Zarządzenie Nr SK.0050.104.2019

Wójta Gminy Świerzno

z 11 września 2019 roku

w sprawie wprowadzenia „Polityki bezpieczeństwa informacji" w Urzędzie Gminy Świerzno wraz z podległymi jednostkami organizacyjnymi

Na podstawie art. 30 ust. 1 i art. 33 ust. 3 ustawy z dnia 8 marca 1990r. o samorządzie gminnym (tj. Dz. U. z 2018r., poz. 994) oraz art. 24 ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE, L 119 z 4.05.2016 t.) zarządzam, co następuje:

§ 1.

Wprowadza się w Urzędzie Gminy Świerzno oraz jednostkach podległych „Politykę bezpieczeństwa informacji", stanowiącą załącznik do niniejszego zarządzenia.

§ 2.

Wykonanie zarządzenia powierza się sekretarzowi Gminy Świerzno .

§ 3.

Zarządzenie wchodzi w życie z dniem podjęcia.

WÓJT

Radosław Drozdowicz

Polityka bezpieczeństwa informacji – dokument główny

Wersja dokumentu 1.01 z dnia 11września 2019 roku.

Urząd Gminy w Świerznie wraz z nadzorowanymi jednostkami organizacyjnymi

ZATWIERDZAM

WÓJT

Radosław Drzewowicz

.....

Podpis Wójta Gminy Świerzno

Świerzno, dnia 11 września 2019 roku

METRYKA

Nazwa jednostki organizacyjnej	Urząd Gminy w Świerznie oraz podległe jednostki organizacyjne		
Tytuł dokumentu	Polityka Bezpieczeństwa Informacji		
Opis	W skład dokumentu wchodzą: Polityka Bezpieczeństwa Informacji, deklaracja zgodności.		
Zastosowanie	Wszystkie komórki organizacyjne Urzędu Gminy w Świerznie oraz wszystkie komórki organizacyjne jednostek nadzorowanych		
Plik	Polityka Bezpieczeństwa Informacji		
Status	Dokument zatwierdzony, obowiązujący do stosowania od dnia 11 września 2019r.	Liczba stron	22

HISTORIA DOKUMENTU

Wersja	Data wersji	Akcja*	Rozdziały**	Autor / Autorzy	Zatwierdził
1.01	11.09.2019r.	utworzenie	wszystkie	Krzysztof Rychel	WÓJT Radosław Drozdowicz

* Np.: utworzenie nowego dokumentu, modyfikacja, weryfikacja, uzupełnienie.

** Wymienić rozdziały, w których dokonano zmian.

Spis treści

Rozdział 1. Deklaracja Wójta Gminy Świerzno

Wójt Gminy Świerzno mając na uwadze kluczową rolę informacji i jej ochrony dla właściwego funkcjonowania nadzorowanych przez Niego jednostek i realizacji przypisanych im celów statutowych, ustanawia niniejszą *Politykę bezpieczeństwa informacji* (PBI). *Polityka bezpieczeństwa informacji* jest dokumentem podstawowym i nadrzędnym nad innymi dokumentami zawierającym zasady i wymagania względem ochrony posiadanych informacji w ramach funkcjonujących w jednostkach systemów informacyjnych. *Polityka bezpieczeństwa informacji* Urzędu Gminy w Świerznie, określa strategię i filozofię podejścia do spraw bezpieczeństwa informacji. Wójt Gminy Świerzno deklaruje pełne wsparcie dla działań związanych z wdrożeniem i dalszym rozwojem Polityki.

Rozdział 2. Podstawowe definicje używane w dokumentacji Polityki Bezpieczeństwa Informacji

Informacja jest jednym z najważniejszych aktywów urzędu. Informacja jest wyrażana i przekazywana za pomocą mowy, znaków, obrazu, dźwięku lub w jakikolwiek inny sposób. Informacja może zostać zapisana, przechowywana i przetwarzana na papierze, elektronicznie, jak i innych nośnikach czy naturalnych tworach.

Klasyfikacja informacji – podział informacji ze względu na wagę i sposób jej ochrony. Niniejszym dokumentem przyjęto jej następujący podział informacji:

- **informacje chronione** o zasadniczym znaczeniu dla jednostki, dostępne tylko dla osób, którym są niezbędne dla realizacji zadań wynikających z powierzonego zakresu czynności (np.: tajemnica służbowa, tajemnica prawnie chroniona, dane osobowe, sposoby zabezpieczenia aktywów jednostki, w tym kopii bezpieczeństwa, informacje przetworzone mające istotne znaczenie dla pracowników bądź interesariuszy jednostki);
- **informacje do użytku wewnętrznego** – istotne dla działania jednostki, udostępniane bez ograniczeń dla pracowników lub podmiotów współpracujących, na podstawie porozumień o zachowaniu poufności (np.: regulaminy wewnętrzne, instrukcje, wytyczne, różnego rodzaju wykazy, plany działania itp.),
- **informacje publiczne** – udostępniane bez ograniczeń, przeznaczone do nieograniczonej publikacji wśród pracowników i interesariuszy jednostki.

Aktywa będące nośnikiem informacji – wszystko, co ma materialną postać i zawiera informacje.

Dokument Polityki Bezpieczeństwa Informacji – zestaw praw, reguł i praktycznych wskazówek dotyczących sposobu zarządzania, ochrony i dystrybucji informacji zarządzanych przez Wójta Gminy Świerzno oraz kierowników podległych jednostek organizacyjnych. Jest dokumentem pierwszego rzędu przy tworzeniu uregulowań wewnętrznych, uchwał i procedur odnoszących się do przetwarzania informacji.

Przetwarzanie informacji – jest to ogół czynności wykonywanych na informacji, do których można w szczególności zaliczyć: zbieranie, utrwalanie, przechowywanie, archiwizowanie, usuwanie,

modyfikowanie, przeglądanie, udostępnianie, opracowywanie. Przetwarzanie informacji nie musi wiązać się z poznaniem jej treści.

Zapewnienie bezpieczeństwa informacji przetwarzanych - rozumiane jest, jako zapewnienie ich poufności, dostępności, integralności, jako atrybutów informacji na odpowiednim poziomie. Miarą bezpieczeństwa przetwarzania informacji jest wielkość ryzyka dotyczącego utraty któregokolwiek z wymienionych atrybutów.

