Załącznik nr 1 do zarządzenia Nr 17/2025
Dyrektora Centrum Usług Społecznych w Będzinie
z dnia 02 stycznia 2025 r.

Polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Centrum Usług Społecznych w Będzinie

§ 1
Postanowienia ogólne

1. Polityka bezpieczeństwa przetwarzania danych osobowych zwana dalej "Polityką", została wydana w związku z § 3 ust. 1 rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych z dnia 09. 11.2017 r. (t.j. Dz. U. z 2017 r. poz. 2247 ze zm.), 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 (ogólnego rozporządzenia o ochronie danych) (dalej jako „RODO") oraz ustawy o ochronie danych osobowych (Dz. U. poz. 1000 z 2018 roku ze zm.).
2. Celem Polityki jest stworzenie podstaw dla właściwego wykonania obowiązków Administratora Danych w zakresie zabezpieczenia i prawidłowej ochrony przetwarzanych danych osobowych.
3. Polityka określa zasady przetwarzania danych osobowych oraz ich zabezpieczania, jako zestaw praw, reguł i zaleceń, regulujących sposób ich zarządzania, ochrony w jednostce
4. Polityka zawiera informacje dotyczące rozpoznawania procesów przetwarzania danych osobowych oraz wprowadzonych zabezpieczeń technicznych i organizacyjnych, zapewniających ochronę przetwarzanych danych osobowych.
5. Niniejszą Politykę stosuje się do:
   1) danych osobowych:
      a. przetwarzanych w systemach informatycznych,
      b. zapisanych na zewnętrznych nośnikach informacji,
      c. przetwarzanych tradycyjnie.
   2) informacji dotyczących bezpieczeństwa przetwarzania danych osobowych:
      a. służących do uwierzytelnienia w systemach informatycznych, w których są przetwarzane dane osobowe,
      b. dotyczących wdrożonych zabezpieczeń technicznych i organizacyjnych.
6. Bez względu na zajmowane stanowisko, miejsce wykonywanej pracy oraz charakter stosunku pracy, zasady określone w niniejszej Polityce oraz w dokumentach powiązanych powinny być znane i stosowane przez pracowników oraz w niezbędnym zakresie przez współpracowników przetwarzających dane osobowe, których administratorem jest niniejsza jednostka organizacyjna

§ 2
Definicje

Użyte w niniejszej Polityce pojęcia są wspólne dla wszystkich dokumentów powiązanych z niniejszą Polityką oraz dla wszystkich pozostałych dokumentów, które zostały przyjęte przez jednostkę, w zakresie ochrony danych osobowych.

1. **Administrator Danych Osobowych** – podmiot, który decyduje o środkach i celach przetwarzania danych osobowych, reprezentowany przez Kierownika jednostki Centrum Usług Społecznych w Będzinie.
2. **Inspektor Ochrony Danych** - osoba wyznaczona przez kierownika jednostki, odpowiedzialna za nadzorowanie stosowania środków technicznych i organizacyjnych zapewniających

ochronę przetwarzanych danych osobowych, w tym w szczególności za przeciwdziałanie dostępowi osób trzecich do systemu, w którym przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie ochrony danych osobowych.

3. **Informatyk Systemów** – pracownik/zleceniobiorca jednostki organizacyjnej na stanowisku informatyk, który w zakresie swoich obowiązków jest odpowiedzialny za funkcjonowanie infrastruktury informatycznej, na którą składa się cały sprzęt informatyczny oraz systemów i aplikacji informatycznych, za ich przeglądy, konserwację oraz za stosowanie technicznych i organizacyjnych środków bezpieczeństwa w systemach informatycznych.
4. **Bezpieczeństwo przetwarzania danych osobowych** - zachowanie poufności, integralności i rozliczalności danych osobowych: dodatkowo, mogą być brane pod uwagę inne własności, takie jak dostępność, autentyczność, niezaprzeczalność i niezawodność.
5. **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.
6. **PUODO** - Prezes Urzędu Ochrony Danych Osobowych.
7. **Integralność danych** - właściwość zapewniająca, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
8. **Naruszenie ochrony danych osobowych** - zamierzone lub przypadkowe naruszenie środków technicznych i organizacyjnych zastosowanych w celu ochrony danych osobowych. W szczególności, gdy stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszanie ochrony danych osobowych.
9. **Poufność** - właściwość zapewniająca, że informacja (np. dane osobowe) jest dostępna jedynie osobom upoważnionym.
10. **Przetwarzanie danych osobowych** - 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.
11. **Rozporządzenie** - rozporządzenie Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych z dnia 09. 11.2017 r. (t.j. Dz. U. z 2017 r. poz. 2247 ze zm.),
12. **Rozliczalność** - właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
13. **System informatyczny** - zespół współpracujących urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
14. **Ustawa** - Ustawa o ochronie danych osobowych z 24 maja 2018 roku (Dz. U. poz. 1000 z 2018 r ze zm.
15. **Użytkownik systemu** - osoba upoważniona do bezpośredniego dostępu do danych osobowych przetwarzanych w systemie informatycznym, która posiada ustalony identyfikator i hasło.
16. **Użytkownik zewnętrzny** - należy przez to rozumieć osobę nie będącą pracownikiem lub stażystą jednostki organizacyjnej, posiadającą uprawnienia do przetwarzania informacji w związku z wykonywaniem czynności na rzecz organizacji.

17. **"ograniczenie przetwarzania"** oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
18. **"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;
19. **"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;
20. **"administrator"** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;
21. **"podmiot przetwarzający"** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
22. **"odbiorca"** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;
23. **"strona trzecia"** 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;
24. **"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;
25. **"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;
26. **"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;
27. **"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;
28. **"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;
29. **Właściciel zasobów danych osobowych** - osoba kierująca komórką organizacyjną, odpowiedzialną za ochronę danych osobowych przetwarzanych w podległej komórce. Jest ona zobowiązana zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych

ochroną, a w szczególności zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy o ochronie danych osobowych oraz nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.

30. **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.
31. **Zbiór nieinformatyczny** - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony lub podzielony funkcjonalnie, prowadzony poza systemem informatycznym, w szczególności w formie kartoteki, skorowidza, księgi, wykazu lub innego zbioru ewidencyjnego.
32. Rozporządzenie Unijne (RODO / GDPR) oznacza 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 (ogólnego rozporządzenia o ochronie danych)

§ 3
Deklaracja Administratora Danych Osobowych

1. ADO zobowiązuje się do podjęcia odpowiednich kroków, mających na celu zapewnienie prawidłowej ochrony danych osobowych, w szczególności do zapewnienia, że przez cały okres ich przetwarzania, dane będą:
   1) przetwarzane zgodnie z prawem.
   2) zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami.
   3) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane.
   4) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.
   5) zabezpieczone środkami technicznymi i organizacyjnymi, które zapewniają rozliczalność, integralność oraz poufność danych.
2. Przy przetwarzaniu danych osobowych w systemach informatycznych jednostki należy stosować wysoki poziom bezpieczeństwa w rozumieniu § 6 ust. 4 Rozporządzenia.

§ 4
Przegląd dokumentacji z zakresu ochrony danych osobowych

1. Niniejsza Polityka oraz dokumenty z nią powiązane powinny być aktualizowane wraz ze zmieniającymi się przepisami prawnymi o ochronie danych osobowych oraz zmianami faktycznymi w ramach jednostki, które mogą powodować, że zasady ochrony danych osobowych określone w obowiązujących dokumentach będą nieaktualne lub nieadekwatne.
2. Fakty wystąpienia poważnych naruszeń ochrony danych osobowych powinny skutkować zmianami w dokumencie niniejszej Polityki i dokumentach powiązanych.
3. Zmiany niniejszej Polityki wymagają przeglądu innych dokumentów obowiązujących w jednostce dotyczących ochrony danych osobowych.
4. Wszelkie znaczące zmiany Polityki powinny być zatwierdzane przez Kierownika jednostki

§ 5
Zarządzanie ochroną danych osobowych

1. Realizację zamierzeń w celu zwiększenia skuteczności ochrony danych osobowych powinny zagwarantować następujące założenia:
   1) przypisanie użytkownikom określonych atrybutów pozwalających na ich identyfikację w systemach informatycznych (np. hasła, identyfikatory), umożliwiających im dostęp do

danych osobowych - stosownie do zakresu upoważnienia i indywidualnych poziomów uprawnień,
2) okresowe sprawdzanie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych osobowych,
3) podejmowanie niezbędnych działań, w celu likwidacji słabych ogniw w systemie ochrony danych osobowych,
4) śledzenie osiągnięć w dziedzinie bezpieczeństwa systemów informatycznych i – w miarę możliwości organizacyjnych i techniczno-finansowych - wdrażanie nowych narzędzi i metod pracy oraz sposobów zarządzania systemami informatycznymi, służących wzmocnieniu bezpieczeństwa przetwarzanych danych osobowych.

2. Na każdym etapie przetwarzania danych osobowych należy brać pod uwagę, w niezbędnym zakresie, integralność, poufność oraz rozliczalność dla przetwarzanych danych osobowych.
3. Administrator Danych Osobowych powinien być zapewniony, że pracownicy, wykonawcy oraz użytkownicy zewnętrzni:
   1) są odpowiednio wprowadzani w swoje obowiązki i odpowiedzialności związane z ochroną danych osobowych i ich przetwarzaniem przed przyznaniem im dostępu do danych osobowych,
   2) otrzymali zalecenia określające wymagania w zakresie bezpieczeństwa danych osobowych związane z ich obowiązkami w jednostce,
   3) wypełniali zalecenia i warunki zatrudnienia, które uwzględniają zasady ochrony danych osobowych oraz właściwe metody pracy,
   4) w sposób ciągły utrzymywali odpowiednie umiejętności i kwalifikacje.
4. Za bieżącą, operacyjną ochronę danych osobowych odpowiada każda osoba przetwarzająca te dane w zakresie zgodnym z zakresem upoważnienia, kompetencjami lub rolą sprawowaną w procesie przetwarzania danych.

