WÓJT GMINY
Ciechocin
woj. kujawsko-pomorskie

ZARZĄDZENIE Nr 81/2023
Wójta Gminy Ciechocin
z dnia 21 grudnia 2023 r.

w sprawie wprowadzenia polityki bezpieczeństwa informacji i ochrony danych oraz polityki zarządzania systemem informatycznym w Urzędzie Gminy Ciechocin

Na podstawie art. 24 ust. 2 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 (Dz.Urz. UE L 119 z 4 maja 2016 r., str. 1 oraz Dz.Urz. UE L 127 z 23 maja 2018 r., str. 2) – zwanego dalej jako RODO oraz § 20 rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2017 poz. 2247) zarządzam, co następuje:

§ 1. Wprowadzam do stosowania:
1) Politykę bezpieczeństwa informacji i ochrony danych w Urzędzie Gminy Ciechocin stanowiącą załącznik nr 1 do zarządzenia;
2) Politykę zarządzania systemem informatycznym w Urzędzie Gminy Ciechocin stanowiącą załącznik nr 2 do zarządzenia.

§ 2. 1. Zobowiązuję wszystkich pracowników Urzędu Gminy Ciechocin do zapoznania się z politykami, o których mowa w § 1 niniejszego zarządzenia oraz ich stosowania.
2. Zobowiązuję – Sekretarza Gminy Ciechocin do przekazania do wiadomości pracowników Urzędu Gminy Ciechocin niniejszego zarządzenia za potwierdzeniem.

§ 3. 1. Wdrożenie i nadzór nad realizacją postanowień Polityki bezpieczeństwa informacji i ochrony danych w Urzędzie Gminy Ciechocin powierzam Inspektorowi Ochrony Danych Osobowych.
2. Wdrożenie i nadzór nad realizacją postanowień Polityki zarządzania systemem informatycznym w Urzędzie Gminy Ciechocin powierzam Pracownikowi zatrudnionemu w Urzędzie Gminy Ciechocin na stanowisku ds. obsługi informatycznej.

§ 4. Traci moc Zarządzenie Nr 31/2018 Wójta Gminy Ciechocin z dnia 25 maja 2018 r. w sprawie wprowadzenia dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji oraz polityk Ochrony Danych opisujących sposób przekazania danych osobowych w Urzędzie Gminy Ciechocin.
§ 5. Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT
Andrzej Okruciński

Załącznik nr 1 do Zarządzenia Nr 81 /2023
Wójta Gminy Ciechocin
z dnia 21 grudnia 2023 r

POLITYKA BEZPIECZEŃSTWA INFORMACJI I OCHRONY DANYCH OSOBOWYCH W URZĘDZIE GMINY CIECHOCIN

UWAGA:
Dokument wyłącznie
do użytku wewnętrznego

Zatwierdzam:

WÓJT
21.12.2023r. Andrzej Okrucinski
.....
data i podpis Administratora

§ 1
WSTĘP

1. Opracowanie i wdrożenie polityki jest obowiązkiem administratora określonym w art. 24 ust. 2 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 (Dz.Urz. UE L 119 z 4 maja 2016 r., str. 1 oraz Dz.Urz. UE L 127 z 23 maja 2018 r., str. 2) – zwanego dalej jako RODO.
2. Niniejsza polityka stanowi zbiór wymogów, zasad i regulacji związanych z ochroną informacji oraz danych osobowych przetwarzanych w szczególności na podstawie:
    1) 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 (Dz.Urz. UE L 119 z 4 maja 2016 r., str. 1 oraz Dz.Urz. UE L 127 z 23 maja 2018 r., str. 2) (ogólne rozporządzenie o ochronie danych);
    2) ustawa z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz.U. z 2023 r. poz. 40 z późn. zm.);
    3) ustawy z dnia 18 lipca 2002 o świadczeniu usług drogą elektroniczną (t.j. z 2020 poz. 344);
    4) ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (t.j. Dz. U. z 2022 r. poz. 902);
    5) ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz. U. z 2022 r. poz. 2509);
    6) ustawy z dnia 29 czerwca 1995 r. o statystyce publicznej (t.j. Dz. U. z 2023, poz. 773) w zakresie art. 10 - Tajemnica statystyczna;
    7) ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz. U. z 2020, poz. 57 z późn. zm.);
    8) ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (t.j. Dz.U. z 2023 r. poz. 775 z późn. zm.)
    9) ustawy z dnia 29 sierpnia 1997 r. - Ordynacja podatkowa (t.j. Dz. U. z 2023 r. poz. 2383 z późn. zm.);
    10) ustawa z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz.U. z 2023 r., poz. 1605 z późn. zm.);
    11) ustawa z dnia 13 września 1996 r. o utrzymaniu czystości i porządku w gminach (t.j. Dz.U. z 2023 poz. 1469 z późn zm.);
    12) ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (t.j. Dz.U. 2023 poz. 1465);
    13) ustawa z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnieniu osób niepełnosprawnych (tj. Dz. U. z 2023 r.,poz. 100 z późn. zm.)
    14) Ustawa z dnia 26 lipca 1991 r. o podatku dochodowym od osób fizycznych (t.j. Dz.U.2022 poz. 2647 z późn. zm).
3. Przez zapewnienie bezpieczeństwa informacji i ochronę danych osobowych należy rozumieć zachowanie następujących cech informacji tj.:
    1) poufności - daje gwarancję, że informacje są dostępne tylko i wyłącznie dla autoryzowanych osób - pracowników, posiadających prawo dostępu do tych informacji;
    2) integralności - zabezpiecza ona dokładność i kompletność zarówno informacji, jak też i stosowanych metod jej ochrony oraz zapewnia, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
    3) dostępności - gwarancja, że użytkownicy posiadający stosowne uprawnienia mają stały dostęp do informacji i zgromadzonych zasobów;
    4) rozliczalności - zapewnieniu, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko jemu;
    5) autentyczności - zapewnieniu, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana (autentyczność dotyczy użytkowników, procesów, systemów i informacji);

6) niezaprzeczalności – braku możliwości wyparcia się swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie;
7) niezawodności – zapewnieniu spójności oraz zamierzonych zachowań i skutków, co można to interpretować jako poprawność danych i właściwa ich interpretacja.

4. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia administrator wprowadza do stosowania niniejszą politykę.
5. Politykę stosuje się przy przetwarzaniu wszelkich informacji w tym danych osobowych, gdzie administrator jest samodzielnym administratorem, współadministratorem oraz podmiotem przetwarzającym.
6. Ryzyko naruszenia praw i wolności osób zostało określone na poziomie niskim – szczegóły zawarto w dokumentacji szacowania ryzyka dla przetwarzania danych osobowych.
7. Z uwagi na brak dużego prawdopodobieństwa spowodowania wysokiego ryzyka naruszenia praw lub wolności osób fizycznych, administrator odstąpił od oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych.
8. Szacowanie ryzyka naruszenia praw lub wolności osób fizycznych jest monitorowane, w przypadku wystąpienia okoliczności mogących je naruszyć podlega oszacowaniu na bieżąco oraz przeglądowi raz do roku, jednak nie rzadziej, niż raz na 3 lata.
9. Doraźnego szacowania naruszenia praw lub wolności osób fizycznych dokonuje się:
   1) na polecenie administratora w przypadku, gdy nastąpiło naruszenie ochrony danych osobowych skutkujące jego zgłoszeniem do organu nadzorczego, zgodnie art. 33 RODO;
   2) w przypadku powstania nowej czynności przetwarzania danych osobowych.
10. Polityka określa techniczne i organizacyjne zabezpieczenia, aby przetwarzanie odbywało się zgodnie z ogólnym rozporządzeniem o ochronie danych i aby móc to wykazać zgodnie z zasadą rozliczalności.
11. Administrator świadomy wagi problemów związanych z ochroną prawa do prywatności, w tym w szczególności prawa osób fizycznych powierzających mu swoje dane osobowe, stosuje właściwe i skuteczne metody ochrony poprzez:
    1) podejmowanie wszystkich działań niezbędnych dla ochrony praw, wolności i usprawiedliwionych interesów jednostki związanych z ochroną osób fizycznych w związku z przetwarzaniem danych osobowych;
    2) stałe podnoszenie świadomości oraz kwalifikacji osób przetwarzających dane osobowe w zakresie problematyki bezpieczeństwa tych danych, w tym propagowania świadomości wartości powierzonych danych osobowych, jako czynnika wpływającego na jakość i ciągłość działalności oraz wiarygodność administratora;
    3) traktowanie obowiązków osób zatrudnionych przy przetwarzaniu danych osobowych jako należących do kategorii podstawowych obowiązków pracowniczych oraz stanowczego egzekwowania ich wykonania przez zatrudnione osoby;
    4) doskonalenie i rozwijanie nowoczesnych metod zabezpieczenia danych przed zagrożeniami związanymi z ich przetwarzaniem, szczególnie w zakresie dotyczącym dynamicznego rozwoju metod i technik przetwarzania tych danych w systemach informatycznych oraz sieciach telekomunikacyjnych.
10. Realizując politykę uwzględniającą stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.

§ 2
PODSTAWOWE POJĘCIA

1) **ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY** 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 (Dz.Urz. UE L 119 z 4 maja 2016 r., str. 1 oraz Dz.Urz. UE L 127 z 23 maja 2018 r., str. 2) – zwane dalej jako RODO;

2) **Administrator** – osoba fizyczna lub prawna, organ publiczny, jednostka 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 – w Urzędzie Gminy Ciechocin jest nim Wójt Gminy Ciechocin.

3) **Polityka bezpieczeństwa informacji i ochrony danych osobowych** – dokument wewnętrzny wdrożony do użytku w organizacji przez administratora- zwany dalej polityką.
Ustanowione procedury i zasady stosuje się do wszystkich osób upoważnionych przez administratora do przetwarzania informacji w tym danych osobowych;

4) **Inspektor Ochrony Danych** – osoba wyznaczona przez administratora lub podmiot przetwarzający na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, zwany dalej inspektorem;

5) **Informatyk/stanowisko ds. obsługi informatycznej** – osoba wyznaczona przez administratora odpowiedzialna za sprawność i konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych do przetwarzania danych osobowy, zwany dalej informatykiem;

6) **Podmiot przetwarzający** - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

7) **Odbiorca** - osoba fizyczna lub prawna, organ publiczny, jednostka 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 uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;

8) **Strona trzecia** - osoba fizyczna lub prawna, 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;

9) **Dane osobowe** – 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;

10) **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;

11) **Ograniczenie przetwarzania** oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;

12) **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;

13) **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.

14) **System do przetwarzania danych osobowych** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych, zwany dalej system TI;
15) **System tradycyjny** - zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji oraz wyposażenia i środków trwałych, w celu przetwarzania danych osobowych na papierze;
16) **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;
17) **Identyfikator** - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
18) **Hasło** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi;
19) **Osoba upoważniona do przetwarzania danych osobowych** – rozumie się przez to osobę, upoważnioną do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający, zwana dalej upoważnionym;
20) **Użytkownik systemu** - osoba upoważniona przez administratora lub podmiot przetwarzający do przetwarzania danych osobowych, której przyznano uprawnienia do przetwarzania danych osobowych w systemie do przetwarzania danych osobowych w zakresie wskazanym w upoważnieniu, zwany dalej użytkownikiem;
21) **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;
22) **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.

§ 3
ORGANIZACJA PRZETWARZANIA DANYCH OSOBOWYCH

1. Rejestr czynności przetwarzania danych osobowych

1) Administrator prowadzi rejestr czynności przetwarzania danych osobowych oraz rejestr wszystkich kategorii czynności jako podmiot przetwarzający;
2) Rejestry wymienione w pkt 1 stanowią formę dokumentowania czynności przetwarzania danych, są jednym z kluczowych elementów umożliwiających realizację zasady rozliczalności przetwarzania danych;.
3) W rejestrze czynności przetwarzania danych osobowych dokumentowane są podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania.

2. Ogólny opis środków służących zapewnieniu bezpieczeństwa informacji i danych osobowych

1) Techniczne:
   a) Wszystkie drzwi zewnętrzne do podmiotu wyposażone są w 2 zamki,
   b) wyznaczono osoby odpowiedzialne za otwieranie i zamykanie jednostki
   c) klucze do drzwi wejściowych wydawane są wskazanym osobom i odpowiadają oni za uniemożliwienie ich wykorzystania przez osoby nieuprawnione,
   d) Klucze zapasowe do budynku przechowane są przez upoważnionych pracowników administratora,
   e) Dane osobowe przechowywane są w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi),
   f) pomieszczenia, w którym przetwarzane są dane osobowe wyposażone są w system alarmowy przeciwwłamaniowy,

g) kody uzbrajające system alarmowy przeciwwłamaniowy posiadają osoby wyznaczone indywidualne,
h) Obszar wyposażony jest w podręczny sprzęt p.poż. zgodnie z aktualnymi przepisami prawa,
i) Dane osobowe w formie papierowej przechowywane są w zamkniętej niemetalowej szafie,
j) dane osobowe w formie papierowej przechowywane są w zamkniętej metalowej szafie – USC,
k) kopie zapasowe/archiwalne danych osobowych przechowywane są w zamkniętej niemetalowej szafie,
l) Dane osobowe w formie papierowej przechowywane są w zamkniętym sejfie lub kasie pancernej – Szafa metalowa znajduje się w USC – część dokumentacji oraz pieczątki, Kasa pancerna znajduje się w biurze nr 7 – druki ścisłego zarachowania, gotówka , dokumenty,
m) klucze do szaf, sejfów i kas pancernych przechowane są przez pracowników i odpowiadają oni za uniemożliwienie ich wykorzystania przez osoby nieuprawnione,
n) klucze zapasowe do pomieszczeń oraz urządzeń stosowanych do przechowywania dokumentów przechowywane są w wyznaczonym miejscu i nadzorowane przez upoważnionego pracownika,
o) pomieszczenie, w którym przetwarzane są dane osobowe zabezpieczone jest przed skutkami pożaru za pomocą systemu przeciwpożarowego i/lub wolnostojącej gaśnicy,
p) dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów,
q) dyski twarde, płyty cd, dvd, dyski zewnętrzne, karty pamięci oraz inne nośniki danych osobowych niszczone są mechanicznie
r) serwerownia wyposażona jest w system awaryjnego zasilania, klimatyzację, monitoring temperatury, wilgotności,
s) okablowanie (informacyjne i zasilające) systemu it jest zabezpieczone przed niepożądanym działaniem,
t) zabezpieczono alternatywne łącza telekomunikacyjne
u) gniazdka rj45 domyślnie wyłączne,
v) dostęp do archiwum ograniczony jest do upoważnionej grupy osób.

2) Organizacyjne:

a) wprowadzono polityki ochrony informacji i danych oraz zarządzania systemem informatycznym,
b) ustanowiono wytyczne dla kierownictwa w zakresie inicjowania oraz kontroli wdrożenia i stosowania bezpieczeństwa informacji w obrębie organizacji,
c) Wyznaczono inspektora ochrony danych,
d) określono dla osób w organizacji zadania i obowiązki w zakresie ochrony danych osobowych,
e) osoby przetwarzające dane osobowe w organizacji posiadają upoważnienia,
f) W jednostce organizacyjnej wyznaczone zostały osoby formalnie odpowiedzialne za zapewnienie funkcjonowania i bezpieczeństwa systemu TI,
g) użytkownicy systemu TI posiadają aktualne uprawnienia do przetwarzania danych osobowych w systemie TI,
h) ruch osób z zewnątrz w obszarze przetwarzania odbywa się pod kontrolą osób upoważnionych,
i) personel sprzątający oraz techniczny wykonuje swoje obowiązki w trakcie pracy organizacji i pod nadzorem osób upoważnionych,

j) na stronie www lub bip znajduje się zakładka dotycząca ochrony danych osobowych, w której znajdą się informacje o administratorze, inspektorze ochronie danych, dane kontaktowe oraz klauzule informacyjne dla klientów,
k) wprowadzono zakaz korzystania z punktów dostępowych free WiFi,
l) osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych,
m) przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego,
n) osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy lub poufności
o) monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane,
p) Zawarto umowy powierzenia przetwarzania danych osobowych z podmiotami świadczącymi usługi specjalistyczne (np. informatyczne, chmura obliczeniowa, hosting, BHP, p.poż., szkoleniowe, obsługę RODO),
q) Wydruk dokumentów odbywa przy użyciu drukarek pracujących w sieci usytuowanych w kilku miejscach budynku.

3) Informatyczne:
a) zastosowano urządzenia typu ups, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania
b) dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła,
c) zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej,
d) zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.
e) użyto system firewall do ochrony dostępu do sieci komputerów,
f) zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych,
g) dostęp do danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła,
h) zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym danych osobowych dla poszczególnych użytkowników systemu informatycznego,
i) hasło dostępu zawiera min. 8 znaków w tym duża i mała literę, cyfrę oraz znak specjalny,
j) dostęp do urządzeń wyjścia (drukarki) tylko dla osób, którym są niezbędne do wykonywania obowiązków,
k) serwer kopii zapasowych znajduje się min. w jednej lokalizacji,
l) tworzona jest kopia zapasowa offline,
m) wykonywane są kopie zapasowe dla zasobów przechowywanych na stacjach roboczych,
n) Częstotliwość wykonywania kopii zapasowych – dzienne,
o) wyznaczono konto informatyka do zasobów serwera – jako administratora systemu IT,
p) hasła do zasobów serwera przechowywane jest przez najwyższe kierownictwo,
q) strona www z bezpiecznym, połączniem https – certyfikat ssl
r) serwer poczty elektronicznej - zawarto umowę powierzenia przetwarzania danych,

s) przy wykorzystaniu poczty elektronicznej korzysta się z protokołu imap oraz certyfikatu ssl,
t) przy pracy zdalnej wszystkie połączenia realizowane są z siecią jednostki za pomocą połączenia vpn lub „zdalnego pulpitu",
u) W systemie monitoringu wizyjnego stworzono konta administratora i użytkowników ze ścisłym wskazaniem uprawnień do przetwarzanych danych(np. podgląd, edycja, kopiowanie, zmiana),
v) Przy wyświetleniu strony www/bip przy komunikacie dot. polityki prywatności oraz informacji o cookies – umieszczono pole z wyborem zgody na cookies -„ciasteczka",
w) W jednostce organizacyjnej zastosowano rozwiązania „chmury obliczeniowej",
x) Urządzenia służące do przetwarzania danych osobowych - Komputery, drukarki, skanery posiadają aktualne licencjonowane oprogramowanie, wspierane przez MICROSOFT,
y) Urządzenia posiadają aktualne oprogramowanie antywirusowe i aktualną bazę.

4) Szczegółowe zasady oraz tryb postępowania przy przetwarzaniu informacji w systemach iinformatycznych określono w odrębnym dokumencie.

3. Administrator ustala cele i sposoby przetwarzania danych, w tym zwłaszcza:

1) Jest odpowiedzialny za przestrzeganie przepisów RODO oraz niniejszej polityki uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, zarówno jako administrator i podmiot przetwarzający. Wdraża odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku:
   a) pseudonimizację i szyfrowanie danych osobowych,
   b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,,
   c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich, w razie incydentu fizycznego lub technicznego,
   d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych, mających zapewnić bezpieczeństwo przetwarzania;
2) Przeprowadza proces szacowania ryzyka naruszenia praw lub wolności osób fizycznych, w tym akceptuje ryzyko szczątkowe;
3) Przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych, w przypadku, jeśli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter kontekst i cele spowoduje wysokie ryzyko naruszenia praw lub wolności osób fizycznych;
4) Przed rozpoczęciem przetwarzania konsultuje się z organem nadzorczym, jeżeli ocena skutków dla ochrony danych, wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby administrator nie zastosował środków, w celu zminimalizowania tego ryzyka;
5) Dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze;
6) Zawiadamia bez zbędnej zwłoki osobę, której dane dotyczą o naruszeniu ochrony danych osobowych, które może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych;
7) Zgłasza organowi nadzorczemu, bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia ochrony danych osobowych, o wystąpieniu naruszenia, jeżeli skutkuje ono ryzkiem naruszenia praw lub wolności osób fizycznych;
8) Jako podmiot przetwarzający, po stwierdzeniu każdego naruszenia ochrony danych osobowych, bez zbędnej zwłoki, zgłasza je administratorowi;
9) Upoważnia osoby fizyczne do przetwarzania danych osobowych, w tym także w przypadkach, gdy występuje jako podmiot przetwarzający. Do podpisywania

upoważnień do przetwarzania danych osobowych w imieniu administratora upoważniony jest również **Sekretarz Gminy Ciechocin**;

10) Wyznacza Inspektora Ochrony Danych;
11) Zapewnia, by Inspektor Ochrony Danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych;
12) Wspiera Inspektora Ochrony Danych w wypełnianiu przez niego zadań, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej;
13) Zapewnia, by Inspektor Ochrony Danych nie otrzymywał instrukcji dotyczących wykonywania swoich zadań od innego personelu;
14) Wyznacza informatyka oraz określa zakres jego zadań i czynności;
15) Informuje każdego odbiorcę, któremu ujawniono dane osobowe, o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, chyba, że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku;
16) Współpracuje z organem nadzorczym w ramach wykonywania swoich zadań;
17) Podejmuje działania w celu zapewnienia, by każda osoba fizyczna działająca z upoważnienia administratora lub podmiotu przetwarzającego, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na jego polecenie, chyba że wymaga tego od niej prawo Unii lub prawo państwa członkowskiego.

2. Inspektor Ochrony Danych:

1) Jest właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych, co zapewniają administrator oraz podmiot przetwarzający;
2) Podlega bezpośrednio administratorowi;
3) Jest zobowiązany do zachowania tajemnicy lub poufności, co do wykonywania swoich zadań;
4) Może wykonywać inne zadania i obowiązki, a administrator lub podmiot przetwarzający zapewniają, by ich wykonywanie nie powodowały konfliktu interesów;
5) Monitoruje przestrzeganie RODO i 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;
6) Udziela na żądanie konsultacji, co do oceny skutków dla ochrony danych oraz monitoruje jej wykonanie;
7) Współpracuje z organem nadzorczym;
8) Pełni funkcję punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzi konsultacje we wszelkich innych sprawach;
9) Wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania;
10) Pełni funkcję punktu kontaktowego dla osób, których dane dotyczą, które mogą kontaktować się z inspektorem, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO.

3. Informatyk/stanowisko ds. obsługi informatycznej

Informatyk realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad systemami do przetwarzania danych, w tym zwłaszcza:

1) Zarządza systemami do przetwarzania danych osobowych;
2) Podejmuje działania uniemożliwiające osobom niepowołanym dostęp do systemu informatycznego, w którym przetwarzane są dane osobowe;
3) Przydziela każdemu użytkownikowi identyfikator oraz hasło do systemu do przetwarzania, dokonuje modyfikacji uprawnień oraz usuwa konta użytkowników, zgodnie z zasadami określonymi w polityce;
4) Podejmuje działania w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego, prowadzi wykaz indywidualnych identyfikatorów przydzielonych użytkownikom;

5) W sytuacji stwierdzenia naruszenia zabezpieczeń systemu do przetwarzania, w którym przetwarzane są dane osobowe informuje administratora oraz Inspektora Ochrony Danych i współdziała z nim przy ustalaniu przyczyn i usuwaniu skutków naruszenia;
6) Pisemnie dokumentuje zaistniałe naruszenia ochrony danych osobowych oraz podjęte czynności naprawcze;
7) Sprawuje nadzór nad wykonywaniem napraw, konserwacją oraz likwidacją urządzeń komputerowych, na których przetwarzane są dane osobowe, nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem, pod kątem ich dalszej przydatności do odtwarzania danych, w przypadku awarii systemu informatycznego;
8) Podejmuje działania służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji;
9) W przypadku niewyznaczenia informatyka, wymienione powyżej obowiązki pełni administrator.

4. Osoba upoważniona do przetwarzania danych osobowych

Każda osoba fizyczna działająca z upoważnienia administratora lub podmiotu przetwarzającego, która ma dostęp do danych osobowych, przetwarza je wyłącznie na polecenie administratora.

1) Z upoważnienia administratora działają:
   a) osoby fizyczne zatrudnione na podstawie umowy o pracę, w momencie jej zawarcia otrzymują pisemne upoważnienie - wzór zał. nr 1 i składają oświadczenie o zachowaniu poufności – wzór zał. nr 2, podpisane dokumenty są włączane do akt osobowych,
   b) osoby fizyczne, które są stroną umowy cywilnej zawartej z administratorem, w momencie jej zawarcia uzyskują upoważnienie do przetwarzania danych osobowych zgodnie z przedmiotem umowy - wzór zapisu w umowie zał. nr 3,
   c) osoby fizyczne, będące stażystami, wolontariuszami, innymi osobami wykonującymi czynności przetwarzania danych osobowych na rzecz administratora otrzymują upoważnienia - wzór zał. nr 1 i składają oświadczenia o zachowaniu poufności - wzór zał. nr 2, dokumenty po ich podpisaniu przekazywane są wraz odpowiednią umową;
2) Za przygotowanie w/w dokumentów odpowiada pracownik ds. kadr, inna osoba odpowiedzialna za przygotowanie umowy lub bezpośredni przełożony;
3) Upoważnienie wygasa z momentem rozwiązania stosunku pracy, zakończenia umowy cywilnej oraz stażu, wolontariatu lub innej formy współpracy z administratorem;
4) Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana do:
   a) przetwarzania danych osobowych wyłącznie na polecenie administratora, zgodnie z zakresem upoważnienia, obowiązków lub umową, tylko w celu wykonywania nałożonych na nią zadań,
   b) zachowania w tajemnicy danych osobowych, sposobów ich zabezpieczenia oraz przestrzegania procedur ich bezpiecznego przetwarzania,
   c) przestrzegania tajemnicy danych osobowych obowiązującej przez cały okres zatrudnienia u administratora, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji, rozwiązaniu umowy i upływu terminu, na który umowa została zawarta,
   d) zgłoszenia naruszenia ochrony danych bezpośredniemu przełożonemu,
   e) zapoznania się z przepisami prawa, aktualizowania wiedzy w zakresie ochrony danych osobowych,
   f) stosowania określonych przez administratora procedur oraz wytycznych, mających na celu zgodne z prawem, w tym zwłaszcza adekwatne, przetwarzanie danych, określone w treści niniejszej polityki,
   g) realizowania obowiązku informacyjnego, o którym mowa w art. 13-14 RODO,
   h) zabezpieczenia danych przed ich udostępnianiem osobom nieupoważnionym,
   i) niepozostawiania bez kontroli dokumentów, nośników danych i sprzętu, zwłaszcza w trakcie przenoszenia lub przetwarzania danych osobowych poza siedzibą,
   j) zmiany hasła do systemu informatycznego w przypadku, gdy oprogramowanie nie wymusza takiego działania,

k) ochrony akt, zewnętrznych nośników i komputerów przenośnych,
l) niszczenia dokumentów w wersji papierowej oraz na nośnikach w niszczarce,
m) przechowywania w szafach zamykanych na klucz wszelkich wydruków zawierających dane osobowe przed opuszczeniem miejsca pracy i po zakończeniu dnia pracy,
n) niepozostawiania osób postronnych w pomieszczeniu, w którym przetwarzane są dane osobowe, bez obecności osoby upoważnionej do przetwarzania danych osobowych.

5. Obszar przetwarzania danych osobowych i sposób jego zabezpieczania fizycznego.

1) Obszarem przetwarzania danych osobowych jest:
   a) siedziba Urzędu Gminy Ciechocin, Ciechocin 172, 87-408 Ciechocin.
2) Pracownicy, współpracownicy, stażyści itp. administratora, w związku z wykonywaniem swoich zadań służbowych, są upoważnieni przez administratora także do przetwarzania danych osobowych poza strefą przetwarzania wskazaną w pkt. 1, przy jednoczesnym zachowaniu zasad określonych w niniejszej polityce;
3) Warunki ochrony obszaru określone zostały w „Zasadach ochrony obszarów, w których przetwarzane są dane osobowe" – zał. nr 4;

6. Przetwarzanie danych osobowych

1) Przetwarzane odbywa się zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość");
2) Dane zbierane są w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych, historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 RODO za niezgodne z pierwotnymi celami („ograniczenie celu");
3) Gromadzone dane powinny ograniczać się do tych danych które są niezbędne do osiągnięcia celów, w których są przetwarzane („minimalizacja danych");
4) Dane powinny być prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość");
5) Dane powinny być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność");
6) Dane osobowe zbierane są od osoby, której dane dotyczą lub z innych źródeł, w granicach dozwolonych przepisami prawa;
7) Dane osobowe mogą być przetwarzane wyłącznie do realizacji celów, dla których zostały pozyskane lub powierzone;
8) Po zakończeniu przetwarzania dane należy poddać anonimizacji lub usunąć, podmiot przetwarzający po zakończeniu przetwarzania zwraca lub usuwa dane, zgodnie z decyzją administratora, oraz usuwa wszelkie ich istniejące kopie;
9) Dane winny być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane te można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1 RODO, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy RODO w celu ochrony praw lub wolności osób fizycznych, których dane dotyczą („ograniczenie przechowywania");
10) Upoważnieni pracownicy zobowiązani są do pisemnego zgłaszania inspektorowi wszelkich zmian otoczenia prawnego i realizowanych zadań, które powodują powstanie nowej czynności przetwarzania danych lub powodują konieczność aktualizacji rejestru czynności przetwarzania danych osobowych oraz rejestru wszystkich kategorii czynności.
11) Zgłoszenie nowej czynności do „Rejestru czynności przetwarzania danych osobowych administratora" odbywa się wg – wzoru określonego w zał. nr 5.

12) Zgłoszenie do „Rejestru wszystkich kategorii czynności przetwarzania danych osobowych procesora" odbywa poprzez przekazanie kopii lub skanu umowy powierzenia przetwarzania danych osobowych lub wzoru określonego w zał. nr 5a.
13) Zgłoszenia dokonuje się niezwłocznie, nie później niż w terminie do 14 dni, od wystąpienia konieczności ujawnienia nowej czynności lub kategorii czynności przetwarzania danych osobowych;
14) W przypadku powstania nowej czynności lub zmiany w czynności przetwarzania danych, jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych;
15) Informatyk, w uzgodnieniu z administratorem i inspektorem ochrony danych określa warunki techniczne dotyczące zabezpieczeń w systemie informatycznym;
16) Upoważniony pracownik, zobowiązany jest w momencie podawania informacji, w przypadku zbierania danych od osoby, której dane dotyczą do stosowania klauzul informacyjnych oraz klauzul zgody;
17) Administrator udostępnia przetwarzane dane osobowe tylko osobom lub podmiotom uprawnionym do ich przetwarzania, na mocy przepisów prawa.

7. Udostępnianie danych osobowych

1) Dane osobowe mogą być udostępniane w następujących przypadkach:
   a) na podstawie wniosku od podmiotu uprawnionego do otrzymywania danych osobowych, na podstawie przepisów,
   b) na podstawie umowy z innym podmiotem, w ramach której istnieje konieczność udostępnienia danych,
   c) na podstawie wniosku osoby, której dane dotyczą;
2) Wniosek o udostępnienie danych osobowych musi być złożony wyłącznie w formie pisemnej pocztą tradycyjną lub elektronicznie przy użyciu profilu zaufanego lub elektronicznego podpisu kwalifikowanego i powinien zawierać informacje umożliwiające wyszukanie żądanych danych osobowych oraz wskazywać ich zakres i przeznaczenie, a w szczególności:
   a) wnioskodawcę,
   b) podstawę prawną upoważniającą udostępnienie danych osobowych, ze wskazaniem konkretnego szczególnego przepisu prawa, z którego wynika obowiązek udostępniania danych,
   c) podstawę faktyczną uzasadniającą potrzeby posiadania danych,
   d) informacje umożliwiające przygotowanie danych do udostępnienia,
   e) wskazanie przeznaczenia dla udostępnionych danych,
   f) zakres danych osobowych, jakie mają być udostępnione,
   g) datę i podpis;
3) Udostępniając dane osobowe należy zaznaczyć, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione;
4) Wniosek o udostępnienie przekazywany jest do upoważnionego merytorycznie pracownika, odpowiedzialnego za daną czynność przetwarzania, który podejmuje decyzję o udostępnieniu danych;
5) W przypadkach skomplikowanych lub merytorycznie trudnych, wniosek konsultowany jest z inspektorem ochrony danych;
6) Upoważniony merytorycznie pracownik jest odpowiedzialny za przygotowanie danych osobowych do udostępnienia, w zakresie wskazanym we wniosku.

8. Powierzenie przetwarzania danych osobowych

1) Powierzenie przetwarzania danych osobowych odbywa się zgodnie z art. 28 RODO, na podstawie umowy lub innego instrumentu prawnego, które wiążą podmiot przetwarzający i administratora, określając przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora;

2) Administrator korzysta wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą;
3) Upoważniony merytorycznie pracownik podejmując czynności zamierzające do zawarcia umowy na realizację usług, dostaw, robót budowlanych z podmiotami gospodarczymi, gdzie może dojść do powierzenia przetwarzania danych osobowych weryfikuje podmiot przetwarzający, ustalając czy posiada, on w szczególności:
   a) środki wymagane na mocy art. 32 RODO,
   b) inspektora ochrony danych osobowych, a w przypadku braku obowiązku jego powołania inną osobę odpowiedzialną za to zagadnienie,
   c) politykę uwzględniającą zadania podmiotu przetwarzającego,
   d) rejestr czynności przetwarzania,
   e) rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora,

   Ponadto ustala:
   a) jeśli jest to możliwe, czy wobec podmiotu nie została wydana decyzja dotycząca naruszenia przez niego zasad przetwarzania danych,
   b) czy w ramach umowy powierzenia zamierza korzystać z usług innego podmiotu przetwarzającego i czy zostanie, lub została zawarta na tą okoliczność umowa powierzenia lub inny instrument prawny;

   Weryfikacja może odbyć się z zastosowaniem „arkusza weryfikacji podmiotu przetwarzającego", stanowiącego zał. nr 3 do wzoru umowy powierzenia przetwarzania danych osobowych. Arkusz można wysłać do wypełnienia potencjalnemu podmiotowi przetwarzającemu lub opublikować wraz z ogłoszeniem o zamówieniu.
4) Upoważniony merytorycznie pracownik, z polecenia administratora, przygotowuje projekt umowy powierzenia dla podmiotu, który przeszedł pozytywnie proces weryfikacji określony wyżej – wzór umowy powierzenia przetwarzania danych osobowych zał. nr 6;
5) Informatyk konsultuje projekt umowy powierzenia przetwarzania danych osobowych, przygotowany w zakresie określenia warunków zabezpieczania systemu do przetwarzania przez podmiot przetwarzający;
7) Upoważniony merytorycznie, odpowiedzialny za załatwienie sprawy przedkłada projekt umowy do konsultacji inspektorowi ochrony danych, a następnie do podpisu administratorowi;
8) Kopia podpisanej umowy powierzania przetwarzania danych osobowych przekazywana jest inspektorowi.

§ 4
PRAWA OSÓB, KTÓRYCH DANE DOTYCZĄ

1. Wykonywanie praw osób.

1) Wniosek o realizację uprawnień przez osobę, której dane dotyczą, musi być złożony wyłącznie w formie pisemnej pocztą tradycyjną lub elektronicznie przy użyciu profilu zaufanego lub elektronicznego podpisu kwalifikowanego, pod rygorem pozostawienia wniosku bez odpowiedzi, o czym informowany jest wnioskodawca kierujący zapytanie w innej formie;
2) Czynności związane z realizacją uprawnień osoby, której dane dotyczą są wykonywane wyłącznie po jednoznacznym zidentyfikowaniu wnioskodawcy, że posiada prawo do danych;
3) Wniosek przekazywany jest do upoważnionego merytorycznie pracownika odpowiedzialnego za daną czynność przetwarzania, który poddaje analizie wniosek, biorąc pod uwagę co najmniej czy:
   a) pochodzi od osoby uprawnionej,
   b) administrator przetwarza dane osobowe osoby, której dane dotyczą,
   c) czy występują przesłanki do odmowy realizacji uprawnień;
4) W przypadkach skomplikowanych lub merytorycznie trudnych, wniosek konsultowany jest z inspektorem ochrony danych;
5) Upoważniony pracownik jest odpowiedzialny za opracowanie projektu odpowiedzi i przygotowanie danych osobowych, w zakresie wskazanym we wniosku;

6) Decyzję o sposobie realizacji wniosku po przedłożeniu dokumentów i analizy dokonanej przez pracownika odpowiedzialnego merytorycznie podejmuje administrator;
7) Za opracowanie ostatecznej wersji odpowiedzi na wniosek oraz jej przesłanie odpowiedzialny jest upoważniony merytorycznie pracownik;
8) W przypadkach, gdy, wniosek skutkuje zmianą danych osobowych w systemie informatycznym wymagającą uprawnień dostępu do danych z poziomu zarządzającego systemem informatycznym, dokonywany jest przez informatyka, po wskazaniu mu zakresu zmian jakich należy dokonać;
9) Udzielenie odpowiedzi na wniosek następuje w terminie do 30 dni od daty otrzymania pisemnego wniosku pochodzącego od osoby, której dane dotyczą.
10) Po wykonaniu w/wym. czynności, kopie dokumentów przekazywane są Inspektorowi Ochrony Danych;
11) Powyższe zasady stosowane są do realizacji wszystkich wniosków dot. realizacji prawa osoby, której dane dotyczą.

2. Obowiązek informacyjny

1) W związku z zasadą przejrzystego i jasnego komunikowania o zasadach przetwarzania, obowiązek informacyjny administratora realizowany jest w przypadkach:
   a) bezpośredniego zbierania danych od osoby, której dane dotyczą,
   b) pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą,
   c) wyrażania zgody na przetwarzanie danych osobowych;
2) Obowiązek informacyjny jest realizowany m. in. w następujący sposób:
   a) poprzez publikację klauzul informacyjnych na stronie www, BIP
   b) poprzez publikację klauzul informacyjnych w siedzibie administratora,
   c) poprzez umieszczenie stosownej klauzuli informacyjnej w dokumentach oraz jej ogłoszenie, doręczenie, przekazanie lub w inny sposób zapoznanie z jej treścią osoby, której dane dotyczą,
   d) poprzez umieszczenie odpowiednich informacji bezpośrednio w treści zgody na przetwarzanie danych osobowych,
   e) w inny sposób, przyjęty przez administratora (np. stopka w wiadomościach e-mail).

3. Prawo dostępu przysługujące osobie, której dane dotyczą

1) Osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji:
   a) cele przetwarzania,
   b) kategorie odnośnych danych osobowych,
   c) o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych,
   d) okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu,
   e) o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczących osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania,
   f) o prawie wniesienia skargi do organu nadzorczego,
   g) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą - wszelkie dostępne informacje o ich źródle,
   h) o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu;
2) Administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, administrator może pobrać opłatę. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się powszechnie stosowaną drogą elektroniczną.

4. Prawo sprostowania danych

Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. W przypadkach potwierdzenia konieczności zmiany posiadanych danych osobowych, pracownik dokonuje aktualizacji danych

osobowych w posiadanej dokumentacji, w tym w systemie do przetwarzania danych osobowych.

5. Prawo usunięcia danych „prawo bycia zapomnianym"

1) Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych;
2) Prawo usunięcia danych może nastąpić, jeżeli zachodzi jedna z przesłanek określonych w art. 17 ust. 1 RODO;
3) W przypadkach potwierdzenia zaistnienia przesłanek, pracownik dokonuje on usunięcia danych osobowych w posiadanej dokumentacji, w tym systemie w informatycznym do przetwarzania danych osobowych;
4) Upoważniony merytorycznie pracownik, o usunięciu danych powiadamia odbiorców (procesorów), którym ujawniono dane osobowe, chyba, że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.

6. Prawo do ograniczenia przetwarzania

1) Osoba, której dane dotyczą, ma prawo żądania od administratora ograniczenia przetwarzania w przypadkach określonych w art. 18 RODO;
2) W przypadkach potwierdzenia zaistnienia przesłanek do ograniczenia przetwarzania, dokonuje on sprostowania danych osobowych w posiadanej dokumentacji w tym systemie informatycznym do przetwarzania danych osobowych;
3) Upoważniony merytorycznie pracownik, o usunięciu danych powiadamia odbiorców (procesorów), którym ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku.

§ 5

Postępowanie w przypadkach naruszenia bezpieczeństwa informacji i ochrony danych osobowych oraz zgłoszenie naruszenia organowi nadzorczemu oraz osobom, których dane dotyczą.

1. Niniejsze zasady stosuje się w przypadku:
   1) podejrzenia naruszenia bezpieczeństwa informacji i ochrony danych osobowych;
   2) stwierdzenia naruszenia bezpieczeństwa informacji i ochrony danych osobowych.
2. Charakterystyka możliwych zagrożeń:
   1) zagrożenia losowe zewnętrzne;
   2) zagrożenia losowe wewnętrzne;
   3) zagrożenia zamierzone, świadome i celowe.
3. Zasady postępowania opisane niżej obowiązują wszystkie osoby upoważnione do przetwarzania danych osobowych oraz pozostały personel administratora.
4. Naruszeniem ochrony danych osobowych są m.in.:
   1) nieuprawnione ujawnienie danych osobowych;
   2) przełamanie zabezpieczeń tradycyjnych – zerwane plomby na drzwiach, szafach, segregatorach;
   3) udostępnienie lub umożliwienie dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną;
   4) kradzież sprzętu komputerowego lub dokumentów zawierających dane osobowe;
   5) niestosowanie się do zabezpieczeń technicznych i organizacyjnych określonych w niniejszej polityce.
5. Naruszeniem ochrony danych osobowych są także zdarzenia związane z procesem przetwarzania danych osobowych przy użyciu systemu informatycznego, a w szczególności:
   1) nieautoryzowany dostęp do danych;
   2) nieautoryzowane modyfikacje lub zniszczenie danych;
   3) udostępnienie danych nieautoryzowanym podmiotom;
   4) nielegalne ujawnienie danych;
   5) pozyskiwanie danych z nielegalnych źródeł;
   6) naruszenie hasła dostępu i identyfikatora (system nie reaguje na hasło lub je ignoruje bądź można przetwarzać dane bez wprowadzenia hasła);
   7) częściowy lub całkowity brak danych albo dostęp do danych w zakresie szerszym niż wynikający z przyznanych uprawnień;

8) braku dostępu do właściwej aplikacji lub zmiany zakresu wyznaczonego dostępu do zasobów serwera;
9) „elektroniczne ślady" próby włamania do systemu informatycznego.

