraz Ustwą o Ochronie Danych Osobowych.

Upoważniam Panią/Pana .....

(imię i nazwisko upoważnianego)

zatrudnioną/-ego na stanowisku .....

w .....

(nazwa Administratora Danych)

do dostępu do danych osobowych:

– .....

– .....

(zakres upoważnienia: wskazanie kategorii danych, które może przetwarzać określona w upoważnieniu osoba, lub rodzaj czynności lub operacji, jakich może dokonywać na danych osobowych)

2. Identyfikator: .....

(wypełnia się w przypadku, gdy dane przetwarzane są w systemie informatycznym)

3. Okres trwania upoważnienia: .....

Wystawił: .....

(podpis Inspektora Ochrony Danych)

Załącznik nr 5
do Procedury nadawania uprawnień do dostępu do danych osobowych.

WNIOSEK

o odebranie prawa dostępu do zbioru danych osobowych

W związku z ……..
Pani/Pana* ……

proszę o wykreślenie w/w. osoby z ewidencji osób biorących udział przy przetwarzaniu danych osobowych
oraz usunięcie praw dostępu do zbioru danych osobowych*:

……..……

……..……

……
(podpis bezpośredniego przełożonego)

....., dnia …….
(miejscowość)

* - *niepotrzebne skreślić*

Załącznik nr 6
do Procedury nadawania uprawnień do dostępu do danych osobowych.

Z O B O W I Ą Z A N I E

(dot. umowy cywilno – prawnej, stażu, praktyki)

Ja, niżej podpisana / ny.....……

Z O B O W I Ą Z U J Ę S I Ę

do przestrzegania Polityki Bezpieczeństwa danych osobowych obowiązującej w Jednostce, zachowania w tajemnicy wszelkich informacji (w tym danych osobowych) pozyskanych w trakcie wykonywania prac/ stażu/ praktyki *:

…….

(wymienić rodzaj prac)

w …….

Równocześnie potwierdzam, iż mam świadomość, że za naruszenie przepisów ustawy o ochronie danych osobowych grożą sankcje karne przewidziane w ustawie o ochronie danych osobowych jak również ewentualne roszczenia odszkodowawcze określone w prawie cywilnym i RODO.

……

(Podpis osoby składającej zobowiązanie)

....., dnia …….

(miejscowość)

* - *niepotrzebne skreślić*

Załącznik nr 8 do PB

P_08	**REGULAMIN KORZYSTANIA Z URZĄDZEŃ MOBLNYCH, NA KTÓRYCH PRZETWARZANE SĄ DANE OSOBOWE POZA JEDNOSTKĄ.**	Wydanie: 01
		Data: 25.05.2018 r.

Regulamin ustala zasady: korzystania z komputerów przenośnych (mobilnych), na których są przetwarzane dane osobowe poza siedzibą jednostki.

§ 1

1. Przetwarzanie danych osobowych na komputerach przenośnych poza siedzibą (obszarem przetwarzania danych osobowych) jednostki, powinno być ograniczone do niezbędnego minimum i może się odbywać wyłącznie na podstawie zgody AD ustalając zakres, czas oraz miejsce przetwarzania.
2. Pracownik korzystający z komputera przenośnego do przetwarzania danych osobowych lub dokumentów stanowiących inne tajemnice prawnie chronione jednostki zobowiązany jest do zwrócenia szczególnej uwagi na zabezpieczenie przetwarzanych informacji, zwłaszcza przed dostępem do nich osób nieupoważnionych oraz przed zniszczeniem. W związku z powyższym zobowiązany jest do:
    a. Przechowywania przedmiotowych danych na dysku szyfrowanym, zabezpieczonym hasłem co najmniej 8 – mio znakowym zawierającym: duże i małe litery, znaki specjalne lub cyfry.
    b. Komputery przenośne muszą być zabezpieczone hasłem na poziomie BIOS-u. Sam dostęp do konfiguracji BIOS-u również wymaga zabezpieczenia hasłem.
    c. Transportu komputera w sposób minimalizujący ryzyko kradzieży lub zniszczenia, a w szczególności:
        - transportowania komputera w odpowiedniej, przeznaczonej do tego celu torbie jako bagażu podręcznego lub innego wskazanego zabezpieczenia;
        - niepozostawiania komputera w samochodzie, przechowalni bagażu, środkach transportu publicznego itp. bez nadzoru.
    d. Korzystania z komputera w sposób minimalizujący ryzyko podejrzenia przetwarzanych danych przez osoby nieupoważnione, w szczególności zabrania się korzystania z komputera w miejscach publicznych i w środkach transportu publicznego.
    e. Uniemożliwienia korzystania z komputera osobom niepowołanym (np. rodzinie, dzieciom, znajomym).
    f. Zabezpieczenia komputera przenośnego hasłem i utrzymanie konfiguracji oprogramowania systemowego w stanie wymuszającym korzystanie z tego hasła.
    g. Blokowania dostępu do komputera przenośnego w przypadku, gdy nie jest on wykorzystywany przez uprawionego użytkownika.
    h. Regularnego i częstego kopiowania danych przetwarzanych na komputerze przenośnym, do systemu informatycznego U w celu umożliwienia wykonania kopii awaryjnej.