Poufność - cecha polegająca na zagwarantowaniu tajemnicy informacji oraz dostępu do nich tylko w zakresie przyznanych uprawnień. Definiowana jest, jako zapewnienie, że chroniona informacja dostępna jest jedynie dla osób upoważnionych.

Dostępność - gwarantuje, że osoby, które są upoważnione do określonej informacji, i którym owe informacje są potrzebne, mają do nich dostęp w odpowiednim miejscu i czasie.

Integralność – cecha polegająca na zapewnieniu identyczności informacji w dwóch punktach czasu i przestrzeni, dająca zapewnienie, że dane nie zostały zmienione w sposób nieautoryzowany na skutek manipulacji celowej lub przypadkowej.

Rozliczalność – zapewnienie możliwości kontrolowania prawidłowości przetwarzania informacji pod katem zachowania jej atrybutów na wszystkich etapach przetwarzania w sytuacji kontroli lub konieczności przedstawienia dowodów.

Incydent to każde wykryty stan, który wskazuje na możliwe naruszenie Polityki Bezpieczeństwa Informacji, błąd zabezpieczenia lub nieznana dotychczas sytuacja, która może być związana z bezpieczeństwem.

Interoperacyjność to zdolność różnych podmiotów oraz używanych przez nie systemów teleinformatycznych i rejestrów publicznych do współdziałania na rzecz osiągnięcia wzajemnie korzystnych i uzgodnionych celów, z uwzględnieniem współdzielenia informacji i wiedzy poprzez wspierane przez nie procesów biznesowych realizowanych za pomocą wymiany danych za pośrednictwem wykorzystywanych przez te podmioty systemów teleinformatycznych.

Osobie upoważnionej do przetwarzania informacji – rozumie się przez to osobę zatrudnioną na podstawie umowy o pracę, umowy zlecenia lub innej umowy, osobę odbywającą staż, praktykę, której nadane zostało przez administratora upoważnienie do przetwarzania informacji lub dostęp do nich wynika z zakresu powierzonych obowiązków.

Właściciel zasobu informacyjnego (dalej: zasobu) – osoba decydująca o sposobie użytkowania konkretnych zasobów oraz o jego udostępnianiu innym użytkownikom systemów informatycznych/informacyjnych, najczęściej jest nim kierownik komórki organizacyjnej (wydziału);

.

Zarządzanie ryzykiem – proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych, przy zachowaniu akceptowalnego poziomu kosztów.

Zmiana infrastruktury (usługa rutynowa) – uzgodnioną i zaakceptowaną wcześniej zmianę konfiguracji urządzeń lub sposobu/zakresu świadczonych usług.

Zmiana infrastruktury (usługa awaryjna) - zmianę podejmowaną w trybie nagłym wynikającym z konieczności usunięcia awarii lub błędu w systemie.

Krajowe Ramy Interoperacyjności - Rozporządzenie Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych

Rozdział 3. Informacje przetwarzane przez systemy informacyjne jednostek organizacyjnych Gminy Świerzno

1. W systemach informacyjnych jednostek Gminy Świerzno przetwarzane są informacje służące do wykonywania zadań własnych i zleconych wynikających z ustawy z dnia 8 marca 1990 r. o samorządzie gminnym oraz pozostałych zadań z zakresu administracji publicznej lub też wynikających z przyjętych statutów poszczególnych jednostek.
2. Informacje te są przetwarzane i składowane zarówno w postaci dokumentów papierowych, jak i w formie elektronicznej.
3. W jednostkach organizacyjnych Gminy Świerzno wyróżnia się następujące kategorie (grupy) informacji:
   - informacji publiczne,
   - informacje do użytku wewnętrznego,
   - informacje chronione.
4. *Polityka bezpieczeństwa informacji* swoimi uregulowaniami nie obejmuje informacji niejawnych w rozumieniu ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych.
5. Każdej grupie informacji przypisane są zasoby biorące udział w przetwarzaniu informacji z tej grupy.
6. Dla każdej grupy informacji zidentyfikowane są wymagania bezpieczeństwa, oszacowane jest ryzyko i na tej podstawie dobrane są odpowiednie mechanizmy kontrolne (zabezpieczenia).

Rozdział 4. Cele Polityki bezpieczeństwa informacji

1. Ustanowienie PBI ma na celu podniesienie i utrzymanie wymaganego poziomu ochrony informacji związanych z funkcjonowaniem jednostek organizacyjnych Gminy Świerzno w sposób odpowiadający wymogom określonym w Obwieszczeniu Prezesa Rady Ministrów z dnia 9 listopada 2017 r. w sprawie ogłoszenia jednolitego tekstu rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych

i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów tele-informatycznych. Wdrożenie PBI zapewnia:

- zachowanie zgodności i spójności procesu w obszarze przetwarzania informacji z przepisami prawa powszechnie obowiązującymi i regulacjami wewnętrznymi,
- zachowanie dostępności do informacji w granicach posiadanych uprawnień z równoczesnym zachowaniem jej integralności, poufności i rozliczalności,
- zmniejszenie ryzyka utraty informacji lub jednego z ww. jej atrybutów, kradzieży aktywów będących jej nośnikami i włamań do systemów przetwarzania informacji,
- minimalizowania negatywnych skutków naruszeń bezpieczeństwa,
- zachowanie ciągłości procesów administracyjnych,
- zarządzanie konfiguracją bez negatywnego wpływu na efektywność funkcjonowania systemów, skuteczność mechanizmów zabezpieczających oraz ogólny poziom bezpieczeństwa,
- wprowadzanie stosownych zmian dotyczących ciągłości działania i świadczenia usług,
- zarządzanie zmianami w sposób zapewniający identyfikowanie nowych wymagań w zakresie bezpieczeństwa,
- utrzymanie dobrego wizerunku jednostek organizacyjnych.