6. W przypadku stwierdzenia naruszenia zabezpieczenia systemu informatycznego lub zaistnienia sytuacji, które mogą wskazywać na naruszenie bezpieczeństwa danych osobowych, każdy pracownik administratora jest zobowiązany przerwać przetwarzanie danych osobowych i powiadomić o tym fakcie bezpośredniego przełożonego, a następnie postępować stosownie do podjętej przez niego decyzji.
7. Bezpośredni przełożony po uzyskaniu informacji o naruszeniu ochrony danych osobowych podejmuje działania mające na celu:
   1) minimalizację negatywnych skutków zdarzenia;
   2) wyjaśnienie okoliczności zdarzenia;
   3) zabezpieczenie dowodów zdarzenia;
   4) umożliwienie dalszego bezpiecznego przetwarzania danych.
8. Czynności w/wym. dokumentuje się w formie notatek, odbiera wyjaśnienia od pracowników oraz w innych formach umożliwiających wyjaśnienie okoliczności naruszenia.
9. O naruszeniu ochrony danych osobowych zaistniałym w związku z przetwarzaniem danych w systemie informatycznym bezpośredni przełożony informuje informatyka i inspektora.
10. Do czasu przybycia na miejsce informatyka lub upoważnionego pracownika należy:
    1) o ile istnieje taka możliwość, niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego zdarzenia, a następnie uwzględnić w działaniu również ustalenie jego przyczyn lub sprawców;
    2) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej, w celu zabezpieczenia miejsca zdarzenia;
    3) zaniechać – o ile to możliwe – dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę incydentu;
    4) zastosować się do instrukcji i regulaminów lub dokumentacji aplikacji, jeśli odnoszą się one do zaistniałego przypadku;
    5) przygotować opis incydentu;
    6) nie opuszczać bez uzasadnionej przyczyny miejsca zdarzenia.
11. Informatyk lub inny pracownik wyznaczony przez administratora po otrzymaniu zawiadomienia, o którym mowa wyżej, powinien niezwłocznie:
    1) przeprowadzić postępowanie wyjaśniające w celu ustalenia okoliczności naruszenia ochrony danych osobowych;
    2) podjąć działania chroniące system przed ponownym naruszeniem.
12. Informatyk, w porozumieniu z administratorem może zarządzić, w razie potrzeby, odłączenie części systemu informatycznego dotkniętej incydentem od pozostałej jego części.
13. W razie odtwarzania danych z kopii zapasowych informatyk obowiązany jest upewnić się, że odtwarzane dane zapisane zostały przed wystąpieniem incydentu (dotyczy to zwłaszcza przypadków infekcji wirusowej).
14. Informatyk, ujawnienie naruszenia ochrony danych osobowych oraz czynności wykonywane w związku naruszeniem dokumentuje, sporządzając pisemne „Zgłoszenie naruszenia ochrony danych osobowych" - wzór zał. nr 7.
15. Niezależnie od informatyka, osoby upoważnione oraz personel administratora, wspólnie z bezpośrednim przełożonym, w przypadku naruszenia ochrony danych osobowych, mają obowiązek sporządzenia pisemnego „Zgłoszenia naruszenia ochrony danych osobowych" - wzór zał. nr 7.
16. Po otrzymaniu zgłoszenia o naruszeniu ochrony danych osobowych, Inspektor Ochrony Danych przeprowadza postępowanie wyjaśniające w trakcie, którego ma prawo m.in.:
    1) żądania wyjaśnień od pracowników;
    2) nakazania przerwania pracy, zwłaszcza w zakresie przetwarzania danych osobowych.
17. Odmowa udzielenia wyjaśnień lub współpracy z Inspektorem Ochrony Danych traktowane będzie jako naruszenie obowiązków pracowniczych.
18. W postępowanie wyjaśniające włączeni zostają członkowie powołanego przez administratora zespołu, w którego skład wchodzą:
    1) Sekretarz Gminy Ciechocin;
    2) Inspektor Ochrony Danych;

3) Informatyk/stanowisko ds. obsługi informatycznej;
4) inne osoby wyznaczone przez administratora na podstawie ustnego polecenia administratora.

19. Zespół, po zapoznaniu się z sytuacją, podjęciu czynności wyjaśniających i naprawczych przez pracowników administratora, dokonuje szacowania ryzyka utraty praw lub wolności osób fizycznych, których dane były przedmiotem naruszenia.
20. Zespół opracowuje raport końcowy, w którym przedstawia przyczyny i skutki zdarzenia oraz wnioski, ograniczające możliwość wystąpienia zdarzenia w przyszłości.
21. Raport przedstawiany jest administratorowi wraz z wnioskami dotyczącymi m.in.:
    1) zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu;
    2) odstąpienia od zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu, w sytuacji, gdy jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych;
    3) zgłoszenia naruszenia ochrony danych osobowych administratorowi, który powierzył dane osobowe do przetwarzania;
    4) zawiadomienia osób, których dane dotyczą o naruszeniu ochrony danych osobowych, w przypadkach obarczonych wysokim ryzykiem naruszenia praw lub wolności osób fizycznych oraz powiadomienia ich jakie muszą podjąć czynności aby ograniczyć, zmniejszyć lub usunąć ryzyko naruszania ich praw lub wolności. Zawiadomienie następuje bez zbędnej zwłoki;
    5) wyznaczenia przez administratora pracownika, który zostanie upoważniony do udzielania informacji w zakresie naruszenia osobom, których dane były przedmiotem naruszenia;
    6) odstąpienia od zawiadomienia osób, których dane dotyczą o naruszeniu ochrony danych osobowych w przypadku:
        a) wdrożenia odpowiednich technicznych i organizacyjnych środków ochrony i gdy środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie,
        b) zastosowania środków eliminujących prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,
        c) gdy wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.
22. Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu następuje niezwłocznie, nie później niż w ciągu 72 godzin po stwierdzeniu naruszenia.
23. Dokumentacja przechowywana jest przez Inspektora Ochrony Danych.

§ 6
AUDYT ZGODNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH Z PRZEPISAMI O OCHRONIE DANYCH OSOBOWYCH

1. Audyty są dokonywane w formie:
    1) audytu planowego – według planu sprawdzeń;
    2) audytu doraźnego – w przypadku nieprzewidzianym w planie audytów, w sytuacji powzięcia przez administratora wiadomości o naruszeniu ochrony danych osobowych lub uzasadnionego podejrzenia wystąpienia takiego naruszenia.
2. Plan audytu określa przedmiot, zakres oraz termin przeprowadzenia poszczególnych audytów oraz sposób i zakres ich dokumentowania
3. W planie audytu uwzględnia się, w szczególności, czynności przetwarzania danych osobowych i systemy informatyczne służące do przetwarzania danych osobowych oraz konieczność weryfikacji zgodności przetwarzania danych osobowych, z zasadami określonymi w RODO i polityce ochrony.
4. Plan audytu jest przygotowywany przez Inspektora Ochrony Danych na okres nie krótszy niż pół roku i nie dłuższy niż trzy lata.
5. Audyt doraźny jest przeprowadzany niezwłocznie po powzięciu wiadomości przez administratora o naruszeniu ochrony danych osobowych lub uzasadnionym podejrzeniu takiego naruszenia.

6. Dokumentowanie audytu może polegać, w szczególności, na utrwaleniu dowodów audytowych z systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych na informatycznym nośniku danych lub dokonaniu wydruku tych danych oraz na:
    1) sporządzeniu notatki z audytu, w szczególności z zebranych wyjaśnień, przeprowadzonych oględzin oraz z czynności związanych z dostępem do urządzeń, nośników oraz systemów informatycznych, służących do przetwarzania danych osobowych;
    2) odebraniu wyjaśnień od osoby, której czynności objęto audytem;
    3) sporządzeniu kopii otrzymanego dokumentu;
    4) sporządzeniu kopii obrazu wyświetlonego na ekranie urządzenia, stanowiącego część systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych;
    5) sporządzeniu kopii zapisów rejestrów systemu informatycznego służącego do przetwarzania danych osobowych lub zapisów konfiguracji technicznych środków zabezpieczeń tego systemu.
9. Kluczowym elementem w trakcie audytów jest włączenie wszystkich pracowników, współpracowników administratora i ścisła współpraca z nimi, która materializuje się obowiązkiem udzielania ustnych i pisemnych wyjaśnień w zakresie prowadzonych audytów na żądanie inspektora.
10. Po zakończeniu audytu, inspektor przygotowuje sprawozdanie:
    1) z audytu planowego – nie później niż w terminie 30 dni od zakończenia sprawdzenia;
    2) z audytu doraźnego – niezwłocznie po zakończeniu sprawdzenia.
11. Ze sprawozdaniem i dokumentacją audytów zapoznaje się administrator.

§ 7
ODPOWIEDZIALNOŚĆ

1. Niezastosowanie się do niniejszej polityki i naruszenie procedur ochrony danych przez pracowników administratora może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52 Kodeksu pracy.
2. Niezależnie od rozwiązania stosunku pracy, osoby popełniające przestępstwo podlegają odpowiedzialności karnej.

§ 8
RETENCJA DANYCH OSOBOWYCH

1. Administrator przetwarza dane osobowe z uwzględnieniem zasady ograniczenia przechowywania i zapewnia, że przechowuje je w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których te dane osobowe są przetwarzane (okres retencji).
2. W przypadku gdy dla określonych danych osobowych nie występują żadne prawnie uzasadnione cele przetwarzania, administrator zaprzestaje realizowania jakichkolwiek operacji na tych danych osobowych, z wyjątkiem ich usunięcia lub nieodwracalnej anonimizacji (przez którą rozumie się modyfikację danych osobowych w taki sposób, że nie jest możliwa identyfikacja podmiotów danych).
3. W przypadkach gdy okres retencji danych osobowych nie wynika wyraźnie z przepisów prawa, administrator ustala te okresy samodzielnie, uwzględniając ogólne zasady przetwarzania danych osobowych przewidziane w RODO. W przypadku gdy okres retencji wynika z przepisów prawa, ma on pierwszeństwo przed postanowieniami niniejszej polityki i rejestru czynności przetwarzania.
4. Dane osobowe mogą być przetwarzane dłużej niż wynosi okres retencji, w przypadku gdy są one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych (na zasadach określonych w art. 89 ust. 1 RODO), pod warunkiem że wdrożone są odpowiednie środki techniczne i organizacyjne w celu ochrony praw i wolności Podmiotów danych.
5. Okresy retencji danych zostały określone w jednolitym rzeczowym wykazie akt oraz rejestrze czynności przetwarzania.
6. Ustalając okresy retencji, uwzględniono w szczególności:

1) obowiązki prawne ciążące na administratorze w zakresie przechowywania określonych danych osobowych lub dokumentów zawierających dane osobowe, wynikające z właściwych przepisów prawa;
2) potencjalną niezbędność przetwarzania danych osobowych dla celów związanych z ustalaniem lub dochodzeniem roszczeń oraz obroną przed takimi roszczeniami i związane z tym okresy przedawnienia roszczeń wynikające z właściwych przepisów prawa.

7. Za faktyczne usuwanie (anonimizację) danych osobowych zgodnie z obowiązującymi okresami retencji odpowiedzialna jest osoba upoważniona do przetwarzania danych osobowych.
8. Przed usunięciem (anonimizacją) danych osobowych należy zweryfikować, czy nie zachodzą przesłanki wydłużenia okresu retencji, w szczególności poprzez sprawdzenie, czy:
   1) nie występuje obowiązek prawny ciążący na administratorze, którego wykonanie wymaga przetwarzania danych osobowych, a który nie został uwzględniony w jednolitym rzeczowym wykazie akt lub w rejestrze czynności przetwarzania;
   2) nie nastąpiło przerwanie lub zawieszenie okresu przedawnienia roszczeń, zgodnie z właściwymi przepisami, skutkujące koniecznością dalszego przetwarzania danych osobowych;
   3) dalsze przechowywanie nie jest konieczne w związku z biegnącym okresem przedawnienia zobowiązań podatkowych.
9. W razie wątpliwości przed usunięciem (anonimizacją) danych osobowych osoba upoważniona do przetwarzania danych zasięga opinii inspektora ochrony danych.
   Usunięcie (anonimizacja) danych osobowych powinno nastąpić niezwłocznie po upływie okresu retencji, z uwzględnieniem okresu koniecznego do podjęcia niezbędnych czynności technicznych i organizacyjnych związanych z usunięciem (anonimizacją) danych osobowych.

§ 9
SZKOLENIA

1. Szkoleniu podlegają wszyscy pracownicy oraz współpracownicy administratora oraz, jeśli jest to uzasadnione, pracownicy i współpracownicy podmiotów przetwarzających.
2. Niezwłocznie po otrzymaniu upoważnienia do przetwarzania danych osobowych, każdy pracownik i współpracownik przechodzą szkolenie. Szkolenie to prowadzi inspektor lub administrator oraz inne osoby posiadające odpowiednią wiedzę i umiejętności w tym zakresie.
3. W trakcie szkolenia w/wym. osoba zapoznawana jest z polityką lub jej wyciągiem.
4. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się przed dopuszczeniem do przetwarzania danych z w/wym. dokumentami, o których mowa ust. 3 oraz złożyć na piśmie stosowne oświadczenie, potwierdzające zrozumienie i znajomość ich treści.
5. Szkolenie w zakresie przetwarzania danych osobowych w systemie informatycznym przeprowadza informatyk, w momencie przekazywania identyfikatora oraz hasła przy pierwszym logowaniu się do systemu.
6. Szkolenia wewnętrzne wszystkich upoważnionych osób przeprowadzane są w przypadku każdej zmiany zasad lub procedur ochrony danych osobowych.
7. Szkolenie dla osób innych niż upoważnione, jest przeprowadzane, jeśli pełnione przez nie funkcje wiążą się z zabezpieczeniem danych osobowych.

§ 10
POSTANOWIENIA KOŃCOWE

1. Niniejsza polityka ma na celu zredukowanie możliwości wystąpienia negatywnych konsekwencji naruszeń w tym zakresie, tzn.:
   1) naruszeń danych o osobach rozumianych jako ich dobro prywatne powierzone administratorowi;
   2) naruszeń przepisów prawa oraz innych regulacji;
   3) utraty lub obniżenia reputacji administratora;
   4) strat finansowych, ponoszonych w wyniku nałożonych kar lub utraty wiarygodności czy klientów.

2. Polityka podlega przeglądowi min. raz na trzy lata oraz w sytuacjach wystąpienia incydentów związanych z wysokim ryzykiem naruszenia praw lub wolności osób fizycznych. W przypadkach istotnych zmian, dokonywana jest jej aktualizacja.
3. Wzory dokumentów określone w załącznikach do polityki mogą być zastąpione innymi wzorami dokumentów jednakże zgodnymi z zasadami określonymi w RODO oraz niniejszej polityce.
4. Polityka wchodzi w życie z dniem zatwierdzenia.

Wykaz załączników:

1. Wzór upoważnienia do przetwarzania danych osobowych.
2. Wzór oświadczenia o zapoznaniu się z przepisami o ochronie danych osobowych i o zachowaniu poufności.
3. Wzór zapisu w umowie zlecenia i o dzieło oraz klauzula informacyjna.
4. Zasady ochrony obszarów, w których przetwarzane są dane osobowe.
5. Wzór zgłoszenia nowej czynności do rejestru czynności przetwarzania danych osobowych administratora.

5a. Wzór zgłoszeni nowej czynności do rejestru wszystkich kategorii czynności przetwarzania danych osobowych procesora.

6. Wzór umowy powierzenia danych osobowych do przetwarzania.
7. Wzór zgłoszenie naruszenia ochrony danych osobowych.
8. Ocena wagi naruszenia

Załącznik nr 1 do Polityki
Bezpieczeństwa Informacji i Ochrony
Danych Osobowych

.....
(pieczęć jednostki)

UPOWAŻNIENIE
do przetwarzania danych osobowych

Na podstawie **art. 29 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 (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119/1 z 04 maja 2016 roku) oraz w związku z:

1) art. 22^{1b} ustawy z dnia 26 czerwca 1974 r. Kodeks pracy*,
2) art. 2b ust 6 pkt 1 ustawy z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych*,
3) art. 8 ust. 1 b ustawy z dnia 4 marca 1994 r. o zakładowym funduszu świadczeń socjalnych*,
4) art. 5a pkt 2 ustawy z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji*,
5) inne* .....
6) inne* .....

Upoważniam:

..... - .....
(imię i nazwisko) (stanowisko)

do przetwarzania danych osobowych w **Urzędzie Gminy Ciechocin** w zakresie niezbędnym do:

1) wykonywania określonych w zakresie obowiązków służbowych*,
2) realizacji umowy zlecenia*,
3) realizacji umowy o dzieło*,
3) inne ..... *.

Upoważnienia udziela się na czas pracy/wykonywania umowy zlecenia, umowy o dzieło/ praktyki/odbycia stażu/wolontariatu/.....*

....
(data wydania upoważnienia) (pieczęć i podpis administratora))

egz. nr 1 akta osobowe
egz. nr 2 osoba upoważniona
*niepotrzebne skreślić lub wpisać wg stanu faktycznego

Załącznik nr 2 do Polityki
Bezpieczeństwa Informacji i Ochrony
Danych Osobowych

Oświadczenie o zachowaniu poufności

Oświadczam, że przed rozpoczęciem wykonywania obowiązków w **Urzędzie Gminy Ciechocin** zostałem/łam zapoznany/a z przepisami prawa dotyczącymi ochrony danych osobowych, a w szczególności z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/W – ogólne rozporządzenie o ochronie danych oraz z ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych, (Dz. U. 2019, poz. 1781)
Zapoznałem/łam się z Polityką Bezpieczeństwa Informacji i Ochrony Danych i rozumiem zasady dotyczące ochrony danych osobowych obowiązujące w **Urzędzie Gminy Ciechocin** oraz zobowiązuję się do ich przestrzegania.

Zobowiązuję się do:

- zachowania w tajemnicy/poufności danych osobowych i innych informacji, do których mam lub będę miał/a dostęp w związku z wykonywaniem czynności zleconych w ramach stosunku pracy, również w sytuacji, gdy ustanie moja umowa obejmująca realizację tych obowiązków w **Urzędzie Gminy Ciechocin** ,
- niewykorzystywania danych osobowych w celach pozasłużbowych/ niezgodnych ze zleceniem/, umową,
- zachowania w tajemnicy/poufności informacji o sposobach zabezpieczenia danych osobowych, o ile nie są one jawne, również w sytuacji, gdy zakończę realizację moich obowiązków służbowych w **Urzędzie Gminy Ciechocin,**
- korzystania z urządzeń technicznych oraz oprogramowania wyłącznie w związku z wykonywaniem obowiązków służbowych lub czynności zleconych przez administratora,
- należytej dbałości o wyposażenie i urządzenia techniczne.

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

.....
(podpis osoby zobowiązanej do przestrzegania zasad)

*niepotrzebne skreślić lub wpisać wg stanu faktycznego

Wzór zapisu w umowie zlecenia i o dzieło

1. Zleceniodawca upoważnia zleceniobiorcę w ramach zakresu niniejszej umowy do przetwarzania danych osobowych, których sam jest administratorem danych i które zostały mu powierzone do przetwarzania.
2. Zleceniobiorca oświadcza, że:
   1) zapoznał się z polityką ochrony danych osobowych Zleceniodawcy oraz zobowiązuje się do jej przestrzegania,
   2) został poinformowany o grożącej odpowiedzialności karnej i cywilnej wynikającej z obowiązujących przepisów prawa związanych z ochroną danych osobowych.
   3) zobowiązuje się do zachowania w tajemnicy wszystkich danych osobowych, które przetwarzał w związku z niniejszą umową, także po jej zakończeniu i sposobu ich zabezpieczenia.
3. Zleceniobiorca zobowiązuje do niezwłocznego, ale nie później niż w terminie do 3 dni od dnia rozwiązania niniejszej umowy:
   1) zwrotu wszystkich dokumentów wytworzonych w wersji tradycyjnej i elektronicznej zawierających dane osobowe, w związku z wykonywaniem niniejszej umowy,
   2) usunięcia wszelkich danych osobowych z nośników elektronicznych pozostających w jego dyspozycji.

Załącznik nr 4 do Polityki
Bezpieczeństwa Informacji i Ochrony
Danych Osobowych

Zasady ochrony obszarów, w których przetwarzane są dane osobowe

1. Obszarem przetwarzania danych osobowych są budynki administratora - **Urząd Gminy Ciechocin, Ciechocin 172, 87-408 Ciechocin.**
2. Teren wokół budyneku administratora objęty jest całodobowym systemem monitoringu wizyjnego oraz systemem alarmowym.
3. Pracownicy administratora są zobowiązani do:
   1) zwracania uwagi na zachowanie osób wchodzących i wychodzących z budynków;
   2) reagowania na wejście do budynku i przebywanie w nim osób będących pod wpływem alkoholu lub innych środków odurzających;
   3) reagowania na próby niszczenia, wynoszenia lub wywożenia mienia z budynku;
   4) reagowania na próby wnoszenia do budynku przedmiotów niebezpiecznych, materiałów lub substancji budzących podejrzenie itp.;
   5) natychmiastowego reagowania poprzez powiadomienie ochrony obiektu, bezpośredniego przełożonego oraz odpowiednich służb o zaobserwowanych próbach stworzenia zagrożenia dla życia i zdrowia, a także utraty lub zniszczenia mienia.
4. Administrator do otwierania obszaru przetwarzania danych oraz rozkodowania systemu alarmowego wyznaczył pracowników, których upoważnił do tej czynności.
5. Pracownicy, którym powierzono klucze, karty dostępu do pomieszczeń oraz kod dostępu do systemu alarmowego mają obowiązek:
   1) wykorzystywania ich zgodnie z przeznaczeniem;
   2) uniemożliwienia kopiowania powierzonych kluczy i kart dostępu oraz nieudostępniania ich osobom trzecim;
   3) nieudostępniania kodów do system alarmowego.
6. Na pracownikach korzystających z pomieszczeń służbowych spoczywa pełna odpowiedzialność za ich zabezpieczenie.
7. Klucze zapasowe do pomieszczeń służbowych przechowywane są w sekretariacie.
8. Klucze zapasowe po ich wykorzystaniu należy niezwłocznie zwrócić.
9. Po otwarciu pomieszczeń biurowych, przed przystąpieniem do pracy, pracownicy sprawdzają stan zastosowanych zabezpieczeń sprzętu biurowego i komputerowego, dokumentacji i innego wyposażenia
10. W przypadku stwierdzenia nieprawidłowości lub naruszenia stanu zabezpieczeń, pracownik, który to stwierdził, natychmiast powiadamia o tym swojego bezpośredniego przełożonego.
11. Po zakończeniu pracy pracownicy zobowiązani są do uporządkowania swoich stanowisk pracy oraz wykonania czynności zabezpieczających adekwatnych do zastosowanych rozwiązań technicznych i organizacyjnych polegających w szczególności na:
    1) umieszczeniu dokumentów i pieczęci urzędowych zawierających dane osobowe w szafach i zamknięcie ich na klucz;
    2) zabezpieczeniu komputerów i nośników informacji;
    3) wyłączeniu wszystkich urządzeń energetycznych zasilanych energią elektryczną (czajniki, wentylatory itp.) zgodnie z zasadami bhp;
    4) zamknięciu okien i drzwi.
12. Czynności związanych ze sprzątaniem pomieszczeń lub pracami konserwacyjnymi wykonywane są pod nadzorem pracowników administratora oraz odbywają się w godzinach ich pracy.
13. Dostęp do serwerowni akt posiadają:
    - informatyk,
    - osoby go zastępująca,
    - inne osoby upoważnione przez administratora.
14. Dostęp do zakładowej składnicy akt posiadają:
    - osoba odpowiedzialna za archiwizację,
    - osoba zastępująca,
    - inne osoby upoważnione przez administratora.

ZATWIERDZAM

Zgłoszenie nowej czynności do rejestru czynności przetwarzania danych osobowych Administratora

Nazwa czynności		
Podstawa prawna		
Cel przetwarzania danych		
Planowany termin rozpoczęcia przetwarzania danych osobowych		
Kategorie osób, których dane będą przetwarzane		
Oznaczenie rodzaju przetwarzanych danych osobowych	Dane wrażliwe*	Dane zwykłe*
Symbol JRWA lub okres przetwarzania danych		
Zakres przetwarzania danych		
Sposób przetwarzania danych osobowych	W systemie informatycznym*	W sposób tradycyjny*
Oprogramowanie wykorzystywane do przetwarzania danych osobowych		
Informatyk: wskaże sposób zabezpieczenia danych osobowych w oparciu od politykę.		
Jakim podmiotom zostaną powierzone dane do przetwarzania. Podaj ich nazwę, adres, NIP.	1. 2.	
Przygotowano projekt umowy powierzenia przetwarzania danych osobowych.	TAK*	NIE*
Sposób udostępniania danych		
Projekt klauzuli informacyjnej lub klauzuli zgody		
Uzasadnienie potrzeby wpisu czynności do rejestru		

.....
data podpis

opinia IOD:

.....
.....

.....
data podpis IOD

Zgłoszenie nowej czynności do rejestru wszystkich kategorii czynności przetwarzania danych osobowych procesora

Kategorie przetwarzań dokonywanych w imieniu konkretnego administratora		
Administrator (nazwa i dane kontaktowe)		
Przedstawiciel administratora		
Inspektor ochrony danych wyznaczony przez administratora (imię i nazwisko, dane kontaktowe)międzynarodowej		
Przekazywanie danych do państwa trzeciego (nazwa organizacji i dane kontaktowe) Przekazywanie danych do organizacji międzynarodowej (nazwa i dane kontaktowe) Podstawa prawna transferu danych do państwa trzeciego lub organizacji		
Kategoria danych osobowych	Dane wrażliwe*	Dane zwykłe*
Sposób przetwarzania danych osobowych	W systemie informatycznym*	W sposób tradycyjny*
Data zawarcia umowy powierzenia		
Termin obowiązywania umowy powierzenia		
Uwagi		

.....
...
data podpis

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

.....
data podpis IOD

UMOWA
POWIERZENIA DANYCH OSOBOWYCH DO PRZETWARZANIA

Pomiędzy: Gminą ……..
reprezentowaną przez: Wójta Gminy …… z siedzibą w ……
NIP ……., REGON ……., zwaną w treść Umowy **„Administratorem"**
a
……..
85-120 ……., ul. …… -
reprezentowany przez: ……NIP: ……KRS ……,
zwany w treść Umowy **„Procesorem"** lub **„Przetwarzającym"**,
w dalszej części Umowy Administrator i Procesor są nazywani łącznie **„Stronami"** lub każde oddzielenie **„Stroną"**

§ 1
PRZEDMIOT UMOWY

1. Strony zawarły w dniu …… umowę nr …… o świadczenie usług: ……., zwaną dalej „Umową usługi".
2. Mając na uwadze, że umowa wskazana powyżej dotyczy przetwarzania danych osobowych, na podstawie art. 28 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 (ogólne rozporządzenie o ochronie danych, dalej jako: „RODO") Administrator powierzenia przetwarzania danych osobowych Procesorowi.
3. Przetwarzanie ma charakter czasowy. Celem przetwarzania jest ……..
4. Powierzenie obejmuje dane zwykłe, szczególne kategorie danych, dane wskazane w art. 10 RODO : pracowników, współpracowników, dzieci, uczniów, kontrahentów, klientów, osób kontaktujących się z administratorem, osób wyznaczonych do kontaktów, pełnomocników (itp.).
5. Procesor uprawniony jest do przetwarzania danych osobowych wyłącznie w celu wykonania umowy określonych w ust. 1,
6. Procesor może przetwarzać powierzone mu dane osobowe dla własnych celów jedynie w przypadku dysponowania w tym zakresie odrębną podstawą prawną, o czym ma obowiązek powiadomić osoby, których dane przetwarza.

§ 2
OŚWIADCZENIA I OBOWIĄZKI PROCESORA

1. Procesor oświadcza, że posiada zasoby infrastrukturalne, doświadczenie, wiedzę oraz wykwalifikowany personel, w zakresie umożliwiającym należyte wykonanie niniejszej Umowy, w zgodzie z obowiązującymi przepisami prawa. W szczególności Procesor oświadcza, że znane mu są zasady przetwarzania i zabezpieczenia danych osobowych wynikające RODO, których zobowiązany jest przestrzegać.

2. Procesor jest zobowiązany:
   1) przetwarzać powierzone dane osobowe zgodnie z RODO oraz innymi obowiązującymi przepisami prawa oraz niniejszą Umową;
   2) przetwarzać powierzone mu dane osobowe wyłącznie na obszarze Europejskiego Obszaru Gospodarczego (z zastrzeżeniem rozdziału 5 Umowy) oraz na urządzeniach zarządzanych przez Procesora i jego personel, z zachowaniem zasad bezpieczeństwa ochrony danych osobowych wymaganych przez obowiązujące przepisy prawa;
   3) udzielać dostępu do powierzonych danych osobowych wyłącznie osobom, które ze względu na zakres wykonywanych zadań otrzymały od Procesora upoważnienie do ich przetwarzania oraz wyłącznie w celu wykonywania obowiązków wynikających z Umowy usługi;
   4) zapewnić, aby osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy, chyba że osoby te podlegają odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
   5) wdrożyć odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych, których dane osobowe będą przetwarzane na podstawie Umowy;
   6) wspierać Administratora w miarę możliwości, poprzez stosowanie odpowiednich środków technicznych i organizacyjnych, w realizacji obowiązku odpowiadania na żądania osób, których dane dotyczą, w zakresie wykonywania ich praw określonych w rozdziale III RODO;
   7) pomagać Administratorowi, uwzględniając charakter przetwarzania oraz dostępne mu informacje, wywiązać się z obowiązków określonych w art. 32-36 RODO, tj. w szczególności w zakresie:
      a) zapewnienia bezpieczeństwa przetwarzania danych osobowych poprzez wdrożenie stosownych środków technicznych oraz organizacyjnych;
      b) dokonywania zgłaszania naruszeń ochrony danych osobowych organowi nadzorczemu oraz zawiadamiania osób, których dane dotyczą o takim naruszeniu (obowiązki Procesora w odniesieniu do zgłaszania naruszeń zostały określone w § 8 Umowy);
      c) przeprowadzenia przez Administratora oceny skutków dla ochrony danych oraz przeprowadzania konsultacji Administratora z organem nadzorczym;
   8) prowadzić, w formie pisemnej (w tym elektronicznej), rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu Administratora,
   9) udostępniać Administratorowi, na jego uzasadnione żądanie wszelkie informacje niezbędne do wykazania spełnienia przez Administratora obowiązków wynikających z art. 28 RODO;
   10) umożliwić Administratorowi lub audytorowi upoważnionemu przez Administratora przeprowadzanie audytów, w tym inspekcji na zasadach określonych w § 6 Umowy;
   11) niezwłocznie informować Administratora, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie RODO lub innych przepisów krajowych lub przepisów Unii lub państwa członkowskiego o ochronie danych;
   12) przechowywać dane osobowe powierzone w związku z wykonywaniem danej

Umowy usługi jedynie przez okres jej obowiązywania, a także bez zbędnej zwłoki anonimizować dane lub ograniczać przetwarzanie wskazanych danych osobowych, zgodnie z wytycznymi Administratora i Umową powierzenia.

§ 3
ŚRODKI ORGANIZACYJNE I TECHNICZNE

Procesor wdraża odpowiednie środki techniczne i organizacyjne, uwzględniając stan wiedzy technicznej, koszt wdrożenia, oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku. Oceniając, czy stopień bezpieczeństwa, jest odpowiedni, Procesor uwzględnia w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

§ 4
PODPOWIERZENIE

1. Jeżeli należyte wypełnienie obowiązków wynikających z realizacji niniejszej Umowy oraz Umowy Głównej będzie tego wymagało, Procesor może dokonać dalszego powierzenia przetwarzania danych.
2. Na dzień zawarcia niniejszej Umowy Procesor zamierza powierzyć dane osobowe następującym podmiotom, co Administrator akceptuje:
   1) .....,
   2) .....,
   3) .....,
3. Procesor oświadcza, że podmioty wymienione w ust. 2 spełniają wymogi, o których mowa w art. 28 Rozporządzenia i zostanie to zagwarantowane w umowach dalszego powierzenia przetwarzania danych. Uprawnienia podmiotów, którym zostanie podpowierzone przetwarzanie danych osobowych, nie mogą być szersze aniżeli uprawnienia Procesora wynikające z niniejszej Umowy.
4. Warunkiem dalszego powierzenia danych osobowych przez Procesora innym podmiotom aniżeli wymienionym w ust. 2 jest uprzednie powiadomienie Administratora drogą elektroniczną o tym fakcie, z jednoczesnym oświadczeniem Procesora, iż podmiot któremu zostaną podpowierzone dane osobowe spełnia wymogi, o których mowa w art. 28 Rozporządzenia i zostanie to zagwarantowane w umowie dalszego powierzenia przetwarzania danych. Uprawnienia podmiotu, któremu zostanie podpowierzone przetwarzanie danych osobowych, nie mogą być szersze aniżeli uprawnienia Procesora wynikające z niniejszej Umowy.
5. Uprawnienie, o którym mowa w ust. 1 powyżej, nie wyłącza możliwości wyrażenia przez Administratora sprzeciwu wobec dalszego powierzenia w terminie w terminie do 7 dni roboczych (rozumianych jako dni od poniedziałku do piątku, godz. 8:00-16:00) od dnia otrzymania powiadomienia, o którym mowa w ust. 4.
6. Procesor zobowiązuje się powiadomić Administratora o rozwiązaniu lub wypowiedzeniu umowy podpowierzenia w terminie 10 dni od tego zdarzenia.

§ 5
TRANSFER DANYCH OSOBOWYCH

1. Procesor nie może przekazywać (transferować) danych osobowych do państwa trzeciego,

które znajduje się poza Europejskim Obszarem Gospodarczym („EOG"), chyba że Administrator udzieli mu uprzedniej zgody zezwalającej na taki transfer.

2. Jeśli Administrator udzieli Procesorowi uprzedniej zgody na przekazanie danych osobowych do państwa trzeciego, Procesor może dokonać transferu tych danych osobowych tylko wtedy, gdy:
   1) państwo docelowe zapewnia adekwatny poziom ochrony danych osobowych do tego, który obowiązuje w Unii Europejskiej; lub
   2) Administrator i Procesor lub dalszy podmiot przetwarzający zawarli umowę w oparciu o standardowe klauzule umowne lub wdrożyli inny mechanizm, który zgodnie z przepisami prawa legalizuje transfer danych do państwa trzeciego.

§ 6
AUDYT

1. Administrator jest upoważniony do przeprowadzenia audytu zgodności z Umową oraz obowiązującymi przepisami prawa, przetwarzania przez Procesora powierzonych mu do przetwarzania danych osobowych.
2. Administrator zawiadomi Procesora o planowanym przeprowadzeniu audytu, co najmniej na 14 dni roboczych przed planowaną datą jego przeprowadzenia.
3. Jeżeli w ocenie Procesora audyt nie może zostać przeprowadzony we wskazanym terminie Procesor powinien poinformować o tym fakcie Administratora. W takim przypadku Strony wspólnie ustalą późniejszy termin audytu.
4. Audyty, o których mowa w ust. 1, mogą być wykonywane przez Administratora w miejscu przetwarzania danych osobowych objętych powierzeniem w dni robocze, w godzinach od 8:00 do 16:00. Jeżeli Administrator nie prowadzi audytu samodzielnie, może zlecić przeprowadzenie audytu jedynie podmiotom lub osobom, profesjonalnie świadczącym usługi tego rodzaju („audytor zewnętrzny") pod warunkiem zawiadomienia, o tym Procesora z wyprzedzeniem co najmniej na 7 dni roboczych.
5. W każdym przypadku, w którym Administrator zamierza zlecić przeprowadzenie audytu, w tym inspekcji, audytorowi zewnętrznemu, Administrator ponosi odpowiedzialność za działania lub zaniechania takiego podmiotu jak za własne.
6. Administrator zobowiązany jest zapewnić, by osoby wykonujące czynności w ramach audytu, w tym audytorzy zewnętrzni, zostały zobowiązane do zachowania w poufności wszelkich informacji, które uzyskają w związku wykonywaniem audytu, a stanowiących tajemnicę przedsiębiorstwa Procesora.
7. Administrator zobowiązany jest zapewnić, by osoby wykonujące czynności w ramach audytu, w tym audytorzy zewnętrzni, nie były zatrudnione, nie były wspólnikami, akcjonariuszami, lub członkami organów podmiotów, wykonujących działalność konkurencyjną w stosunku do działalności prowadzonej przez Procesora, ani nie prowadzą takiej działalności konkurencyjnej we własnym imieniu.
8. Na żądanie Procesora, Administrator przedstawi w powyższym zakresie stosowne oświadczenie w formie pisemnej, pod rygorem bezskuteczności niedopuszczenia te osoby lub podmiotu do przeprowadzenia audytu. W przypadku braku złożenia tego oświadczenia, uznaje się, że wskazana osoba, w tym w audytor zewnętrzny, nie ma umocowania do przeprowadzenia audytu. Procesor będzie wówczas uprawniony do wezwania Administratora do wskazania innej osoby lub podmiotu do przeprowadzenia audytu i przedstawienia stosownego oświadczenia, dotyczącego tej osoby lub podmiotu. Do czasu

wykonania tego obowiązku, Procesor będzie uprawniony do niedopuszczenia wskazanej osoby do wykonywania czynności audytowych. Postanowienia niniejsze nie naruszają uprawnienia Administratora do przeprowadzenia audytu samodzielnie.

9. Procesor, w zakresie niezbędnym do przeprowadzenia audytu, będzie współpracować z Administratorem i upoważnionymi przez niego audytorami, w szczególności zapewni im dostęp do:
   1) pomieszczeń i dokumentów obejmujących dane osobowe oraz informacje o sposobie przetwarzania danych osobowych,
   2) infrastruktury teleinformatycznej oraz systemów IT,
   3) osób mających wiedzę na temat procesów przetwarzania danych osobowych realizowanych przez Procesora, z uwzględnieniem konieczności zapewnienia ciągłości działalności gospodarczej i procesów biznesowych realizowanych na bieżąco przez Procesora. Administrator zapewni, że prowadzony audyt nie będzie kolidował z bieżącym wykonywaniem przez Procesora czynności w ramach prowadzonej działalności gospodarczej.
10. Po przeprowadzonym audycie Administrator sporządza protokół pokontrolny, który podpisują przedstawiciele obu Stron.
11. Koszty związane z przeprowadzeniem audytu ponosi każda ze Stron w swoim zakresie. Procesor nie jest zobowiązany do zwrotu Administratorowi jakichkolwiek kosztów związanych z wykonanym audytem, niezależnie od jego wyniku.

§ 7
POUFNOŚĆ

1. Strony mają obowiązek ochrony informacji poufnych, niezależnie od formy ich przekazania i przetwarzania, rozumianych jako informacje takie jak:
   1) dane osobowe, w tym szczególne kategorie danych osobowych (w rozumieniu art. 9 ust. 1 RODO),
   2) informacje stanowiące tajemnicę przedsiębiorstwa (w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji),
   3) informacje wymagające ochrony ze względu na ich znaczenie dla interesów Stron, w tym wszelkie dane techniczne, finansowe i handlowe, materiały i dokumenty,
   4) inne informacje bez względu na fakt, czy są one utrwalone w formie pisemnej lub w jakikolwiek inny sposób, zapisane w jakiejkolwiek formie i na jakimkolwiek nośniku, dotyczące Strony lub jej klientów, kontrahentów, dostawców, a także informacje dotyczące usług, polityki cenowej, sprzedaży, wynagrodzeń pracowników, które druga Strona otrzymała w okresie obowiązywania Umowy, lub o których dowiedziała się, czy też do których miała dostęp lub będzie w ich posiadaniu, w związku z prowadzonymi rozmowami i negocjacjami, a które nie są powszechnie znane.
2. Strony będą zwolnione z obowiązku zachowania w tajemnicy informacji poufnych w przypadku, gdy obowiązek ujawnienia informacji poufnych wynikać będzie z bezwzględnie obowiązujących przepisów prawa, bądź też prawomocnego orzeczenia lub decyzji uprawnionego sądu lub organu. O każdorazowym powzięciu informacji o takim obowiązku Strona jest zobowiązana niezwłocznie powiadomić drugą Stronę. W takim przypadku Strona zobowiązana do ujawnienia informacji poufnych będzie obowiązana do:
   1) ujawnienia tylko takiej części informacji poufnych, jaka jest wymagana przez prawo,

2) podjęcia wszelkich możliwych działań w celu zapewnienia, iż ujawnione informacje poufne będą traktowane w sposób poufny i wykorzystywane tylko w zakresie uzasadnionym celem ujawnienia.

3. Zobowiązanie do zachowania poufności w odniesieniu do danych powierzonych w związku z daną Umową usługi jest nieograniczone w czasie.

§ 8
ZGŁASZANIE NARUSZEŃ

1. Procesor po stwierdzeniu naruszenia ochrony danych osobowych, bez zbędnej zwłoki, nie później niż w ciągu 24 godzin od stwierdzenia naruszenia, zgłasza je Administratorowi.
2. Procesor informuje o okolicznościach naruszenia i potencjalnych zagrożeniach dla ochrony powierzonych danych osobowych oraz jest zobowiązanych pisemnie określić:
   1) charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,
   2) możliwe konsekwencje naruszenia ochrony danych osobowych,
   3) zastosowane lub proponowane środki w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków,
3. Procesor, bez zbędnej zwłoki, podejmuje wszelkie rozsądne działania mające na celu ograniczenie i naprawienie negatywnych skutków naruszenia.
4. Procesor nie jest uprawniony ani zobowiązany do powiadamiania o naruszeniu:
   1) osób, których dane dotyczą; ani
   2) organu nadzorczego

§ 9
CZAS TRWANIA UMOWY I ODPOWIEDZIALNOŚĆ

1. Niniejsza umowa zostaje zawarta na okres obowiązywania Umowy Głównej, o których mowa w § 1 ust. 1 z zastrzeżeniem § 9 ust. 2.
2. Administrator uprawniony jest do rozwiązania Umowy ze skutkiem natychmiastowym, w przypadku rażącego lub powtarzającego się naruszenia Umowy przez Procesora, a także w przypadku, gdy:
   1) organ nadzoru nad przestrzeganiem zasad przetwarzania danych osobowych stwierdzi, na podstawie prawomocnej decyzji, że Procesor lub dalszy podmiot przetwarzający nie przestrzega zasad przetwarzania danych osobowych,
   2) prawomocne orzeczenie sądu powszechnego wykaże, że Procesor nie przestrzega zasad przetwarzania danych osobowych – pod warunkiem uprzedniego pisemnego wezwania Procesora do zaniechania naruszeń i usunięcia ich skutków, wyznaczenia, w tym celu dodatkowego terminu, nie krótszego niż 30 dni, i bezskutecznego upływu tego terminu.
3. Administrator zobowiązuje Procesora do anonimizacji wszystkich powierzonych danych osobowych oraz usunięcia ich kopii niezwłocznie po zakończeniu obowiązywania Umowy w terminie uzasadnionym względami technicznymi lecz w żadnym wypadku nie później niż w ciągu 30 dni, chyba że właściwe przepisy prawa krajowego lub unijnego nakazują przechowywanie tych danych osobowych. O usunięciu danych Procesor powiadomi Administratora pisemnie, w terminie 5 dni od dnia usunięcia danych, zgodnie z

załącznikiem nr 1 do niniejszej umowy

4. Procesor jest zobowiązany do podjęcia stosownego działania w celu wyeliminowania możliwości dalszego przetwarzania danych powierzonych na podstawie niniejszej Umowy.

§ 10
POSTANOWIENIA KOŃCOWE

1. Wszelka korespondencja w sprawach związanych z Umową będzie prowadzona w następujący sposób:
   - ze strony Procesora – na adres poczty elektronicznej: .....@.....pl;
   - ze strony Administratora – na adres poczty elektronicznej: .....@.....pl .
2. Wszelkie oświadczenia i zawiadomienia mogą być składane za pośrednictwem poczty elektronicznej, zabezpieczonej w sposób uzgodniony przez Strony, chyba że Umowa lub bezwzględnie obowiązujące przepisy prawa wymagają formy pisemnej, pod rygorem nieważności.
3. Zmiana adresów nie stanowi zmiany Umowy. O każdej zmianie danych Strony powiadomią się na piśmie, lub drogą elektroniczną, wskazując nowe dane kontaktowe.
4. Do chwili złożenia oświadczenia o zmianie danych, oświadczenia i zawiadomienia kierowane na dotychczasowe adresy uważa się za skuteczne.
5. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej Strony.
6. Zmiany Umowy są możliwe wyłącznie w formie pisemnej pod rygorem nieważności z zastrzeżeniem sytuacji, w których Umowa wprost przewiduje inną formę dokonywania zmian.
7. Użyte w Umowie pojęcia należy interpretować zgodnie z RODO.
8. Spory mające związek z Umową rozstrzygać będzie sąd właściwy dla siedziby Administratora.

Administrator **Procesor**

Załącznik nr 1
do umowy powierzenia
przetwarzania danych osobowych

..... dnia, ...

.....
(Pełna nazwa podmiotu przetwarzającego dane)

.....
(Adres siedziby podmiotu przetwarzającego dane)

.....
(dane administratora)

Informacja o zaprzestaniu przetwarzania danych osobowych

Zgodnie z art. 28 ust. 3 lit. g 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, zwanego dalej „RODO"). Informuję, że zgodnie z Umową Powierzenia Przetwarzania Danych zawartą w dniu .....dane osobowe przekazane przez ..... po wygaśnięciu umowy zostały usunięte - zniszczone i nie będą wykorzystywane w dalszej działalności.

.....
(pieczątka i podpis)

Załącznik nr 2
do umowy powierzenia przetwarzania danych osobowych

ARKUSZ WERYFIKACJI PODMIOTU PRZETWARZAJĄCEGO DANE OSOBOWE

Lp.	Pytanie	Odpowiedź	Uwagi
1.	Czy jako podmiot przetwarzający dane osobowe planujesz wyznaczyć/wyznaczyłeś Inspektora Ochrony Danych Osobowych (IOD)?	- tak zaplanowano wyznaczenie - tak wyznaczono - nie zaplanowano wyznaczenia (uzasadnienie: np. nie jest wymagane przepisami prawa) - zaplanowano wyznaczenie (kiedy: podać przewidywaną datę)	Jeśli wyznaczyłem IOD podaj jego imię i nazwisko oraz dane kontaktowe ..... e-mail..... tel. .....
2.	Jeżeli nie planuje wyznaczyć/nie został wyznaczony IOD to proszę o wskazanie innej osoby do kontaktu w kwestiach związanych z ochroną danych osobowych.	Osoba do kontaktu..., stanowisko/funkcja..., numer tel.	
3.	Czy jako podmiot przetwarzający dane osobowe wprowadziłeś środki techniczne i organizacyjne w tym politykę ochrony danych osobowych/bezpieczeństwa informacji/zarzadzania systemem informatycznym, które będą spełniały wymogi RODO oraz innych aktów regulujących legalne przetwarzanie danych osobowych?	TAK/NIE	**Jeśli tak np. jakie, skreśl niepotrzebne.** 1. Obszar przetwarzania objęty jest zamykany/objęty ochroną/ monitoringiem wizyjnym. 2. Dostęp do stref szczególnie chronionych ograniczony jest do osób upoważnionych (serwerownia, archiwum, itp.) 3. Posiadamy niszczarki do dokumentów papierowych oraz nośników pamięci. 4. Wprowadzono politykę ochrony danych, politykę zarzadzania systemem informatycznym, inne regulaminy i procedury. 5. Wyznaczono osobę odpowiedzialną za ciągłość działania systemu informatycznego. 6. Pracownicy otrzymali upoważnienia do przetwarzania danych osobowych oraz odebrano od nich oświadczenie o zachowaniu danych w poufności. 7. Pracownicy posiadają aktualne uprawnienia do przetwarzania danych w systemach

			informatycznych. 8. Pracownicy zostali przeszkoleni w zakresie ochrony danych osobowych oraz przetwarzania danych w systemach informatycznych. 9. Tworzoną są kopie zapasowe danych. 10. Dyski twarde komputerów oraz zewnętrzne nośniki pamięci są szyfrowane. 11. Posiadamy aktualne oprogramowanie antywirusowe oraz używamy firewall. 12. Poczta elektroniczne wykorzystuje protokoły imap/pop oraz certyfikat ssl. 13. Urządzenia posiadają bieżące wsparcie oprogramowania operacyjnego. 14. Logowanie do systemów odbywa się na podstawie loginu i hasła. 15. Wprowadzono zasady określające złożoność haseł i jego zmian do komputerów, serwera, sieci internetowej. 16. Dostęp do sieci Wifi opatrzony jest hasłem. 17. Stosowane jest rozwiązanie „chmury obliczeniowej" 18. Przeprowadzono szacowanie ryzyka dla ochrony danych osobowych.
4.	Czy jako podmiot przetwarzający dane osobowe korzystasz z dalszych przetwarzających dane osobowe w procesie przetwarzania danych osobowych na zlecenie administratora danych osobowych?	TAK/NIE	(jeśli tak, to przygotuj wykaz tych podmiotów w celu załączenia do umowy powierzania) 1..... 2..... 3.....
5.	Jeżeli jako podmiot przetwarzający dane osobowe korzystasz z dalszych procesorów to czy są oni zlokalizowani w ramach EOG?	TAK/NIE	
6.	Jeżeli transfer danych odbywa się poza EOG to na jakiej podstawie prawnej?	TAK/NIE	

7.	Czy z dalszymi procesorami zostały zawarte umowy powierzenia przetwarzania danych i czy stosują one środki techniczne i organizacyjne spełniające wymogi RODO?	TAK/NIE	
8.	Czy Twoi pracownicy, którzy będą przetwarzać powierzone dane, mają wydane upoważnienia do przetwarzania danych osobowych oraz odebrano od nich zobowiązanie do zachowaniu danych w poufności/tajemnicy	TAK/NIE	
9.	Czy prowadzisz rejestr czynności przetwarzania.	TAK/NIE	
10.	Czy jako podmiot przetwarzający dane osobowe prowadzisz rejestr kategorii czynności dla powierzonych operacji przetwarzania danych osobowych?	TAK/NIE	
11.	Czy jako podmiot przetwarzający jesteś w stanie wspomagać administratora poprzez odpowiednie środki techniczne i organizacyjne, by wywiązać się z obowiązku odpowiadania na żądanie osoby, której dane dotyczą, w zakresie wykonywania jej praw?	TAK/NIE	
12.	Czy jako podmiot przetwarzający dysponujesz środkami, które pozwalają na trwałe usunięcie lub zwrot wszelkich danych osobowych oraz usunięcie ich wszelkich istniejących kopii?	TAK/NIE	Jeśli TAK to jakie są to środki? Program do usuwania danych - ..... Niszczarka do dokumentów oraz nośników danych -.....
13.	Czy umożliwisz administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzania audytów, w tym inspekcji?	TAK/NIE	
14.	Czy jako podmiot przetwarzający dane osobowe wdrożyłeś procedury dotyczące zarządzania incydentami bezpieczeństwa?	TAK/NIE	
15.	Czy jako podmiot przetwarzający jesteś w stanie informować administratora niezwłocznie, nie później niż w ciągu 24 godzin, o naruszeniach ochrony danych osobowych, do których u Ciebie dojdzie?	TAK/NIE	

16.	Czy jako podmiot przetwarzający wprowadziłeś środki zapewniające, że systemy IT używane do przetwarzania danych osobowych są zgodne z RODO oraz innymi aktami regulującymi przetwarzanie danych osobowych?	TAK/NIE	
17.	Czy jako podmiot przetwarzający realizujesz regularne audyty z zakresu bezpieczeństwa danych osobowych? Jeżeli tak to w jakich odstępach czasu odbywają się audyty? czy możesz udostępnić raporty?	TAK/NIE	
18.	Czy jako podmiot przetwarzający dane osobowe posiadasz aktualny certyfikat ISO 27001 /stosujesz zatwierdzony kodeks postepowania/uzyskałeś inny certyfikat/klauzulę zgodności	TAK/NIE	(jeśli TAK wskaż właściwe)
19.	Czy wobec ciebie jako administratora lub podmiot przetwarzający została wydana decyzja dotycząca naruszenia zasad przetwarzania danych lub toczy się postepowanie związane z naruszeniem?	TAK/NIE	Jeśli TAK jakie i w jakim zakresie? Proszę podać nr decyzji UODO lub jej kopię.

*Właściwe podkreślić/uzupełnić

_____

Podpis osoby
upoważnionej lub reprezentującej
podmiotu przetwarzający

Załącznik nr 7 do Polityki Bezpieczeństwa Informacji i Ochrony Danych Osobowych

Zgłoszenie naruszenia ochrony danych osobowych

Sporządzający zgłoszenie:
Imię i nazwisko ..... stanowisko .....
Rodzaj naruszenia bezpieczeństwa danych osobowych .....

1. Miejsce, dokładny czas i data ujawnienia naruszenia ochrony danych osobowych (piętro, nr pokoju, godzina, itp.):
   .....
   .....
2. Osoby , które uczestniczyły w zdarzeniu związanym z naruszeniem ochrony danych
   .....
   .....
3. Działanie wskazujące na naruszenie ochrony danych osobowych:
   .....
   .....
4. Określenie informacji mogących wskazywać na przyczynę naruszenia:
   .....
   .....
5. Określenie wszelkich kroków podjętych po ujawnieniu naruszenia:
   .....
   .....
6. Osoby powodujące naruszenie (które swoim działaniem lub zaniechaniem przyczyniły się do naruszenia ochrony danych osobowych):
   .....
7. Opis charakteru naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazanie kategorii i przybliżonej liczbę osób, których dane dotyczą, oraz kategorii i przybliżonej liczby osób, których dotyczy naruszenie.
   .....
   .....
8. Opis możliwych konsekwencji naruszenia ochrony danych osobowych.
   .....
   .....
9. Opis zastosowanych środków lub propozycje zastosowania środków mających na celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
   .....
   .....
10. Zabezpieczone materiały lub inne dowody związane z wydarzeniem
    .....
    .....
11. Wnioski:
    .....

.....
(miejsce, data i godzina sporządzenia podpis sporządzającego)

Zapoznałem się:

OCENA WAGI NARUSZENIA

W dniu ..... r. Zespół ds. wdrożenia i stosowania RODO .....w składzie:
..... – przewodnicząca zespołu
..... – członek zespołu
..... - członek zespołu
w związku ze stwierdzonym w dniu ..... r. naruszeniem ochrony danych osobowych w ....., dokonał oceny wagi naruszenia w celu ustalenia:

1. czy naruszenie skutkowało ryzykiem naruszania praw lub wolności osób fizycznych,
2. czy naruszenie podlega zgłoszeniu do Prezesa Urzędu Ochrony Danych Osobowych oraz poinformowaniu osób, których dane naruszono.

Zespół zastosował poniższą metodologią:
WN=KPD x PI + ON
gdzie:
WN – Waga naruszenia
KPD – Kontekst Przetwarzania danych – Główny czynnik określający poziom krytyczności zestawu naruszonych danych w określonym kontekście przetwarzania

KPD = A + B

A- Rodzaj i poziom wrażliwości danych:

1 pkt – dane podstawowe

2 pkt – dane dotyczące zachowań osoby
3 pkt - dane finansowe
4 pkt – dane szczególnych kategorii

B – kontekst przetwarzania, który może podwyższyć lub obniżyć wycenę:

Szeroki zakres danych/wolumen (+)
Charakter danych (+/-)
Specyfika podmiotu danych lub administratora (+/-)
Możliwe negatywne skutki dla podmiotu danych (+)
Publiczna dostępność danych przed naruszaniem (-)

PI - Prawdopodobieństwo identyfikacji:

Znikome	= 0,25
Ograniczone	= 0,5
Wysokie	= 0,75
Maksymalne	= 1

ON – Okoliczności naruszenia – ON = NP+ NI + ND + + IDS

Naruszenie poufności – dane ujawnione
znanym odbiorcom danych (+0,25)
nieznanej liczbie obiorców danych (+0,5)
Naruszanie Integralności – dane zmienione
Możliwe jest ich odzyskanie (+0,25)
Brak jest możliwości ich odzyskania (+0,5)
Naruszenie Dostępności – niedostępność danych

Czasowe (+025)
Pełna i brak możliwości ich odzyskania przez administratora lub podmiot danych (+0,5)
Intencjonalne działanie sprawcy (+0,5)

wynik	Waga naruszenia	opis
WN < 2	Niska	**Osoby nie zostaną dotknięte naruszeniem lub wywoła ono drobne niedogodności**
2<=WN<3	Średnia	**Osoby mogą napotkać niedogodności**
3<+WN<4	Wysoka	**Mogą wystąpić konsekwencje możliwe do pokonania, ale z poważnymi skutkami**
4<=WN	krytyczna	**Mogą wystąpić znaczące, nawet nieodwracalne konsekwencje**

Mając na względzie zaistniałe naruszenie należy przyjąć przy zastosowaniu wzoru:
WN=KPD x PI + ON
KPD = A + B
A - Rodzaj i poziom wrażliwości danych stwierdzono, że naruszanie dotyczyło danych podstawowych, w postaci danych osobowych powiązanych z danymi finansowymi – przyjęto **0 pkt.**
B – po przeanalizowaniu kontekstu przetwarzania danych ustalono, że naruszenie dotyczy szerokiego zakresu danych osobowych – przyjęto **0 pkt.**
KPD = 0 pkt
PI - Prawdopodobieństwo identyfikacji
Po przeprowadzaniu analizy materiałów naruszenia oraz mając na uwadze kontekst przetwarzania oraz charakter naruszonych danych ustalono, że prawdopodobieństwo identyfikacji jest na poziomie znikomym – **0 pkt.**
PI = 0 pkt
ON – Okoliczności naruszenia – ON = NP+ NI + ND + + IDS
Naruszenie poufności – dane ujawnione – przyjęto 0 **pkt.**
Naruszanie Integralności – dane zmienione – przyjęto **0 pkt.**
Naruszenie Dostępności – niedostępność danych – przyjęto **0,25 pkt.**
Intencjonalne działanie sprawcy - z przeprowadzonych ustaleń wynika, że sprawca działa umyślnie – przyjęto + **0 pkt.**
ON - 0 + 0 + 0 + 0,0= 0 pkt

WPN = 0 x 0 + 0 = 0
Po przeprowadzeniu analizy czynników mających wpływ na wagę naruszenia ustalono, że wynosi ona 0 pkt wobec czego należy uznać, że waga naruszenia jest niska/średnia/wysoka/ krytyczna i powoduje, że osoby, których dane naruszono .....
Wnioski:
Na podstawie przeprowadzonej oceny wagi naruszenia, zespół wnosi aby uznać, że naruszenia ujawnione i stwierdzone w dniu ..... r.:

1. .....
2. .....

.....
.....

Załącznik nr 2 do Zarządzenia Nr 81 /2023
Wójta Gminy Ciechocin
z dnia 21 grudnia 2023 r

POLITYKA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM W URZĘDZIE GMINY CIECHOCIN

UWAGA:
Dokument wyłącznie
do użytku wewnętrznego

Zatwierdzam:

WÓJT

21.12.2023r. Andrzej Okruciński

data i podpis Administratora

§ 1
Postanowienia Ogólne

1. Polityka określa zasady oraz tryb postępowania przy przetwarzaniu informacji w systemach informatycznych w celu zapewnienie bezpieczeństwa tych informacji zgodnie z Rozporządzenia Parlamentu Europejskiego i Rady(UE) Nr 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 – EODO) oraz Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2017 poz. 2247).
2. Przez zapewnienie bezpieczeństwa informacji należy rozumieć zachowanie:
    1) **poufności** - daje gwarancję, że informacje są dostępne tylko i wyłącznie dla autoryzowanych osób - pracowników, posiadających prawo dostępu do tych informacji,
    2) **integralności** - zabezpiecza ona dokładność i kompletność zarówno informacji, jak też i stosowanych metod jej ochrony oraz zapewnia, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
    3) **dostępności** - gwarancja, że użytkownicy posiadający stosowne uprawnienia mają stały dostęp do informacji i zgromadzonych zasobów,
    4) **rozliczalności** - zapewnienie, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko jemu,
    5) **autentyczności** - zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana (autentyczność dotyczy użytkowników, procesów, systemów i informacji),
    6) **niezaprzeczalności** – brak możliwości wyparcia się swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie,
    7) **niezawodności** – zapewnienie spójności oraz zamierzonych zachowań i skutków, co można interpretować jako poprawność danych i właściwą ich interpretację.
3. Przestrzeganie zasad i procedur zawartych w instrukcji ma na celu zmniejszenie ryzyka utraty poufności, integralności i dostępności informacji przetwarzanych w Systemie Informatycznym w zakresie zidentyfikowanych zagrożeń:
    1) włamania do systemu informatycznego i pozyskania informacji przez osoby nieuprawnione.
    2) pozyskania informacji przez osoby nieuprawnione na skutek bezpośredniego dostępu do komputera,
    3) pozyskania informacji przez osoby nieuprawnione w trakcie przesyłania ich siecią publiczną (INTERNET),
    4) dokonywania modyfikacji informacji przez osoby nieuprawnione,
    5) utraty informacji bądź jej dezintegracji,
    6) utraty czasowej dostępności do informacji.
4. Podstawowe pojęcia:
    1) **Administrator – Wójt Gminy Ciechocin**
    2) **Inspektor Ochrony Danych** – osoba wyznaczona przez administratora lub podmiot przetwarzający na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, zwany dalej inspektorem.
    3) **Administrator sytemu informatycznego (ASI) - Informatyk** – osoba wyznaczona przez administratora odpowiedzialna za sprawność i konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych do przetwarzania informacji i danych osobowych, zwany dalej informatykiem lub ASI. W przypadku niewyznaczenia informatyka, jego obowiązki pełni administrator.

4) **System do przetwarzania informacji w tym danych osobowych** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych, zwany dalej system TI.
5) **Identyfikator** - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych
w systemie informatycznym
6) **Hasło** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi.
7) **Użytkownik systemu** - osoba upoważniona przez administratora lub podmiot przetwarzający do przetwarzania informacji i danych osobowych, której przyznano uprawnienia do przetwarzania danych osobowych w systemie do przetwarzania danych osobowych w zakresie wskazanym w upoważnieniu, zwany dalej użytkownikiem.

5. Wzory dokumentów określone w załącznikach do polityki mogą być zastąpione innymi wzorami dokumentów jednakże zgodnymi z zasadami określonymi niniejszej polityce.

§ 2
System teleinformatyczny

1. Przetwarzanie danych osobowych odbywa się na:
   1) serwerze,
   2) stacjach roboczych użytkowników,
   3) urządzeniach mobilnych takich m.in. jak laptopy, smartfony, tablety itp.
   4) urządzeniach peryferyjnych takich m.in. jak: drukarki, skanery, faxy itp., a także w sposób zdalny i mobilny.
2. Sprzęt informatyczny połączony jest z siecią publiczną z wyjątkiem rejestrów państwowych, które przekazano do przetwarzania administratorowi.
3. Przetwarzanie danych odbywa się także w sposób zdalny i mobilny.
4. Informacje dotyczące sprzętu informatycznego oraz oprogramowania stosowanego do przetwarzania danych osobowych zawiera zał. nr 1.

§ 3
Poziom bezpieczeństwa

1. Uwzględniając kategorie danych osobowych i informacji przetwarzanych przez administratora oraz konieczność zachowania bezpieczeństwa ich przetwarzania w systemie TI połączonym z siecią publiczną, wprowadza się wysoki poziom bezpieczeństwa, który zostanie uzyskany przy zastosowaniu n/wym. zasad.
2. Zabezpieczenie obszaru przetwarzania danych w tym infrastruktury informatycznej i telekomunikacyjnej realizowane jest przez:
   1) zabezpieczenie obszaru przetwarzania danych przed dostępem osób nieuprawnionych podczas nieobecności upoważnionych pracowników administratora;
   2) nadzór osób upoważnionych nad przebywającymi w obszarze przetwarzania danych osobami nieuprawnionymi;
   3) kontrolę dostępu do pomieszczeń serwerowni.
   4) zabezpieczenia przed skutkami awarii zasilania (UPS) dla serwerów i pozostałych kluczowych elementów systemu,
   5) autonomiczne klimatyzatory w pomieszczeniach serwerowni.
3. Urządzenia i nośniki zawierające dane przekazywane poza obszar przetwarzania danych, zabezpiecza się w sposób zapewniający ich poufność i integralność.
4. Okablowanie sieciowe zostało zaprojektowane w ten sposób, że dostęp do linii transmisyjnych jest możliwy tylko z pomieszczeń zamykanych na klucz.

5. Wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej stosuje się środki kryptograficznej ochrony.
6. Przesyłanie poczty elektronicznej odbywa się za pomocą łącza szyfrowanego odpowiadającego właściwościom certyfikatu SSL.
7. Przeglądarki internetowe stanowisk komputerowych domyślnie ustawione są w sposób uniemożliwiający automatyczne uzupełnianie formularzy i haseł dostępu do kont pocztowych i programów.
8. System informatyczny jest zabezpieczony przed działaniem niebezpiecznego oprogramowania poprzez:
    1) zastosowanie środków ochrony przed szkodliwym oprogramowaniem,
    2) użycie systemu Firewall do ochrony dostępu do sieci komputerowej,
    3) aktualizację oprogramowania systemowego, a w razie zakończenia wsparcia przez producenta oprogramowania, wybór i zainstalowanie innego spełniającego wymogi aktualnego bezpieczeństwa,
    4) zainstalowanie na komputerach programów antywirusowych,
    5) centralnie zarządzany system antywirusowy pozwalający monitorować stan oprogramowania antywirusowego na stanowiskach komputerowych,
    6) regularne skanowanie stanowisk komputerowych programem antywirusowym zgodnie z harmonogramem
    7) skanowanie stanowisk komputerowych programem antywirusowym wg potrzeb i zaleceń informatyka,
    8) zainstalowanie na serwerach i stanowiskach komputerowych użytkowników wyłącznie programów spełniających wymogi legalności,
    9) mechanizm wymuszający skanowanie zewnętrznych nośników informacji na obecność wirusów i innego szkodliwego oprogramowania przed ich użyciem na stanowisku komputerowym,
9. System Informatyczny jest chroniony przed zagrożeniami pochodzącymi z sieci publicznej przez wdrożenie fizycznych i logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem poprzez:
    1) monitorowanie stanowisk komputerowych użytkowników pod kątem legalności oprogramowania,
    2) zablokowanie dostępu do kategorii stron internetowych, które mogą wpływać na obniżenie poziomu bezpieczeństwa przetwarzania danych systemu,
    3) konfigurację oprogramowania minimalizującą ryzyko naruszenia bezpieczeństwa,
    4) mechanizmy monitorujące aktywność użytkowników w sieci publicznej,
    5) mechanizm wymuszający okresową zmianę haseł dostępu,
    6) przydzielanie uprawnionym indywidualnych identyfikatorów,
    7) mechanizm uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła,
    8) zakaz ponownego stosowania identyfikatorów, które utracił ważność,
    9) mechanizmy pozwalające na określenie odpowiednich praw dostępu do danych dla poszczególnych użytkowników, informatyka i administratora,
    10) mechanizm automatycznego wygaszania ekranów na stanowiskach komputerowych po upływie 5 min. bezczynności i konieczność ponownego zalogowania do systemu po wznowieniu pracy,
    11) mechanizm wymuszający ponowne zalogowanie do systemu po wznowieniu pracy na stanowisku komputerowym.
10. Zabezpieczenie systemu do przetwarzania danych przed zagrożeniami pochodzącymi z sieci publicznej realizowane jest przez:
    1) odseparowanie sieci obsługującej przetwarzanie rejestrów państwowych,
    2) blokowanie nieuprawnionego dostępu do sieci administratora z sieci publicznej,
    3) ustalenie reguł zdalnego serwisu użytkowanych programów,
    4) ograniczenie kategorii dostępnych stron WWW,
    5) kontrolę antywirusową odwiedzanych stron WWW,
    6) kontrolę antywirusową treści informacji przekazywanych do i z sieci publicznej,

7) ewidencję wszystkich połączeń z siecią publiczną,
8) kontrolę antywirusową treści informacji przekazywanych do i z sieci publicznej,
9) generowanie okresowych raportów o wykorzystaniu dostępu do sieci publicznej.

§ 4
Zasady korzystania z sieci Internet

1. Strony WWW mogące być źródłem ataków lub szkodliwego oprogramowania są niedostępne dla użytkowników.
2. Wykaz kategorii i adresów stron internetowych zablokowanych w systemie informatycznym stanowi zał. nr 2.
3. O zablokowaniu dostępu do strony WWW niezbędnej do wykonywania czynności służbowych, użytkownik informuje informatyka, podając pełny adres zablokowanej strony; jeżeli dostęp został zablokowany przypadkowo, to po pozytywnej weryfikacji zawartości strony WWW informatyk odblokowuje ją, a w przypadkach wątpliwych, o odblokowaniu strony WWW decyduje administrator.
4. Informatyk może odmówić odblokowania strony WWW, jeżeli w wyniku tego obniżyłby się poziom bezpieczeństwa sytemu i sieci.
5. Zdalny dostęp do systemu z sieci publicznej, a w szczególności do aplikacji służących do przetwarzania danych osobowych jest możliwy jedynie przy zastosowaniu technicznych zabezpieczeń zapewniających rozliczalność, autentyczność i niezaprzeczalność osób, a także integralność i poufność przetwarzanych danych. Dostęp realizowany jest przy wykorzystaniu szyfrowanych protokołów transmisji danych.
6. Dostęp do systemu z sieci publicznej jest możliwy dla osób i podmiotów do tego uprawnionych i dotyczy to następujących sytuacji:
    1) świadczenia serwisu zdalnego:
        a) dostęp w ramach zawartych umów dotyczących serwisu oprogramowania zainstalowanego w systemie - na czas trwania umowy, zasady dostępu do danych osobowych precyzuje zawarta dodatkowo umowa powierzenia przetwarzania danych osobowych pomiędzy administratorem, a podmiotem, który świadczy usługi serwisowe,
        b) dostęp jest możliwy wyłącznie na czas wykonywania prac serwisowych i jest blokowany po ich zakończeniu,
        c) dostęp polegający na zdalnej kontroli pulpitu użytkownika jest możliwy tylko za pomocą licencjonowanych narzędzi programowych zapewniających szyfrowanie transmisji;
    2) wykonywania czynności kontrolnych, konserwacyjnych, diagnostycznych oraz naprawczych przez informatyka.
7. Informatyk może ograniczyć lub zablokować dostęp do sieci publicznej użytkownikowi nie przestrzegającemu zasad polityki ochrony danych.
8. Informatyk może ograniczyć lub zablokować dostęp do sieci publicznej użytkownikowi nie przestrzegającemu zasad niniejszej polityki.

§ 5
Procedura nadawania, zmiany, zawieszenia i cofnięcia uprawnień do przetwarzania danych w systemie TI oraz stosowane środki uwierzytelnienia.

1. Uprawnienia do systemu informatycznego otrzymuje wyłącznie osoba posiadająca upoważnienie administratora wydane zgodnie z politykami bezpieczeństwa informacji stosowanymi przez administratora.
2. Tworzy się dwa konta administratora służące do zarzadzania systemem serwera. Oba konta posiadają te same uprawnienia w zakresie zarządzania systemem z wyjątkiem wzajemnej możliwości haseł dostępowych.
    1) Pierwsze konto o identyfikatorze - ASI - zarządzane jest przez informatyka.

2) Drugie konto o identyfikatorze – admin – tworzone jest dla administratora. Hasło do konta nadawane jest przy pierwszym uruchomieniu serwera.

3. Hasła do kont składają się min. z 8 znaków zawierających cyfry, duże i małe litery oraz znak specjalny.
4. Hasło do konta – ASI – zmieniane jest raz na rok, hasło to nie może być podobne do 2 ostatnio używanych.
5. Hasło do konta admin przechowywane jest w zapieczętowanej kopercie przez- administratora. Hasło to podlega użyciu w przypadku wystąpienia naruszenia bezpieczeństwa systemu informatycznego do przetwarzania danych lub braku możliwości wykorzystania konta – ASI
6. Wykorzystanie hasła do konta – admin 2 podlega pisemnemu udokumentowaniu.
7. Uprawnienia oraz zmiany w zakresie uprawnień do kont ASI i admin określa administrator zgodnie ze wzorem - zał. nr 3 do polityki.
8. W procesie uwierzytelnienia użytkowników systemu TI wykorzystywane są identyfikatory i hasła.
9. Nadawanie, cofnięcie, zmianę lub zawieszenie uprawnień do systemu TI lub poczty elektronicznej następuje na podstawie wniosku przełożonego pracownika, a w przypadku osoby nie będącej pracownikiem na wniosek przełożonego pracownika koordynującego lub nadzorującego pracę takiej osoby zgodnie ze wzorem - zał. nr 3 do polityki.
10. Wnioski o nadanie, zmianę, zawieszenie i cofnięcie uprawnień przechowuje informatyk.
11. Uprawnienia do systemu TI na podstawie wniosku przydziela informatyk.
12. W przypadku nadawania użytkownikowi systemu uprawnień do danego systemu informatycznego po raz pierwszy, informatyk dokonuje nadania użytkownikowi systemu identyfikatora oraz adresu poczty elektronicznej i wygenerowania hasła.
13. Identyfikator użytkownika w systemie informatycznym oraz adres poczty elektronicznej musi być unikalny dla użytkownika i zawierać minimum 3 znaki.
14. Zabronione jest stosowanie identyfikatora, który w przeszłości był już stosowany w systemie TI. Sprawdzenie unikalności identyfikatora dokonuje informatyk na podstawie wniosków o nadanie uprawnień do przetwarzania informacji i danych osobowych.
15. Odbiór identyfikatora do systemu i adres poczty elektronicznej oraz hasło pierwszego logowania użytkownik systemu TI kwituje we wniosku – wzór zał. nr 3.
16. Zasady określające proces uwierzytelniania obowiązują w przypadku pracy na stacjonarnym, jak i mobilnym sprzęcie informatycznym.
17. Hasła dostępu do systemu informatycznego z wyjątkiem urządzeń mobilnych typu smartfon, tablet, terminal mobilny muszą spełniać poniższe warunki:
    1) posiadać długość co najmniej 8 znaków,
    2) zawierać litery małe i duże,
    3) zawierać cyfry lub znaki specjalne.
18. Użytkownik systemu jest zobowiązany do zmiany hasła nie rzadziej niż co 3 miesięcy, chyba że zmiana hasła jest wymuszona przez system informatyczny lub niezwłocznie w przypadku podejrzenia, iż mogły z nim się zapoznać nieuprawnione osoby. Jeżeli użytkownik nie posiada uprawnień do zamiany hasła, czynność tą wykonuje informatyk.
19. Hasło powinno różnić się od 2 poprzednio stosowanych.
20. Informatyk przekazując dane pierwszego logowania przeprowadza szkolenie użytkownika systemu wskazując zasady korzystania ze sprzętu informatycznego oraz poczty elektronicznej.
21. Użytkownik po zalogowaniu do systemu z wykorzystaniem otrzymanego hasła jest zobowiązany do dokonania jego natychmiastowej zmiany, nawet jeżeli system informatyczny nie wymusza takiego działania.
22. Na stanowiskach komputerowych, dopuszcza się zastosowanie konta z uprawnieniami „gość" nieopatrzonego hasłem.
23. Użytkownik systemu zobowiązany jest do:
    1) nieujawniania hasła innym osobom, w tym innym użytkownikom,
    2) zachowania hasła w tajemnicy, również po jego wygaśnięciu,
    3) postępowania z hasłami w sposób uniemożliwiający dostęp do nich osobom trzecim,
    4) przestrzegania zasad dotyczących jakości i częstości zmian hasła,

5) wprowadzania hasła do systemu w sposób minimalizujący ujawnianie go przez innych użytkowników systemu.

24. Wykorzystanie identyfikatora i hasła innego użytkownika, w tym w ramach pełnionego zastępstwa, stanowi naruszenia zasad bezpieczeństwa informacji i może naruszać podstawowe obowiązki pracownicze.
25. Monitor stanowiska komputerowego powinien być ustawiony w taki sposób, aby uniemożliwić wgląd w dane przebywającym w pomieszczeniu osobom nieupoważnionym.
26. W przypadku zapomnienia hasła użytkownik systemu powinien zwrócić się do informatyka o wygenerowanie nowego hasła.
27. W przypadku stwierdzenia naruszenia bezpieczeństwa informacji w związku z utratą poufności hasła użytkownik systemu jest zobowiązany do natychmiastowej zmiany hasła oraz powiadomienia o zaistniałym fakcie informatyka oraz bezpośredniego przełożonego, który podejmuje działania zgodnie z § 12 niniejszej polityki. W innym przypadku informatyk nadaje użytkownikowi nowe hasło logowania i pisemnie dokumentuje tą czynność.

§ 6
Procedura rozpoczęcia, zawieszenia i zakończenia pracy w systemie TI

1. Rozpoczynając pracę w systemie informatycznym użytkownik systemu:
   1) uruchamia komputer,
   2) wprowadza identyfikatory i hasła,
   3) w przypadku problemów z rozpoczęciem pracy, spowodowanych odrzuceniem przez system wprowadzonego identyfikatora i hasła, weryfikuje poprawność wpisanych znaków (capslook, num lock, układ klawiatury), jeśli te czynności okażą się nieskuteczne kontaktuje się z informatykiem.
2. Zawieszenie pracy na stanowisku komputerowym:
   1) użytkownik, opuszczający czasowo stanowisko pracy, wyloguje się, przez użycie kombinacji klawiszy Windows+L,
   2) w przypadku, gdy użytkownik planuje przerwać pracę na dłuższy okres lub zakończyć pracę - zobowiązany jest do wyłączenia stanowiska komputerowego,
   3) stosuje się wygaszacze ekranów aktywujące się po 5 minutach od moment braku aktywności w systemie informatycznym. Ponowne rozpoczęcie pracy następuje po wprowadzeniu identyfikatora oraz hasła,
3. Zakończenie pracy na stanowisku komputerowym:
   1) Opuszczając pomieszczenie, w którym przetwarzane są informacje, jeżeli w pomieszczeniu tym nie przebywa inna osoba upoważniona, pracownik zobowiązany jest do zabezpieczenia pomieszczenia przed dostępem osób nieuprawnionych. Zabronione jest pozostawianie bez nadzoru pomieszczeń, w których przetwarzane są informacje.
   2) Kończąc pracę w systemie informatycznym pracownik wylogowuje się ze wszystkich aplikacji, z których korzystał, wyłącza stację roboczą i zabezpiecza nośniki danych oraz dokumentację papierową.

§ 7
Zasady pracy użytkowników systemu

1. Podczas pracy na stanowisku komputerowym niedozwolone jest:
   1) podłączanie prywatnych urządzeń mobilnych (telefon, tablet, itp.) do portów USB stanowiska komputerowego,
   2) korzystanie z prywatnych nośników danych (Pendrive, płyty CD/DVD, dyski przenośne, itp.),
   3) korzystania z prywatnej poczty e-mail,
   4) w sytuacji wystąpienia konieczności odczytu informacji z nośników danych należy się zgłosić do informatyka, który wyznaczy dedykowane stanowisko do odczytu i przeniesienia danych,
   5) podejmowanie prób omijania mechanizmów zabezpieczeń i kontroli,

6) testowanie zabezpieczeń pod kątem możliwości ich złamania,
7) skanowanie urządzeń sieciowych, serwerów oraz stacji komputerowych pod kątem badania świadczonych usług,
8) wyłączanie programów uruchamianych automatycznie przy starcie systemu,
9) podejmowanie jakichkolwiek prób ingerencji w sprzęt komputerowy, poza czynnościami związanymi z codzienną eksploatacją,
10) wyłączanie, blokowanie, odinstalowywanie zmiana parametrów oprogramowania chroniącego stanowisko komputerowe przed szkodliwym oprogramowaniem,
11) przechowywanie na dysku lokalnym oraz w zasobie sieciowym udostępnionym użytkownikowi, dokumentów nie związanych z zakresem czynności (gier, filmów, obrazów, dźwięków),
12) przenoszenie i przełączanie stanowisk komputerowych między stanowiskami pracy bez wiedzy informatyka,
13) dopuszczanie do pracy na stanowisku komputerowym osób postronnych,
14) kopiowanie i przechowywanie na stanowisku komputerowym lub nośnikach zewnętrznych danych osobowych, za wyjątkiem czynności udostępniania informacji podmiotom uprawnionym,
15) podłączanie aktywnych urządzeń sieciowych (switch, router, access point, itp.) do gniazd sieci komputerowej.

2. Użytkownicy zgłaszają informatykowi wszelkie nieprawidłowości w działaniu stanowiska komputerowego, mogące wskazywać na zainfekowanie szkodliwym oprogramowaniem (uruchamianie się nieznanych wcześniej programów, pojawianie się nieznanych komunikatów, spowolnienie działania systemu).

§ 8
Zasady korzystania z poczty elektronicznej

1. Poczta elektroniczna znajduje się w domenie internetowej: www.ciechocin.pl.
2. Użytkownik poczty elektronicznej:
   1) odpowiada za treść i zabezpieczenie wysyłanych wiadomości,
   2) jest zobowiązany do przesyłania zaszyfrowanych dokumentów zawierających dane osobowe, jednocześnie przekazywanie hasła do zabezpieczonych informacji plików i folderów następuje poprzez użycie innego kanału komunikacji np.: sms, telefonicznie.
3. Użytkownik powinien:
   1) zwracać szczególną uwagę na wiadomości nieznanego pochodzenia mogące stwarzać zagrożenie bezpieczeństwa,
   2) przekazywać wg właściwości wiadomości skierowane do niewłaściwego adresata oraz poinformowanie o tym nadawcy wiadomości,
4. Informatyk konfiguruje na stanowisku komputerowym użytkownika konto pocztowe, w programie do obsługi poczty elektronicznej,
5. W przypadku wykrycia zagrożenia bezpieczeństwa systemu ze strony konta poczty elektronicznej, informatyk:
   1) blokuje konto,
   2) informuje użytkownika konta o zaistniałym incydencie,
   3) zabezpiecza wiadomości poczty elektronicznej dla zagrożonego konta na stanowiskach komputerowych użytkowników i na serwerze pocztowym,
   4) analizuje incydent i wprowadza zabezpieczenia minimalizujące jego powtórne wystąpienie,
   5) informuje bezpośredniego przełożonego - jeżeli incydent spowodowany został przez zamierzone działanie osób trzecich.
6. użytkownicy poczty elektronicznej w stopce każdej wiadomości wpiszą informację:
   KLAUZULA POUFNOŚCI
   Ta wiadomość pocztowa i wszelkie załączone do niej pliki są poufne i podlegają ochronie prawnej. Jeśli nie jesteś jej prawidłowym adresatem, jakiekolwiek jej ujawnienie, reprodukcja, dystrybucja lub inne rozpowszechnienie, są ściśle zabronione. Jeśli otrzymał Pan/Pani niniejszy

przekaz wskutek błędu, proszę o niezwłocznie powiadomienie nadawcy i usunięcie otrzymanych informacji.

7. użytkownicy podczas wysyłania wiadomości e-mail do więcej niż jednego odbiorcy korzystają z opcji „ukryta kopia"/ „UDW".

§ 9
Kopie zapasowe

1. Kopie zapasowe danych wykonywane są w celu zachowania ciągłości działania systemu TI.
2. Za wykonywanie, przechowywanie i testowanie poprawności kopii zapasowych odpowiada informatyk.
3. Ze względu na krótkotrwały charakter przetwarzania danych osobowych w wersji elektronicznej na nośnikach elektronicznych wbudowanych w sprzęt informatyczny lub stanowiących element tego systemu, w tym na zewnętrznych nośnikach danych, kopie zapasowe oraz kopie bezpieczeństwa tych danych nie są wykonywane.
4. Czas przechowywania danych na nośnikach elektronicznych wbudowanych w sprzęt informatyczny oraz na zewnętrznych nośnikach danych ma być niezbędny do spełnienia celu dla jakiego zostały pozyskane, a przede wszystkim zgodny z przepisami prawa. Po ustaniu czasu przechowywania zawartość nośnika podlega on usunięciu.
5. Obowiązek usunięcia danych z nośnika lub jego zniszczenie spoczywa na użytkowniku.
6. Zabrania się używania i kopiowania danych na prywatne zewnętrzne nośniki pamięci takiej jak np.: pendrive, karty pamięci, płyty CD, DVD.
7. Kopie zapasowe danych zapisanych na serwerze podlegają kopiowaniu codziennie i są przechowywane przez okres 1 miesiąca.
8. Wykonywanie kopii zapasowych części danych zlecono w ramach usługi informatycznej podmiotom zewnętrznym (hosting, poczta elektroniczna, oprogramowanie płacowe,)
9. Kopie zapasowe danych służących do ich przetwarzania wykonywane są w celu zachowania ciągłości działania Systemu Informatycznego.
10. Za wykonywanie, przechowywanie i testowanie poprawności kopii zapasowych odpowiada informatyk.
11. Kopie zapasowe danych i danych użytkowników przetwarzanych na serwerach baz danych i zasobach sieciowych udostępnionych użytkownikom wykonywane są automatycznie według ustalonego harmonogramu przy wykorzystaniu dedykowanego oprogramowania.
12. Kopie zapasowe oprogramowania systemowego
    1) zainstalowanego na serwerach - przechowywane są w formie nośników instalacyjnych,
    2) zainstalowanego na stanowiskach komputerowych - przechowywane są w formie nośników instalacyjnych.
13. Kopie zapasowe wykonane na nośnikach zewnętrznych przechowywane są w zamkniętej niemetalowej szafie, w kasecie posiadającej certyfikat producenta w zakresie odporności mechanicznej, wodnej i termicznej.
14. W celu zweryfikowania poprawności wykonania kopii zapasowych informatyk wykonuje testy odtwarzania.
15. Kopie zapasowe wykonywane są na nośnikach typu „dysk zewnętrzny" oraz „dysk sieciowy NAS".

§ 10
Postępowanie ze sprzętem informatycznym, nośnikami danych, naprawa, serwis sprzętu, utylizacja

1. Przeglądy, konserwacja, naprawy oraz utylizacja sprzętu komputerowego przeprowadzane są w sposób uniemożliwiający dostęp do informacji osobom nieuprawnionym Bieżącą naprawę i konserwację sprzętu informatycznego wykonuje informatyk.
2. Prace serwisowe wykonywane w siedzibie administratora przez podmioty zewnętrzne podlegają bezpośredniemu nadzorowi informatyka lub innego wyznaczonego pracownika.
3. Poważne naprawy i konserwacja wykonywane przez personel zewnętrzny realizowane są w siedzibie administratora lub w siedzibie podmiotu wykonującego usługę jedynie po zawarciu z nim umowy o powierzenie przetwarzania danych osobowych oraz w przypadku, gdy sprzęt przekazywany jest wraz z danymi.
4. Przekazanie sprzętu potwierdzane jest protokołem, pozwalającym na jednoznaczne wskazanie osoby przekazującej i osoby odbierającej sprzęt – wzór załącznik nr 4
5. Wycofany z eksploatacji sprzęt służący do przetwarzania danych osobowych może być zbywany dopiero po trwałym usunięciu danych, a urządzenia uszkodzone mogą być przekazywane w celu utylizacji (jeśli trwałe usunięcie danych wymagałoby nadmiernych nakładów ze strony administratora) właściwym podmiotom, z którymi także zawiera się umowy powierzenia przetwarzania danych osobowych.
6. Informatyk dokumentuje wszelkie prace naprawy wykonywane przez podmioty zewnętrzne, jak i informatyka.
7. Dokumentując czynności informatyk uwzględnia następujące informacje:
    1) wskazanie osoby przeprowadzającej naprawy oraz podmiotu, którego osoba ta jest pracownikiem,
    2) wskazanie osoby nadzorującej przebieg naprawy (dotyczy sytuacji, gdy prace realizowane są w siedzibie administratora)
    3) przedmiot napraw (w szczególności identyfikator sprzętu w przypadku prac serwisowych dotyczących sprzętu),
    4) zakres napraw,
    5) czas przeprowadzania napraw.
8. Jako elektroniczne nośniki informacji wykorzystane są w szczególności:
    1) pamięci masowe (dyski twarde) serwerów baz danych, serwerów plików i serwerów kopii zapasowych,
    2) pamięć typu flash
    3) karty pamięci
    4) płyt CD, DVD
    5) oraz inne urządzenia do kopiowania i przenoszenia danych.
9. Przekazywanie urządzeń lub nośników zawierających dane osobowe, poza obszar przetwarzania danych osobowych, zabezpieczane są w sposób zapewniający poufność, integralność i rozliczalność tych danych, przez co rozumie się:
    1) ograniczenie dostępu do danych osobowych hasłem zabezpieczającym dane przed osobami nieupoważnionymi,
    2) stosowanie metod kryptograficznych,
    3) stosowanie odpowiednich zabezpieczeń fizycznych,
    4) stosowanie odpowiednich zabezpieczeń organizacyjnych.
10. Zabronione jest wykorzystywanie prywatnych nośników danych.
11. Osoby uprawnione mają prawo wykorzystywać wyłącznie nośniki danych oraz sprzęt informatyczny przydzielony im przez administratora.
12. Ewidencjonowanie oraz wydawanie sprzętu mobilnego i elektronicznych nośników informacji dokumentowane jest przez informatyka. Nie dotyczy to płyt CD i DVD.
13. Polecenie wydania osobie uprawnionej mobilnego sprzętu informatycznego oraz elektronicznego nośnika informacji podejmuje jego bezpośredni przełożony, nie dotyczy to płyt CD i DVD.
14. Osoby uprawnione do przetwarzania danych osobowych powinny pamiętać zwłaszcza, że:
    1) Dane z nośników niebędących kopiami zapasowymi po wprowadzeniu do systemu informatycznego administratora powinny być trwale usuwane z tych nośników przez fizyczne zniszczenie (np. płyty CD-ROM) lub usunięcie danych programem trwale

usuwającym pliki. Jeśli istnieje uzasadniona konieczność, dane pojedynczych osób mogą być przechowywane na specjalnie oznaczonych nośnikach. Nośniki te muszą być przechowywane w zamkniętych na klucz szafach, nieudostępnianych osobom postronnym. Po ustaniu przydatności tych danych nośniki powinny być trwale kasowane lub niszczone.

2) Uszkodzone nośniki należy zniszczyć fizycznie – wzór – zał. nr 5.
3) W przypadku wycofania sprzętu komputerowego z użycia dane osobowe na nim zapisane są kasowane przy użyciu dedykowanego oprogramowania do bezpiecznego usuwania danych. W przypadku braku możliwości programowego usunięcia danych, dysk podlega fizycznemu zniszczeniu. Za zniszczenie danych odpowiada informatyk. Zniszczenie nośnika potwierdzane jest protokołem w skład komisji wchodzą informatyk oraz użytkownik lub inna wskazana osoba - wzór – zał. nr 5.

15. Protokoły, o których mowa wyżej lub ich kopie przechowywane są przez informatyka.

§ 11
Zasady korzystania z informatycznego sprzętu mobilnego

1. Przetwarzanie danych osobowych przy użyciu mobilnego sprzętu informatycznego powinno być ograniczone do niezbędnych przypadków. Administrator wyraża zgodę na przetwarzanie danych osobowych przy użyciu takiego rodzaju sprzętu poza strefą przetwarzania danych osobowych pracownikom, którzy zgodnie z zakresem swoich obowiązków wykonują pracę poza siedzibą administratora.
2. Administrator zakazuje użytkownikowi korzystania z publicznych dostępowych punktów HOTSPOT.
3. Administrator zobowiązuje użytkowników do wyłącznego korzystania z WiFi udostępnianego w służbowych smartfonach.
4. Hasło do tego punktu dostępowego powinno posiadać **minimum 8 znaków zawierających duże i małe litery cyfrę oraz znak specjalny**.
5. Osoba korzystająca z mobilnego sprzętu informatycznego w celu przetwarzania danych osobowych zobowiązana jest do zwrócenia szczególnej uwagi na zabezpieczenie przetwarzanych informacji, zwłaszcza przed dostępem do nich osób nieupoważnionych oraz przed zniszczeniem.
6. Użytkownik mobilnego sprzętu informatycznego zobowiązany jest do:
    1) Transportu mobilnego sprzętu informatycznego w sposób minimalizujący ryzyko kradzieży lub zniszczenia, a w szczególności:
        a) transportowania mobilnego sprzętu informatycznego w bagażu podręcznym,
        b) nie pozostawiania mobilnego sprzętu informatycznego przechowalni bagażu oraz w widocznym miejscu w samochodzie,
        c) zaleca się przenoszenie i przewożenie mobilnego sprzętu informatycznego w torbie specjalnie do tego przeznaczonej.
    2) Korzystania z mobilnego sprzętu informatycznego w sposób minimalizujący ryzyko przejrzenia przetwarzanych danych przez osoby nieupoważnione, w szczególności w miejscach publicznych i w środkach transportu publicznego.
    3) Uniemożliwienie korzystania osobom nieupoważnionym z mobilnego sprzętu informatycznego, na którym przetwarzane są dane osobowe.
    4) Ochrony sprzętu przed uszkodzeniami fizycznymi, a ze względu na działanie silnego pola elektromagnetycznego mają obowiązek przestrzegać zaleceń producentów dotyczących ochrony sprzętu.
    5) Korzystania z mobilnego sprzętu informatycznego zabezpieczanego hasłem.
    6) Blokowania dostępu do mobilnego sprzętu informatycznego w przypadku gdy nie jest on wykorzystywany przez pracownika poprzez zastosowanie wygaszacza ekranu lub wylogowania z systemu.
    7) Hasło dostępu do urządzenia mobilnego typu: smartfon, tablet, terminal mobilny składa się z 4 znaków – cyfr lub wzoru.

8) Blokada ekranu urządzenia następuje po max 30 sek. od momentu moment braku aktywności w systemie urządzenia.
9) Hasło dostępu do urządzenia użytkownik nadaje osobiście niezwłocznie po jego otrzymaniu.
10) użytkownik w/wym. urządzeń zobowiązany do zmiany hasła nie rzadziej niż co 3 miesiące chyba że zmiana hasła jest wymuszona przez system informatyczny lub niezwłocznie w przypadku podejrzenia, iż mogły z nim się zapoznać nieuprawnione osoby
11) hasło powinno różnić się od poprzednio używanego,
12) wprowadzania danych osobowych przetwarzanych na mobilnym sprzęcie informatycznym do systemu informatycznego w celu umożliwienia ich dalszego przetwarzania,

7. Przetwarzania danych przy użyciu sprzętu mobilnego jest dopuszczalne zgodnie z n/wym. zasadami:
1) dane przechowywane na elektronicznych nośnikach wbudowanych w sprzęt informatyczny mogą być przetwarzane do czasu spełnienia celu w jakim zostały one na nośniku zapisane;
2) po upływie czasu przechowywania zawartość nośnika podlega usunięciu;
3) obowiązek usunięcia danych z nośnika lub jego zniszczenia spoczywa na użytkowniku;
4) zabrania się używania i kopiowania danych na prywatne zewnętrzne nośniki pamięci takiej jak np.: pendrive, karty pamięci, płyty CD, DVD.
8. Informatyk zobowiązany jest do podjęcia działań mających na celu zabezpieczenie mobilnego sprzętu informatycznego tj. m.in. do:
1) konfiguracji oprogramowania w sposób wymuszający korzystanie z haseł, jeżeli system umożliwia taką konfigurację. Wykorzystywanie haseł odpowiedniej jakości zgodnie z wytycznymi dotyczącymi tworzenia haseł w systemie informatycznym przetwarzającym dane osobowe oraz wymuszającym okresową zmianę haseł zgodnie z wymaganiami dla systemu informatycznego przetwarzającego dane osobowe;
2) instalacji i konfiguracji oprogramowania antywirusowego na sprzęcie mobilnym;
9. W razie zgubienia lub kradzieży mobilnego sprzętu informatycznego pracownik zobowiązany jest do natychmiastowego powiadomienia bezpośredniego przełożonego.

§ 12
Reagowanie na incydenty bezpieczeństwa oraz przywracanie sprawności działania systemu TI

1. Informatyk odpowiada za obsługę incydentów bezpieczeństwa teleinformatycznego.
2. Po wykryciu incydentu bezpieczeństwa systemu TI, w tym działania szkodliwego oprogramowania w systemie TI:
1) blokuje dostęp do zagrożonego stanowiska komputerowego,
2) informuje bezpośredniego przełożonego, administratora oraz inspektora ochrony danych o zaistniałym incydencie,
3) zabezpiecza logi systemu operacyjnego na zainfekowanym stanowisku komputerowym,
4) zabezpiecza logi połączeń z siecią publiczną zainfekowanego stanowiska komputerowego,
5) przywraca stanowisko komputerowe do stanu z przed incydentu,
6) analizuje incydent i wprowadza zabezpieczenia minimalizujące jego powtórne wystąpienie,
7) informuje bezpośredniego przełożonego lub administratora - jeżeli incydent spowodowany został przez zamierzone działanie osób trzecich,
8) sporządza opis incydentu bezpieczeństwa zawierający:

a) identyfikator stanowiska komputerowego (numer IP i numer inwentarzowy), na którym wykryte zostało szkodliwe oprogramowanie,
b) dokładaną datę i czas wykrycia,
c) rodzaj wykrytego wirusa lub innego oprogramowania,
d) opis podjętej akcji naprawczej mającej na celu przywrócenie właściwego poziomu bezpieczeństwa.

3. W przypadku zablokowania baz danych w systemie TI podejmuje działania przywracające dostępność danych przy zastosowaniu kopii zapasowych wykonywanych w jednostce.
4. Szczegółowe zasady reagowania na incydenty związane z działaniem systemu TI opisano w załączniku nr 6.

Załączniki:

1. Wzór wykazu sprzętu informatycznego oraz oprogramowania stosowanego do przetwarzania informacji.
2. Kategorie stron internetowych (WWW) podlegających zablokowaniu lub częściowemu zablokowaniu
3. Wniosek o nadanie/cofnięcie/zmianę/zawieszenie uprawnień do przetwarzania informacji i danych osobowych w systemie informatycznym
4. Protokół przekazania sprzętu komputerowego do naprawy/serwisu/utylizacji
5. Protokół zniszczenia sprzętu komputerowego/nośnika danych
6. Procedura zarządzania incydentami z zakresu bezpieczeństwa systemów teleinformatycznych i informacji

Załącznik nr 1 do
Polityki Zarządzenia Systemem
Informatycznym

Wykaz sprzętu informatycznego oraz oprogramowania stosowanego do przetwarzania informacji w Urzędzie Gminy Ciechocin.

1. **Wykaz oprogramowania**

Lp.	Nazwa oprogramowania	oprogramowanie posiada licencję	uwagi
1.	Biuletyn Informacji Publicznej	Tak	
2.	System Podatki i Opłaty Lokalne	Tak	
3.	System Finansowo-Księgowy FoKa Pro	Tak	
4.	Koncesje Alkoholowe	Tak	
5.	Środki Trwałe	Tak	
6.	Radni.info	Tak	
7.	Radni.TV	Tak	
8.	Biuletyn Informacji Publicznej - archiwum	Tak	
9.	System Ewidencji Ludności (SELWIN)	Tak	
10.	Obsługa wyborów samorządowych (SEL-WIN_WYBORY)	Tak	
11.	KADRY VULCAN	Tak	
12.	Pła-ce VULCAN wraz z Nadzorem Płacowym VULCAN	Tak	
13.	Artykuł30	Tak	
14.	ERGO	Tak	
15.	vMix - system transmisji sesji	Tak	
16.	Legislator Standard	Tak	
17.	Hydrosoft AnkoSystem	Tak	
18.	Moduł Extranet - aktualizacja strony	Tak	
19.	Lex Administracja Standard	Tak	
20.	BeSTi@	Nie	**Darmowe oprogram owanie.**
21.	Proton	Tak	
22.	Thunderbird	Nie	**Darmowy klient pocztowy.**

2. **Wykaz sprzęt informatyczny:**

Lp.	Nazwa przedmiotu	Ilość
1.	Komputer Stacjonarny	24
2.	Laptop	9
3.	Mysz	24
4.	Klawiatura	30
5.	Słuchawki	6
6.	Głośniki	9
7.	Radio	7
8.	Niszczarka	6
9.	Skaner	1
10.	Urządzenie wielofunkcyjne	8
11.	Drukarka	6
12.	Monitor	24
13.	Serwer	2
14.	FAX	1
15.	Rejestrator Monitoringu	1
16.	Kamery	6
17.	Switch	3

Załącznik nr 2 do
Polityki Zarządzenia Systemem
Informatycznym

Kategorie stron internetowych (WWW) podlegających zablokowaniu lub częściowemu zablokowaniu.

1. **Violence, Hate & Racism**

Przemoc, Nienawiść i Rasizm

Witryny, które przedstawiają ekstremalną szkodę fizyczną ludziom lub mieniu, lub które opowiadają się lub dostarczają wskazówek, jak powodować takie szkody. Obejmuje również witryny, które przemawiają lub przedstawiają wrogość, opowiadają się za agresją lub ośmieszają każdą osobę lub grupę na podstawie rasy, religii, płci, narodowości, pochodzenia etnicznego lub innych nieumyślnych cech.

2. **Nudism**

Nudyzm

Witryny zawierające nago lub półnagie obrazy ludzkiego ciała. Te przedstawienia niekoniecznie są intencją seksualną, ale mogą zawierać witryny zawierające nagie obrazy lub galerie zdjęć o charakterze artystycznym. Do tej kategorii należą również nagrania nudystów lub naturystów zawierające zdjęcia nagich osób.

3. **Pornography**

Pornografia

Witryny, które zawierają materiał pornograficzny w celu wywołania seksualnego lub żarliwego zainteresowania

4. **Weapons**

Bronie

Witryny sprzedające, przeglądające lub opisujące broń, takie jak pistolety, noże lub urządzenia sztuk walki i ich akcesoria, lub dostarczające informacji na temat ich użytkowania lub innych modyfikacji. Nie obejmuje witryn promujących zbieranie broni lub grup, które popierają lub sprzeciwiają się użyciu broni.

5. **Adult/Mature Content**

Dorosłe / Starsze treści

Witryny zawierające materiały o charakterze dorosłym, które niekoniecznie zawierają nadmierną przemoc, treści seksualne lub nagość. Miejsca te zawierają bardzo lubieżną lub wulgarną treść i miejsca, które nie są odpowiednie dla dzieci.

6. **Cult/Occult**

Kult / okultyzm

Witryny, które promują lub oferują metody, środki instruktażowe lub inne zasoby, które mają wpływać na rzeczywiste wydarzenia lub wpływać na nich poprzez użycie zaklęć, przekleństw, mocy magicznych lub nadprzyrodzonych istot.

7. **Drugs/Illegal Drugs**

Narkotyki / Narkotyki Nielegalne

Witryny narkotyków, które promują, oferują, sprzedają, dostarczają, zachęcają lub w inny sposób popierają rekreacyjne lub niezgodne z prawem używanie, uprawę, wytwarzanie lub dystrybucję narkotyków, farmaceutyków, odurzających roślin lub chemikaliów i związanych z nimi elementów. Ponadto strony, które dyskutują lub promują używanie i nadużywanie leków regulowanych oraz urządzeń związanych z lekami regulowanymi, a także miejscami, które dostarczają informacji o zatwierdzonych lekach i ich zastosowaniach medycznych oraz promują stosowanie substancji chemicznych, które nie są regulowane przez FDA .

8. **Illegal Skills/Questionable Skills**

Nieprawidłowe umiejętności / wątpliwe umiejętności

Witryny, które przemawiają lub udzielają porad na temat czynów nielegalnych, takich jak kradzieże usług, unikają egzekwowania prawa, oszustw, technik włamań i plagiatu. Obejmuje również witryny, które dostarczają lub sprzedają wątpliwe materiały edukacyjne, takie jak dokumenty okresowe.

9. **Sex Education**

Edukacja seksualna

Witryny dostarczające graficznej informacji na temat reprodukcji, rozwoju seksualnego, bezpiecznych praktyk seksualnych, seksualności, kontroli urodzin i rozwoju seksualnego. Obejmuje również witryny, które oferują wskazówki dotyczące lepszego seksu, a także produktów wykorzystywanych do poprawy seksualności.

10. Gambling

Hazard

Witryny, w których użytkownik może postawić zakład lub wziąć udział w puli zakładów (w tym loteriach) online. Zawiera również witryny, które dostarczają informacji, pomocy, zaleceń lub szkoleń dotyczących zakładów lub uczestniczących w grach losowych. Nie obejmuje witryn, które sprzedają produkty lub maszyny związane z hazardem lub witryny kasyna hotelu lub offline (o ile te witryny nie spełniają jednego z powyższych wymagań).

11. Alcohol/Tobacco

Alkohol / Tytoń

Witryny, które promują lub oferują wyroby alkoholowe / tytoniowe lub udostępniają sposoby ich tworzenia. Obejmuje również witryny, w których uwielbiam, tout lub zachęcasz do spożywania alkoholu / tytoniu. Nie obejmuje to witryn, które sprzedają alkohol lub tytoń jako podzbiór innych produktów.

12. Abortion/Advocacy Groups

aborcyjne / propagujące

Witryny, które dostarczają informacji lub argumentów na rzecz lub przeciw aborcji, opisują procedury aborcyjne, oferują pomoc w uzyskiwaniu lub unikaniu aborcji lub udzielaniu informacji o skutkach lub braku ich aborcji.

13. Online Brokerage/Trading

Online Brokerage / Trading

Witryny, które świadczą lub reklamują papiery wartościowe i zarządzanie aktywami inwestycyjnymi (online lub offline). Obejmuje również witryny ubezpieczeniowe, a także witryny, które oferują strategie inwestycyjne finansowe, cytaty i nowości.

14. Games

Gry

Witryny dostarczające informacje na temat gier lub pobierania gier wideo, gier komputerowych, gier elektronicznych, porad i porad na temat gier lub pobierania kody. Obejmuje również witryny poświęcone sprzedaży gier planszowych, a także czasopism i czasopism poświęconych grze. Obejmuje witryny, które obsługują lub organizują zamachy online i prezenty.

15. Military

Wojskowy

Witryny promujące lub dostarczające informacje o oddziałach wojskowych lub uzbrojonych.

16. Hacking/Proxy Avoidance Systems

Systemy zapobiegania włamaniom / proxy

Witryny dostarczające informacje o nielegalnym lub wątpliwym dostępie do sprzętu lub oprogramowania komunikacyjnego lub udostępniają informacje o pomijaniu funkcji serwera proxy lub uzyskiwanie dostępu do adresów URL w jakikolwiek sposób, który pomija serwer proxy.

17. Personals & Dating

Randki i Randki

Witryny promujące relacje międzyludzkie.

18. Malware

Szkodliwe oprogramowanie

Witryny obsługujące oprogramowanie, które jest ukryte w systemie użytkownika w celu zbierania informacji i monitorowania aktywności użytkownika. Ponadto witryny zakaźne destrukcyjnymi lub złośliwymi programami, takimi jak wirusy, trojany lub robaki, które są specjalnie zaprojektowane do uszkodzenia, zakłócenia, ataku lub manipulowania systemami komputerowymi bez zgody użytkownika.

- kategorie zablokowane dla wszystkich użytkowników
- kategorie odblokowane dla wszystkich użytkowników
- kategorie odblokowane dla użytkowników posiadających uprawnienia dodatkowe
- kategorie odblokowane po potwierdzeniu wykorzystania do celów służbowych

Załącznik nr 3 do Polityki Zarządzenia Systemem Informatycznym

ZATWIERDZAM
data i podpis administratora

Wniosek**

o nadanie/cofnięcie/zmianę/zawieszenie * uprawnień do przetwarzania informacji i danych osobowych w systemie informatycznym
oraz
utworzenie/usunięcie/zawieszenie konta poczty elektronicznej*

Wnioskuję o:

I. nadanie/cofnięcie/zmianę/zawieszenie* uprawnień z powodu: (przyjęcia do pracy, zmiany zakresu obowiązków pracowniczych, wprowadzenia nowego oprogramowania, zwolnienia z pracy, zawarcie/zakończenia umowy cywilnej, podjęcia/zakończenia stażu, praktyki, wolontariatu, inne .....)*
II. utworzenie poczty elektronicznej*

dla: .....
Imię i nazwisko

Przetwarzanych w n/wym. programach, systemach i urządzeniach:

I.

Lp.	Wypełnia osoba składająca wniosek		
	nazwa programu/systemu/ urządzenia służącego do przetwarzania danych osobowych	Rodzaj Działania A – nadanie B – cofnięcie C - zmiana	rodzaj uprawnień /konta 1.administrator 2. użytkownik
1.	Stanowisko dostępowe		
2.	Poczty elektronicznej		

Uprawnienia należy nadać/cofnąć/zmienić/zawiesić* od .....

.....
data, podpis osoby wnioskującej

II. Wypełnia informatyk po zatwierdzeniu wniosku przez administratora

	identyfikator	data nadania	data zmiany/ zawieszenia	data usunięcia konta	Podpis informatyka
Stanowisko dostępowe					
Poczta elektroniczna					

III. Wypełnia osoba, której przyznano uprawnienia oraz informatyk.

Nr programu systemu/urządzenia wg wniosku z pkt I.	Potwierdzanie odbioru identyfikatora (podpis uprawnionego)	Potwierdzenie odbioru hasła pierwszego logowania oraz odbycia szkolenia w zakresie użytkowania systemu informatycznego (Podpis uprawnionego)	Podpis szkolącego informatyka
Stanowisko dostępowe			
Poczta elektroniczna			

*- zaznacz prawidłowe
** - dokument przechowuje informatyk

Załącznik nr 4 do Polityki Zarządzenia Systemem Informatycznym

Protokół przekazania sprzętu komputerowego do naprawy/serwisu/utylizacji*		**Miejscowość:**	**Data:**
Administrator pełna nazwa	Informatyk – imię i nazwisko/dane firmy	Nazwa i adres podmiotu wykonującego naprawę/serwis/utylizację*	
Działając na podstawie „Polityki ochrony danych			
Przekazano do naprawy/serwisu/utylizacji/ .....* niżej wymieniony sprzęt komputerowy/nośniki			
Zawarto umowę powierzenia przetwarzania danych osobowych. TAK/NIE*			
Nazwa sprzętu komputerowego/nośnika*	**Numer identyfikacyjny/inwentarzowy sprzętu komputerowego/nośnika**	**uwagi**	
Potwierdzam przekazanie sprzętu komputerowego/nośnika* data, pieczęć i podpis		Potwierdzam przejęcie sprzętu komputerowego/nośnika* data, pieczęć i podpis	

*niepotrzebne skreślić

Załącznik nr 5 do Polityki Zarządzenia Systemem Informatycznym

PROTOKÓŁ ZNISZCZENIA
SPRZĘTU KOMPUTEROWEGO/NOŚNIKA DANYCH*

Komisja w składzie

1. Przewodniczący – .....
2. Członek – .....

W dniu ..... w .....

Działając na podstawie .....

komisja dokonała zniszczenia n/wymienionego sprzętu komputerowego/nośnika danych*

1. Laptopa* marki ....., typ.....,
   rodzaj..... nr ....., inne
   cechy identyfikacyjne.....
   Użytkowanego
   przez.....
2. Dysku twardego* marki ....., typ....., rodzaj .....
   nr ....., inne cechy
   identyfikacyjne.....
   Użytkowanego
   przez.....
3. Nośnika danych CD/DVD/karty pamięci, pendrive*, marki
   ....., typ.....,
   rodzaj....., nr ....., inne cechy
   identyfikacyjne.....
   Użytkowanego
   przez.....
4. ..... marki
   ....., typ....., rodzaj.....,
   nr ....., inne cechy
   identyfikacyjne.....

Użytkowanego

przez.....

5. marki ....., typ.....,

   rodzaj....., nr ....., inne cechy

   identyfikacyjne.....

   Użytkowanego

   przez.....

6. marki ....., typ.....,

   rodzaj....., nr ....., inne cechy

   identyfikacyjne.....

   Użytkowanego

   przez.....

Zniszczenia dokonano w następujący sposób:

1. Nadpisanie programowe danych przy użyciu programu ..... *
2. Demagnetyzacji*
3. Wiórkowanie przy użyciu niszczarki (dotyczy nośników CD,DVD, karty pamięci)*
4. Chemiczny*
5. Zeszlifowanie oraz pocięcie nośnika pamięci*
6. Poddanie nośnika działaniu wysokiej temperatury-spalenie*
7. .....
8. .....

.....

.....

*Niepotrzebne skreślić

Załącznik nr 6 do Polityki Zarzadzania
Systemem Informatycznym

Procedura zarządzania incydentami z zakresu bezpieczeństwa systemów teleinformatycznych i informacji w Urzędzie Gminy Ciechocin

2023

1. Skróty i definicje.

Administrator Danych (AD) – Wójt Gminy Ciechocin;
IOD – Inspektor Ochrony Danych
CSK – Centrum Sieci Komputerowych
CERT – Rządowy Zespół Reagowania na Incydenty Komputerowe
Administrator Systemów Informatycznych (ASI) – pracownik administrujący określonym systemem IT. Rolą ASI jest zapewnienie efektywnego zarządzania operacyjnego danego systemu IT i sprawnej jego pracy. Do typowych zadań administratora należy nadzorowanie pracy powierzonych systemów IT, zarządzanie kontami i uprawnieniami użytkowników (na poziomie systemowym), konfiguracja zasobu, instalowanie i aktualizacja oprogramowania, nadzorowanie, wykrywanie i eliminowanie błędów oraz nieprawidłowości, asystowanie i współpraca z zewnętrznymi specjalistami przy pracach instalacyjnych, konfiguracyjnych i naprawczych, a także zapewnienie aktualności dokumentacji takiego zasobu obejmującego również dokumentację zmian mających bezpośredni wpływ na jego funkcjonalność. ASI odpowiada za właściwą i aktualną informację o systemach.

2. Cel procedury.

Celem Procedury Zarządzania Incydentami Związanymi z Bezpieczeństwem Informacji jest zapewnienie, monitorowania zdarzeń związanych z bezpieczeństwem informacji oraz słabości systemów informacyjnych, a także możliwość zgłaszania i szybkiego podejmowania działań korygujących.

3. Zakres stosowania.

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

4. Odpowiedzialność.

Odpowiedzialność za prawidłowe zgłoszenie incydentów dotyczących bezpieczeństwa infrastruktury informatycznej spoczywa na pracownikach dokonujących zgłoszeń. ASI odpowiedzialny za rozwiązanie problemu lub zapobieżenie incydentowi działa zgodnie z niniejszą procedurą.

Zespół ds. monitorowania zagrożeń i utrzymania Systemu Zarządzania Bezpieczeństwem Informacji, w którego skład wchodzą Administrator Systemu Informatycznego, Inspektor Ochrony Danych oraz Sekretarz Gminy jest odpowiedzialny za:

1) Niezwłoczne reagowanie na incydenty bezpieczeństwa informacji w określony i z góry ustalony sposób;
2) Ocenę istniejących i potencjalnych zagrożeń w zakresie bezpieczeństwa informacji;
3) Ocenę przyczyn i skutków incydentów naruszenia bezpieczeństwa informacji w tym gromadzenie materiału dowodowego;

5) Dokonywanie okresowego przeglądu i aktualizacji polityk regulujących bezpieczeństwo informacji ;
6) Prowadzenie działań zmierzających do wzrostu świadomości w zakresie zapewnienia bezpieczeństwa informacji wśród pracowników;
7) Współpracę z Rządowym Zespołem Reagowania na Incydenty Komputerowe CERT.

5. Klasyfikacja incydentów.

Podział zdarzeń:

1) **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.
2) **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.
3) **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:
    a) nieuprawniony dostęp do danych z zewnątrz (włamanie do systemu),
    b) nieuprawniony dostęp do danych z sieci wewnętrznej,
    c) nieuprawniony transfer danych,
    d) pogorszenie funkcjonowania sprzętu i oprogramowania (np.: działanie wirusów),
    e) bezpośrednie zagrożenie materialnych składników systemu (np.: kradzież sprzętu).

Przykłady zdarzeń, które mogą być zakwalifikowane jako uzasadnione podejrzenie naruszenia bezpieczeństwa informacji:

1) 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.
2) Niewłaściwe parametry środowiska jak zbyt wysoka temperatura lub nadmierna wilgotność (w szczególności dotyczy to serwerowni).
3) Awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie systemu, a w tym sam fakt pozostawienia serwisantów bez nadzoru.
4) Pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu.
5) Jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikacje w systemie.
6) Nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie.
7) Stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji).
8) Nastąpiła niedopuszczalna manipulacja danymi w systemie.

9) Ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą elementy systemu zabezpieczeń.
10) 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.
11) Ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. „bocznej furtki", itp.
12) Podmieniono lub zniszczono nośniki z danymi bez odpowiedniego upoważnienia lub w niedozwolony sposób skasowano lub kopiowano dane osobowe
13) Rażąco naruszono dyscyplinę pracy w zakresie przestrzegania bezpieczeństwa (nie wylogowanie się, pozostawienie włączonego komputera po zakończeniu pracy, nie zamknięcie pokoju z komputerem, nie wykonywanie w ustalonych terminach kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.)
14) Stwierdzenie nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych, w tym także osobowych (otwarte szafy, regały, biurka).

6. Zgłaszanie incydentów

Pracownicy mają obowiązek zgłaszać zauważone przez siebie incydenty oraz notować wszystkie szczegóły związane z incydentem. Incydenty należy zgłaszać do informatyka e-mail: daniel.bozykowski@ciechocin.pl lub telefonicznie pod numery **56 683 77 81 wew. 37**. Zgłoszenie musi zawierać (zał. nr 2):

a) imię i nazwisko zgłaszającego,
b) miejsce i datę wystąpienia incydentu,
c) opis zdarzenia.

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 zainfekowania komputera wirusa należy niezwłocznie skontaktować się z ASI.

7. Postępowanie z incydentami

Obsługa incydentu rozpoczyna się od jego dokładnego rozpoznania - ustalenia oznak naruszenia bezpieczeństwa, identyfikacji rodzaju incydentu, identyfikacji i zabezpieczenia dowodów oraz poinformowania o zdarzaniu odpowiednich osób.

1) Za obsługę incydentów bezpieczeństwa teleinformatycznego odpowiada ASI, który przyjął zgłoszenie (zał. nr 3), powiadamia niezwłocznie IOD.
2) Po analizie zdarzenia i okoliczności z nim związanych ASI wprowadza dane o incydencie do rejestru incydentów oraz zabezpiecza materiał dowodowy.
3) Zespół zbiera się niezwłocznie, dokonuje analizy materiału dowodowego i podejmuje decyzję o sposobie dalszego postępowania. Gromadzenie materiału dowodowego:

a) 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
b) 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).

4) W przypadku, gdy zgłoszone zdarzenie zostało uznane za incydent bezpieczeństwa informacji, Zespół dokonuje oceny istotności incydentu oraz zawiadamia AD o zaistnieniu incydentu oraz poziomie zagrożenia dla bezpieczeństwa informacji. Zespół ds. monitorowania zagrożeń i utrzymania Systemu Zarządzania Bezpieczeństwem Informacji ocenia poziom istotności incydentu dla jednostki kierując się następującymi kryteriami:
   a) wpływ incydentu na ciągłość działania jednostki i wypełnianie jego zadań statutowych;
   b) krytyczność systemów dotkniętych skutkami incydentu bezpieczeństwa;
   c) wrażliwość informacji, których poufność, integralność czy dostępność naruszono (na przykład czy naruszono bezpieczeństwo informacji prawnie chronionej — np.: danych osobowych, informacji niejawnych);
   d) rozległość wpływu incydentu na działanie systemów (nie działa jeden komputer, cała sieć itp.);
   e) rozmiar szkód powstałych skutkiem incydentu;
   f) koszt usunięcia i naprawy skutków incydentu bezpieczeństwa;
   g) szacowany czas przywrócenia ciągłości działania dotkniętego incydentem bezpieczeństwa systemu;
   h) 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.);
5) Jeżeli istotność incydentu jest wysoka, należy zawiadomić Rządowy Zespół Reagowania na Incydenty Komputerowe **CERT.GOV.PL** pełniący rolę głównego zespołu CERT w obszarze administracji rządowej. Wyznaczony przez przewodniczącego członek zespołu wypełnia formularz zgłoszenia incydentu, ściągnięty ze strony www.cert.gov.pl oraz wysyła go do CERT zgodnie z informacją zamieszczoną na tej stronie. Incydent zgłaszany jest dwutorowo, faksem na numer **+48 22 58 58 833** oraz pocztą elektroniczną na adres incydent@cert.gov.pl .Dalsza korespondencja z CERT w sprawie tego incydentu odbywa się za pomocą szyfrowanej poczty elektronicznej.
6) W przypadku, gdy zgłoszone zdarzenie nie zostało zaklasyfikowane jako incydent bezpieczeństwa informacji, ma charakter fałszywego alarmu ASI powiadamia zgłaszającego o zdarzeniu, że zdarzenie nie stanowi incydent bezpieczeństwa.
7) W przypadku stwierdzenia działań umyślnych i ustaleniu sprawcy incydentu zespół przekazuje wyniki analizy wraz z zabezpieczonym materiałem dowodowym AD w celu

wyciągnięcia konsekwencji dyscyplinarnych wobec sprawcy, ewentualnego zawiadomienia organów ścigania lub podjęcia kroków prawnych wobec osób trzecich.

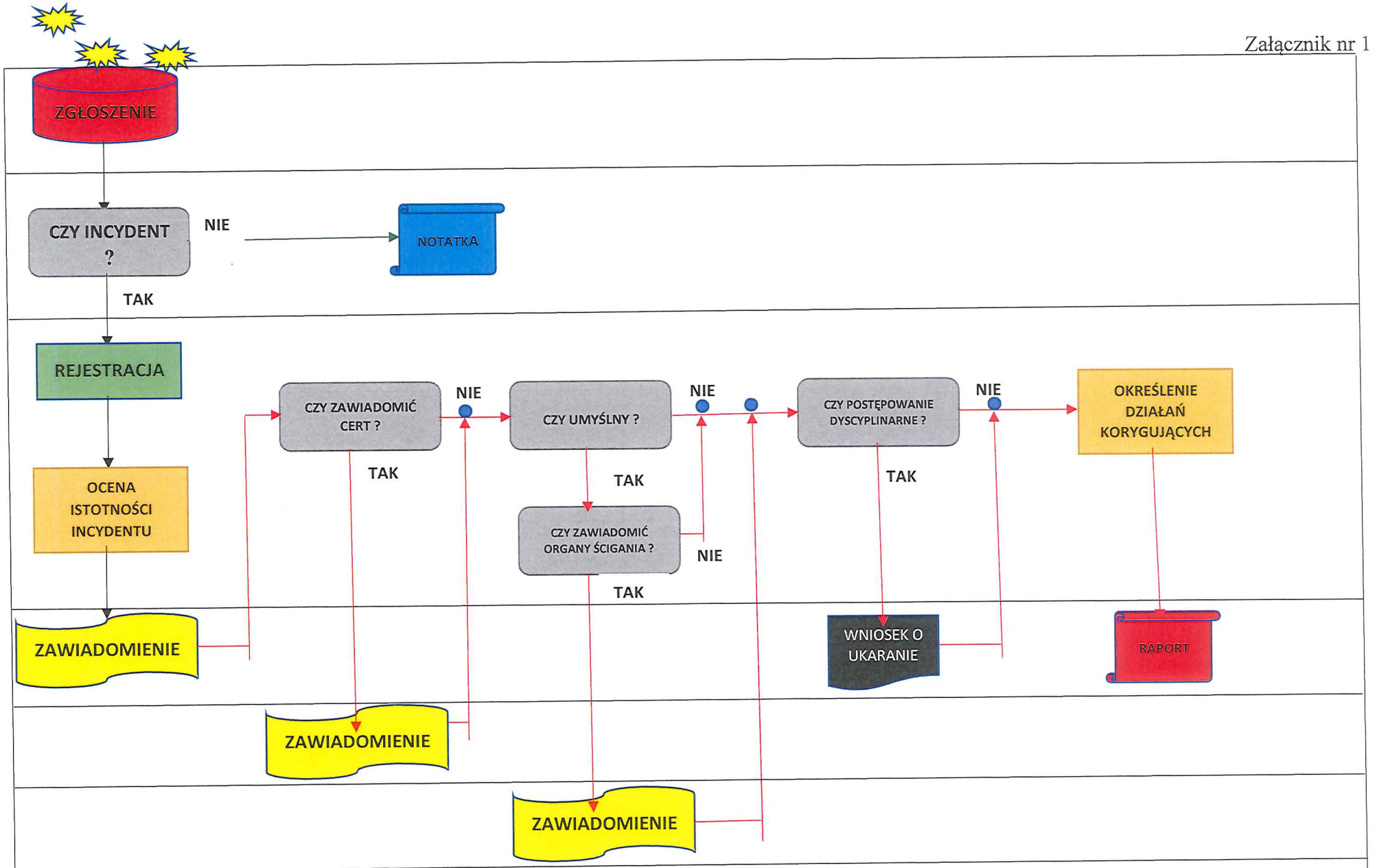
8) Zespół ds. monitorowania zagrożeń i utrzymania Systemu Zarządzania Bezpieczeństwem Informacji inicjuje działania naprawcze zmierzające do zniwelowania szkód wyrządzonych przez incydent, wyciąga wnioski z każdego incydentu i określa, jeśli to możliwe działania korygujące i zapobiegawcze w celu uniknięcia ponownego wystąpienia incydentu.
9) Zespół na bieżąco dokumentuje swoje działania na każdym z etapów procesu zarządzania incydentem w formie notatki. Obsługa incydentu kończy się raportem zatwierdzonym przez AD zawierającym opis incydentu oraz wnioski co do działań na przyszłość. (zał. nr 1)

8. Szkolenia.

Brak wiedzy i umiejętności poprawnego rozpoznania i klasyfikacji oraz oceny poziomu istotności incydentu po stronie zgłaszającego nie może być przyczyną zaniechania powiadomienia osób odpowiedzialnych w jednostce o zaistniałym incydencie lub podejrzeniu jego wystąpienia. Dlatego w miarę posiadanych zasobów, co najmniej raz do roku należy przeprowadzać okresowe szkolenia pracowników w zakresie bezpieczeństwa teleinformatycznego i zarządzania incydentami. Niezależnie od prowadzonych szkoleń wskazane jest przeprowadzanie szkolenia każdego nowozatrudnionego pracownika celem zapewnienia znajomości zasad prawidłowego zgłaszania incydentów. (zał. nr 4)

Załączniki:

1. Schemat postępowania z incydentami związanymi z bezpieczeństwem informacji
2. Zgłoszenie wstępne z naruszenia ochrony danych osobowych
3. Dziennik Ewidencji Incydentów Bezpieczeństwa TI
4. Dziennik Ewidencji Szkoleń w Zakresie Bezpieczeństwa TI
5. Wykaz przykładowych incydentów


ZGŁOSZENIE
CZY INCYDENT ?
NIE
NOTATKA
TAK
REJESTRACJA
OCENA ISTOTNOŚCI INCYDENTU
ZAWIADOMIENIE
CZY ZAWIADOMIĆ CERT ?
NIE
TAK
ZAWIADOMIENIE
CZY UMYŚLNY ?
NIE
TAK
CZY ZAWIADOMIĆ ORGANY ŚCIGANIA ?
NIE
TAK
ZAWIADOMIENIE
CZY POSTĘPOWANIE DYSCYPLINARNE ?
NIE
TAK
WNIOSEK O UKARANIE
OKREŚLENIE DZIAŁAŃ KORYGUJĄCYCH
RAPORT

Załącznik nr 2

1. Data ..... Godzina .....
2. Osoba powiadamiająca o naruszeniu oraz inne osoby zaangażowane lub odpytane w związku z naruszeniem (imię, nazwisko, stanowisko służbowe,):
   .....
   .....
   .....
   .....
3. Lokalizacja zdarzenia (nr. pokoju, nazwa pomieszczenia, określenie komputerowego stanowiska roboczego, nazwa programu lub aplikacji itp.):
   .....
   .....
   .....
   .....
4. Rodzaj naruszenia i określenie okoliczności towarzyszących naruszeniu:
   .....
   .....
   .....
   .....
   .....
5. Podjęte działania:
   .....
   .....
   .....
   .....
   .....
   .....
   .....
6. Wstępna ocena przyczyn wystąpienia naruszenia:
   .....
   .....
   .....
   .....
   .....
7. Postępowanie wyjaśniające i naprawcze:
   .....
   .....
   .....
   .....
   .....
   .....
   .....
   .....
   .....

.....
(podpis zgłaszającego)

Załącznik nr 3

DZIENNIK EWIDENCJI INCYDENTÓW BEZPIECZEŃSTWA TI

Lp.	Imię i nazwisko oraz funkcja osoby zgłaszającej incydent	Opis incydentu, data oraz okoliczności jego wykrycia	Opis dalszego postępowania	Imię i nazwisko osoby dokonującej zapisu	Uwagi
1.	2.	3.	4.	5.	6.

Załącznik nr 4

DZIENNIK EWIDENCJI SZKOLEŃ W ZAKRESIE BEZPIECZEŃSTWA TI

Lp.	Data szkolenia	Zakres szkolenia	Uczestnik/cy szkolenia	Uwagi/ podpis prowadzącego szkolenie
1.				
2.				
3.				
4.				
5.				
6.				
6.				
8.				

Załącznik nr 5

Wykaz przykładowych incydentów

FORMY NARUSZEŃ	SPOSOBY POSTĘPOWANIA
W ZAKRESIE WIEDZY	
Ujawnianie sposobu działania aplikacji i systemu oraz jej zabezpieczeń osobom niepowołanym.	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. **Bezzwłocznie powiadomić inspektora ochrony danych osobowych (IOD).**
Ujawnianie informacji o sprzęcie i pozostałej infrastrukturze informatycznej.	
Dopuszczanie i stwarzanie warunków, aby ktokolwiek taką wiedzę mógł pozyskać np. z obserwacji lub dokumentacji.	
W ZAKRESIE SPRZĘTU I OPROGRAMOWANIA	
Opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji umożliwiającej dostęp do bazy danych osobowych.	Niezwłocznie zakończyć działanie aplikacji.
Dopuszczenie do korzystania z aplikacji umożliwiającej dostęp do bazy danych osobowych przez jakiekolwiek inne osoby niż osoba, której identyfikator został przydzielony.	Wezwać osobę bezprawnie korzystającą z aplikacji do opuszczenia stanowiska przy komputerze.
Pozostawienie w jakimkolwiek niezabezpieczonym, a w szczególności w miejscu widocznym, zapisanego hasła dostępu do bazy danych osobowych lub sieci.	Natychmiast zabezpieczyć notatkę z hasłami w sposób uniemożliwiający odczytanie.
Dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania umożliwiającego dostęp do bazy danych osobowych osobom nieuprawnionym.	Wezwać osobę nieuprawnioną do opuszczenia stanowiska. Ustalić, jakie czynności zostały przez osoby nieuprawnione wykonane. Przerwać działające programy.
Samodzielne instalowanie jakiegokolwiek oprogramowania.	Pouczyć osobę popełniającą wymienioną czynność, aby jej zaniechała. Wezwać Informatyka w celu odinstalowania programów. **Bezzwłocznie powiadomić administratora systemu informatycznego (ASI).**
Modyfikowanie parametrów systemu i aplikacji.	Wezwać osobę popełniającą wymieniona czynność, aby jej zaniechała. **Bezzwłocznie powiadomić administratora systemu informatycznego (ASI).**

Odczytywanie wymiennych nośników danych przed sprawdzeniem ich programem antywirusowym.	Pouczyć osobę popełniającą wymienioną czynność, aby zaczęła stosować się do wymogów bezpieczeństwa pracy w systemie. Wezwać Administratora Systemu Informatycznego lub informatyka w celu wykonania kontroli antywirusowej. Sporządzić raport.
W ZAKRESIE DOKUMENTÓW I OBRAZÓW ZAWIERAJĄCYCH DANE OSOBOWE	
Pozostawienie dokumentów w otwartych pomieszczeniach bez nadzoru.	Zabezpieczyć dokumenty.
Przechowywanie dokumentów niewłaściwie zabezpieczonych przed dostępem osób niepowołanych.	Powiadomić przełożonych. Spowodować poprawienie zabezpieczeń.
Wyrzucanie dokumentów w stopniu zniszczenia umożliwiającym ich odczytanie.	Zabezpieczyć niewłaściwie zniszczone dokumenty. **Bezzwłocznie powiadomić Inspektora ochrony danych osobowych (IOD).**
Dopuszczanie do kopiowania dokumentów i utraty kontroli nad kopią.	Zaprzestać kopiowania. Odzyskać i zabezpieczyć wykonaną kopię. Powiadomić przełożonych.
Dopuszczanie, aby inne osoby odczytywały zawartość ekranu monitora, na którym wyświetlane są dane osobowe.	Wezwać nieuprawnioną osobę odczytującą dane do zaprzestania czynności, wyłączyć monitor.
Sporządzanie kopii danych na nośnikach danych w sytuacjach nie przewidzianych procedurą.	Spowodować zaprzestanie kopiowania. Podjąć próbę odzyskania oraz zabezpieczyć wykonaną kopię. **Bezzwłocznie powiadomić (ASI).**
Utrata kontroli nad kopią danych osobowych.	Podjąć próbę odzyskania kopii. **Bezzwłocznie powiadomić (ASI).**
W ZAKRESIE POMIESZCZEŃ I INFRASTRUKTURY SŁUŻĄCYCH DO PRZETWARZANIA DANYCH OSOBOWYCH	
Opuszczanie i pozostawianie bez dozoru nie zamkniętego pomieszczenia, w którym zlokalizowany jest sprzęt komputerowy używany do przetwarzania danych osobowych, co stwarza ryzyko dokonania na sprzęcie lub oprogramowaniu modyfikacji zagrażających bezpieczeństwu danych osobowych.	Zabezpieczyć pomieszczenie.
Wpuszczanie do pomieszczeń osób nieznanych i dopuszczanie do ich kontaktu ze sprzętem komputerowym.	Wezwać osoby bezprawnie przebywające w pomieszczeniach do ich opuszczenia, próbować ustalić ich tożsamość.
Dopuszczanie, aby osoby spoza służb informatycznych i telekomunikacyjnych podłączały jakiekolwiek urządzenia do sieci	Wezwać osoby dokonujące zakazanych czynność do ich zaprzestania. Postarać się ustalić ich tożsamość. **Powiadomić (ASI).**