i. Cyklicznego podłączania komputera do sieci informatycznej w celu wykonania aktualizacji wzorców wirusów w programie antywirusowym.

3. ASI zobowiązany jest do podjęcia działań mających na celu zabezpieczenie komputerów przenośnych, w szczególności:
   a. Dokonanie konfiguracji oprogramowania w sposób wymuszający korzystanie z haseł odpowiedniej jakości oraz ich cyklicznej zmiany, zgodnie z wytycznymi.
   b. W przypadku przetwarzania danych osobowych znajdujących się bezpośrednio na komputerze przenośnym - zabezpieczyć je dodatkowo poprzez wykorzystanie oprogramowania szyfrującego.
   c. Instalacji i konfiguracji oprogramowania antywirusowego.
   d. Przeprowadzenie aktualizacji wzorców wirusów zgodnie z zasadami zarządzania programem antywirusowym.
4. ASI lub osoba wskazana przez AD jest odpowiedzialny za prowadzenie ewidencji komputerów przenośnych wykorzystywanych do przetwarzania danych poza siedzibą Jednostki. W szczególności ewidencja powinna obejmować:
   a. Typ i numer seryjny komputera przenośnego.
   b. Imię i nazwisko osoby będącej użytkownikiem komputera.
   c. Wykaz oprogramowania zainstalowanego na komputerze, służącego do przetwarzania danych osobowych.
   d. Rodzaj i zakres danych osobowych przetwarzanych na komputerze.
5. W razie zgubienia lub kradzieży komputera przenośnego, pracownik zobowiązany jest do natychmiastowego powiadomienia ASI lub osoby uprawnionej zgodnie z zasadami informowania w przypadku naruszenia ochrony danych osobowych.

§ 2
Postanowienia końcowe

Każdemu pracownikowi umożliwia się zapoznanie z niniejszym regulaminem.

Załącznik nr 9 do PB

P_09	**REGULAMIN FUNKCJONOWANIA MONITORINGU WIZYJNEGO.**	Wydanie: 01
		Data: 25.05.2018 r.

Niniejszy regulamin określa zasady funkcjonowania monitoringu wizyjnego na terenie **Placówki oświatowej**, w tym zasady rejestracji, zapisu i usuwania informacji, sposób ich zabezpieczenia, a także zasady udostępniania danych pozyskanych z tytułu funkcjonowania monitoringu wizyjnego.

Cel monitoringu:

Celem funkcjonowania monitoringu wizyjnego jest zapewnienie bezpieczeństwa i porządku publicznego oraz ochrony dóbr i mienia na obszarze placówki.

W szczególności:

1. Zapobieganie zachowaniom mogącym sprowadzić niebezpieczeństwo utraty zdrowia lub życia dla osób;
2. Uniemożliwienie dystrybucji narkotyków, alkoholu oraz innych substancji zakazanych;
3. Ustalenie sprawców oraz zmniejszenie ilości bójek, kradzieży, niszczenia mienia.

Monitoring wizyjny został wdrożony po dokonaniu planowania i zdefiniowania zagrożeń bezpieczeństwa jako najbardziej adekwatne narzędzie służące osiągnięciu celu, po dokonaniu analizy potrzeb i celowości wraz z prognozą jego skuteczności w kontekście wpływu na zachowanie prywatności osób przebywających na terenie placówki w zakresie obowiązku zapewnienia bezpieczeństwa.
Na system monitoringu wizyjnego składają się kamery, urządzenie rejestrujące, monitor umożliwiający wgląd do utrwalonego zapisu oraz okablowanie.