§ 6

Dokumenty powiązane

Na dokumentacje ochrony danych osobowych w jednostce składają się:

1. Ewidencja osób upoważnionych przez Administratora Danych Osobowych do przetwarzania danych osobowych.
2. Ewidencja zbiorów danych osobowych przetwarzanych w jednostce organizacyjnej oraz programów zastosowanych do ich przetwarzania.
3. Oryginały i kopie dokumentów dotyczących ochrony danych osobowych (w tym kopie wniosków o rejestrację/aktualizacje zbiorów danych osobowych , zarządzenia, polityki itd. dotyczące ochrony danych osobowych)
4. Regulamin zarządzania incydentami w jednostce.
5. Plan ciągłości działania w jednostce.
6. Analiza ryzyka IT w jednostce..
7. Zarządzanie kopiami zapasowymi w jednostce.

§ 7

Odpowiedzialność Administratora Danych Osobowych

1. Administrator Danych Osobowych jest odpowiedzialny za przetwarzanie i ochronę danych osobowych zgodnie z przepisami prawa, w tym wprowadzenie do stosowania procedur postępowania zapewniających prawidłowe przetwarzanie danych osobowych, rozumiane jako ochronę danych przed ich udostępnieniem osobom nieupoważnionym, zmianą lub zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem Ustawy oraz utratą, uszkodzeniem lub zniszczeniem.
2. Do kompetencji Administratora Danych Osobowych należy w szczególności:
   1) wyznaczenie Inspektora Ochrony Danych,

2) wyznaczanie Właścicieli zasobów danych osobowych,
3) określenie celów i strategii ochrony danych osobowych,
4) podział zadań i obowiązków związanych z organizacją ochrony danych osobowych.

3. Do obowiązków Administratora Danych Osobowych należy:
   1) zapewnienie szkoleń dla pracowników w zakresie przepisów o ochronie danych osobowych oraz zagrożeń związanych z ich przetwarzaniem,
   2) przyjmowanie i zatwierdzanie niezbędnych, wymaganych przez przepisy prawa dokumentów regulujących ochronę danych osobowych w CUS,
   3) nadawanie upoważnień pracownikom CUS oraz użytkownikom zewnętrznym do przetwarzania danych osobowych,
   4) zapewnienie środków finansowych na ochronę fizyczną pomieszczeń, w których przetwarzane są dane osobowe,
   5) zapewnienie środków finansowych niezbędnych do ochrony danych osobowych przetwarzanych w systemach informatycznych oraz w zbiorach nieinformatycznych,
   6) zapewnienie środków finansowych na merytoryczne przygotowanie osób odpowiedzialnych za nadzór nad ochroną danych osobowych,
   7) prowadzenie rejestru zbiorów danych osobowych przetwarzanych w jednostce z uwzględnieniem wyłączeń z mocy ustawy.

§ 8

Odpowiedzialność Inspektora Ochrony Danych.

1. Administrator Danych Osobowych wyznacza Inspektora Ochrony Danych, który nadzoruje przestrzeganie zasad ochrony danych osobowych zarówno w systemach informatycznych, jak również w zbiorach danych osobowych prowadzonych w formie papierowej i elektronicznej.
2. Do kompetencji Inspektora Ochrony Danych należy:
   1) określenie zasad ochrony danych osobowych,
   2) wnioskowanie o ukaranie osób winnych naruszenia przepisów i zasad dotyczących ochrony danych osobowych.
3. Do obowiązków Inspektora Ochrony Danych należy:
   a) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy Rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
   b) monitorowanie przestrzegania Rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
   c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania;
   d) współpraca z PUODO;
   e) pełnienie funkcji punktu kontaktowego dla PUODO w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 Rozporządzenia, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.
   f) przeprowadzenie szkoleń dla pracowników w zakresie ochrony danych osobowych;
   g) udzielanie konsultacji w zakresie ochrony danych osobowych.

Inspektor Ochrony Danych w zakresie realizacji swoich obowiązków, ma prawo żądania od pozostałych osób, bez względu na rangę ich stanowiska udzielania natychmiastowej pomocy w razie stwierdzenia, że doszło do naruszenia przepisów o ochronie danych osobowych.

§ 9

Odpowiedzialność pracownika/zleceniobiorcy na stanowisku Informatyk realizującego obsługę systemów informatycznych

1. Zadania z zakresu obsługi systemów realizują pracownicy na stanowisku – informatyk.
2. Do kompetencji informatyków należy:
    1) zabezpieczenie systemów przetwarzania danych osobowych, w zależności od kategorii przetwarzanych w tym systemie danych,
    2) zapewnienie poufności, integralności, dostępności i rozliczalności danych przetwarzanych w systemach informatycznych.
3. Do obowiązków pracownika na stanowiskach - informatyk należy:
    1) bieżący nadzór oraz zapewnianie optymalnej ciągłości działania systemu informatycznego,
    2) reagowanie bez zbędnej zwłoki, w przypadku naruszenia bądź powstania zagrożenia bezpieczeństwa danych osobowych,
    3) przeciwdziałanie próbom naruszenia bezpieczeństwa danych osobowych,
    4) zapewnienie zgodności wszystkich wdrażanych systemów przetwarzania danych osobowych z Ustawą oraz z niniejszą Polityką bezpieczeństwa i instrukcją zarządzania systemem informatycznym w Centrum Usług Społecznych w Będzinie ,
    5) instalacja i konfiguracja oprogramowania i sprzętu typu „stand-alone", sieciowego i serwerowego używanego do przetwarzania danych osobowych,
    6) konfiguracja i administracja oprogramowaniem systemowym i sieciowym zabezpieczającym dane osobowe przed nieupoważnionym dostępem,
    7) nadzór nad czynnościami związanymi ze sprawdzaniem systemu pod kątem obecności szkodliwego oprogramowania,
    8) nadzór nad systemem komunikacji w sieci komputerowej oraz przesyłaniem danych za pośrednictwem urządzeń teletransmisji,
    9) nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe,
    10) przyznawanie ściśle określonych praw dostępu do danych osobowych w danym systemie,
    11) świadczenie pomocy technicznej w ramach oprogramowania a także serwis sprzętu komputerowego będącego na stanie Centrum Usług Społecznych w Będzinie służącego do przetwarzania danych osobowych,
    12) diagnozowanie i usuwanie awarii sprzętu komputerowego oraz realizacje umów z firmami świadczącymi usługi pogwarancyjnego sprzętu komputerowego,
    13) wykonywanie i zarządzanie kopiami awaryjnymi oprogramowania systemowego (w tym danych osobowych oraz zasobów umożliwiających ich przetwarzanie) i sieciowego,
    14) nadzór nad wdrożeniem i zarządzanie aplikacjami (przeglądanie, nadawanie i odbieranie uprawnień użytkownikom, itp.), w których przetwarza się dane osobowe.

§ 10

Odpowiedzialność Właścicieli zasobów danych osobowych

1. Administrator Danych Osobowych wyznacza Właścicieli zasobów danych osobowych, którzy są odpowiedzialni za ochronę przypisanych i przetwarzanych zbiorów danych osobowych w podległej komórce organizacyjnej. Właścicielami zasobów danych osobowych w jednostce są wskazani pracownicy.
2. Do kompetencji Właścicieli zasobów danych osobowych należy:
    1) określanie celów w jakich mają być przetwarzane dane osobowe, zakresu oraz czasu trwania przetwarzania danych osobowych,
    2) określenie sposobu przetwarzania danych osobowych (czy w systemach informatycznych, czy w zbiorach nieinformatycznych).
3. Do obowiązków Właścicieli zasobów danych osobowych należy:
    1) zapewnienie podstaw prawnych do przetwarzania danych osobowych od chwili zebrania

danych osobowych do chwili ich usunięcia,
2) zapewnienie aktualności, adekwatności oraz merytorycznej poprawności danych osobowych przetwarzanych w określonym przez nich celu,
3) realizację obowiązku informowania o przetwarzaniu danych osobowych osób, których dane osobowe są pozyskiwane,
4) w przypadku utworzenia nowego zbioru danych osobowych ustalenie, kogo dotyczą dane osobowe, jaki jest ich zakres (np. imię i nazwisko, adres zamieszkania, NIP, PESEL itp.), cel przetwarzania oraz komu dane osobowe mają być udostępniane. Wszystkie te informacje powinny zostać przekazane do Inspektora Ochrony Danych.
5) Dokonywanie analizy ryzyka ochrony danych osobowych zgodnie z obowiązującą polityką i Rozporządzeniem.

§ 11

Odpowiedzialność pracowników i użytkowników systemu

1. W celu osiągnięcia i utrzymania wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych konieczne jest zaangażowanie ze strony każdego pracownika i użytkownika zewnętrznego w zakresie ochrony danych osobowych.
2. Pracownicy jednostki oraz użytkownicy zewnętrzni są zobowiązani do informowania o wszelkich podejrzeniach naruszeniach lub zauważonych naruszeniach oraz słabościach systemu przetwarzającego dane osobowe bezpośrednio do Inspektora Ochrony Danych.
3. Pracownicy / użytkownicy zewnętrzni są zobowiązani do:
   1) postępowania zgodnie z Polityką,
   2) zachowania w tajemnicy danych osobowych oraz informacji o sposobach ich zabezpieczenia,
   3) ochrony danych osobowych oraz środków przetwarzających dane osobowe przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem,
   4) wykonywania konkretnych działań i procesów w celu zapewnienia ochrony danych osobowych.
4. Pracownicy / użytkownicy zewnętrzni powinni mieć świadomość możliwości zaistnienia sytuacji naruszenia ochrony danych osobowych. W tym celu powinni:
   1) informować Inspektora Ochrony Danych o podejrzanych osobach,
   2) pracownicy / użytkownicy zewnętrzni powinni na podstawie dokonanej identyfikacji ewentualnych zagrożeń, przedkładać Administratorowi Bezpieczeństwa Informacji projekty i propozycje nowych rozwiązań, których celem jest zwiększenie poziomu ochrony danych osobowych.

§ 12

Sankcje za naruszenie zasad ochrony danych osobowych

1. Naruszenie zasad ochrony danych osobowych przez pracownika / użytkownika zewnętrznego może skutkować postawieniem mu zarzutu popełnienia, jednego z przestępstw określonych w Rozdziale 8 Ustawy.
2. Zgodnie z art. 100 § 2 pkt 5 Kodeksu Pracy, pracownik jest obowiązany przestrzegać tajemnicy określonej w odrębnych przepisach. Dane osobowe, którym jednostka nadaje charakter poufny mają charakter takiej tajemnicy, a jej ujawnienie w zależności od zakresu ujawnionych danych osobowych oraz nastawienia pracownika dopuszczającego się nieuprawnionego ujawnienia danych, może mieć charakter naruszenia lub ciężkiego naruszenia obowiązków pracowniczych.