2. Wspomniane cele są osiągane w drodze:

- wdrożenia dokumentu polityki i zapoznania z nią wszystkich pracowników, osób i podmiotów współpracujących oraz realizujących zadania na rzecz jednostek przez jej upublicznienie i zapewnienie szkoleń dla wymienionych użytkowników informacji,
- przeglądu dokumentu polityki w formie audytu pod kątem jej adekwatności, kompletności, zgodności z obowiązującymi przepisami prawa, przeprowadzanego nie rzadziej niż raz w roku,
- aktualizacji dokumentu polityki w sytuacji pojawiania się nowych zadań wymagających przetwarzania informacji,
- ustanowienia systemu zarządzania bezpieczeństwem informacji (SZBI) opartego na zarządzaniu ryzykiem,
- bieżącej koordynacji działań wszystkich jednostek organizacyjnych na rzecz bezpieczeństwa informacji,
- uwzględnieniu w dokumencie polityki oraz w przypadku jego modyfikacji wymogów określonych normą PN-ISO/IEC 27001:2007,

Rozdział 5. Zakres stosowania Polityki bezpieczeństwa informacji

Dokumentacja wchodząca w skład *Polityki bezpieczeństwa informacji* swoim zakresem obejmuje:

1. Wszystkie jednostki organizacyjne znajdujące się w strukturze Gminy Świerzno.
2. Wszystkie pomieszczenia jednostek organizacyjnych wskazanych w pkt.1.
3. Zasoby informacyjne (aktywa) zaangażowane w realizację zadań publicznych, a w szczególności:
   - potencjał ludzki, czyli wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, konsultantów oraz ekspertów zewnętrznych, stażystów oraz inne osoby i instytucje mające dostęp do informacji podlegających ochronie;
   - dokumenty papierowe i elektroniczne będące własnością jednostek, interesariuszy, innych instytucji i osób współpracujących z jednostkami, o ile zostały przekazane na podstawie przepisów prawnych lub umów;
   - sprzęt komputerowy oraz inne nośniki informacji (np. magnetyczne (dyskietka, taśma) optyczne (CD-R, DVD-R), elektroniczne (przenośne dyski, pamięci masowe), na których znajdują się informacje;
   - technologie służące pozyskiwaniu, selekcjonowaniu, analizowaniu, przetwarzaniu, zarządzaniu i udostępnianiu informacji, do których zalicza się zarówno systemy papierowe, jak i elektroniczne.
4. Wszystkie urządzenia przenośne użytkowane przez pracowników będące nośnikami informacji oraz zestawy lub pojedyncze dokumenty, na których wykonywane są czynności przetwarzania na terenie jednostek oraz poza nim.

Rozdział 6. System Zarządzania bezpieczeństwem informacji (SZBI)

1. *System zarządzania bezpieczeństwem informacji* (SZBI) opiera się na podejściu procesowym. W ramach systemu wyróżniono **proces zarządzania ryzykiem**. Proces ten składa się z następujących działań:
   - przygotowanie i ustanowienie SZBI, polegające na określeniu celów, procesów i procedur istotnych dla zarządzania ryzykiem oraz doskonalenie bezpieczeństwa informacji tak, aby uzyskać wyniki zgodne z ogólnymi politykami i celami jednostek,
   - wdrożenie i eksploatacja SZBI poprzez wdrożenie odpowiednich zabezpieczeń, procesów i procedur;
   - monitorowanie i przegląd SZBI poprzez szacowanie i tam gdzie ma zastosowanie pomiar wydajności procesów w odniesieniu do celów;
   - utrzymanie i doskonalenie SZBI poprzez podejmowanie działań korygujących

i zapobiegawczych w oparciu o wyniki wewnętrznego przeglądu, niezależnego audytu lub innych istotnych informacji, celem zapewnienia ciągłego doskonalenia systemu.

2. Sposób funkcjonowania SZBI określają odrębne dokumenty wchodzące w skład *Polityki bezpieczeństwa informacji.*

Rozdział 7. Zarządzanie ryzykiem

1. Wszystkie jednostki przetwarzające informacje zobowiązane są do zarządzania ryzykiem związanym z utratą atrybutów przypisanych informacji (tj. poufności, dostępności, integralności.
2. Zarządzanie ryzykiem polega na:
    - identyfikacji zagrożeń dla przetwarzanych zasobów informacyjnych pod kątem utraty któregokolwiek z atrybutów wskazanych w pkt. 1 z szacowaniem prawdopodobieństwa jego wystąpienia i wielkości negatywnych skutków dla jednostki;
    - opracowaniu mechanizmów kontrolnych ograniczających możliwość wystąpienia zagrożenia, bądź wielkość negatywnych skutków w przypadku, gdyby zagrożenie się spełniło do poziomu akceptowalnych przez kierownictwo jednostki wartości;
    - wdrożenie opracowanych mechanizmów i ich monitorowanie;
    - w oparciu o wyniki i wnioski będące efektem monitorowania – korygowanie wprowadzonych mechanizmów pod kątem ich skuteczności i efektywności./
3. Identyfikacja zagrożeń oraz opracowanie adekwatnych mechanizmów kontrolnych jest efektem przeprowadzenia tzw. analizy ryzyka.
4. Analiza ryzyka jest przeprowadzana w oparciu o metodologię stanowiącą załącznik do Polityki ochrony danych osobowych.
5. Niezależnie od wyników analizy ryzyka:
    - jednostka w przypadkach przewidzianych w ustawie z dnia 22 listopada 2018 r. o dokumentach publicznych stosuje zabezpieczenia określone w art. 43 ust. 2 wskazanej ustawy,
    - jednostka w przypadku posiadania fizycznych serwerów tworzy odrębne pomieszczenie zwane „serwerownią", do których dostęp mają jedynie upoważnione osoby, fakt dostępu jest rejestrowany, pomieszczenie jest zabezpieczone przed włamaniem, pożarem i wyposażone w system UPS oraz w system klimatyzacji.
6. Analiza ryzyka sporządzana jest minimum raz w roku lub każdorazowo w przypadku identyfikacji ujawnionego zagrożenia, dotychczas nieobjętego jej wynikami, bądź w sytuacji istotnych zmian w środowisku wewnętrznym jednostki lub jej otoczeniu, mających wpływ na bezpieczeństwo informacji.

7. Analizę ryzyka sporządza Administrator Systemu Informatycznego przy czynnym uczestnictwie osób przez niego wskazanych.
8. Wyniki analizy ryzyka muszą zostać zatwierdzone przez kierownika jednostki.

Rozdział 8. Role i odpowiedzialności związane z bezpieczeństwem informacji

1. Za bezpieczeństwo informacji **odpowiedzialny jest każdy pracownik** oraz każdy podmiot mający dostęp do aktywów informacyjnych. W szczególności wymienieni odpowiadają za przestrzeganie zasad bezpieczeństwa wynikających z PBI, zgłaszanie incydentów z tym związanych oraz wszelkich innych zagrożeń dla bezpieczeństwa przetwarzanych informacji.
2. We wszystkich umowach zawieranych przez jednostki, które mogą dotyczyć przetwarzania informacji, należy uwzględnić zapisy zobowiązujące drugą stronę do przestrzegania odpowiednich zasad przetwarzania informacji gwarantujących odpowiedni poziom ich bezpieczeństwa.
3. W celu opracowania, wdrożenia i doskonalenia *Systemu zarządzania bezpieczeństwem informacji* została powołana następująca struktura organizacyjna bezpieczeństwa informacji:
   - **Wójt Gminy Świerzno** jest odpowiedzialny za opracowanie, wdrożenie w Urzędzie Gminy oraz nadzór nad wdrożeniem w jednostkach podległych rozwiązań wynikających z przyjętej PBI oraz inicjowanie i wspieranie wszelkich działań związanych z bezpieczeństwem informacji i ciągłością działania. Ponadto pełni funkcję *Administratora danych osobowych* **(ADO)** w odniesieniu do danych osobowych przetwarzanych przez Urząd Gminy;
   - **Kierownik jednostki organizacyjnej** jest odpowiedzialny za wdrożenie w podległej jemu jednostce rozwiązań wynikających z przyjętej PBI oraz inicjowanie i wspieranie wszelkich działań związanych z bezpieczeństwem informacji i ciągłością działania. Ponadto pełni funkcję Administratora danych osobowych (ADO) w odniesieniu do danych osobowych przetwarzanych przez jednostkę;
   - **Administrator Systemu Informatycznego (ASI)** osoba zatrudniona w jednostce, oddelegowana z innej jednostki lub podmiot zewnętrzny odpowiedzialny za nadzór i bezpieczne eksploatowanie systemów informatycznych użytkowanych w jednostce.
   - **Inspektor Ochrony Danych (IOD)** osoba zatrudniona w jednostce lub podmiot zewnętrzny pełniący funkcję doradczą i kontrolną w odniesieniu do informacji klasyfikowanych, jako dane osobowe.
4. Szczegółowe role i odpowiedzialności związane z bezpieczeństwem informacji i ciągłością działania są zawarte w:
   - Regulaminach organizacyjnych poszczególnych jednostek,
   - Politykach ochrony danych osobowych poszczególnych jednostek,

- Instrukcjach zarządzania systemem informatycznym poszczególnych jednostek,
- Opisach stanowisk pracy i szczegółowych zakresach czynności.

Rozdział 9. Zarządzanie uprawnieniami związanymi z dostępem do informacji.

1. W przypadku każdej osoby zatrudnionej w jednostce dostęp do informacji winien wynikać z powierzonego zakresu czynności lub opisu stanowiska pracy, a w odniesieniu do informacji klasyfikowanych, jako dane osobowe z imiennego pisemnego upoważnienia.
2. Powierzony zakres czynności winien uwzględniać przyjęty w jednostce system zastępstw.
3. W przypadku, gdy w trakcie zatrudnienia pojawi się konieczność przetwarzania przez pracownika innych informacji, niż wynika to z opisu stanowiska pracy lub powierzonego zakresu czynności, sytuacja taka wymaga zaktualizowania przypisanego pracownikowi zakresu czynności.
4. Za aktualizację powierzonego zakresu czynności, jak i utworzenie adekwatnego systemu zastępstw odpowiedzialność ponosi bezpośredni przełożony pracownika.
5. W przypadku przetwarzania informacji w postaci danych osobowych dodatkowo wymagane są pisemne upoważnienia, których sposób nadawania, odbierania i ewidencjonowania określa Polityka ochrony danych osobowych.
6. Osoby pełniące funkcję przełożonego w odniesieniu do innych pracowników, są zobowiązane do:
   - bieżącego nadzoru nad zakresem informacji przetwarzanych przez osobę podległą i kontrolą adekwatności przedmiotowego zakresu z powierzonymi zakresem czynności podległej osobie,
   - aktualizowania odpowiednio zakresów powierzonych czynności lub przypisanych uprawnień do przetwarzania informacji,
   - prowadzenia w formie wykazu, zestawienia imiennej ewidencji podległych im pracowników ze wskazaniem: rodzaju informacji, które przetwarzają, wskazaniem systemów informatycznych służących do ich przetwarzania (jeżeli są wykorzystywane) ze wskazaniem wykorzystywanego loginu lub innego identyfikatora, określeniem czy dostęp do informacji wynika z zakresu czynności pracownika bądź opisu stanowiska pracy, czy też odrębnego upoważnienia (np. w przypadku danych osobowych.
7. Wszyscy pracownicy jednostki niezależnie od zajmowanego stanowiska i pełnionej funkcji (za wyjątkiem kierownika jednostki), są zobowiązani do:
   - przed podjęciem czynności przetwarzania informacji, upewnienia się, że posiadają uprawnienia do ich przetwarzania wynikające z opisu stanowiska pracy, powierzonego zakresu czynności bądź odrębnego upoważnienia,
   - powstrzymania się z działaniami związanymi z przetwarzaniem informacji w przypadku braku posiadania kompetencji wskazanych w odnośniku powyżej,

- do niezwłocznego powiadomienia przełożonego o fakcie braku uprawnień do przetwarzania informacji.

8. Za niedopuszczalne należy uznać wszelkie działania polegające na:
   - używaniu takich samych loginów, identyfikatorów przez różne osoby,
   - podejmowanie działań związanych z przetwarzaniem informacji wykorzystując login, identyfikatory innych pracowników.

Rozdział 10. Przetwarzanie mobilne informacji oraz w trakcie pracy na odległość

1. Przez przetwarzanie mobilne rozumie się przetwarzanie, odbieranie oraz wysyłanie informacji bez konieczności utrzymywania przewodowego połączenia z siecią.

2. W przypadku pracy na odległość w sytuacji, kiedy następuje wysyłanie i odbieranie informacji obowiązują zasady, jak przy przetwarzaniu mobilnym.

3. Do urządzeń mobilnych w szczególności zalicza się: laptopy, notebooki, tablety, smartfony, czytniki kart pamięci, pendrivy.

4. Procedurę przygotowania sprzętu służącego przetwarzaniu mobilnemu określa Instrukcja zarządzania systemem informatycznym.

5. Do podstawowych zasad regulujących przetwarzanie mobilne informacji zalicza się:
   - posiadanie zgody kierownika na wykorzystywanie urządzeń mobilnych,
   - urządzenia mobilne muszą być przygotowane do przetwarzania informacji poprzez: zaszyfrowanie pamięci dyskowej w urządzeniach lub zaszyfrowanie samych nośników pamięci (pendrivy, karty pamięci), posiadanie zainstalowanego i aktualnego oprogramowania antywirusowego, zainstalowane aplikacje i oprogramowanie służące przetwarzaniu wobec, którego jednostka posiada licencję i możliwość aktualnego wsparcia technicznego,
   - przy przetwarzaniu mobilnym zakazuje się korzystania z publicznych sieci internetowych. Przetwarzanie jest możliwe wyłącznie z wykorzystaniem dostępu do kanałów komunikacyjnych skonfigurowanych na urządzeniu mobilnym i zatwierdzonych przez ASI.

6. ASI prowadzi wykaz urządzeń umożliwiających mobilne przetwarzanie informacji oraz osób posiadających uprawnienia do tego rodzaju czynności.

7. Za mobilne przetwarzanie należy rozumieć zdalny dostęp do kont służbowej poczty e-mail, oraz innych zasobów informacyjnych jednostki.

8. Wykonywanie pracy na odległość w tym telepracy wymaga zgody kierownika jednostki.

9. W odniesieniu do osoby realizującej pracę na odległość stosuje się wszystkie zasady i postanowienia wynikające z PBI, a sama osoba jest zobowiązana do przestrzegania wszystkich zasad wynikających z dokumentacji PBI.

10. Praca na odległość może być realizowana wyłącznie w oparciu o infrastrukturę sprzętową i programistyczną będącą własnością jednostki.

Rozdział 11 Reagowanie na incydent

1. Fakt wystąpienia incydentu związanego z przetwarzaniem informacji może zostać ujawniony przez każdego pracownika jednostki, jak i przez każdą inną osobę nie będącą jej pracownikiem

2. Każdy pracownik niezależnie od zajmowanego stanowiska i niezależnie od sposobu pozyskania wiedzy o wystąpieniu incydentu związanego z przetwarzaniem informacji jest zobowiązany do:

   - podjęcia działań adekwatnych do posiadanych kompetencji i możliwości mających na celu ograniczenie negatywnych skutków incydentu dla poufności, integralności i dostępności informacji (np. zabezpieczenie dokumentów, wyłączenie jednostki komputerowej będącej przedmiotem incydentu itp.)

   - zabezpieczeniu wszelkich możliwych dowodów mogących służyć postępowaniu wyjaśniającemu przyczyny wystąpienia incydentu w sytuacji, gdy zaniechanie tych czynności spowodowałoby bezpowrotną utratę materiału dowodowego,

   - niezwłocznego powiadomienia bezpośredniego przełożonego lub kierownika jednostki o powzięciu wiedzy o wystąpieniu zdarzenia mającego charakter incydentu,

   - w przypadku incydentu związanego z szeroko rozumianą infrastrukturą informatyczną pierwszą w kolejności osobą przed bezpośrednim przełożonym i kierownikiem jednostki, którą należy powiadomić o wystąpieniu incydentu jest ASI,

   - powiadomienie o wystąpieniu incydentu może zostać zrealizowane w drodze równoległego powiadomienia bezpośredniego przełożonego, kierownika jednostki i ASI,

   - na każde wezwanie kierownika czynnie uczestniczyć w postępowaniu wyjaśniającym przyczyny wystąpienia i przebieg incydentu w szczególności poprzez złożenie odpowiednich wyjaśnień.

3. Kierownik jednostki powziąwszy wiedzę o wystąpieniu incydentu związanego z obszarem przetwarzania informacji jest zobowiązany do:

- podjęcia wszelkich możliwych działań związanych z zadysponowaniem wszelkich dostępnych zasobów techniczny, organizacyjnych, ludzkich mających na celu ograniczenie skutków incydentu i zabezpieczenie materiału niezbędnego do wyjaśnienia jego przyczyn i przebiegu,

- powołania zespołu wyjaśniającego przyczyny przebieg i ocenę skutków wystąpienia incydentu. Skład zespołu jest determinowany merytoryczną wiedzą z zakresu zagadnień będących przedmiotem incydentu związanego z przetwarzaniem informacji. W jego skład mogą wejść osoby niezatrudnione w jednostce, jeżeli posiadana przez nich wiedza jest niezbędna dla postępowania wyjaśniającego. Kierownik jednostki osobiście kieruje pracą zespołu lub wyznacza inną osobę z zespołu, której powierzy przedmiotowe kompetencje,

- w przypadku incydentu związanego z szeroko rozumianą infrastrukturą informatyczną stałym członkiem zespołu procedującego postepowanie wyjaśniające jest ASI, który równocześnie kieruje pracami zespołu i podlega bezpośrednio kierownikowi jednostki.

4. Wszystkie czynności prowadzone przez zespół prowadzący postępowanie muszą być dokumentowane. Za dokumentowanie przedmiotowych czynności odpowiada osoba kierująca pracami zespołu.

5. Każdy incydent mający charakter:

   - skanowania systemów informatycznych,

   - spamu przesyłanego za pośrednictwem polskich serwerów,

   - ataków typu DoS (Denial of Service) i DDoS (Distributed Denial of Service),

   - włamań i prób włamania,

   Powinien być przedmiotem zgłoszenia do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV.

6. Za dokonanie zgłoszenia, o którym mowa w pkt. 5 w terminie 24 h od momentu powzięcia wiedzy o incydencie zawierającego elementy wymienione w art. 23 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, odpowiedzialny jest ASI.

7. W odniesieniu do informacji w postaci danych osobowych procedura postępowania w przypadku wystąpienia incydentu została zawarta w Księdze procedur.

8. Końcowym etapem postepowania wyjaśniającego jest ponowne przeprowadzenie analizy ryzyka dla przetwarzania informacji z uwzględnieniem wniosków wynikających z postępowania wyjaśniającego.

Rozdział 12. Szkolenia i upowszechnianie wiedzy z zakresu bezpieczeństwa przetwarzania informacji

1. System szkoleń z zakresu bezpiecznego przetwarzania informacji obejmuje:
   - wszystkich pracowników na stanowiskach urzędniczych, niezależnie od miejsca w strukturze organizacyjnej oraz na stanowiskach nie urzędniczych niezależnie od formy zatrudnienia, jeżeli powierzone obowiązki wymagają przetwarzania informacji,
   - wszystkie zagadnienia wyszczególnione w Polityce Bezpieczeństwa Informacji i pozostałych dokumentach wchodzących w jej skład.
2. Szkolenia mają formę:
   - szkolenia stanowiskowego, realizowanego przez bezpośredniego przełożonego na każdym etapie zatrudnienia,
   - szkolenia wstępnego organizowanego na etapie zatrudniania. Szkolenie wstępne jest dwuetapowe, gdzie każdy z etapów jest odrębnie realizowany przez IOD oraz ASI. Terminy szkolenia wstępnego ustala bezpośredni przełożony zatrudnianego pracownika. Termin szkolenia musi zostać określony nie później niż w 7 dniu od daty zatrudnienia,
   - szkolenia okresowe realizowane cyklicznie, co najmniej raz w roku prowadzone przez ASI w zakresie bezpiecznego wykorzystywania infrastruktury informatycznej przy przetwarzaniu informacji oraz IOD w zakresie obowiązujących przepisów regulujących obszar przetwarzania informacji,
   - propozycję terminu szkolenia cyklicznego IOD i ASI przedkłada kierownikowi jednostki każdego roku do końca stycznia,
   - wszystkie szkolenia, niezależnie od rodzaju są potwierdzane zaświadczeniem wydawanym przez osobę prowadzącą szkolenie. Zaświadczenia są przechowywane w komórce kadr.

Rozdział 13. Struktura dokumentów Polityki bezpieczeństwa informacji

1. Dokumentacja Polityki Bezpieczeństwa ustanawia metody zarządzania oraz wymagania niezbędne dla zapewnienia skutecznej i spójnej ochrony przetwarzanych informacji.
2. Dokumentację *Polityki Bezpieczeństwa Informacji* stanowią:
   - Dokument główny - *Polityka bezpieczeństwa informacji,*
   - *Instrukcja zarządzania systemem informatycznym,*
   - *Polityka ochrony danych osobowych,*
   - *Regulamin monitoringu (dotyczy jednostek, w których funkcjonuje monitoring*

wewnętrzny),

Rozdział 14. Rozpowszechnienie i zarządzanie dokumentem polityki

1. Niniejszy dokument *Polityki Bezpieczeństwa Informacji* jest **dokumentem nadrzędnym** nad wszystkimi dokumentami dotyczącymi bezpieczeństwa informacji w Urzędzie Gminy oraz nadzorowanych jednostkach.
2. Zasady określone przez dokumenty *Polityki bezpieczeństwa informacji* mają zastosowanie do **całego systemu informacyjnego** Urzędu Gminy i pozostałych jednostek w szczególności do:
   - wszystkich systemów informacyjnych i informatycznych, w których są lub będą przetwarzane informacje podlegające ochronie,
   - informacji będących w dyspozycji jednostek przetwarzanych przez inne podmioty, o ile zostały im przekazane przez jednostkę na podstawie stosownych umów,
   - wszystkich nośników papierowych, magnetycznych, optycznych, elektronicznych i innych, na których są lub będą znajdować się informacje podlegające ochronie,
   - wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie.
3. Do stosowania zasad określonych przez dokumenty wchodzące w skład *Polityki Bezpieczeństwa Informacji* **zobowiązani są wszyscy pracownicy** w rozumieniu przepisów Kodeksu Pracy, **konsultanci, stażyści i inne osoby mające dostęp do informacji podlegającej ochronie**.
4. Z treścią dokumentacji Polityki Bezpieczeństwa Informacji, **powinni zapoznać się wszyscy pracownicy** (niezależnie od zajmowanego stanowiska) **i inne osoby mające dostęp do informacji** przetwarzanej w jednostkach, przed przystąpieniem do jej przetwarzania.
5. Niniejszy dokument jest dostępny dla wszystkich pracowników jednostki i może być przedstawiany podmiotom, z którymi jednostki związane są umową, lub innym podmiotom współpracującym jeżeli nawiązane relacje wymagają przetwarzania informacji.
6. Wszelkie propozycje zmian do PBI wymagają uzyskania pozytywnej opinii IOD oraz ASI, a ostateczną decyzję podejmuje Wójt Gminy Świerzno.
7. Obowiązek stosowania dokumentu *Polityki bezpieczeństwa informacji* oraz wszelkie jego zmiany realizowane są w drodze zarządzenia Wójta Gminy Świerzno.

Rozdział 15. Przeglądy Polityki bezpieczeństwa informacji i audyty systemu

1. Polityka Bezpieczeństwa Informacji powinna być poddawana planowemu sprawdzenia przynajmniej raz na rok pod kątem jej zgodności z obowiązujacymi przepisami prawa w formie zadania audytowego.

2. Ponadto Polityka Bezpieczeństwa Informacji może być poddawana przeglądowi w formie pozaplanowego sprawdzenia w razie:
   - powziecia informacji o naruszeniu bezpieczeństwa informacji o charakterze chronionym,
   - wniosku ze strony instytucji nadzorujących i kontrolujących działalność Wójta Gminy Świerzno,
   - potrzeb wynikających ze zmian dotyczących przetwarzania informacji chronionych na skutek: zmian w budowie systemu informatycznego, zmian organizacyjnych, zmian obowiązujących przepisów prawa, pojawienia się nowego dotychczas niezidentyfikowanego zagrożenia.

Rozdział 16. Zapewnienie interoperacyjności (na poziomie semantycznym)

1. Jednostka zmierza do osiagnięcia interoperacyjności (zgodności) działania poprzez:
   - stosowanie rozwiązań informatycznych w postaci infrastruktury technicznej umozliwiajacej korzystanie z rejestrów publicznych innych podmitów tj. zapewnienie odpowiedniego łącza umożliwiajacego przesyłanie i wymianę informacji za pomocą protokołów komunikacyjnych określonych przepisami prawa, bądź rekomendacjami krajowej jednostki normalizacyjnej lub opublikowanym przez ministra właściwego do spraw informatyzacji. Ponadto zapewnia się użycie odpowiednich urzadzeń końcowych umożliwiajacych komunikację,
   - stosowanie rozwiazań programistycznych umozliwiajacych przetwarzanie informacji i ich wymianę w co najmniej jednym formacie wskazanym w załączniku nr 2 do KRI,
   - stosowanie rozwiazań programistycznych zapewniajacych odwoływanie się do rejestrów publicznych zawierajacych dane referencyjne w zakresie realizowanych zadań,
   - zastosowanie rozwiązań programistycznych zapewniających wysyłanie i odbieranie dokumentów, w których kodowanie znaków pisma będzie realizowane w oparciu o standard unicode połączony z kodowaniem UTF-8.

Rozdział 17. Wykaz usług zabronionych

1. Zabrania się wykorzystywania jednostek komputerowych, zainstalowanego na nich oprogramowania oraz dostępu do usług sieciowych w celach prywatnych, bądź nie związanych z realizacją powierzonych obowiązków.
2. W szczególności zabrania się:
   - korzystania z usług poczty elektronicznej do obsługi kont e-mail innych niż zaakceptowane przez kierownika jednostki (prywatnej), usług bankowości elektronicznej innej niż zaakceptowana przez kierownika jednostki, usług serwisów handlowych, randkowych, społecznościowych, erotycznych

- prowadzenia prywatnych rozmów przez Internet (tzw. chat, IRC, komunikatory osobiste) z wyłączeniem usług zatwierdzonych przez kierownika jednostki i wskazanych w Rejestrze Oprogramowania,
- prowadzenia gier sieciowych i uprawianie hazardu
- korzystania z sieci typu: P2P, sieci anonimizujących („TOR")
- łączenie się z prywatnymi komputerami,
- łączenie się z prywatnymi komputerami poprzez VPN.

3. W celach wymiany zasobów informacyjnych przez jednostki gminne i ich interesariuszy:
   - do danych zawierających dokumenty tekstowe,
   - do danych zawierających informację graficzną,
   - do danych zawierających informację dźwiękową,
   - do kompresji dokumentów elektronicznych,
   - do tworzenia stron WWW,
   - do określenia struktury i wizualizacji dokumentu,

   stosuje się wyłącznie formaty danych określone w załączniku nr 2 do Krajowych Ram Interoperacyjności.
4. Wiadomości e-mail zawierające inne formaty danych niż określone w pkt. 2 będą blokowane, co będzie skutkowało brakiem możliwości ich odebrania lub wysłania.
5. Celem weryfikacji przestrzegania postanowień dotyczących usług zabronionych w jednostkach Gminy Świerzno wprowadza się monitoring użytkowanych przez pracowników stacji roboczych oraz monitoring ruchu sieciowego. Powyższe zadanie będzie realizowane za pomocą dedykowanego oprogramowania do zarządzania bezpieczeństwem IT.
6. Pracownicy jednostek są świadomi, że wszelkie ich działania związane z wykorzystaniem udostępnionej infrastruktury informatycznej są monitorowane, a potwierdzeniem powyższego jest złożenie oświadczenia wg załącznika nr 1 do niniejszego dokumentu.

Rozdział 18. Określenie środków technicznych i organizacyjnych stosowanych przy przetwarzaniu informacji

1. Wyróżnia się następujące środki bezpieczeństwa przy przetwarzaniu informacji:
   - środki ochrony fizycznej, do których w szczególności można zaliczyć: drzwi ochronne, zamykane szafy, monitoring wizyjny, pracownika ochrony fizycznej, portiera itp.

- środki techniczne, do których w szczególności można zaliczyć: elektroniczne systemy dozoru, podtrzymania zasilania, przeciwpożarowe, ewidencje: wejść i wyjść, dostępu, oprogramowanie: firewall, antywirus, wspomagające zarządzaniem systemem informatycznym,
- środki organizacyjne do których w szczególności można zaliczyć: kompletną dokumentację PBI określającą zasady obowiązujące przy przetwarzaniu informacji, w tym dostępu do pomieszczeń i informacji, wyznaczanie obszarów przetwarzania informacji, ewidencjonowanie osób i przypisanie zakresu przetwarzanych informacji, regularne testowanie kopii zapasowych, testowanie skuteczności przyjętych zabezpieczeń, przyjęte procedury postepowania w określonych sytuacjach, system szkoleń pracowników itd.

2. Zastosowanie konkretnych środków bezpieczeństwa w jednostce wynika z:

   - przepisów szczególnych regulujących obszar przetwarzania konkretnych informacji,
   - zasad określonych dokumentacją PBI,
   - analizy ryzyka zagrożeń i ich skutków .

3. Za dobór i zastosowanie środków bezpieczeństwa przetwarzania informacji z uwzględnieniem dyspozycji zawartych w pkt. 1-2 odpowiada kierownik jednostki lub osoba, której w formie pisemnej obowiązek ten został powierzony.

4. Ustala się minimalny zakres środków bezpieczeństwa dla użytkowanych systemów informatycznych:

   - Systemy informatyczne, programy i aplikacje winny być aktualizowane w sposób bieżący,
   - Stosowane firewalle muszą posiadać zdolność do weryfikowania źródła przychodzących wiadomości oraz filtrowania przesyłanych pakietów,
   - Stosowane firewalle muszą posiadać zdolność wykrywania obecności wirusów w przesyłanej poczcie drogą elektroniczną i na stronach www,
   - w przypadku posiadania przez jednostkę własnych serwerów, urządzenia serwerowe muszą znajdować się w pomieszczeniu zwanym serwerownią, do których mają wyłącznie dostęp osoby upoważnione do ich obsługi, a wszelkie wejścia i wyjścia są ewidencjonowane,
   - pomieszczenie serwerowni musi być wyposażone w system klimatyzacji, utrzymujący w zadanym zakresie temperaturę powietrza, czujnik dymu i wody oraz system UPS podtrzymujący pracę urządzeń serwerowych na wypadek zaniku napięcia zewnętrznego,

- zarządzanie systemami informatycznymi jednostki wymaga takiej ich konfiguracji, aby możliwym było gromadzenie informacji o osobach i czasie ich wykorzystania. Ponadto dokumentowaniu w postaci zapisów w dziennikach systemów podlegają wszelkie działania dostępu do systemów informatycznych w zakresie ich konfiguracji, zabezpieczeń. Informacje, o których mowa w niniejszym punkcie są przechowywane przez okres , co najmniej 2 lat.

5. W celu zapewnienia środków wskazanych w pkt. 4 możliwym jest wykorzystanie specjalistycznego oprogramowania do zarządzania infrastrukturą IT w jednostce, które traktowane jest, jako jedno z podstawowych i niezbędnych narzędzi pracy ASI.

6. Za zapewnienie środków bezpieczeństwa wskazanych w pkt. 4 odpowiada kierownik jednostki oraz osoba lub podmiot sprawujący funkcję ASI. Z przedmiotowej odpowiedzialności ASI może zostać zwolniony jedynie w sytuacji, gdy udokumentuje, iż ich brak wynikał z decyzji kierownika jednostki (negatywnie rozpatrzone wnioski o wprowadzeniu właściwych środków bezpieczeństwa)..

Rozdział 19. Bezpieczeństwo w umowach zawieranych przez jednostki

1. W przypadku zawierania przez jednostki umów gospodarczych, cywilnych, kontraktowych cywilnoprawnych - jeżeli w ramach ich wykonywania będzie wymagany dostęp do zasobów informacyjnych jednostki, osoba wnioskująca o zawarcie umowy, ma obowiązek:
   - w przypadku, gdy przedmiotem udostępnienia będą informacje klasyfikowane, jako dane osobowe przygotować odrębną umowę powierzenia danych wg wzoru stanowiącego załącznik do Polityki ochrony danych osobowych lub załączyć jej treść do treści umowy głównej,
   - w przypadku pozostałych informacji nie stanowiących danych osobowych wprowadzić w umowie klauzule bezpieczeństwa dotyczące obowiązku przestrzegania przez kontrahenta zasad bezpieczeństwa informacji określonych niniejszym dokumentem.
2. Do podstawowych zapisów będących przedmiotem klauzuli bezpieczeństwa można zaliczyć w szczególności:
   - zobowiązanie kontrahenta do bezpiecznego przetwarzania przekazanych informacji gwarantujących ich poufność, integralność, dostępność oraz rozliczalność,
   - zobowiązanie kontrahenta do zapewnienia, iż jego pracownicy posiadający dostęp do informacji przetwarzanych w jednostce w związku z zawartą umową, zobligowani są do zachowania ich w poufności w trakcie, jak i po wygaśnięciu zatrudnienia,
   - powzięcie przez jednostkę wiedzy, że udostępnione informacje są przetwarzane przez kontrahenta w sposób niezapewniający zachowania atrybutów: poufności, integralność, dostępność oraz rozliczalność, będzie stanowiło podstawę rozwiązania umowy z kontrahentem z jego winy i wiązało się ze wszystkimi negatywnymi skutkami, takimi, jak kary umowne, odszkodowania itp.

- w przypadku przetwarzania przez kontrahenta przekazanych jemu informacji w sposób nie dający gwarancji ich bezpieczeństwa w przypadku powstania szkody, będzie on zobowiązany do jej pokrycia w pełnej wysokości.

Rozdział 20. Ewidencjonowanie infrastruktury informatycznej i zapewnienie ciągłości działania

1. W celu: zapewnienia kontroli nad używaną infrastrukturą informatyczną, jej aktualnością, adekwatnością do potrzeb oraz zapewnieniu ciągłości działania prowadzona jest ewidencja użytkowanych urządzeń i wykorzystywanego oprogramowania.
2. Ewidencja wskazana w pkt. 1 zawiera:
   - nazwę ewidencji
   - określenie (nazwę) stanowiska pracy,
   - określenie jednostki komputerowej (nr inwentarzowy wynikający z ewidencji środków), jej parametrów technicznych w odniesieniu do pamięci RAM, pojemności dyskowej, częstotliwości pracy procesora,
   - określenie podłączonych do ww. jednostki urządzeń peryferyjnych ze wskazaniem jego rodzaju (drukarka, skaner itp.) oraz typu (urządzenie wielofunkcyjne, laserowe), modelu i nr inwentarzowego,
   - określenie użytkowanego systemu operacyjnego wraz ze wskazaniem jego wersji oraz rodzaju licencji – OEM lub BOX,
   - określenie zainstalowanego pakietu biurowego ze wskazaniem parametrów analogicznych, jak dla systemów operacyjnych,
   - określenie zainstalowanych programów ze wskazaniem dla każdego z nich: nazwy, wersji, rodzaju licencji, nośnika instalacyjnego, wymagań sprzętowych, konieczności wykonywania kopii danych ze wskazaniem jej rodzaju, częstotliwości jej wykonywania, nośnika kopii i miejsca jego przechowywania.
3. Odpowiedzialnym za sporządzenie, prowadzenie i bieżącą aktualizację ewidencji jest osoba/podmiot pełniący funkcję ASI.
4. Przyjmuje się, że lokalizacja miejsca przechowywania fizycznego nośnika kopii danych musi być różna od lokalizacji, w której wykorzystuje się oprogramowanie, z którego wykonuje się kopie danych. Powyższe ma zastosowanie do wszelkich nośników zainstalowanego oprogramowania i systemów operacyjnych.
5. W miarę możliwości w przypadku zakupu oprogramowania systemowego oraz użytkowego podejmowane są działania związane z pozyskaniem licencji z możliwością migrowania zainstalowanego produktu na inne jednostki komputerowe.

6. W przypadku wystąpienia zdarzenia natury katastroficznej jednostka odtwarza swoją działalność na terenie innej jednostki ze wskazaniem na Szkołę Podstawową.
7. Przy odtwarzaniu działalności jednostki głównym źródłem sprzętu komputerowego (jednostki główne wraz z urządzeniami peryferyjnymi), będą inne jednostki Gminy Świerzno udostępniające przedmiotowy sprzęt, ze wskazaniem na szkolną pracownie komputerową.
8. W odniesieniu do przywracania użytkowanego oprogramowania i zapisów w nim zawartych głównym źródłem będą kopie bezpieczeństwa danych niezależnie od rodzaju nośnika, na których zostały wykonane (nośnik fizyczny, wirtualna przestrzeń dyskowa)
9. Odtworzenie sieci komputerowej nastąpi w oparciu o zabezpieczoną sieć WI-FI.
10. Czas odtwarzania podstawowej działalności jednostki niezależnie od jej rodzaju nie powinien przekroczyć 72 h.

Rozdział 21. Postanowienia końcowe

1. Niniejszy dokument obowiązuje wszystkie jednostki organizacyjne, nad którymi nadzór sprawuje Wójt Gminy Świerzno w stopniu odpowiadającym rodzajowi i zakresowi przetwarzania informacji będących przedmiotem regulacji PBI.
2. Dokument Polityki Bezpieczeństwa wchodzi w życie z dniem jego zatwierdzenia w drodze zarządzenia wydanego przez Wójta Gminy Świerzno.
3. Osobami odpowiedzialnymi za wdrożenie postanowień wynikających z Polityki Bezpieczeństwa Informacji są kierownicy poszczególnych jednostek.