Definicje:

1. **Monitoring wizyjny** — kamery, okablowanie, rejestrator oraz oprogramowanie wykorzystywane do zbierania oraz przechowywania wizerunku.
2. **Dane osobowe** — wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, jeżeli nie wymaga to nadmiernych kosztów, czasu lub działań.
3. **Polityka Bezpieczeństwa (PB)** — obowiązująca w placówce.
4. **Zbiór danych osobowych** — każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
5. **Administrator Danych Osobowych (ADO)** — należy przez to rozumieć AD placówki.
6. **Przetwarzanie danych osobowych** — wykonywanie wszelkich operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie.
7. **Zbieranie danych** — wejście w posiadanie danych osobowych.

8. **Usuwanie danych** — fizyczne niszczenie danych lub taka ich modyfikacja, która uniemożliwia ustalenie osoby, której dane dotyczą.
9. **Utrwalanie** — zapisanie informacji na materialnym nośniku.
10. **Udostępnianie** — objęcie w posiadanie danych osobowych przez innego Administratora Danych Osobowych lub podmiotu przetwarzającego.
11. **Wgląd** — fizyczne przeglądanie zawartości zbioru danych osobowych bez wejścia w posiadanie przeglądanego zbioru.
12. **Osoba upoważniona** — osoba posiadająca upoważnienie wydane przez Administratora Danych Osobowych dopuszczona do przetwarzania danych osobowych w zakresie wskazanym w upoważnieniu zgodnie z Polityką Bezpieczeństwa.

Podstawa prawna:

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).

Zabezpieczenia techniczne i organizacyjne (rozmieszczenie kamer).

1. Zabrania się instalowania kamer w toaletach, pomieszczeniach socjalnych czy też poszczególnych pomieszczeniach biurowych – co mogłoby prowadzić do naruszenia prywatności.
2. Osobom mającym dostęp do zapisu rejestratora monitoringu należy wydać **upoważnienia** do przetwarzania danych osobowych i uwzględnić je w **ewidencji.** W przypadku potrzeby powierzenia zapisu monitoringu innym podmiotom należy zawrzeć stosowną umowę powierzenia przetwarzania danych osobowych.
3. Za nadzór nad rejestratorem odpowiedzialny jest AD / ASI.

Obowiązki informacyjne - Klauzula informacyjna dla monitoringu.

Treść klauzuli	Sposób wprowadzenia
 „**Obiekt monitorowany całodobowo**” Administratorem Danych jest: **Zespół Szkół Zawodowych** **im. gen. Stanisława Maczka** **86-010 Koronowo ul. Dworcowa 53** Monitoring wizyjny prowadzony jest w celu zapewnienia bezpieczeństwa i porządku publicznego oraz ochrony dóbr i mienia. Dodatkowe informacje można uzyskać w Sekretariacie.	Wywieszka przy wejściu na teren placówki.

Zasady monitoringu.

1. Zbieraniu, utrwalaniu oraz przechowywaniu wizerunku jako danej osobowej podlega wyłącznie obraz (wizja) z kamer systemu monitoringu. Funkcjonujący w jednostce system nie rejestruje dźwięku (fonii).
2. Wykaz obszarów objętych monitoringiem wizyjnym oznakowany jest tablicami informacyjnymi (piktogramami).
3. Miejsca objęte monitoringiem wizyjnym zostały przeanalizowane pod kątem poszanowania prywatności i intymności pracowników oraz innych osób przebywających na terenie placówki.
4. Miejsca objęte monitoringiem są oznakowane poprzez umieszczenie informacji zawierającej piktogram informujący o objęciu obszaru monitoringiem oraz z informacją o:
    a. Administratorze Danych Osobowych,
    b. Celu istnienia monitoringu,
    c. Prawie oraz sposobie uzyskania dodatkowych informacji.
5. Wzór oznakowania informującego o objęciu monitoringiem stanowi Załącznik nr 1 niniejszego Regulaminu.
6. Monitoring funkcjonuje całodobowo.
7. Efekty wprowadzenia monitoringu wizyjnego wraz z ich wpływem na bezpieczeństwo pracowników i osób przebywających na terenie placówki są na bieżąco monitorowane.

Zasady rejestracji monitoringu.