§ 13

Wymiana informacji dotyczących danych osobowych

1. Pracownicy jednostki oraz użytkownicy zewnętrzni w celu ochrony wymienianych informacji dotyczących danych osobowych powinni podczas przetwarzania uwzględniać następujące zasady:

1) wykorzystywanie technik kryptograficznych do ochrony poufności, integralności i rozliczalności danych osobowych przesyłanych publicznymi sieciami telekomunikacyjnymi,
2) ochrona wymienianych danych osobowych przed przechwyceniem, kopiowaniem, modyfikacją, błędnym wyborem drogi komunikacji i zniszczeniem,
3) zabezpieczenia i ograniczenia związane z możliwościami przekazywania wiadomości za pomocą środków komunikacji,
4) zakaz pozostawiania informacji zawierających dane osobowe przy urządzeniach drukujących, np. kopiarkach, drukarkach, faksach, do których mogą mieć dostęp osoby nieupoważnione,
5) upewnienie się przed przekazaniem danych osobowych, czy rozmówca jest osobą upoważnioną do uzyskania określonych danych osobowych,
6) zachowania szczególnej ostrożności w trakcie rozmów telefonicznych, unikając podsłuchania danych osobowych przez osoby nieupoważnione.

2. Transport danych osobowych w formie elektronicznej i papierowej pomiędzy obszarami, w których są przetwarzane dane osobowe powinien być prowadzony przez osoby upoważnione w sposób ograniczający możliwość ich pozyskanie i odczyt przez osoby nieupoważnione.

§ 14

Przetwarzanie danych osobowych w obszarach bezpiecznych

1. Dane osobowe w jednostce mogą być przetwarzane wyłącznie w pomieszczeniach przetwarzania danych osobowych.
2. Na pomieszczenia przetwarzania danych osobowych składają się pomieszczenia biurowe oraz części pomieszczeń, gdzie jednostka prowadzi działalność.
3. Do pomieszczeń przetwarzania danych osobowych zalicza się:
   1) serwerownia,
   2) pomieszczenia biurowe, w których zlokalizowane są stacje robocze,
   3) pomieszczenia, w których zlokalizowane są zbiory nieinformatyczne.
4. Przebywanie wewnątrz obszarów, o których mowa w ust. 3, osób nieuprawnionych do przetwarzania danych osobowych jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania tych danych lub za zgodą Właściciela zasobów danych osobowych.
5. Budynek lub pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane podczas nieobecności osób upoważnionych do przetwarzania danych osobowych, w sposób ograniczający możliwość dostęp do nich osobom nieupoważnionym.
6. Obszary bezpieczne powinny być odpowiednio zabezpieczone przed skutkami pożaru.
7. Przetwarzanie danych osobowych jest zakazane w tych pomieszczeniach, w których osoby trzecie wykonują prace techniczne.
8. Każdorazowe uchybienie zabezpieczeń fizycznych chroniących dane osobowe powinno być zgłaszane do Inspektora Ochrony Danych.

§ 15

Dopuszczenie osób do przetwarzania danych osobowych

1. Przetwarzanie danych osobowych jest możliwe wyłącznie po uzyskaniu przez pracownika / użytkownika zewnętrznego formalnego upoważnienia do przetwarzania danych osobowych zaakceptowanego przez Administratora Danych Osobowych.
2. Oświadczenia i upoważnienia, o których mowa w ust. 1 przechowuje się w aktach osobowych pracownika.
3. Przełożony pracownika / użytkownika zewnętrznego jest zobowiązany niezwłocznie po ustaniu potrzeby przetwarzania danych osobowych przez pracownika / użytkownika zewnętrznego złożyć rezygnację do Inspektora Ochrony Danych dotyczącą jego dostępu do danych osobowych.

§ 16

Ewidencja osób upoważnionych do przetwarzania danych osobowych

1. Osoby upoważnione do przetwarzania danych osobowych powinny być wpisywane do ewidencji. Ewidencja osób upoważnionych do przetwarzania danych osobowych (ewidencja) powinna być prowadzona przez Inspektora Ochrony Danych.
2. Właściciele zasobów danych osobowych, przełożeni pracowników / użytkowników zewnętrznych odpowiadają za natychmiastowe zgłoszenie do Inspektora Ochrony Danych osób, które utraciły uprawnienia dostępu do danych osobowych.
3. Inspektor Ochrony Danych w oparciu o informacje, o których mowa w ust. 2 powinien podjąć działania, których celem jest uniemożliwienie tym osobom dostępu do danych osobowych i wyrejestrować z ewidencji, o której mowa w ust. 1.

§ 17

Rejestracja zbiorów danych osobowych

1. Upoważnieni pracownicy są zobowiązani do wnioskowania Informatykowi zamiaru utworzenia nowego zbioru danych osobowych wraz z wskazaniem podstawy przetwarzania danych, uzasadnieniem celowości, zakresu i sposobu zbierania danych osobowych.
2. Inspektora Ochrony Danych weryfikuje wniosek o utworzeniu nowego zbioru danych osobowych oraz analizuje nowy zbiór danych pod kątem rejestracji w rejestrze zbiorów danych osobowych.
3. Inspektor Ochrony Danych sprawdza opisane w zgłoszeniu rejestracyjnym warunki techniczne i organizacyjne dotyczące zabezpieczeń w systemie informatycznym, a w przypadku niewystarczającego poziomu zabezpieczeń występuje z wnioskiem do informatyków o podniesienie poziomu tych zabezpieczeń.
4. Informatyk rejestruje zbiór danych w rejestrze zbiorów i wyznacza właściciela danych osobowych dla zarejestrowanego zbioru,

§ 18

Udostępnianie danych osobowych

1. Dane osobowe mogą być udostępniane podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa.
2. Udostępnianie danych osobowych osobie nieupoważnionej do przetwarzania danych osobowych może nastąpić wyłącznie za zgodą Właściciela zasobów danych osobowych. Zarówno wniosek jak i zgoda powinny być wystosowane z zachowaniem formy pisemnej.
3. Udostępniając dane osobowe należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
4. Na pisemny wniosek pochodzący od osoby, której dane dotyczą, informacje o osobie powinny być udzielone w terminie 30 dni od daty złożenia wniosku.
5. Za przygotowanie danych osobowych do udostępnienia w zakresie wskazanym we wniosku jest odpowiedzialny Właściciel zasobów danych osobowych.
6. Informacje zawierające dane osobowe są przekazywane uprawnionym podmiotom lub osobom za potwierdzeniem odbioru, np. w następujący sposób:
   1) listem poleconym za pokwitowaniem odbioru,
   2) teletransmisjia danych zgodnie z zasadami wymiany informacji opisanymi niniejszym dokumencie,
   3) innym bezpiecznym, określonym wymogiem prawnym lub umową.

§ 19

Powierzanie przetwarzania danych osobowych

1. Powierzenie przetwarzania danych osobowych występuje wówczas, gdy podmioty zewnętrzne współpracujące z jednostką mają dostęp do danych osobowych przetwarzanych przez tę jednostke.

2. Wskazane w ust. 1 powierzenie przetwarzania danych osobowych może się odbywać wyłącznie w trybie przewidzianym w art. 31 ustawy poprzez zawarcie na piśmie umowy powierzenia przetwarzania danych osobowych, pomiędzy jednostką organizacyjną a danym podmiotem, któremu zleca się czynności związane z przetwarzaniem danych osobowych lub uwzględnienie kwestii powierzenia w umowach.
3. W sytuacji powierzenia przetwarzania danych osobowych podmiotowi zewnętrznemu, w umowie powierzenia przetwarzania danych osobowych określa się przede wszystkim:
   1) cel i zakres przetwarzania danych osobowych, obowiązek zachowania w tajemnicy danych osobowych oraz informacji o zabezpieczeniach tych danych,
   2) konsekwencje prawne i kary finansowe wynikające z niestosowania się do warunków umowy (z punktu widzenia ochrony danych osobowych),
   3) wymagania bezpieczeństwa dla procesu przetwarzania danych osobowych.

§ 20

Postępowanie w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych

1. Poniższe postanowienia mają zastosowanie zarówno w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych przetwarzanych w systemach informatycznych, jak i w zbiorach nieinformatycznych.
2. Przed przystąpieniem do pracy pracownicy / użytkownicy zewnętrzni zobowiązani są dokonać sprawdzenia stanu urządzeń informatycznych oraz oględzin swojego stanowiska pracy, w tym zwrócić szczególną uwagę, czy nie zaszły okoliczności wskazujące na naruszenie lub próby naruszenia ochrony danych osobowych.
3. Za okoliczności, które uznaje się za naruszenie lub podejrzenie naruszenia ochrony systemu przetwarzającego dane osobowe, uważa się w szczególności:
   1) nieuprawniony dostęp lub próbę dostępu do danych osobowych lub pomieszczeń, w których się one znajdują,
   2) nieuprawnione naruszenie lub próby naruszenia poufności, integralności i rozliczalności danych i systemu,
   3) niezamierzoną zmianę lub utratę danych zapisanych na kopiach zapasowych,
   4) nieuprawniony dostęp do danych osobowych (sygnał o nielegalnym logowaniu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu),
   5) udostępnienie osobom nieupoważnionym danych osobowych lub ich części,
   6) inny stan systemu informatycznego lub pomieszczeń, niż pozostawiony przez użytkownika po zakończeniu pracy,
   7) wydarzenia losowe, obniżające poziom ochrony systemu (np. brak zasilania lub pożar),
   8) kradzież sprzętu informatycznego lub nośników zewnętrznych zawierających dane osobowe (np. wydruków komputerowych, dyskietek, płyt CD/DVD, dysków twardych, pamięci zewnętrznych, itp.).
4. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych pracownicy zobowiązani są do bezzwłocznego powiadomienia o tym fakcie Inspektora Ochrony Danych.
5. Do czasu przybycia Inspektora Ochrony Danych, zgłaszający:
   1) powstrzymuje się od rozpoczęcia lub kontynuowania pracy, jak również od podejmowania jakichkolwiek czynności, mogących spowodować zatarcie śladów naruszenia bądź innych dowodów,
   2) zabezpiecza elementy systemu informatycznego lub kartotek, przede wszystkim poprzez uniemożliwienie dostępu do nich osobom nieupoważnionym,
   3) podejmuje, stosownie do zaistniałej sytuacji, wszelkie niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych,
   4) wykonuje polecenia Inspektora Ochrony Danych.

6. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych Inspektor Ochrony Danych, po przybyciu na miejsce:
   1) ocenia zastałą sytuację, biorąc pod uwagę w szczególności stan pomieszczeń, w których przetwarzane są dane osobowe oraz stan urządzeń, a także szacuje wielkość negatywnych następstw incydentu,
   2) wysłuchuje relacji osoby, która dokonała powiadomienia oraz innych osób związanych z incydentem,
   3) podejmuje decyzje o toku dalszego postępowania, stosownie do zakresu naruszenia lub zasadności podejrzenia naruszenia ochrony danych osobowych.
7. Informatyk sporządza raport z przebiegu zdarzenia, w którym powinny się znaleźć w szczególności informacje:
   1) data i godzina powiadomienia,
   2) godzina pojawienia się w pomieszczeniach, w których przetwarzane są dane,
   3) o sytuacji jaką zastał,
   4) podjętych działaniach i ich uzasadnieniu.
8. W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych, użytkownik może kontynuować pracę dopiero po otrzymaniu pozwolenia od Inspektora Ochrony Danych.
9. W przypadku, gdy naruszenie ochrony danych osobowych jest wynikiem uchybienia obowiązującej w jednostce dyscypliny pracy, Inspektor Ochrony Danych wyjaśnia wszystkie okoliczności incydentu i podejmuje stosowne działania wobec osób, które dopuściły się wskazanego naruszenia.
10. Po zakończeniu czynności naprawczych system powinien utrzymać poziom ochrony nie niższy niż przed wystąpieniem incydentu związanego z naruszeniem ochrony danych osobowych.
11. Administrator danych w przypadku stwierdzenia, że naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, zawiadamia niezwłocznie organ nadzorczy, jednak nie później niż w ciągu 72 godz. od identyfikacji naruszenia.
12. Administrator danych zawiadamia osoby, których dane dotyczą, w przypadku wystąpienia wobec nich naruszeń skutkujących ryzykiem naruszenia ich praw lub wolności, przez zamieszczenie stosownego komunikatu zgodnie z załącznikiem na swojej stronie internetowej jednostki organizacynej.
13. Administrator danych dokumentuje naruszenia, które skutkują naruszeniem praw i wolności osób fizycznych.

§ 21

Zasady ochrony danych osobowych w zbiorach nieinformatycznych

1. Zbiory nieinformatyczne powinny być odpowiednio zabezpieczone przed nieuprawnionym dostępem i zniszczeniem.
2. Dokumenty i wydruki, zawierające dane osobowe, należy przechowywać w zamykanych pomieszczeniach, do których dostęp mają jedynie uprawnione osoby.
3. Na czas nie użytkowania, dokumenty i wydruki zawierające dane osobowe powinny być zamykane w szafach biurowych lub zamykanych szufladach.
4. Wydruki robocze, błędne lub zdezaktualizowane powinny być niezwłocznie niszczone przy użyciu niszczarki do papieru lub w inny sposób zapewniający skuteczne ich usunięcie lub zanonimizowanie.

§ 22

Sposób przydziału identyfikatorów i haseł dla użytkowników

Mając na względzie, iż system informatyczny przetwarzający dane osobowe powinien być wyposażony w mechanizmy uwierzytelniania użytkownika oraz kontroli dostępu do tych danych – dla każdej osoby upoważnionej ustalany jest odrębny identyfikator i hasło. Bezpośredni dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu

identyfikatora i właściwego hasła. Hasła dostępu i identyfikatory przyznawane są indywidualnie dla każdego z użytkowników i znane są tylko właścicielowi.

1. Identyfikator użytkownika:
   a) jest niepowtarzalny,
   b) po wyrejestrowaniu użytkownika z systemu informatycznego nie jest przydzielany innej osobie,
   c) nie podlega zmianie, z wyjątkiem sytuacji, gdy zostanie ujawniony
   d) użytkownicy zobowiązani są do zachowania w tajemnicy ustalonych dla nich identyfikatorów.
2. Hasło użytkownika:
   a) jest przydzielane indywidualnie dla każdego z użytkowników i znane tylko użytkownikowi, który nim się posługuje,
   b) zostaje zmienione przez użytkownika przy pierwszym zalogowaniu,
   c) nie jest zapisywane w systemie w postaci jawnej,
   d) jest utrzymywane w tajemnicy, również po upływie jego ważności,
   e) nie może składać się z kombinacji znaków mogących prowadzić do odszyfrowania przez inne osoby.
3. Użytkownik jest odpowiedzialny za wszystkie czynności wykonywane przy użyciu hasła
4. Użytkownik obowiązany jest utrzymywać hasła, którymi się posługuje lub posługiwał w ścisłej tajemnicy, co obejmuje, w szczególności dołożenie przez niego wszelkich starań w celu uniemożliwienia zapoznania się przez osoby trzecie z hasłem nawet po ustaniu jego ważności, czy też użycia hasła przez te osoby.
5. W przypadku powzięcia przez użytkownika podejrzenia lub stwierdzenia, że z hasłem mogły zapoznać się osoby trzecie, obowiązany jest on niezwłocznie zmienić hasło i powiadomić o tym Inspektora Ochrony Danych.
6. Identyfikator użytkownika jest blokowany lub całkowicie usuwany z systemu informatycznego w każdym przypadku utraty przez niego uprawnień do dostępu do danych osobowych, co ma miejsce w przypadku:
   a) ustania zatrudnienia tego użytkownika w CUS – o czym informację Inspektor Ochrony Danych uzyskuje od pracownika prowadzącego sprawy kadrowe,
   b) zmiany zakresu obowiązków tego użytkownika – o czym informację Inspektor Ochrony Danych uzyskuje od pracownika prowadzącego sprawy kadrowe lub bezpośrednio przełożonego użytkownika.
7. Zablokowanie lub usunięcie identyfikatora użytkownika, który utracił uprawnienia do systemu informatycznego powoduje, że osoba ta nie ma możliwości zalogowania się do sieci lub aplikacji.

§ 23

Kopie bezpieczeństwa
i bezpieczeństwo przed szkodliwym oprogramowaniem

1. Tworzenie, przechowywanie, kontrolowanie i likwidację kopii bezpieczeństwa realizuje informatyk. Szczegóły odnośnie kopii zapasowych określone są w załączniku nr 12 do zarządzenia
2. Na bieżące i bezpośrednie sprawdzanie obecności szkodliwego oprogramowania (wirusów komputerowych) pozwala oprogramowanie automatycznie monitorujące występowania w/w oprogramowania w trakcie załączania i wczytywania danych z zewnętrznych nośników danych, sieci lokalnej czy też Internetu.
3. Nadzór nad instalowaniem nowego oprogramowania antywirusowego oraz nad bieżącą jego aktualizacją sprawuje informatyk.

§ 24

Procedury rozpoczęcia i zakończenia pracy

1. Przed przystąpieniem do pracy w systemie użytkownik obowiązany jest dokonać sprawdzenia stanu urządzeń komputerowych służących do przetwarzania danych osobowych oraz dokonać oględzin swojego stanowiska pracy, ze szczególnym uwzględnieniem czy nie zaszły okoliczności wskazujące na naruszenie ochrony danych osobowych.
2. W przypadku, gdy przerwa w pracy trwa dłuższy okres oraz kończąc pracę użytkownik obowiązany jest wylogować się z aplikacji i systemu komputerowego. Sprawdzić czy nie zostały pozostawione bez zamknięcia nośniki informacji. Opuszczając stanowisko użytkownik zamyka używane przez niego szafy i pomieszczenia, w których przechowuje się dokumentację i nośniki informacji.
3. W przypadku zauważenia przez użytkownika naruszenia zabezpieczenia systemu informatycznego, zauważenia, że stan urządzenia, wartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń danych osobowych, użytkownik ten obowiązany jest niezwłocznie poinformować o tym fakcie Inspektora Ochrony Danych.

§ 25

Eksploatacja, konserwacja systemów i sprzętu.

1. Przeglądy i konserwacje sprzętu komputerowego dokonuje się w miarę potrzeb wynikających z jego obciążenia, warunków zewnętrznych, w których eksploatowane są dane, urządzenia oraz ważności sprzętu dla funkcjonowania całości systemu informatycznego
2. Prace dotyczące przeglądów, konserwacji i napraw wymagające autoryzowanych firm zewnętrznych, są wykonywane przez uprawnionych przedstawicieli tych firm (serwisantów) pod nadzorem Informatyka lub upoważnionej przez niego osoby, bez możliwości dostępu do danych osobowych.
3. Urządzenia, dyski lub inne informatyczne nośniki informacji, przeznaczone do napraw, gdzie wymagane jest zaangażowanie autoryzowanych podmiotów zewnętrznych, pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej przez Inspektora Ochrony Danych.
4. Urządzenia, na których są przetwarzane dane osobowe muszą być wyposażone w sprawne zasilacze awaryjne (UPSy).
5. Sprzęt przenośny taki jak np. tablety, laptopy muszą być zabezpieczone podczas transportu przed uszkodzeniem fizycznym i kradzieżą oraz zabezpieczone przed dostępem osób nieuprawnionych (np. hasłem).

§ 26

Użytkowanie sprzętu komputerowego oraz oprogramowania.

1. Sprzęt informatyczny powinien być użytkowany wyłącznie w celach służbowych. Na stanowiskach pracy może być wykorzystywane wyłącznie oprogramowania legalne oraz zawierające dane niezbędne do wykonywania zadań służbowych.
2. Instalacje oprogramowania na stanowiskach pracy w jednostce dokonywane są z nośników znajdujących się w zasobach ww. jednostki przez upoważnione osoby. Zabrania się nieuprawnionego instalowania oprogramowania, zwłaszcza oprogramowania, którego jednostka organizacyjna nie ma prawa używać np. z powodu braku wymaganych licencji.
3. Zabrania się dokonywania nieuprawnionych zmian w systemach informatycznych lub informacji w nich przetwarzanych.
4. Zabrania się wykorzystywania komputera, a w szczególności sieci Internet i poczty elektronicznej do celów innych niż służbowe, a w szczególności:
   - powszechnie uznanych za szkodliwe, niewłaściwe, niemoralne lub nielegalne,
   - ściągania z Internetu i rozsyłania przy pomocy poczty elektronicznej informacji niezwiązanych z realizowanymi zadaniami służbowymi,

− nieprzestrzegania praw autorskich w stosunku do materiałów zamieszczonych w sieci.

5. Zabrania się wprowadzania nieuprawnionych zmian w zatwierdzonej konfiguracji bazowej, stosowania nielegalnego oprogramowania, nieupoważnionego logowania się poza nominalnymi godzinami pracy (chyba, że pracownik posiada zgodę na inny czas pracy), prób dostępu do plików i folderów do których użytkownik nie ma dostępu. Zabrania się nieuprawnionego pozyskiwania informacji o zasobach informatycznych i środkach ich ochrony.
6. Zabrania się wyłączania lub wstrzymywania funkcjonowania oprogramowania antywirusowego i monitorującego komputer.
7. Zabrania się instalowania, podłączania nośników danych (płyt CD, DVD, dyskietek, pendrive'ów, aparatów cyfrowych, kart pamięci itd.) nie stanowiących własności jednostki organizacyjnej.
8. Zabrania się ingerowania w sprzęt komputerowy (w tym otwierania) znajdujący się w jednostce organizacyjnej osobom nieupoważnionym.
9. Wykorzystywanie komputera, Internetu i poczty elektronicznej, a także infrastruktury sieciowej CUS jest monitorowane. Wszelkie nieprzestrzeganie przepisów i ustaleń w przedmiotowym zakresie stanowić będzie poważne naruszenie obowiązków służbowych oraz dyscypliny pracy.
10. Podejmowanie nieuprawnionych działań mogących obniżyć poziom bezpieczeństwa infrastruktury teleinformatycznej jednostki organizacyjnej, wynikających z niezastosowania się do reguł, o których mowa w tym dokumencie, będzie uznane za działanie na szkodę jednostki organizacyjnej, jak również stanowić będzie naruszenie obowiązków pracowniczych i może być przyczyną pociągnięcia do odpowiedzialności służbowej lub karnej.
11. Pracownik podpisuje oświadczenie, że przyjmuje do wiadomości i stosowania przepisy Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym w jednostce organizacyjnej.

§ 27

Procedura DPIA *(Data Protection Impact Assessment)*

1. Ocenę skutków dla ochrony danych osobowych (DPIA) przeprowadza każdorazowy właściciel procesu wskazany przez administratora danych z wykorzystaniem załącznika nr 1.

2. DPIA jest przeprowadzana przy każdorazowej istotnej zmianie procesu przetwarzania danych osobowych, np. zmiana sposobu przetwarzania danych.

3. DPIA jest przeprowadzana wraz z analizą ryzyka nie rzadziej niż raz w roku w stosunku do procesów, które w wyniku poprzednio przeprowadzonego DPIA wykazały wysokie ryzyko dla praw i wolności osób, których dane dotyczą

§ 28

1. „Każdy przypadek zgłoszenia przez osobę, której dane dotyczą, woli skorzystania z praw przewidzianych w rozporządzeniu administrator danych rozpatruje indywidualnie.

2. Administrator danych niezwłocznie realizuje następujące prawa osób, których dane dotyczą:

a) prawo dostępu do danych,
b) prawo do sprostowania danych,
c) prawo do usunięcia danych,
d) prawo do przenoszenia danych,
e) prawo do sprzeciwu wobec przetwarzania danych,
f) prawo do niepodlegania decyzjom oparty wyłącznie na profilowaniu.

3. W przypadku realizacji prawa do sprostowania, usunięcia i ograniczenia przetwarzania danych administrator danych niezwłocznie informuje odbiorców danych, którym udostępnił on przedmiotowe dane, chyba że jest to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.

4. Administrator danych odmawia realizacji praw osób, których dane dotyczą, **je**żeli możliwość taka wynika z przepisów rozporządzenia, jednak każda odmowa realizacji praw osób, których dane dotyczą, wymaga uzasadnienia z podaniem podstawy prawnej wynikającej z rozporządzenia.

§ 29

1. W każdym przypadku pobierania danych bezpośrednio od osoby, której dane dotyczą, administrator danych informuje osobę, której dane dotyczą, zgodnie z załącznikiem nr 12.
2. W każdym przypadku pobierania danych z innych źródeł niż osoba, której dane dotyczą, administrator danych informuje osobę, której dane dotyczą, niezwłocznie, jednak nie później niż przy pierwszym kontakcie z osobą, której dane dotyczą, zgodnie z załącznikiem nr 12.
3. W każdym przypadku odbierania zgody od osoby, której dane dotyczą, korzysta się z klauzul zgody zgodnie z załącznikiem nr 12.

§ 30

W sprawach nieuregulowanych stosuje się przepisy rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych z dnia 09. 11.2017 r. (t.j. Dz. U. z 2017 r. poz. 2247 ze zm.), 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 (ogólnego rozporządzenia o ochronie danych) (dalej jako „RODO") oraz ustawy o ochronie danych osobowych (Dz. U. poz. 1000 z 2018 roku).

załącznik nr 1
do Polityki bezpieczeństwa i
instrukcji zarządzania
systemem informatycznym

UPOWAŻNIENIE
DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1) – dalej **RODO** – nadaję upoważnienie Pani/Panu:

…….
(imię i nazwisko)

(stanowisko)

do przetwarzania danych osobowych w zakresie pełnionych obowiązków służbowych na zajmowanym stanowisku, tj. uzyskuje Pani/Pan upoważnienie do przetwarzania danych osobowych:

…….
(Nazwa zbioru(ów) / Oznaczenie zbioru (ów/ nazwa czynności przetwarzania))

Jednocześnie zobowiązuję Panią/Pana do przetwarzania danych osobowych, zgodnie z udzielonym upoważnieniem oraz z przepisami RODO, Kodeksu pracy, a także z Polityką ochrony danych osobowych Pracodawcy.
Jednocześnie upoważniam Panią/Pana do tworzenia/posiadania dla potrzeb wykonywanej pracy zestawień, ewidencji oraz rejestrów z danymi osobowymi, z zachowaniem pełnej ich ochrony przy zastosowaniu środków technicznych i organizacyjnych wdrożonych w jednostce organizacyjnej .
Okres ważności
od:
do:

……
podpis osoby uprawnionej do nadania upoważnienia

Data wygaśnięcia* ……..……..
Odwołano, dnia …….

……
podpis osoby uprawnionej do odwołania upoważnienia

* Data rozwiązania stosunku pracy/umowy cywilnoprawnej

załącznik nr 2
do Polityki bezpieczeństwa i
instrukcji zarządzania
systemem informatycznym

_____
imię i nazwisko

_____
stanowisko służbowe

OŚWIADCZENIE

Oświadczam, że przyjąłem/przyjęłam do wiadomości i stosowania przepisy Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym w jednostce organizacyjnej, a w szczególności, iż istnieje **całkowity zakaz**:

- samodzielnego podłączania jakichkolwiek urządzeń oraz nośników zewnętrznych do służbowych komputerów;
- dokonywania nieuprawnionych zmian w systemach informatycznych lub informacji w nich przetwarzanych;
- dokonywania nieuprawnionych prób testowania zauważonych podatności (luk w zabezpieczeniu systemu);
- wykorzystywania komputera, Internetu i poczty elektronicznej do celów innych niż służbowe, a w szczególności:
  1. uznanych powszechnie za szkodliwe, niewłaściwe, niemoralne lub nielegalne;
  2. ściągania z Internetu i rozsyłania przy pomocy poczty elektronicznej informacji niezwiązanych z realizowanymi zadaniami służbowymi;
  3. nieprzestrzegania praw autorskich w stosunku do materiałów zamieszczonych w sieci.

- wprowadzania nieuprawnionych zmian w zatwierdzonej konfiguracji bazowej, stosowania nielegalnego oprogramowania, nieupoważnionego logowania się poza nominalnymi godzinami pracy (chyba, że pracownik posiada zgodę na inny czas pracy), prób dostępu do plików i folderów do których użytkownik nie ma dostępu;
- nieuprawnionego pozyskiwania informacji o zasobach informatycznych i środkach ich ochrony;
- nieuprawnionego instalowania oprogramowania, zwłaszcza oprogramowania, którego jednostka organizacyjna nie ma prawa używać np. z powodu braku wymaganych licencji.

Sprzęt informatyczny winien być użytkowany wyłącznie w celach służbowych.

Na stanowiskach pracy mogą być wykorzystywane wyłącznie oprogramowania legalne oraz zawierające dane niezbędne do wykonywania zadań służbowych.

Instalacje oprogramowania na stanowiskach pracy w jednostce dokonywane są z nośników znajdujących się w zasobach ww. jednostki przez upoważnione osoby.

Wykorzystywanie komputera, Internetu i poczty elektronicznej, a także infrastruktury sieciowej CUS jest monitorowane.

Wszelkie nieprzestrzeganie przepisów i ustaleń w przedmiotowym zakresie stanowić będzie poważne naruszenie obowiązków służbowych oraz dyscypliny pracy. Podejmowanie nieuprawnionych działań mogących obniżyć poziom bezpieczeństwa infrastruktury teleinformatycznej jednostki, wynikających z niezastosowania się do reguł, o których mowa w niniejszym zarządzeniu, będzie uznane za działanie na szkodę jednostki, jak również stanowić będzie naruszenie obowiązków pracowniczych i może być przyczyną pociągnięcia do odpowiedzialności służbowej lub karnej.

Za zainstalowane oprogramowania na serwerach jednostki odpowiadają administratorzy tych serwerów wg posiadanych uprawnień. Dodatkowe, legalne oprogramowanie może być zainstalowane na pisemny wniosek zaakceptowany przez Inspektora Ochrony Danych i Informatyka.

Informatyk prowadzą kontrolę legalności oprogramowania, do której mogą być wykorzystywane programy kontrolne. Nadzór nad wykonywaniem przepisów zarządzenia sprawują Informatyk

Zapoznanie się z w/w poleceniami i potwierdzam własnoręcznym podpisem.

miejscowość	*data*	*podpis składającego oświadczenie*

załącznik nr 3
do Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym

LP	Nazwa czynności przetwarzania	Jednostka organizacyjna (departament, dział itp.)	Cel przetwarzania	Kategorie osób	Kategorie danych	Podstawa prawna	Źródło danych	Planowany termin usunięcia kategorii danych *(jeżeli jest to możliwe)*	Nazwa współadministratora i dane kontaktowe *(jeśli dotyczy)*	Nazwa podmiotu przetwarzającego i dane kontakowe *(jeśli dotyczy)*	Kategorie odbiorców *(innych niż podmiot przetwarzający)*	Nazwa systemu lub oprogramowania	Ogólny opis technicznych i organizacyjnych srodków bezpieczeństwa zgodnie z art. 32 ust. 1 ***(jeżeli jest to możliwe)***	DPIA (jeśli tak, lokalizacja raportu)	Transfer do kraju trzeciego lub org. międzynarodowej	
															Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiotu)	Jeśli transfer i art. 49 ust. 1 akapit drugi - dokumentacja odpowiednich zabezpieczeń
			Art.. 30 ust. 1 pkt b	**Art.. 30 ust. 1 pkt c**	**Art.. 30 ust. 1 pkt c**			**Art.. 30 ust. 1 pkt f**	**Art.. 30 ust. 1 pkt a**	**Art.. 30 ust. 1 pkt d**	**Art.. 30 ust. 1 pkt d**		**Art.. 30 ust. 1 pkt g**		**Art. 30 ust. 1 pkt e**	**Art. 30 ust. 1 pkt e**
1																

załącznik nr 4
do Polityki bezpieczeństwa
i instrukcji zarządzania systemem informatycznym

Ewidencja osób upoważnionych przez Administratora Danych Osobowych do przetwarzania danych osobowych

L.p.	Numer	Imię i nazwisko	Data		Uwagi	Zakres
			Nadania	Ustania		
1.	*2.*	*3.*	*4.*	*5.*	*6.*	*7.*

** - Zakres: p – przetwarzanie danych osobowych, k – przetwarzanie danych osobowych oraz obsługa systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych Centrum Usług Społecznych w Będzinie*

załącznik nr 5
do Polityki bezpieczeństwa
i instrukcji zarządzania systemem informatycznym

Wykaz obszaru przetwarzania danych osobowych w jednostce organizacyjnej

Dane osobowe w jednostce organizacyjnej są przetwarzane w niżej wymienionych lokalizacjach:

a) budynek jednostki organizacyjnej , w tym:
   - pomieszczenia biurowe,
   - serwerownia,
b) budynek w którym mieści się Archiwum,

załącznik nr 6
do Polityki bezpieczeństwa
i instrukcji zarządzania systemem informatycznym

Raport z naruszenia bezpieczeństwa systemu w jednostce organizacyjnej

1. Data, godzina i miejsce zdarzenia *(np. nr pokoju, nazwa pomieszczenia)*:

   _____

   _____

2. Osoba powiadamiająca o zaistniałym zdarzeniu *(imię, nazwisko, stanowisko służbowe)*:

   _____

   _____

3. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

   _____

   _____

   _____

   _____

4. Podjęte działania:

   _____

   _____

   _____

   _____

5. Przyczyny występowania zdarzenia:

   _____

   _____

   _____

   _____

_____

(podpis Inspektora Ochrony Danych)

załącznik nr 8 do Polityki
bezpieczeństwa i instrukcji zarządzania
systemem informatycznym

Wykaz osób, które zostały zapoznane z "Polityką bezpieczeństwa i instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w jednostce organizacyjnej

Przyjąłem/Przyjęłam do wiadomości i stosowania zapisy "Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w jednosce.

L.p.	**Imię i nazwisko**	**Stanowisko**	**Data**	**Podpis**
1.	*2.*	*3.*	*4.*	*5.*

Załącznik
nr 9 do Polityki
bezpieczeństwa i
instrukcji
zarządzania
systemem
informatycznym

REGULAMIN ZARZĄDZANIA INCYDENTAMI W JEDNOSTCE

§ 1.

Regulamin zarządzania incydentami w jednostce wprowadza procedury reagowania na incydenty. W dokumencie tym opisano sposoby działania w przypadku wystąpienia incydentów związanych z bezpieczeństwem informacji. Regulamin zawiera również listę incydentów. Ilekroć w regulaminie jest mowa o:

1) **Pełnomocniku Bezpieczeństwa Cyberprzestępczości (PBC)** – rozumie się przez to osobę odpowiedzialną za bezpieczeństwo w dziedzinie informatycznej;
2) **Administratorze Danych Osobowych (ADO) –** rozumie się przez to kierownika jednostki
3) **Inspektorze Ochrony Danych (IOD) –** rozumie się przez to osobę odpowiedzialną za ochronę danych osobowych;
4) **Operatorze obsługi incydentu** - rozumie się przez to osobę wyznaczoną przez IOD, której rolą jest podejmowanie działań związanych z usunięciem incydentu – Informatyk;
5) **Zdarzeniu związanym z bezpieczeństwem informacji** - rozumie się przez to określony stan systemu, usługi lub sieci, który wskazuje na możliwe naruszenie polityki bezpieczeństwa informacji, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem;
6) **Incydencie związanym z bezpieczeństwem informacji** - rozumie się przez to pojedyncze zdarzenie lub serię niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań i zagrażają bezpieczeństwu informacji;
7) **Liście incydentów** – rozumie się przez to listę zdarzeń, które mogą zostać zaklasyfikowane jako incydent bezpieczeństwa informacji. Lista ta stanowi pomoc poszczególnym pracownikom i osobom współpracującym w ramach właściwego rozpoznania i reakcji na potencjalny incydent;
8) **Rejestrze incydentów** – rozumie się przez to rejestr zawierający zaistniałe incydenty bezpieczeństwa informacji wraz z określonym statusem i odpowiedzialnościami w zakresie incydentu bezpieczeństwa.

§ 2.

Zgłaszanie zdarzeń związanych z bezpieczeństwem informacji oraz postępowanie z incydentami.

1. Pracownik, który podejrzewa, że zaistniało zdarzenie, które powinno być zaklasyfikowane jako incydent bezpieczeństwa zgłasza jak najszybciej dane zdarzenie na podstawie listy incydentów. Incydenty zgłaszane są w formie telefonicznej lub przy pomocy poczty elektronicznej do Informatyka, PBC lub IOD.
2. W przypadku gdy zachodzi konieczność natychmiastowej reakcji na zaistniały incydent (np. kradzież lub wyciek dokumentów) należy dodatkowo poinformować bezpośredniego przełożonego.
3. W przypadku, gdy zdarzenie ma miejsce poza godzinami pracy jednostki zdarzenie to należy zgłosić do swojego przełożonego, który zobowiązany jest bezzwłocznie

dany incydent eskalować zgodnie ze zdefiniowaną ścieżką kontaktową.

§ 3.

Proces weryfikacji incydentów bezpieczeństwa informacji.

1. Informatyk lub IOD dokonuje wstępnej identyfikacji zdarzenia i na podstawie dostępnych informacji oraz analizy okoliczności kwalifikuje zdarzenie (lub serię zdarzeń) jako:
   1) zdarzenie nie mające cech naruszenia bezpieczeństwa informacji, np. zaplanowana przerwa technologiczna,
   2) błąd w działaniu elementu systemu teleinformatycznego, infrastruktury teleinformatycznej lub infrastruktury biurowej,
   3) awaria techniczna czasowo blokująca dostępność informacji,
   4) incydent niskiej kategorii - związany z naruszeniem bezpieczeństwa informacji, a szczególnie jej integralności i poufności, nie generujący kar finansowych, jednak powodujący pośrednio lub bezpośrednio utrudnienia w realizacji jakiegokolwiek procesu głównego jednostki,
   5) incydent średniej kategorii - związany z naruszeniem bezpieczeństwa informacji skutkujący pośrednio lub bezpośrednio zatrzymaniem realizacji jakiegokolwiek procesu ustawowego i/lub stratami finansowymi nie przekraczającymi kwoty wynikającej z art. 4 pkt 8 ustawy prawo zamówień publicznych (j.t. Dz.U.2015.2164 ze zm.) oraz możliwością konsekwencji prawnych i/lub utraty wizerunku,
   6) incydent wysokiej kategorii - związany z naruszeniem bezpieczeństwa informacji, którego skutkiem jest destrukcja (zniszczenie, utrata) kluczowych zasobów i przerwanie funkcjonowania procesów jednostki; skutki tego incydentu powodują uruchomienie Planu Ciągłości Działania i wznowienie funkcjonowania jednostki; incydentem wysokiej kategorii jest również incydent, którego skutki mogą spowodować straty przekraczające kwotę wynikającej z art. 4 pkt 8 ustawy prawo zamówień publicznych (j.t. Dz.U.2015.2164 ze zm.).
2. O możliwości zaistnienia przypadku naruszenia bezpieczeństwa informacji mogą świadczyć:
   1) nadmierne, w stosunku do wykonywanych zadań (zakresu upoważnienia), uprawnienia użytkownika do zasobów systemu,
   2) niestabilna praca systemu teleinformatycznego,
   3) korzystanie z zasobów systemu poza godzinami pracy (bez zgody przełożonego),
   4) nowe „podejrzane" (nieznane) konta użytkowników,
   5) wysoka aktywność kont, które długo pozostawały niewykorzystane,
   6) zanotowanie w krótkim czasie dużej liczby nieudanych prób logowania,
   7) anomalie w pracy systemu lub programu (świadczące np. o obecności wirusa komputerowego),
   8) naruszenie lub wadliwe funkcjonowanie zabezpieczeń fizycznych w pomieszczeniach, w których następuje przetwarzanie informacji w jednostce (uszkodzone zamki, okna, drzwi, naruszone plomby, itp.).
3. PBC wraz z IOD dokonuje ostatecznej klasyfikacji incydentu oraz przeprowadza analizę incydentu.
4. Analiza incydentu uwzględnia następujące kryteria:
   1) charakter incydentu i jego znaczenie związane z naruszeniem bezpieczeństwa fizycznego lub teleinformatycznego,
   2) miejsce wystąpienia incydentu - identyfikacja punktu, w którym nastąpiło zdarzenie (lokalizacja, serwer, stacja robocza itp.),
   3) liczba komórek organizacyjnych jednostki, zakres zasobów dotkniętych incydentem,
   4) identyfikację zasobów potrzebnych przy dalszych działaniach w ramach postępowania z

incydentem związanym z bezpieczeństwem informacji,
5) możliwości rozszerzania się incydentu i sposoby jego ograniczania,
6) szacowany poziom szkód finansowych,
7) rodzaj ujawnionej informacji (jeśli ma zastosowanie – np. dane osobowe),
8) szacunkowy czas, po którym skutki incydentu zostaną zlikwidowane, jeżeli nie ma możliwości natychmiastowego usunięcia stanu naruszenia bezpieczeństwa informacji,
9) skutki organizacyjne i prawne (wstępny szacunek).

5. W przypadku, gdy incydent ma skutki przekładające się na możliwość zakłócenia działalności ustawowej bądź statutowej CUS, IOD informuje niezwłocznie kierownika jednostki.

7. W przypadku, gdy zasięg i szacunkowy czas trwania powoduje zakwalifikowanie incydentu jako incydentu wysokiej kategorii, IOD informuje niezwłocznie kierownika jednostki.

8. W przypadku, gdy zasięg incydentu wykracza poza system teleinformatyczny jednostki, Informatyk, w porozumieniu z IOD i z zastrzeżeniem posiadania stosownej umowy o poufności z właściwymi podmiotami zewnętrznymi, może przekazać do podmiotu zewnętrznego informacje o incydencie zawierające:
1) typ zdarzenia,
2) informacje o odległym systemie, który może być źródłem naruszenia, w tym nazwy serwerów, adresy IP, identyfikatory użytkowników,
3) wszystkie zapisy z rejestrów zdarzeń w określonym przedziale czasowym,
4) inne informacje określone w umowie z podmiotem zewnętrznym.

9. W przypadku, gdy rodzaj i zasięg incydentu, zidentyfikowany na którymkolwiek z etapów postępowania, uzasadnia potrzebę powiadomienia organów ścigania, to decyzję o sposobie i terminie powiadomienia podejmuje kierownik jednostki.

10. W przypadku wystąpienia incydentu komputerowego PBC informuje właściwy zespół CERT.

§ 4.

Ograniczanie skutków incydentu

1. Informatyk prowadzi bieżącą dokumentację incydentu. Dokumentacja ta w szczególności obejmuje:
1) wszystkie zdarzenia zachodzące w systemie informacyjnym (zapisy systemowych dzienników audytu zdarzeń i dzienników audytu, lub zapisy z elektronicznych systemów zabezpieczeń),
2) wszystkie podejmowane działania (opatrzone datą i czasem).

2. Dokumentacja incydentu podlega rygorom ochrony przez tworzenie autoryzowanych kopii tych elementów systemu, które mają zastosowanie przy postępowaniu z incydentem tzn. rejestry urządzeń, systemów operacyjnych i aplikacji, kopie zapasowe, pliki konfiguracyjne i systemowe, bezpieczne przechowywanie tych kopii, przyjęcia dokumentacji oraz jej wszystkich części.

3. Informatyk przeprowadza działania zmierzające do ograniczenia skutków incydentu i zidentyfikowania źródła naruszenia bezpieczeństwa. W tym celu mogą spowodować zablokowanie części systemu lub dostępnych usług.

4. W przypadku, gdy działania opisane w ust. 3 obejmują wyłączenie lub ograniczenie funkcjonowania zasobów niezbędnych do realizowania celów ustawowych bądź statutowych jednostki, Informatyk przedstawiają decyzję do akceptacji kierownikowijednostki.

§ 5.

Odtwarzanie systemu informacyjnego

1. Z zastrzeżeniem ust. 4, Informatyk przystępuje do odtworzenia systemu po zidentyfikowaniu i usunięciu lub zablokowaniu źródła incydentu.

2. W przypadku zaistnienia sytuacji, kiedy nastąpiło uruchomienie Planu Ciągłości Działania, odtwarzanie systemu jest realizowane w oparciu o procedury opisane w tym planie.

3. Odtwarzanie systemu odnosi się do punktu odtworzenia, co do którego Informatyk ma uzasadnioną pewność, że nie zawiera źródła incydentu.

4. Zasoby w postaci oprogramowania oraz danych są odtwarzane z oryginalnych źródeł dystrybucji oprogramowania oraz kopii zapasowych.

§ 6.

Rejestrowanie informacji o incydentach

1. IOD prowadzi rejestr incydentów zawierający następujące informacje:

1) opis incydentu,
2) datę i godzinę zgłoszenia incydentu,
3) dane identyfikujące osobę zgłaszającą,
4) dane osoby poinformowanej o incydencie,
5) datę zarejestrowania incydentu,
6) dane identyfikujące osobę rejestrującą incydent,
7) informację o zgromadzonych materiałach dowodowych,
8) informacje dotyczące sposobu postępowania z incydentem.

2. IOD zapewnia właściwe wykorzystanie informacji o incydentach związanych z bezpieczeństwem informacji dla celów szkoleniowych i doskonalenia systemu zarządzania bezpieczeństwem informacji.

załącznik nr 1
do Regulaminu zarządzania incydentami

Lista incydentów związanych z bezpieczeństwem informacji

Obszar teleinformatyczny.

1. Zidentyfikowanie złośliwego oprogramowania np. wirus, spyware (stacje robocze oraz systemy lub serwery).
2. Niestabilna praca systemów zaklasyfikowanych jako ważne i krytyczne oraz stacji roboczych.
3. Awaria systemu informatycznego.
4. Niedostępność systemu informatycznego.
5. Awaria zasilania urządzeń przetwarzających informacje (stacje robocze oraz systemy lub serwery).
6. Utrudniona praca w systemie np. zbyt duże obciążenie procesora, przekroczenie dostępnych zasobów systemowych.
7. Nadmierne uprawnienia w systemach w stosunku do wykonywanej pracy.
8. Nieuprawniona zmiana danych lub ich uszkodzenie.
9. Utrata danych.
10. Fizyczne zniszczenie lub uszkodzenie sprzętu oraz nośników przetwarzających informacje.
11. Kradzież sprzętu przetwarzającego informacje.
12. Błędy w obsłudze i konserwacji sprzętu komputerowego służącego do przetwarzania informacji.
13. Błędy w przechowywaniu, eksploatacji oraz konserwacji oprogramowania.
14. Włamanie do sieci i systemów teleinformatycznych (np. atak hackera).
15. Niewykonanie kopii bezpieczeństwa.
16. Niezweryfikowanie możliwości odtworzenia danych z kopii zapasowych.

Incydenty bezpieczeństwa informacji związane ze stronami zewnętrznymi.

1. Ujawnienie danych osobom nieuprawnionym.
2. Brak stosownych zabezpieczeń w umowach ze stronami trzecimi.
3. Pozostawienie bez nadzoru przedstawicieli strony trzeciej (np. serwisanci).

Incydenty związane z bezpieczeństwem osobowym.

1. Nowy pracownik nie podpisał oświadczenia o zachowaniu poufności.
2. W wyniku rozwiązania umowy z pracownikiem nie podjęto działań związanych z odebraniem uprawnień.
3. Pracownik nie rozliczył się z powierzonych środków przetwarzania informacji.

Bezpieczeństwo fizyczne i środowiskowe.

1. Nieuprawniony dostęp do strefy administracyjnej.
2. Umieszczono środki przetwarzania informacji w strefie ogólnodostępnej.
3. Wejście do strefy administracyjnej.
4. Wejście do pomieszczeń teletechnicznych.
5. Pozostawienie otwartych okien, drzwi po zakończeniu pracy.
6. Pożar, zalanie.
7. Pozostawienie środków przetwarzania informacji bez nadzoru.
8. Nieprzestrzeganie polityki czystego biurka.
9. Odnotowanie dokumentów w koszu na śmieci.
10. Pozostawienie wydruków na ogólnodostępnej drukarce.
11. Nieautoryzowane wykonanie kopii klucza do pomieszczeń biurowych.
12. Wyniesienie klucza poza CUS w Będzinie.

13. Zagubienie klucza.

Incydenty związane z zarządzaniem aktywami.

1. Zidentyfikowano środek przetwarzający informacje nieznanego pochodzenia (sprzęt, nośnik).
2. Wykorzystano niezinwentaryzowany środek przetwarzania informacji.

Incydenty związane z pracą w systemie informatycznym.

1. Wykorzystanie nielegalnego oprogramowania oraz narzędzi służących do obchodzenia zabezpieczeń w systemach informatycznych.
2. Próba instalacji niezatwierdzonego oprogramowania.
3. Wykorzystanie ogólnodostępnych serwisów pocztowych (np. Wirtualna Polska, Onet.pl, o2.pl) w celach służbowych.
4. Wykorzystanie służbowej poczty elektronicznej do celów prywatnych.
5. Niezgłaszanie informacji o nieprawidłowym działaniu systemów bezpieczeństwa (firewall, program AV).
6. Zmiana konfiguracji sprzętowej oraz programowej systemów oraz stacji roboczych przez niepowołane osoby.
7. Wykonywanie pracy na odległość (zdalnej) przy pomocy komputera innego niż służbowy.
8. Zablokowane konto w systemach informatycznych.
9. Podjęcie pracy w stanie zagrożenia bezpieczeństwa informacji.
10. Niestosowanie się do wymagań dotyczących złożoności haseł.
11. Niezablokowana stacja robocza.
12. Przesłanie wiadomości e-mail do niewłaściwego adresata.
13. Przechowywanie haseł w niewłaściwy sposób.
14. Przekazywanie haseł innym osobom.
15. Pojawienie się nieautoryzowanej informacji na stronie internetowej.
16. Niewłaściwe niszczenie nośników z danymi pozwalającymi na ich odczyt.
17. Wykorzystanie służbowych środków przetwarzania informacji do celów prywatnych

Załącznik nr 2
do Regulaminu zarządzania incydentami

Wzór raportu z incydentu

RAPORT O INCYDENCIE BEZPIECZEŃSTWA INFORMACJI

A. ZGŁOSZENIE INCYDENTU

(wypełnia osoba zgłaszająca zdarzenie/incydent)

DANE OSOBY ZGŁASZAJĄCEJ

imię i nazwisko.....

stanowisko

służbowe .....

OPIS INCYDENTU:

.....

.....

.....

.....

.....

.....

.....

.....

komu zgłoszono:

.....

data i godzina zgłoszenia: .....

Podpis osoby zgłaszającej .....

B. DZIAŁANIA PO ZAISTNIENIU INCYDENTU

(wypełnia osoba rozpatrująca zgłoszenie incydentu)

OSOBY, KTÓRA PRZYJĘŁA ZGŁOSZENIE INCYDENTU

- Informatyk/ Inspektor Ochrony Danych

imię i nazwisko.....

stanowisko

służbowe .....

INFORMACJE O INCYDENCIE

Nr incydentu zgodny z rejestrem incydentów (nr/rok) .....

Data i czas zajścia incydentu .....

Data i czas wykrycia incydentu .....

Data i czas zgłoszenia incydentu .....

Czy incydent jest zakończony? a) TAK b) NIE

Jeśli tak, to jak długo trwał (dni/godziny/minuty)? .....

Jeśli nie, należy określić jak długo już trwa? .....

Kogo powiadomiono z kierownictwa? .....

OPIS WSTĘPNY / PODJĘTE DZIAŁANIA / ZABEZPIECZENIE MATERIAŁU DOWODOWEGO

.....

.....
.....
.....
.....

Załączniki (materiał dowodowy):

1. .....
2. .....
3. .....

OPIS ROZWIĄZANIA PROBLEMU

.....
.....
.....
.....

Data i podpis: .....

Załącznik nr 3
do Regulaminu zarządzania incydentami

Rejestr incydentów

(pod rejestr należy podpiąć raport z incydentu stanowiący integralną część)

Nr incydentu (nr/rok)	**Osoba zgłaszająca**	**Rodzaj (typ) incydentu**	**Data incydentu**

załącznik nr 10
do Polityki bezpieczeństwa
i instrukcji zarządzania
systemem informatycznym

PLAN CIĄGŁOŚCI DZIAŁANIA W JEDNOSTCE ORGANIZACYJNEJ

§ 1.
Wprowadzenie

Utrata możliwości funkcjonowania jednostki organizacyjnej, w konsekwencji zajścia niekorzystnych incydentów operacyjnych może stać się przyczyną zakłóceń w funkcjonowaniu społeczeństwa lokalnego, wynikających z niemożności świadczenia usług.

W celu minimalizacji wpływu incydentów i zakłóceń w funkcjonowaniu jednostki organizacyjnej wdrożony został niniejszy Plan Ciągłości Działania systemów informatycznych rozumiany jako zestaw środków technicznych i organizacyjnych umożliwiających utrzymanie - w przypadku poważnej awarii lub katastrofy - ciągłości realizacji lub jak najszybsze odtworzenie najważniejszych procesów informatycznych przy minimalizacji wpływu zaistniałej sytuacji na działanie jednostki organizacyjnej.

§ 2.
Przypadki zastosowania.

1. Plan Ciągłości Działania opracowany został na wypadek czasowych lub długotrwałych sytuacji kryzysowych dwojakiego rodzaju, ogólnie określonych jako:

a) awaria informatycznych systemów przetwarzania w lokalizacji podstawowej jednostki, która może skutkować koniecznością użycia systemów zapasowych,

b) niemożność korzystania z siedziby jednostki organizacyjnej.

2. Rodzaj pierwszy oznacza sytuacje, w których generalnie ujmując nie jest dostępny przynajmniej jeden z niżej wymienionych elementów:
   a) systemy informatyczne obsługujące lokalizacje podstawową,
   b) systemy komunikacyjne obsługujące lokalizacje podstawową,
   c) dostawa mediów niezbędnych do funkcjonowania systemów w skali lokalnej (np. energia elektryczna).
3. Drugi rodzaj to sytuacja, w której lokalizacja podstawowa jest niedostępna lub nie może być używana, co może być spowodowane m.in. zagrożeniem lub atakiem terrorystycznym, pożarem lub brakiem mediów.

§ 3.
Odpowiedzialność i uprawnienia.

1. Za opracowanie i realizację niniejszego Planu Ciągłości Działania odpowiedzialny jest Inspektor Ochrony Danych.
2. Za nadzór nad realizacją działań związanych z opracowaniem i utrzymaniem Planu Ciągłości Działania odpowiedzialni są Informatycy.

§ 4.
Działania.

W poniższej tabeli przedstawiono działania mające na celu przywrócenie funkcjonowania jednostki. Czynności te należy dostosować do zaistniałej sytuacji, a czas przywrócenia funkcjonowania powinien być jak najkrótszy.

Lp.	Funkcja	Opis działań	Realizacja planu/osoby odpowiedzialne
1.	zweryfikować zasadność zgłoszenia użytkownika	sprawdzić czy zgłoszenie dotyczy incydentu spowodowanego awarią systemu informatycznego	zapewnić dostęp do infrastruktury informatycznej skąd pochodzi zgłoszenie odpowiedzialny: informatyk
2.	ustalić źródło awarii	ustalić przyczynę awarii: − przerwa w zasilaniu prądem − brak połączenia z internetem − wadliwe działanie sprzętu − wadliwe działanie aplikacji − wadliwe działanie systemu na którym uruchomiona jest aplikacja	zapewnić: − dostęp do serwerowni oraz sprzętu który uległ awarii − kontakt z osobą, która może w porze nocnej zapewnić dostęp do budynku jednostki odpowiedzialny: IOD, Informatyk
3.	określić skalę (obszar) awarii	ustalić czy awaria ma wpływ na pracę: − jednego użytkownika − jednego pomieszczenia (do 3 osób) − jednego referatu (4-15 osób) całego budynku	zapewnić: − kontakt z kierownikami referatów oraz kierownikami jednostek organizacyjnych mieszczących się w budynku odpowiedzialny: IOD
4.	ustalić czy wznawianie usługi może odbywać się w dotychczasowej lokalizacji	działanie ma na celu zweryfikowanie czy wznawiane usługi uruchamiane będą w dotychczasowej lokalizacji czy w lokalizacjach alternatywnych	zapewnić: − możliwość uruchomienia dodatkowych usług w danej lokalizacji (zasilanie prądem, infrastruktura sieciowa) odpowiedzialny:Informatyk
5.	zakupić niezbędne elementy wyposażenia, dokonać naprawy (wymiany) urządzeń, uruchomić aplikacje	w przypadku braku możliwości zakupu należy zastosować rozwiązanie alternatywne (np. przeniesienie aplikacji na stałe na inny serwer).	zapewnić: − środki potrzebne na zakup elementów potrzebnych do uruchomienia nowego systemu odpowiedzialny: Informatyk, IOD
6.	rozpatrzyć i zweryfikować	sprawdzić czy aplikacja może być uruchomiona na którymś	odpowiedzialny: Informatyk

	możliwość przeniesienia aplikacji na inny serwer	z prawidłowo działających serwerów	
7.	przygotować serwer zastępczy	uruchomić serwer zastępczy i uruchomić odpowiedni system informatyczny/aplikację. Po uruchomieniu aplikacji na serwerze zastępczym należy przetestować jej działanie.	zapewnić: − serwer zastępczy, który w podstawowym zakresie pozwoli na uruchomienie podstawowych usług odpowiedzialny: Informatyk
8.	podjąć decyzję o terminie odtworzenia serwera	w razie konieczności należy skontaktować się z kierownikami referatów i komórek organizacyjnych	zapewnić: − kontakt z kierownikami referatów oraz kierownikami jednostek organizacyjnych mieszczących się w budynku odpowiedzialny: IOD
9.	przywrócić funkcjonowanie aplikacji/systemu	spróbować usunąć przyczynę nieprawidłowego działania, a w razie konieczności odtworzyć aplikację korzystając z kopii zapasowych	zapewnić: − dostęp do najbardziej aktualnej wersji aplikacji − dostęp do najbardziej aktualnej bazy danych odpowiedzialny: Informatyk
10.	sprawdzenie aplikacji/systemu	po przeniesieniu i uruchomieniu aplikacji należy zweryfikować jej działanie na serwerze	odpowiedzialny: Informatyk
11.	uruchomienie usługi w systemie teleinformatycznym CUS	po uruchomieniu usługi należy powiadomić o tym fakcie odpowiednie osoby	zapewnić: − kontakt z kierownikami referatów oraz kierownikami jednostek organizacyjnych mieszczących się w budynku odpowiedzialny: IOD

§ 5.
Lokalizacja zapasowa (awaryjna)

1. Lokalizacja zapasowa (awaryjna) jest uruchamiana w przypadku gdy lokalizacja podstawowa jest niedostępna lub nie może być używana (sytuacja kryzysowa).
2. Informatyk zapewnia możliwość działania jednostki w lokalizacji zapasowej. W tym celu należy weryfikować stan informatyczny lokalizacji zapasowej.
3. W lokalizacji zapasowej wyznacza się pomieszczenia umożliwiające funkcjonowanie jednostki.
4. Po zakończeniu sytuacji kryzysowej powinno nastąpić przywrócenie pełnej funkcjonalności jednostki organizacyjne w lokalizacji podstawowej.

§ 6.
Ogólne procedury odtworzeniowe

1. Ogólne procedury odtworzeniowe określają tryb postępowania w zakresie zarządzania sytuacją kryzysową. Plan Odtworzeniowy zawiera wykaz i informację o lokalizacji ogólnych procedur odtworzeniowych w sieci informatycznej jednostki.
2. Plan Odtworzeniowy stanowi załącznik nr do Planu Ciągłości Działania,

§ 7.
Testowanie planu i jego aktualizacje

1. W celu testowania Planu Ciągłości Działania należy przeprowadzać symulacje różnego rodzaju awarii, a następnie uruchomić procedury opisane w §4.
2. Testowanie planu winno być dokonane przynajmniej raz w roku.
3. Z wykonanego testu należy sporządzić protokół określony w załączniku nr 3 do Planu Ciągłości Działania.
4. W razie potrzeby należy zaktualizować Plan Ciągłości Działania.
5. Po przeprowadzeniu testu należy wyciągnąć wnioski i podjąć działania mające na celu odpowiedniego zabezpieczenia lub przygotowania się na wypadek wystąpienia testowanej awarii.