1. Zaleca się, aby zebrany obraz utrwalony na rejestratorze, zlokalizowany w placówce przechowywany był przez okres 30 dni, po tym czasie może zostać nadpisany.
2. W uzasadnionych przypadkach, w szczególności, gdy system monitoringu wizyjnego zarejestrował wydarzenia niezgodne z prawem zapis może zostać przeniesiony na elektroniczny nośnik pamięci.
3. Nośniki z zachowanym nagraniem przechowuje AD.
4. Nośniki zawierające przeniesiony z rejestratora zapis obrazu przechowujemy wyłącznie do momentu zaprzestania jego użyteczności, np. do czasu wyjaśnienia sprawy lub zakończenia odpowiednich postępowań nie dłużej niż jeden rok.
5. Zapisany obraz z monitoringu może zostać udostępniony zgodnie z zasadami określonymi w Polityce Bezpieczeństwa. Wzór wniosku o udostępnienie nagrania określa Załącznik nr 2 niniejszego regulaminu.
6. Nośniki zawierające utrwalony zapis wizyjny polegają obowiązkowi tworzenia kopii zapasowych zgodnie z procedurami określonymi w Polityce Bezpieczeństwa.
7. W momencie zaprzestania użyteczności nagrania zapisanego na zewnętrznym nośniku, jest ono usuwane zgodnie z procedurą określoną w Polityce Bezpieczeństwa.
8. Dostęp do zapisu wizyjnego utrwalonego w rejestratorze oraz zewnętrznych nośników posiada wyłącznie Administrator Danych Osobowych oraz upoważnione przez Niego osoby zgodnie z procedurami określonymi w Polityce Bezpieczeństwa.
9. Rejestrator oraz zewnętrzne nośniki zawierające zapisany obraz zabezpieczony jest przed dostępem osób nieupoważnionych poprzez zastosowanie środków technicznych oraz organizacyjnych określonych w Polityce Bezpieczeństwa.

Udostępnianie danych objętych monitoringiem.

1. Administrator Danych zabezpiecza zdarzenia zarejestrowane przez monitoring, które zagrażają bezpieczeństwu, życiu i zdrowiu pracowników i osób przebywającym na terenie, niszczeniu i kradzieży mienia dla celów dowodowych:
    a. na wniosek osób trzecich;
    b. na wniosek organów prowadzących postępowania np. policji, prokuratury, sądów;
    c. zaobserwowane przez osoby obsługujące monitoring, które mogą być dowodem na popełnienie czynu niedozwolonego.
2. Zabezpieczenie danych monitoringu polega na ich zarejestrowaniu na nośniku danych, umożliwiającym ich powielanie.
3. Nośniki danych zawierające zarejestrowane dane powinny być zabezpieczone i przechowywane w specjalnie wyznaczonym do tego miejscu.
4. Zabezpieczone dane z monitoringu są udostępniane tylko organom prowadzącym postępowanie w sprawie zarejestrowanego zdarzenia np. policji, prokuraturze, sądom, które działają na podstawie odrębnych przepisów.
5. Zabezpieczone dane mogą być również przekazywane ubezpieczycielowi placówki w ramach prowadzonej likwidacji szkody osobowej lub majątkowej zgłoszonej przez osoby trzecie.
6. Każdorazowe zabezpieczenie zdarzeń zarejestrowanych przez monitoring odbywa się na pisemny wniosek podmiotów w/w wskazanych.
7. Dane z monitoringu zabezpieczone na wniosek podmiotu uprawnionego są przechowywane przez AD przez okres jednego roku od dnia złożenia wniosku. Po upływie tego terminu zabezpieczone dane są niszczone.
8. Z czynności zniszczenia danych, o której mowa powyżej sporządza się notatkę, która powinna zawierać:
    a. czas i miejsce zarejestrowanego obrazu zdarzeń podlegającego zniszczeniu;
    b. sposób zniszczenia;
    c. imię, nazwisko, stanowisko służbowe osoby dokonującej zniszczenia;
    d. czas i miejsce zniszczenia;
    e. podpis osoby dokonującej zniszczenia.

Załącznik nr 1
do Regulaminu funkcjonowania monitoringu wizyjnego.

WZÓR OZNAKOWANIA INFORMUJĄCEGO O OBJĘCIU MONITORINGIEM

Załącznik nr 2
do Regulaminu funkcjonowania monitoringu wizyjnego.

WNIOSEK O UDOSTĘPNIENIE NAGRANIA Z MONITORINGU WIZYJNEGO

1. Wniosek do:

2. Wnioskodawca:

(nazwisko, imię i adres zamieszkania wnioskodawcy ew. NIP oraz REGON)

3. Data, godzina i miejsce, w którym został dokonany zapis monitoringu wizyjnego:

4. Wskazanie przeznaczenia dla udostępnionego zapisu:

5. Informacje umożliwiające wyszukiwanie nagrania: