Zarządzenie Nr SK – 0050.29.2012
Wójta Gminy Świerzno
z dnia 2 kwietnia 2012 r.

w sprawie wprowadzenia dokumentacji opisującej sposób przetwarzania danych osobowych oraz środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych osobowych

Na podstawie art. 36 ustawy z dnia 29 sierpnia 1997 r o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) oraz § 3 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r Nr 100, poz. 1024) zarządzam co następuje

§ 1.

1. Wprowadzam dokumentację opisującą sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych w Urzędzie Gminy w Świerznie.
2. Na dokumentację, o której mowa w ust. 1 składa się:

1) Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Gminy Świerzno stanowiąca załącznik nr 1 do zarządzenia,
2) Polityka bezpieczeństwa zarządzania systemem informatycznym służącym do przetwarzania danych osobowych stanowiąca załącznik nr 2 do zarządzenia

§ 2.

Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT
Krzysztof Atras

Załącznik nr 1 do
Zarządzenia Nr SK – 0050.29.2012
Wójta Gminy Świerzno
z dnia 2 kwietnia 2012 r.

INSTRUKCJA
ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM
SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

Rozdział I.
CZĘŚĆ
OGÓLNA

§ 1.

Instrukcja określa sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych w Urzędzie Gminy Świerzno.

§ 2.

Ilekroć w niniejszej instrukcji mowa o:

1) Urzędzie - należy rozumieć przez to Urząd Gminy Świerzno,
2) Administratorze Danych Osobowych - należy rozumieć przez to Wójta Gminy Świerzno,
3) Administratorze Bezpieczeństwa Informacji - należy rozumieć przez to osobę wyznaczoną przez Administratora Danych Osobowych do pełnienia tej funkcji,
4) Lokalnym Administratorze Bezpieczeństwa Informacji - należy rozumieć przez to Kierownika Referatu lub pracownika zatrudnionego na samodzielnym stanowisku, przewidzianych w strukturze organizacyjnej Urzędu,
5) użytkowniku danych osobowych - należy rozumieć każdego pracownika, który wykonując czynności służbowe przetwarza dane osobowe, tzn. wykonuje na nich jakiekolwiek operacje, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, usuwanie.
6) systemie informatycznym - należy rozumieć przez to system informatyczny wdrożony w Urzędzie Gminy Świerzno.

§ 3.

Informacje zawarte w prowadzonych w Urzędzie różnego rodzaju rejestrach, ewidencjach, kartotekach, wykazach oraz w systemach informatycznych dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, pozwalające na bezpośrednie lub pośrednie określenie tożsamości tej osoby uznaje się za dane osobowe.

§ 4.

1. Do obowiązków Administratora Bezpieczeństwa Informacji należy:
   1) czuwanie nad wdrażaniem w Urzędzie niniejszej instrukcji oraz dbanie o bieżące jej uaktualnianie stosownie do zmieniających się technologii informatycznych oraz zagrożeń bezpieczeństwa systemów informatycznych,
   2) identyfikowanie i analizowanie zagrożeń oraz ryzyka, na które narażone może być przetwarzanie danych osobowych w systemach informatycznych,
   3) określanie potrzeb w zakresie bezpieczeństwa systemów informatycznych, w których przetwarzane są dane osobowe,
   4) nadawanie identyfikatorów użytkownikom danych osobowych,
   5) zabezpieczenie i kontrolowanie prawidłowości przebiegu czynności serwisowych sprzętu komputerowego oraz systemów informatycznych,
   6) pozbawianie zapisu danych osobowych lub uszkadzanie w sposób uniemożliwiający odczytanie urządzeń lub nośników, które przeznaczone są do likwidacji,
   7) instalowanie zabezpieczeń w systemach informatycznych,
   8) wyrejestrowywanie i rejestrowanie z systemu użytkowników w czasie instalowania oraz modyfikacji systemu,
   9) przydzielanie uprawnień do poszczególnych systemów,
   10) wykonywanie kopii awaryjnych danych z serwera, właściwe przechowywanie nośników, sprawdzanie poprawności zapisu oraz ich likwidowanie,
   11) dokonywanie wyboru lub migracji do technologii minimalizującej zagrożenia uzyskania dostępu do sieci osobom nieupoważnionym,
   12) nadzorowanie procesu monitorowania sieci pod kątem zabezpieczenia przed dostępem osób nie upoważnionych,
   13) sporządzanie oraz bieżące aktualizowanie listy osób upoważnionych do pobierania kluczy od pomieszczeń, w których przetwarzane są dane osobowe,
   14) prowadzenie ewidencji pracowników zatrudnionych przy przetwarzaniu danych osobowych.

2. Do obowiązków Lokalnego Administratora Bezpieczeństwa Informacji należy:
   1) wykonywanie poleceń Administratora Bezpieczeństwa Informacji w zakresie zarządzania podległymi systemami informatycznymi,
   2) czuwanie nad właściwym eksploatowaniem podległych im systemów informatycznych,
   3) stwarzanie właściwych warunków organizacyjno-technicznych gwarantujących

bezpieczeństwo podległych im systemów informatycznych,

4) nadzorowanie właściwej lokalizacji sprzętu komputerowego, tj. ustawiania monitorów i drukarek uniemożliwiającego wgląd w dane osobowe osobom nieupoważnionym lub kradzież wymiennych nośników danych,
5) występowaniem do Administratora Danych Osobowych z wnioskiem o upoważnienie pracowników do przetwarzania danych osobowych,
6) nadawanie haseł dostępu użytkownikom oraz ustawianie uprawnień w podległych im systemach
7) pozbawianie zapisu danych osobowych z nośników, które przeznaczane są do przekazania innemu podmiotowi, nieuprawnionemu do otrzymania tych danych,
8) pozbawianie zapisu danych osobowych lub uszkadzanie w sposób uniemożliwiający odczytanie nośników, które przeznaczone są do likwidacji,
9) prowadzenie, uaktualnianie na bieżąco oraz przesyłanie Administratorowi Bezpieczeństwa Informacji danych dotyczących:
   - listy użytkowników danych osobowych wraz z przydzielonymi im uprawnieniami do poszczególnych funkcji systemu,
   - lokalizacji pomieszczeń, w których te dane są przetwarzane, w przypadku jakichkolwiek zmian tych danych,
   - rodzaju systemów informatycznych funkcjonujących w zakresie ich działania,
   - czynności serwisowych wykonywanych w podległych systemach informatycznych,
   - zdarzeń wpływających na bezpieczeństwo systemów informatycznych, w tym m.in.
   - wykrytych wirusów, koni trojańskich itp. oprogramowania nielegalnego lub zainstalowanego bez upoważnienia, awarii systemu informatycznego lub jego
   - nieprawidłowego działania, stwierdzenia faktu korzystania z systemu informatycznego przez osobę niepowołaną, awarii zasilania,
10) zgłaszanie Administratorowi Bezpieczeństwa Informacji potrzeb w zakresie zabezpieczenia podległych im systemów informatycznych.

§ 5.

1. Dostęp pracowników do obsługi systemu informatycznego przetwarzającego dane osobowe oraz urządzeń wchodzących w jego skład możliwy jest wyłącznie na podstawie upoważnienia wydanego przez Administratora Danych Osobowych.
2. Użytkownicy danych osobowych obowiązani są do zachowania ich w tajemnicy podczas wykonywania czynności służbowych, jak i po ustaniu zatrudnienia.

3. Oświadczenia o zachowaniu tajemnicy służbowej, o której mowa w ust. 2 przechowywane są w aktach osobowych pracowników.
4. Przed dopuszczeniem do pracy przy przetwarzaniu danych osobowych każda osoba powinna być zaznajomiona z przepisami dotyczącymi ochrony danych osobowych.

§ 6.

1. Udostępnianie danych osobowych ze zbioru danych osobom lub podmiotom uprawnionym do ich otrzymania odbywać się może na pisemny umotywowany wniosek.
2. Decyzję o udostępnieniu danych osobowych podejmuje Administrator Danych Osobowych, po uzyskaniu opinii wydziału merytorycznego.
3. Po otrzymaniu zgody od Administratora Danych Osobowych, dane do udostępnienia przygotowuje użytkownik danych osobowych. Użytkownik jest zobowiązany do odnotowania w systemie informatycznym informacji o odbiorcach, którym dane zostały udostępnione, dacie i zakresie tego udostępnienia.

Rozdział II.
ZASADY PRZYDZIAŁU HASEŁ DLA UŻYTKOWNIKÓW

§ 7.

1. Dla każdego użytkownika systemu informatycznego, w którym przetwarzane są dane osobowe przydziela się odrębny identyfikator i hasło oraz uprawnienia w systemie zgodnie z zakresem obowiązków.
2. Przyznany użytkownikom identyfikator jest niezmienny, natomiast użytkownik jest zobowiązany do zmiany hasła raz na miesiąc.
3. Za przydział i rejestrację identyfikatorów dostępu do systemów przetwarzających dane osobowe odpowiedzialny jest Administrator Bezpieczeństwa Informacji.
4. Za przydział i rejestrację haseł dostępu do poszczególnych systemów przetwarzających dane osobowe odpowiedzialny jest Lokalny Administrator Bezpieczeństwa Informacji.
5. Lokalny Administrator Bezpieczeństwa Informacji wyrejestrowuje z podległego mu systemu identyfikator i hasło pracownika, który utracił uprawnienia dostępu do danych osobowych. Administrator Bezpieczeństwa Informacji wyrejestrowuje konto takiego użytkownika w systemie sieciowym.
6. Identyfikatory pracowników oraz hasła dostępu do systemu informatycznego stanowią

tajemnicę służbową.

7. Użytkownik po otrzymaniu indywidualnego identyfikatora oraz hasła powinien je zapamiętać. Nie wolno ich zapisywać w miejscach, które umożliwiłyby osobom trzecim zapoznanie się z nimi.
8. W przypadku, gdy dane osobowe przetwarzane są w programach typu Office na pojedynczym komputerze, użytkownik danych osobowych zobowiązany jest zabezpieczyć plik hasłem.

Rozdział III.
PROCEDURY ROZPOCZĘCIA I ZAKOŃCZENIA PRACY PRZY KOMPUTERZE

§ 8.

1. Przed rozpoczęciem pracy użytkownik powinien sprawdzić, czy stan sprzętu komputerowego nie wskazuje na próbę uruchomienia komputera przez osobę niepowołaną.
2. Użytkownicy uzyskują bezpośredni dostęp do danych w aplikacji po podaniu identyfikatora i właściwego hasła.
3. Kończąc pracę użytkownik powinien:
   1) wykonać kopię awaryjną (zapasową),
   2) zamknąć program oraz wyjść z systemu i wyłączyć komputer wraz z drukarką,
   3) sprawdzić, czy pozostawione stanowisko nie stwarza jakichkolwiek zagrożeń i czy są prawidłowo zabezpieczone przed uruchomieniem ich przez osoby postronne.
   4) sprawdzić czy w napędach komputera nie pozostały nośniki zawierające dokumenty lub informacje zawierające dane osobowe, niejawne lub inne do których wgląd modą mieć jedynie wybrani pracownicy urzędu.

4. Wszystkie zauważone usterki i mankamenty na stanowisku użytkownik winien natychmiast zgłosić bezpośredniemu przełożonemu, odpowiednim służbom konserwacyjnym oraz Administratorowi Bezpieczeństwa Informacji.

§ 9.

1. W przypadku stwierdzenia przez użytkownika danych osobowych naruszenia zabezpieczeń
   systemu informatycznego, na które mogą wskazywać:
   1) stan stacji roboczej (problemy z uruchomieniem, rozkręcona obudowa),

2) różnice w funkcjonowaniu systemu (np. komunikaty informujące o błędach, brak dostępu do funkcji programu, nieprawidłowości w wykonywanych opcjach),
3) różnica w zawartości zbioru danych osobowych (np. brak lub nadmiar danych), jest on zobowiązany niezwłocznie powiadomić o tym bezpośredniego przełożonego oraz Administratora Bezpieczeństwa Informacji, a w przypadku ich nieobecności - bezpośrednio Administratora Danych Osobowych.

2. Administrator Bezpieczeństwa Informacji lub inna upoważniona przez niego osoba powinna
w pierwszej kolejności:
1) zapisać wszelkie informacje związane z danym zdarzeniem, a w szczególności dokładny czas uzyskania informacji o naruszeniu zabezpieczenia danych osobowych i czas samodzielnego wykrycia tego faktu,
2) na bieżąco wygenerować i wydrukować (jeżeli zasoby systemu na to pozwalają) wszystkie możliwe dokumenty i raporty, które mogą pomóc w ustaleniu okoliczności zdarzenia, opatrzyć je datą i podpisem,
3) przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, zwłaszcza do określenia skali zniszczeń i metody dostępu do danych osoby niepowołanej,
4) niezwłocznie podjąć odpowiednie kroki w celu powstrzymania lub ograniczenia dostępu do danych osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów jej ingerencji,
5) przywrócić normalny stan działania systemu.

3. Po wyeliminowaniu bezpośredniego zagrożenia Administrator Bezpieczeństwa Informacji ma obowiązek przeprowadzić analizę stanu systemu informatycznego, a w szczególności
sprawdzić:
1) stan urządzeń wykorzystywanych do przetwarzania danych osobowych,
2) zawartość zbioru danych osobowych,
3) sposób działania programu,
4) jakość komunikacji w sieci telekomunikacyjnej,
5) obecność wirusów komputerowych.

Rozdział IV.
METODY I CZĘSTOTLIWOŚĆ TWORZENIA KOPII AWARYJNYCH ORAZ SPOSÓB I CZAS ICH PRZECHOWYWANIA

§10.

1. Dane zgromadzone w pamięciach komputerów powinny być zabezpieczone przed ich utratą przez tworzenie ich kopii awaryjnych w cyklach:

   - codziennym,
   - tygodniowym,
   - miesięcznym.

2. Za archiwizację danych przechowywanych w pamięci komputerów lokalnych odpowiedzialni są użytkownicy danych osobowych. Archiwizacji należy dokonywać w każdym dniu, w którym dokonywane były jakiekolwiek zmiany. Dane powinny być kopiowane na wyznaczony dysk sieciowy, dyskietki 1,44 MB, płyty CD-R lub nośnik USB, a następnie przechowywać je w pomieszczeniu wskazanym przez Lokalnego Administratora Bezpieczeństwa.

3. Za archiwizację danych przechowywanych w pamięci serwerów sieciowych odpowiedzialny jest Administrator Bezpieczeństwa Informacji. W cyklu codziennym należy archiwizować zmiany, a w cyklu tygodniowym całą zawartość baz danych przechowywanych w pamięci serwerów sieciowych. Zarchiwizowane dane należy przechowywać w odpowiednio chronionym i zabezpieczonym pomieszczeniu, poza pomieszczeniem w którym umieszczony jest serwer sieciowy.

4. Kopie zapasowe danych z serwera archiwizowane w cyklu miesięcznym należy przechowywać w odpowiednio zabezpieczonym pomieszczeniu innym niż pomieszczenie w którym przechowywane są dane z cykli codziennych i tygodniowych, poza pomieszczeniem w którym znajduje się serwer. Za archiwizowanie danych z pamięci serwerów w cyklu miesięcznym odpowiedzialny jest Administrator Bezpieczeństwa Informacji.

Rozdział V.
SPOSÓB I CZAS PRZECHOWYWANIA NOŚNIKÓW INFORMACJI

§ 11.

1. Nośniki informatyczne, wydruki zawierające dane osobowe oraz kopie awaryjne, o których mowa w § 10 ust. 2-4, przechowywać należy w wyznaczonych pomieszczeniach, w zamkniętych szafach.
2. Kopie zapasowe, o których mowa w § 10 ust. 2 i 3 powinny być przechowywane przynajmniej 7 dni.
3. Kopie zapasowe, o których mowa w § 10 ust. 4 winny być przechowywane przynajmniej przez 6 miesięcy.
4. Użytkownicy na koniec każdego okresu, o którym mowa w ust. 2 i 3, winni dokonać analizy przydatności kopii awaryjnych.
5. Za wydruki zawierające dane osobowe odpowiedzialni są użytkownicy danych osobowych, którzy je wykonali. Wydruki te winny być przechowywane zgodnie z terminami określonymi w instrukcji kancelaryjnej dla urzędów gmin.
6. Każdy użytkownik ma obowiązek pozbawiania zapisu danych osobowych z nośników, które przeznaczane są do przekazania innemu podmiotowi, nieuprawnionemu do otrzymania tych danych oraz do pozbawiania zapisu danych osobowych lub uszkadzanie w sposób uniemożliwiający odczytanie nośników, które przeznaczone są do likwidacji.

Rozdział VI.
DOKONYWANIE PRZEGLĄDÓW I KONSERWACJI SYSTEMU I ZBIORU DANYCH OSOBOWYCH

§ 12.

1. Raz na kwartał Administrator Bezpieczeństwa Informacji lub wyznaczona przez niego osoba, dokonuje przeglądu i konserwacji systemu informatycznego i zbioru danych osobowych.
2. W przypadku konieczności oddania sprzętu zawierającego dane osobowe do naprawy na zewnątrz, Administrator Bezpieczeństwa Informacji zobowiązany jest do usunięcia zapisanych danych. W przypadku gdy nie można tych danych usunąć, naprawa sprzętu winna być dokonywana pod nadzorem Administratora Bezpieczeństwa Informacji.

Rozdział VII.
SPOSÓB POSTĘPOWANIA W ZAKRESIE ZWIĘKSZENIA BEZPIECZEŃSTWA SIECI KOM PU TEROWEJ

§ 13.

1. Ogranicza się w Urzędzie obieg dyskietek i innych nośników informatycznych poprzez ich ostemplowanie pieczęcią Urzędu Gminy Świerzno.
2. Wprowadza się zakaz obiegu nośników nie oznakowanych w sposób, o którym mowa w ust. 1, a wszystkie nośniki przychodzące od jednostek zewnętrznych mogą być wykorzystane tylko do jednorazowego odczytu z nich danych po uprzednim sprawdzeniu programem antywirusowym u informatyków Urzędu.

§ 14.

Systemy do przetwarzania danych osobowych są zabezpieczone przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu, przez odpowiednie oprogramowanie.

§ 15.

Zabrania się:

1) udostępniania stanowisk roboczych oraz istniejących na nich danych (w postaci elektronicznej jak i wydruków) osobom nieupoważnionym,
2) wykorzystywania sieci komputerowej w celach innych niż służbowych,
3) samowolnego instalowania i używania programów komputerowych (posiadających lub nie posiadających licencji),
4) trwałego lub czasowego kopiowania programów komputerowych w całości lub w części jakimikolwiek środkami i w jakiejkolwiek formie,
5) publicznego rozpowszechniania programów komputerowych lub ich kopii,
6) przenoszenia programów komputerowych z własnego stanowiska roboczego na inne stanowisko,
7) udostępniania osobom postronnym programów komputerowych i danych przez możliwość dostępu do zasobów sieci wewnętrznej lub Internetu,
8) wykorzystywania oprogramowania lub materiałów ściąganych z Internetu do masowego rozpowszechniania bez wyraźnego upoważnienia Administratora Bezpieczeństwa Informacji,
9) używania prywatnych skrzynek mailowych działających na innych serwerach niż urzędowy bez uzgodnienia z Administratorem Bezpieczeństwa Informacji,

10) uruchamiania programów otrzymanych pocztą elektroniczną oraz odczytywania listów o wątpliwej treści,
11) kopiowania całości lub części baz danych zawierających dane osobowe na jakichkolwiek nośnikach bez zgody Administratora Danych Osobowych.

Załącznik nr 2 do
Zarządzenia Nr SK – 0050.29.2012
Wójta Gminy Świerzno
z dnia 2 kwietnia 2012 r.

POLITYKA BEZPIECZEŃSTWA

w Urzędzie Gminy w Świerznie

Marzec 2012

Spis treści

5.2. Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe

5.3. Postępowanie w przypadku naruszenia ochrony danych osobowych

5.4. Postępowanie w przypadku naruszenia bezpieczeństwa danych osobowych

Niniejszy dokument opisuje reguły dotyczące bezpieczeństwa danych osobowych Urzędzie Gminy w Świerznie. Opisane reguły określają granice dopuszczalnego zachowania wszystkich użytkowników systemów informatycznych wspomagających pracę w Urzędzie Gminy w Świerznie. Dokument zwraca uwagę na konsekwencje, jakie mogą ponosić osoby przekraczające określone granice oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń. Odpowiednie zabezpieczenia, ochrona przetwarzanych danych oraz niezawodność funkcjonowania są podstawowymi wymogami stawianymi współczesnym systemom informatycznym. „Polityka bezpieczeństwa" wskazuje sposób postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych, przeznaczona jest dla osób przetwarzających dane osobowe, zatrudnionych w Urzędzie Gminy w Świerznie oraz odbywających staż Urzędzie Gminy w Świerznie .

Obowiązek opracowania w formie pisemnej i wdrożenia polityki bezpieczeństwa wynika z § 3 i § 4 *rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100 poz. 1024).* Pojęcie „Polityka bezpieczeństwa" w tym przypadku należy rozumieć jako zbiór spójnych, precyzyjnych i zgodnych z obowiązującym prawem przepisów, reguł i procedur, według których dana organizacja buduje, zarządza oraz udostępnia zasoby i systemy informacyjne i informatyczne. Określa ona, które zasoby mają być chronione i w jaki sposób. Zgodnie z art. 36 ust. 2 oraz art. 39a *ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. 2002 r. Nr 101 poz. 926; z póź. Zmianami)*, polityka bezpieczeństwa, o której mowa w rozporządzeniu powinna odnosić się całościowo do problemu zabezpieczenia danych osobowych u Administratora Danych tj. zarówno do zabezpieczenia danych przetwarzanych tradycyjnie, jak i danych przetwarzanych w systemach informatycznych.

Celem Polityki Bezpieczeństwa jest stworzenie podstawy dla metod zarządzania, procedur i wymagań niezbędnych dla zapewnienia w Urzędzie Gminy w Świerznie właściwej ochrony informacji. Polityka Bezpieczeństwa określa podstawowe zasady ochrony informacji, niezależnie od systemów ich przetwarzania (informatyczny, papierowy) oraz sposobu ich przetwarzania w tych systemach. Obejmuje bezpieczeństwo fizyczne, logiczne i komunikacji przetwarzanych informacji. Swoim zasięgiem obejmuje zarówno sprzęt i oprogramowanie, za pomocą których informacje są przetwarzane, jak i ludzi, którzy te informacje przetwarzają.

Celem zabezpieczania systemów informatycznych jest uniemożliwienie nieautoryzowanego dostępu do danych osobowych gromadzonych i przetwarzanych w Urzędzie Gminy w Świerznie zgodnie z obowiązującym w Polsce prawem, nakładającym na Urząd Gminy w Świerznie określone obowiązki.

Postanowienia ogólne:

1. „Polityka bezpieczeństwa" określa tryb postępowania w przypadku, gdy stwierdzono naruszenie zabezpieczenia systemu informatycznego oraz gdy stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji sieci informatycznej mogą wskazywać lub sugerować naruszenie zabezpieczeń tych danych.
2. „Polityka bezpieczeństwa" obowiązuje wszystkich pracowników Urzędu Gminy w Świerznie oraz osoby odbywające staż Urzędzie Gminy w Świerznie.
3. Wykonywanie postanowień tego dokumentu ma zapewnić właściwą reakcję, ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa systemów oraz zapewnić właściwy tryb działania w celu przywrócenia bezpieczeństwa danych przetwarzanych w systemach informatycznych Urzędu Gminy w Świerznie.
4. Administrator Danych, swoją decyzją wyznacza „Administratora Bezpieczeństwa Informacji", nadzorującego przestrzeganie zasad ochrony przetwarzanych danych osobowych.
5. Administrator Bezpieczeństwa Informacji realizuje zadania w zakresie ochrony danych, a w szczególności:
   - ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach Urzędu Gminy w Świerznie;
   - podejmowania stosownych działań zgodnie z niniejszą „Polityką bezpieczeństwa" w przypadku wykrycia nieuprawnionego dostępu do danych osobowych lub naruszenia zabezpieczenia tych danych;
   - niezwłocznego informowania Administratora Danych o przypadkach naruszenia przepisów ustawy o ochronie danych osobowych;
   - nadzoru i kontroli systemów informatycznych służących do przetwarzania danych osobowych i użytkowników.
6. Osoba zastępująca Administratora Bezpieczeństwa Informacji powyższe zadania realizuje tylko w przypadku jego nieobecności,
7. Osoba zastępująca, składa Administratorowi Bezpieczeństwa Informacji relacje z podejmowanych działań w czasie jego zastępstwa.

Słownik:

Ilekroć w niniejszej dokumencie jest mowa o:

1. **Zbiorze danych osobowych** - rozumie się przez to „Listę osób klientów UG" oraz „Listę pracowników"
2. **Przetwarzaniu danych osobowych** - rozumie się przez to jakąkolwiek operację wykonywaną na danych osobowych, takie jak zbieranie, utrwalanie, przetwarzanie, opracowywanie, zmienianie, udostępnianie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
3. **Systemie informatycznym** - rozumie się przez to zespół współpracujących ze sobą urządzeń programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
4. **Administratorze Danych** – rozumie się przez to Wójta Urzędu Gminy w Świerznie,
5. **ABI** - rozumie się przez to Administratora Bezpieczeństwa Informacji,
6. **ASI** - rozumie się przez to Administratora Systemu Informatycznego,
7. **Użytkowniku** - rozumie się przez to użytkownika systemu, pracownika Urzędu Gminy w Świerznie oraz osobę odbywająca staż, przetwarzającą dane osobowe,
8. **UG** - rozumie się przez to Urząd Gminy w Świerznie.

Podstawa prawna:

Podstawę prawną do niniejszej instrukcji stanowią:

a) *Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz.U. 2002 r. Nr 101, poz. 926, z późn. zmianami)*

b) *Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100 poz. 1024),*

c) *Ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. Nr 196, poz. 1631 z późn. zmianami),*

d) *Rozporządzenie Prezesa Rady Ministrów z dnia 25 sierpnia 2005 roku w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych (Dz. U. Nr 171, poz. 1433).*

1. **Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe.**

Dane osobowe z użyciem stacjonarnego sprzętu komputerowego przetwarzane są w budynku Urzędu Gminy w Świerznie, Świerzno 13, 72-405 Świerzno – parter, I piętro.

Wykaz pomieszczeń Urzędu Gminy w Świerznie, w których przetwarzane są dane osobowe

Nr pokoju	Referat/Stanowisko	Lokalizacja
Archiwum	Referat Księgowości – Archiwum Urzędu Gminy	I piętro
2	Urząd Stanu Cywilnego	Parter
3	Stanowisko d/s Gospodarki Przestrzennej	Parter
3	Stanowisko d/s Gospodarki Gruntami	Parter
4	Referat Księgowości	I piętro
4	Stanowisko d/s Obsługi Rady Gminy i jej organów, Kadr, Ochrony Zdrowia i Oświaty	I piętro
5	Referat Księgowości	I piętro
6	Sekretariat, Stanowisko d/s Ewidencji Działalności Gospodarczej	I piętro
6	Skarbnik	I piętro
8	Stanowisko ds. obywatelskich, Zarządzania kryzysowego, Spraw Obronnych i Obrony Cywilnej, Pełnomocnik d/s Ochrony Informacji Niejawnych	I piętro

Przebywanie osób nieuprawnionych do dostępu do danych osobowych w pomieszczeniach znajdujących się wewnątrz ww. obszaru jest dopuszczalne tylko w obecności użytkownika.

Pomieszczenia, w których przetwarzane są dane osobowe zamykane są na czas nieobecności w nich użytkowników, w sposób uniemożliwiający dostęp do nich osób trzecich.

Określenie miejsc przechowywania nośników informacji zawierających dane osobowe:

- Szafy z dokumentacją papierową i stacje komputerowe zlokalizowane są w poszczególnych pokojach.

- Serwer oraz szafa metalowa z sejfem, w której przechowywane są dyskietki oraz kopie na płytach CD i DVD i taśmach znajdują się na I Piętrze.
- Uszkodzone komputerowe nośniki danych (dyski twarde, dyskietki, taśmy, płyty CD itp.) składowane są na I pietrze.

2. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.

Budynek: Urzędu Gminy w Świerznie 72-405 Świerzno 13

Nazwa zbioru danych osobowych	**Program do przetwarzania**	**Pokój**	**Uwagi**
podatnicy	Podatki	4	
pracownicy	Płace	5	
	Płatnik 8	5	
	Home Banking BS	5	
USC	USC	2	
Ewidencja Gruntów	Geoinfo	3, 4	
Ewidencja Działalności Gospodarczej	EDG	6, 4	
Zezwolenia na alkohol	MS WORD - zezwolenia na alkohol	6	
Usługi hotelarskie	MS WORD – usługi hotelarskie	6	
Oświata	SIO	4	
Kadry	MS WORD - Kadry	4	
Rada Gminy	MS WORD – rada Gminy	4	
Ewidencja psów	INDEXEL	4	
Faktury	FK	5, 6	
Ewidencja ludności	CLANET – Ewidencja Ludności	8	
Baza PESEL	CLANET – PESEL	8	
Dowody Osobiste	Dowody Osobiste	8	
Kwalifikacja wojskowa	MS WORD - kwalifikacja wojskowa	8	

Tabela 1.

Dane osobowe ze zbioru o nazwie „Lista osób klientów UG" przetwarzane są w Systemie Informatycznym .

Zbiór danych przetwarzanych w aplikacjach: Płatnik 8 i Home Banking dotyczy tych samych osób, a aplikacje te korzystają z importu plików wygenerowanych w aplikacji

MODUŁ Płace		**PLIK**		**APLIKACJA do której importuje się PLIK**
→	Eksport	Dokumenty zgłoszeniowe ZUS (pliki *.kdu)	Import	Płatnik 8
→		Dokumenty rozliczeniowe ZUS (pliki *.kdu)		Płatnik 8
→		Dokumenty rozliczeniowe Pracowników ZUS (pliki *.kdu)		Płatnik 8
→		Przelewy i przekazy (pliki *.*)		Home Banking

W aplikacjach tych dane przenoszone są pomiędzy systemami półautomatycznie – przy wykorzystaniu funkcji eksportu/importu danych – wykonywanych w określonych odstępach czasowych.

Dane z aplikacji Płatnik przekazywane są do ZUS za pośrednictwem Internetu (automatyczna wysyłka).

Dane z aplikacji Home Banking przekazywane są do banku BS za pośrednictwem Internetu.

Do transmisji danych osobowych do ZUS wykorzystuje się identyfikator, hasło, klucz publiczny i prywatny.

Do transmisji danych osobowych do banku BS każdy dokument podpisywany jest elektronicznie dwa razy (Skarbnik i Wójt Gminy lub osoby upoważnione).

3. Opis struktury zbiorów danych osobowych przechowywanych w systemach informatycznych oraz sposób przepływu danych pomiędzy systemami informatycznymi

Opis struktury zbiorów danych osobowych.

Z uwagi na objętość informacji zawartych w opisach struktury danych przechowywanych w eksploatowanych systemach informatycznych i programach Administrator Danych Osobowych w Urzędzie Gminy w Świerznie dopuszcza możliwość przechowywania opisów struktur danych w postaci dokumentów elektronicznych. Dokumenty te są każdorazowo częścią dokumentacji technicznej i użytkowej przygotowanej przez producentów eksploatowanych systemów informatycznych i programów oraz są w każdym momencie dostępne w postaci elektronicznej.

Administrator Danych Osobowych przy każdorazowej aktualizacji eksploatowanych systemów informatycznych i programów ma obowiązek sprawdzić, czy nie zaszły zmiany w strukturze danych osobowych oraz zweryfikować opis struktury danych pod względem zgodności ze stanem aktualnym.

Sposób przepływu informacji pomiędzy systemami informatycznymi.

Dane osobowe podatników, obecnych i byłych pracowników oraz pozostałych współpracowników Urzędu Gminy w Świerznie przetwarzane są w programach wyszczególnionych w tabeli 1 Polityki Bezpieczeństwa.

Dostęp do programów oraz funkcjonalności realizowana jest za pomocą identyfikatorów, haseł i uprawnień. Funkcjonalność programów opisana jest w dokumentacji użytkowej wykonanej przez producenta systemu.

Kadry umożliwia wymianę danych z innymi programami informatycznymi poprzez wbudowane, przez producenta systemu, mechanizmy wymiany danych.

a) jednostronną wymianę danych z programem Płatnik w postaci generowanego stosownie do wymogów i potrzeb zestawu danych wymaganych przez Zakład Ubezpieczeń Społecznych dla realizacji wymogów dotyczących ubezpieczenia społecznego i zdrowotnego. Dane te mają ściśle określoną strukturę i są zapisywane w sposób jawny, wyłącznie na urządzeniach i nośnikach danych podlegających zabezpieczeniu przed nieuprawnionym dostępem osób nieupoważnionych.

b) jednostronną wymianę danych z programem Home Banking w postaci generowanego stosownie do wymogów i potrzeb zestawu danych wymaganych przez Bank Spółdzielczy dla poprawnej realizacji zleconych operacji finansowych. Dane te mają ściśle określoną strukturę i są zapisywane w sposób jawny, wyłącznie na urządzeniach i nośnikach danych podlegających zabezpieczeniu przed nieuprawnionym dostępem osób nieupoważnionych.

Program Płatnik umożliwia wymianę danych z systemem informatycznym Zakładu Ubezpieczeń Społecznych poprzez wbudowane, przez producenta systemu, mechanizmy wymiany danych. Mechanizmy te obejmują:

a) transmisję przetworzonych informacji do rozproszonego systemu informatycznego Zakładu Ubezpieczeń Społecznych. Transmitowane dane zawierają informacje przedstawione w sposób niejawny, możliwe do odczytania wyłącznie w systemie, do którego transmisja została wysłana.

b) informacje zwrotne odbierane drogą teletransmisji z rozproszonego systemu informatycznego Zakładu Ubezpieczeń Społecznych. Transmitowane dane zawierają informacje przedstawione w sposób niejawny, możliwe do odczytania wyłącznie w systemie, do którego transmisja została wysłana.

Program Home Banking umożliwia wymianę danych z innymi systemami informatycznymi i programami poprzez wbudowane, przez producenta systemu, mechanizmy wymiany danych. Dostęp do programu realizowany jest za pomocą identyfikatorów i haseł.

Mechanizmy te obejmują:

a) transmisję przetworzonych informacji do systemu informatycznego Banku Spółdzielczego. Transmitowane dane zawierają informacje przedstawione w sposób niejawny, możliwe do odczytania wyłącznie w systemie, do którego transmisja została wysłana.

b) informacje zwrotne odbierane drogą teletransmisji z systemu informatycznego Banku Spółdzielczego. Transmitowane dane zawierają informacje przedstawione w sposób niejawny, możliwe do odczytania wyłącznie w systemie, do którego transmisja została wysłana.

Program Dowody Osobiste umożliwia wymianę danych z systemem informatycznym MSWiA poprzez wbudowane, przez producenta systemu, mechanizmy wymiany danych.

Dostęp do programu realizowany jest za pomocą identyfikatorów i haseł, kart dostępowych.

Mechanizmy te obejmują:

a) transmisję przetworzonych informacji do rozproszonego systemu informatycznego MSWiA. Transmitowane dane zawierają informacje przedstawione w sposób niejawny, możliwe do odczytania wyłącznie w systemie, do którego transmisja została wysłana.

4. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

4.1. Pojęcie zabezpieczeń danych osobowych

Zabezpieczenia to praktyki, procedury i mechanizmy zmniejszające ryzyko, chroniące przed zagrożeniami, zmniejszające podatność aktywów, ograniczające następstwa, wykrywające niepożądane incydenty i ułatwiające odtwarzanie prawidłowego stanu systemu. Efektywna ochrona wymaga zwykle kombinacji różnych zabezpieczeń w celu utworzenia właściwej ochrony dla zasobów systemu informatycznego. Zabezpieczenie systemu oraz ochrona zawartych w nich danych zależy od jednoczesnego spełnienia wszystkich warunków dotyczących organizacji pracy, kwestii kadrowych, zabezpieczenia fizycznego obiektów i pomieszczeń, prawidłowej eksploatacji platformy sprzętowej oraz stosowanego oprogramowania użytkowego.

4.2. Obowiązki Administratora Danych

Administrator Danych osobowych jest zobowiązany do zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych w systemach informatycznych UG, a w szczególności:

a) zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym;
b) zapobieganie przetwarzaniu danych z naruszeniem ustawy oraz zmianie, utracie, uszkodzeniu lub zniszczeniu tych danych.

4.3. Sposoby zabezpieczeń organizacyjnych przed dostępem do danych osób nieuprawnionych

Celem wprowadzonych niniejszą Polityką bezpieczeństwa zabezpieczeń i obostrzeń jest ochrona danych osobowych zawartych w eksploatowanym systemie informatycznym oraz ochrona dokumentów papierowych zawierających dane osobowe. Określone niżej sposoby zabezpieczeń dotyczą:

- zabezpieczeń przed nieautoryzowanym dostępem do baz danych Urzędu Gminy w Świerznie ;
- zabezpieczeń przed nieautoryzowanym dostępem do baz danych Urzędu Gminy w Świerznie poprzez Internet;
- ochrony danych zarchiwizowanych na nośnikach zewnętrznych;
- systemu zabezpieczeń stacji roboczych przed zanikiem (wahaniami) zasilania;
- opracowania i wdrożenia programu szkoleń w zakresie zabezpieczeń systemu informatycznego;
- monitoringu i kontroli przestrzegania zasad zabezpieczenia danych osobowych;
- systemu zabezpieczeń organizacyjnych przed dostępem do danych, osób niepowołanych.

4.3.1. Zabezpieczenia przed nieautoryzowanym dostępem do baz danych Urzędu Gminy w Świerznie

- aby uzyskać dostęp do zasobów sieci należy zwrócić się do Administratora Danych w celu podania wszystkich danych niezbędnych do nadania uprawnień w odpowiednim programie przechowującym bazę danych;
- w systemie informatycznym UG zastosowano potrójną autoryzację użytkownika. Pierwsza autoryzacja dokonuje się w momencie uzyskania dostępu do BIOS podając hasło. Druga autoryzacja następuje po uruchomieniu systemu operacyjnego oraz po podaniu poprawnego loginu i hasła, trzecia po uruchomieniu programu oraz po podaniu poprawnego loginu i hasła.

4.3.2. Zabezpieczenia przed nieautoryzowanym dostępem do baz danych Urzędu Gminy w Świerznie poprzez Internet

- w zakresie dostępu do sieci wewnętrznej Urzędu Gminy w Świerznie z rozległej sieci Internet zastosowano router programowy z firewallem, oraz router mikrotik, umożliwiający konfigurację określonych portów (dla protokołów TCP i UDP) oraz filtrowanie URL;
- zablokowano nieużywane porty celem zmniejszenia potencjalnych luk, które mogą być wykorzystane przez osobę próbującą uzyskać nieautoryzowany dostęp do sieci wewnętrznej;
- do ochrony antywirusowej stosuje się oprogramowanie antywirusowe dostępne w Internecie (skanery on-line) oraz program antywirusowy;

- dane osobowe przesyłane pocztą internetową są każdorazowo szyfrowane (SSL) – przeznaczone do konkretnej jednostki i tylko dla niej możliwe do wykorzystania;
- przesyły tworzone poprzez eksport danych z programów z bazą danych są szyfrowane. Mogą być zaimportowane tylko w identycznych programach lub aplikacjach do tego przeznaczonych w jednostce, którą wskazano podczas tworzenia przesyłu.

4.3.3. Ochrona danych zarchiwizowanych na nośnikach zewnętrznych oraz w formie papierowej

- fizyczny dostęp do pomieszczeń, w których przetwarzane są dane osobowe blokują drzwi, a cały budynek UG zabezpieczony jest przez system alarmowy;
- kopie bazy danych, w przypadku awarii umożliwiających odtworzenie danych, przechowywane są na nośnikach magazynu masowego w szafie pancernej, zabezpieczonej drzwiami antywłamaniowymi oraz wyposażonej w alarm;
- kopię bazy danych Płatnik, kopię bazy danych Home Banking, kopię systemu bazy danych Ewidencja Ludności, USC, Podatki, Kadry, FK, EDG przechowuje się na Dyskach przeznaczonych dla kopii zapasowych;
- nośniki zawierające kopie bazy danych po utracie ich przydatności są formatowane w taki sposób aby nie można było odtworzyć ich zawartości lub niszczone trwale w sposób mechaniczny;
- kopiowanie danych osobowych na nośniki informacji oraz robienie wydruków jest zabronione, chyba, że istnieje konieczność ich sporządzenia, która wynika z nałożonych na użytkownika obowiązków i jest dozwolona przepisami prawa, wykorzystanie nośników informacji lub wydruków w innym celu jest zabronione;
- okresową weryfikację kopii baz danych i innych danych pod kątem ich przydatności do odtworzenia danych wykonuje ASI;
- w pomieszczeniach z komputerami i innymi urządzeniami znajduje się gaśnica proszkowa, która jest okresowo kontrolowana i legalizowana.

4.3.4. Podstawowe zasady bezpieczeństwa dla dokumentów (nośników) papierowych

- dokumenty papierowe zawierające dane osobowe należy chronić przed ich fizycznym uszkodzeniem lub zniszczeniem, które uniemożliwiałoby odczytanie lub odzyskanie informacji na nich zawartych;

- dokumenty zawierające dane osobowe powinny być fizycznie ochronione przed ich utratą oraz dostępem osób nieupoważnionych, wychodząc z budynku UG należy dokładnie sprawdzić czy są one schowane w odpowiednich meblach i pomieszczeniach zamykanych na klucz;
- każdy dokument papierowy zawierający informacje chronione, sporządzony jako dokument roboczy, należy najpóźniej na koniec dnia pracy zniszczyć w niszczarce do papieru lub zamknąć w bezpiecznym miejscu uniemożliwiającym dostęp osób nieupoważnionych;
- kserokopie dokumentów zawierających dane osobowe powinny być niezwłocznie zabierane z urządzeń kserujących, skanujących, drukujących itp.;
- dokumenty wpływające, w tym zawierające również dane osobowe rejestrowane są w dzienniku korespondencji;
- pracownik lub upoważniona osoba pobierający dokument kwituje pobranie dokumentu własnoręcznym podpisem w odpowiedniej rubryce w dzienniku korespondencji i od tej chwili jest odpowiedzialny za ochronę dokumentu przed zniszczeniem, uszkodzeniem i ujawnieniem informacji w nim zawartych osobom nieupoważnionym;
- utrata dokumentu papierowego powinna być natychmiast zgłoszona bezpośredniemu przełożonemu.

Do pomieszczeń, w których następuje przetwarzanie danych osobowych mają dostęp tylko użytkownicy. Przebywanie osób nieuprawnionych do dostępu do danych osobowych wewnątrz obszaru przetwarzania danych osobowych jest dopuszczalne tylko w obecności pracownika UG. Po godzinach urzędowania i w przypadku nieobecności pracownika UG pomieszczenia te są zamykane na klucz.

4.3.5. System zabezpieczeń serwerów przed zanikiem (wahaniami) zasilania

- ochronę stacji roboczych przed zanikiem (wahaniami) zasilania zapewniają zasilacze UPS.

4.3.6. Opracowanie i wdrożenie programu szkoleń w zakresie zabezpieczeń systemu informatycznego

System szkoleń obejmuje nowozatrudnionych pracowników UG a także osób odbywających staż w UG, przed dopuszczeniem do przetwarzania danych osobowych.

Szkolenia dokonuje ASI w porozumieniu z ABI.

Tematyka szkoleń obejmuje: przepisy i instrukcje wewnętrzne dotyczące ochrony danych archiwizacji zasobów i przechowywania nośników informacji, niszczenia wydruków i zapisów na nośnikach magnetycznych i optycznych, zakresy obowiązków pracowników związanych bezpośrednio z bezpieczeństwem danych i ochrona systemów na poszczególnych stanowiskach.
Szkolenie kończy się wydaniem zaświadczenia zgodnie z wzorem stanowiącym załącznik nr 1 do niniejszej Polityki bezpieczeństwa.

4.3.7. Monitoring i kontrola przestrzegania zasad zabezpieczenia danych osobowych

Administrator Danych lub osoba przez niego wyznaczona sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych wynikających z ustawy o ochronie danych osobowych oraz zasad ustanowionych w niniejszym dokumencie oraz zastrzega sobie prawo kontroli stanu bezpieczeństwa danych osobowych. Komputery umiejscowione w UG podlegają monitoringowi.

4.3.8. System zabezpieczeń organizacyjnych przed dostępem do danych osób niepowołanych

Zabezpieczenie przed nieuprawnionym dostępem do danych, prowadzone jest przez ABI, zgodnie z przyjętymi procedurami nadawania uprawnień do systemu informatycznego.

Do zastosowanych środków organizacyjnych należą:
- zapoznanie każdej osoby zatrudnionej w UG lub odbywającej w UG staż, z przepisami dotyczącymi ochrony danych osobowych oraz przepisami o odpowiedzialności karnej za przestępstwa przeciwko ochronie informacji, przed dopuszczeniem jej do pracy przy przetwarzaniu danych osobowych;
- użytkownicy - pracownicy odchodzący z pracy albo osoba kończąca staż składa zobowiązanie o nie ujawnianiu danych osobowych, objętych ochroną, z którymi zapoznał się podczas pracy, odbywania stażu w UG, zgodnie z wzorem oświadczenia stanowiącym załącznik nr 2 do niniejszej Polityki bezpieczeństwa;
- użytkownicy mają obowiązek chronienia swoich haseł dostępowych do systemu przed osobami nieupoważnionymi.

- zagadnienia związane z ochroną danych osobowych i obowiązki stąd wynikające są ujęte w zakresach czynności pracowników, zgodnie z wzorem oświadczenia stanowiącym załącznik nr 3 do niniejszej Polityki bezpieczeństwa;
- zapoznaje się każdego z użytkowników z zasadami pracy oprogramowania oraz podpisuje się z pracownikami stosowne porozumienia określające odpowiedzialność osób zatrudnionych w zakresie przestrzegania ustalonych w Urzędzie procedur dotyczących zasad używania oprogramowania, zgodnie z wzorem oświadczenia stanowiącym załącznik nr 4 do niniejszej Polityki bezpieczeństwa;
- stosuje się system odpowiedniego zamykania pomieszczeń na klucz, w których są przetwarzane dane osobowe, przez ostatnią wychodzącą z niego osobą i przekazania klucza do miejsca gdzie są przechowywane dane klucze;
- w pokojach, do których dostęp mają osoby nieupoważnione monitory komputerowe ustawione muszą być w ten sposób, by osoby nieupoważnione nie widziały zapisów na ekranie;
- w przypadku bezczynności komputera trwającej 5 minut uruchamiane są tzw. wygaszacze ekranu.

Niezależnie od niniejszych zasad opisanych w dokumencie „Polityka bezpieczeństwa" w zakresie bezpieczeństwa mają zastosowanie wszelkie wewnętrzne regulaminy lub instrukcje dotyczące bezpieczeństwa ludzi i zasobów informacyjnych oraz indywidualne zakresy zadań osób zatrudnionych przy przetwarzaniu danych osobowych w określonym systemie.
Pomieszczenia w których przetwarzane są dane osobowe oraz spis systemów informatycznych UG i ich zabezpieczenia opisane są w rozdziale I niniejszego dokumentu.

5. Naruszenie ochrony danych osobowych

5.1. Opis zdarzeń naruszających ochronę danych osobowych

Zagrożenie to potencjalna przyczyna niepożądanego incydentu, którego skutkiem może być szkoda dla systemu informatycznego lub urzędu. Każda sytuacja, która powoduje niedostępność danych (czasowe lub trwałe uniemożliwienie przetwarzania zbiorów danych), ich niekontrolowany wypływ, ujawnienie czy utratę lub przekłamanie – jest zagrożeniem systemu, niezależnie od tego czy jest to celowy sabotaż, czy przypadkowe zdarzenie

Wyróżnia się następujące rodzaje zagrożeń:

- **zagrożenia losowe zewnętrzne** (np. klęski żywiołowe, przerwy w zasilaniu); ich wystąpienie może prowadzić do utraty integralności danych, ich zniszczenia, a także uszkodzenia infrastruktury technicznej systemu; ciągłość systemu zostaje zakłócona, ale nie dochodzi zazwyczaj do naruszenia poufności danych;
- **zagrożenia losowe wewnętrzne** (np. niezamierzone pomyłki operatorów, ASI, awarie sprzętowe, błędy oprogramowania); ich wystąpienie również może prowadzić do utraty integralności danych, ich zniszczenia; może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych;
- **zagrożenia zamierzone**, czyli świadome i celowe – jest to najpoważniejszy rodzaj zagrożenia – naruszenie poufności danych; zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy. Zagrożenia takie możemy podzielić na:
  - nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu);
  - nieuprawniony dostęp do systemu z jego wnętrza;
  - pogorszenie jakości sprzętu i oprogramowania;
  - nieuprawniony przekaz danych;
  - bezpośrednie zagrożenie materialnych składników systemu.

5.2. Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe:

- sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu, jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, niepożądana ingerencja ekipy remontowej, itp.;
- niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie silnego pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych;
- awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym fakt pozostawienia serwisantów bez nadzoru;
- pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu;

- jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenie systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie;
- nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie;
- stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji);
- nastąpiła niedopuszczalna manipulacja danymi osobowymi w systemie;
- ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń, np. login użytkownika i jego hasło;
- praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych – np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.;
- ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. „bocznej furtki", itp.;
- podmieniono, lub zniszczono nośniki z danymi osobowymi bez odpowiedniego upoważnienia lub w inny niedozwolony sposób skasowano lub skopiowano dane osobowe;
- rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowano się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, w skanerze nie zamkniecie pomieszczenia z komputerem, prace na danych osobowych w celach prywatnych, itp.);
- wyniesiono poza teren UG danych osobowych zapisanych na nośnikach danych: dyskietki 1,44, płyty CD-R, DVD, taśmy Streamer, pendrive, zewnętrzne dyski twarde, laptopy.

Za naruszenie ochrony uważa się również stwierdzone nieprawidłowości w zakresie bezpieczeństwa miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, dyskietkach w formie niezabezpieczonej, itp.).

5.3. Postępowanie w przypadku naruszenia ochrony danych osobowych

Każda informacja o naruszeniu systemu bezpieczeństwa, pochodząca z któregokolwiek źródła, wymaga od ABI wszczęcia postępowania wyjaśniającego, aby określić:

- czas naruszenia systemu zabezpieczeń;
- charakter;
- miejsce;
- sposób;
- skutki;
- w jaki sposób usunąć i/lub zminimalizować skutki;
- jakie dodatkowe środki należy zastosować w celach profilaktycznych;
- sprawcę i cel, gdy istnieje ku temu możliwość.

Miejscem zagrożenia bezpieczeństwa systemu może być:

- strefa przetwarzania zasobów;
- sprzęt komputerowy i inne urządzenia wykorzystywane do przetwarzania;
- oprogramowanie systemowe, sieciowe i użytkowe;
- zawartość baz danych, rejestrów, ewidencji i innych dokumentów.

5.3.1. Sposób naruszenia bezpieczeństwa danych osobowych

Sposób naruszenia bezpieczeństwa to:

- osłabienie odporności systemu zabezpieczeń, a w szczególności tworzenie potencjalnych zagrożeń dla systemu (np. niezamykanie pomieszczeń i/lub sejfów, pozostawianie dokumentacji i/lub dostępu do aplikacji na opuszczonym stanowisku pracy albo wynoszenie dokumentacji poza chronioną strefę, samowolna instalacja niedozwolonych programów i/lub sprzętu na lokalnych stanowiskach pracy, itp.);
- nieuprawnione „przeglądanie", sporządzanie notatek, wyciągów, raportów, kopii, itp.;
- zmiana zawartości zgromadzonych danych naruszająca ich integralność i/lub wiarygodność;
- usunięcie części danych lub ich uszkodzenie;
- fizycznie zniszczenie zasobów, kradzież sprzętu i/lub oprogramowania;
- przekazywanie zgromadzonych danych osobom nieuprawnionym do ich posiadania.

5.3.2. Postępowanie w przypadku naruszenie bezpieczeństwa danych osobowych

1. W przypadku stwierdzenia naruszenia:
   - zabezpieczenia systemu informatycznego;
   - technicznego stanu urządzeń;
   - zawartości zbioru danych osobowych;
   - ujawnienia metody pracy lub sposobu działania programu;
   - jakości transmisji danych w sieci telekomunikacyjnej mogącej wskazywać na naruszenie zabezpieczeń tych danych;
   - innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. zalanie, pożar, itp.);

   Każdy użytkownik jest obowiązany niezwłocznie powiadomić o tym fakcie ABI. W razie niemożności zawiadomienia ABI lub osoby przez niego upoważnionej, należy powiadomić bezpośredniego przełożonego.
2. Do czasu przybycia na miejsce naruszenia ochrony danych osobowych ABI lub upoważnionej przez niego osoby, należy:
   - niezwłocznie podjąć czynności niezbędne do powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn i sprawców;
   - rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia;
   - zaniechać – o ile to możliwe – dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę;
   - podjąć inne działania przewidziane i określone w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących naruszeniu;
   - podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji użytkowej;
   - zastosować się do innych instrukcji i regulaminów, jeśli odnoszą się one do zaistniałego przypadku;
   - udokumentować wstępnie zaistniałe naruszenie;
   - nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia ABI lub osoby upoważnionej.

3. Po przybyciu na miejsce ujawnienia lub naruszenia ochrony danych osobowych, ABI lub osoba go zastępująca:
   - rozpoznaje zaistniałą sytuację i dokonuje wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy UG;
   - może żądać dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem;
   - rozważa celowość i potrzebę powiadamiania o zaistniałym naruszeniu Administratora Danych;
   - nawiązuje bezpośredni kontakt, jeżeli zachodzi taka potrzeba, ze specjalistami spoza UG.
4. ABI dokumentuje zaistniały przypadek naruszenia oraz sporządza raport, który powinien zawierać w szczególności:
   - wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem;
   - określenie czasu i miejsca naruszenia i powiadomienia;
   - określenie rodzaju naruszenia i okoliczności towarzyszących;
   - wyszczególnienie wziętych pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania;
   - wstępną ocenę przyczyn wystąpienia naruszenia;
   - ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.

   Wzór raportu stanowi załącznik nr 5 do niniejszej Polityki bezpieczeństwa".
5. Raport z naruszenia zasad bezpieczeństwa ABI niezwłocznie przekazuje Administratorowi Danych, a w przypadku jego nieobecności osobie uprawnionej.

Załącznik nr 1
do „Polityki bezpieczeństwa"

ZAŚWIADCZENIE NR .....

Stwierdzające odbycie przeszkolenia w zakresie ochrony danych osobowych

Stwierdza się, że Pan/Pani

Imię i nazwisko: .....

Data urodzenia: .....

Odbył/a przeszkolenie w zakresie ochrony danych osobowych i zabezpieczeń systemu informatycznego służącego do przetwarzania danych osobowych.

Program szkolenia obejmował m.in.:
- przepisy i instrukcje wewnętrzne dotyczące ochrony danych osobowych,
- zasady archiwizacji zasobów i przechowywania nośników informacji,
- zasady niszczenia wydruków i zapisów na nośnikach magnetycznych i optycznych,
- zakresy obowiązków pracowników związanych bezpośrednio z bezpieczeństwem danych i ochrona systemów na poszczególnych stanowiskach.

.....

(data i podpis Administratora Systemu Informatycznego)

.....

(podpis Administratora Bezpieczeństwa Informacji)

Załącznik nr 2
do „Polityki bezpieczeństwa"

.....
Imię i nazwisko

.....
stanowisko

.....
komórka organizacyjna

OŚWIADCZENIE

(wypełnić przy zdawaniu obowiązków)

Stwierdzam własnoręcznym podpisem, że zobowiązuję się nie ujawniać danych osobowych, z którymi zapoznałem się podczas pełnienia obowiązków służbowych w **Urzędzie Gminy w Świerznie.**
Oświadczam, że zostałem poinformowany o odpowiedzialności karnej.

.....
(data i podpis składającego oświadczenie)

.....
(podpis Wójta)

Załącznik nr 3
do „Polityki bezpieczeństwa"

Pan/Pani

.....

Zatrudniony/a w Urzędzie Gminy
w Świerznie

na stanowisku.....

Indywidualny zakres obowiązków nałożonych na użytkownika systemu informatycznego

1. Pracownik zobowiązany jest dbać o bezpieczeństwo powierzonych mu do przetwarzania, archiwizowania lub przechowywania danych zgodnie z obowiązującą w Urzędzie Polityką Bezpieczeństwa, regulaminami i instrukcjami wewnętrznymi, w tym m.in.:
   a) chronić dane osobowe przed dostępem osób nieupoważnionych;
   b) chronić dane osobowe przed przypadkowym lub nieumyślnym zniszczeniem, utratą lub modyfikacją;
   c) chronić nośniki magnetyczne i optyczne oraz wydruki komputerowe przed dostępem osób nieupoważnionych oraz przed przypadkowym zniszczeniem;
   d) utrzymywać w tajemnicy powierzone identyfikatory, hasła, częstotliwość ich zmiany oraz szczegóły technologiczne systemów także po ustaniu zatrudnienia w UG Świerzno.
2. Zabrania się pod rygorem odpowiedzialności służbowej i karnej:
   a) ujawniać dane – w tym dane osobowe zawarte w obsługiwanych systemach;
   b) kopiować bazy danych lub ich części poza przewidzianymi instrukcją technologiczną kopiami bezpieczeństwa;
3. Zobowiązuję się użytkowników w przypadku stwierdzenia fizycznej ingerencji w systemie lub innych podejrzeń dotyczących możliwości naruszenia bezpieczeństwa systemu do niezwłocznego zawiadomienia o tym fakcie ABI.

.....
(Wójt Gminy Świerzno)

.....
(data i podpis pracownika Urzędu Gminy)

Załącznik nr 4

do „Polityki bezpieczeństwa"

POROZUMIENIE

Niniejsze porozumienie (zwane dalej „Porozumieniem") zostało zawarte w dniu ..... r. w ..... pomiędzy:

Urzędem Gminy w Świerznie z siedzibą w Świerznie, 72-405 Świerzno 13, reprezentowanym przez **Wójta Krzysztofa Atrasa**, (zwanym dalej „Pracodawcą"); oraz

Panią/Panem ..... zamieszkałą/ym w.....

przy ul..... (zwaną/ym dalej „Pracownikiem");

Wstęp:

(A) Pracownik zatrudniony jest przez Pracodawcę na podstawie umowy o pracę zawartej w dniu .....r.

(B) Pracodawca wyposażył stanowisko pracy Pracownika w oprogramowanie komputerowe ....., na używanie którego licencję nabył od ..... („Oprogramowanie"). Odpowiednie przepisy regulują w sposób szczegółowy zasady korzystania z Oprogramowania.

(C) Pracownik korzysta z Oprogramowania w związku z wykonywaniem obowiązków pracowniczych.

1. Pracodawca i Pracownik uzgadniają, że do podstawowych obowiązków Pracownika należy korzystanie z Oprogramowania w związku z wykonywaniem obowiązków pracowniczych, zgodnie z obowiązującymi przepisami prawa oraz wyłącznie w celach wykonywania obowiązków pracowniczych jak również nie korzystanie z jakiegokolwiek oprogramowania komputerowego, do używania którego Pracodawca nie jest uprawniony, w czasie pracy, w miejscu pracy ani przy użyciu sprzętu Pracodawcy.
2. Pracownik oświadcza, iż jest świadomy odpowiedzialności karnej o której mowa w artykułach: 278 § 2, 293 w związku z 291 oraz 292 *ustawy z dnia 6 czerwca 1997 r. kodeks karny (tekst jednolity: Dz. U. z 1997 r. Nr 88 poz. 553, ze zmianami)* oraz odpowiedzialności karnej i cywilnej przewidzianej w artykułach 116 i nast. *ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (tekst jednolity: Dz. U. z 2000 r. Nr 80 poz. 904, ze zmianami)* za niezgodne z prawem korzystanie, rozpowszechnianie, utrwalanie, uzyskiwanie lub zwielokrotnianie Oprogramowania.
3. Pracodawca i Pracownik uzgadniają, że naruszenie przez Pracownika jego podstawowych obowiązków pracowniczych w zakresie wskazanym powyżej, może stanowić podstawę do podjęcia przez Pracodawcę przysługujących mu środków prawnych, a w szczególności, może stanowić przyczynę uzasadniającą wypowiedzenie przez Pracodawcę umowy o pracę łączącej Pracodawcę z Pracownikiem lub rozwiązanie przez Pracodawcę tejże umowy o pracę bez wypowiedzenia z winy pracownika, zgodnie z przepisami *ustawy z dnia 26 czerwca 1974 r. Kodeks Pracy (tekst jedn.: Dz. U. z 1998 r. Nr 21 poz. 94, ze zmianami).*
4. Niniejsze Porozumienie zostało sporządzone w dwóch egzemplarzach, po jednym dla każdej ze stron.
5. Zmiana, uzupełnienie oraz rozwiązanie niniejszego Porozumienia za zgodą obu stron wymaga formy pisemnej pod rygorem nieważności.

....

data i podpis Pracownika data i podpis Wójta

Załącznik nr 5

do „Polityki bezpieczeństwa"

RAPORT

Z NARUSZENIA BEZPIECZEŃSTWA SYSTEMU INFORMATYCZNEGO

URZĘDZIE GMINY W ŚWIERZNIE

1. Data: ..... Godzina: .....

(dd.mm.rrrr)

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

.....

(imię, nazwisko, stanowisko służbowe, nazwa użytkownika (jeśli występuje)

3. Lokalizacja zdarzenia:

.....

(np. nr pokoju, nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

.....

.....

.....

5. Przyczyny wystąpienia zdarzenia:

.....

.....

.....

6. Podjęte działania:

.....

.....

.....

7. Postępowanie wyjaśniające:

.....

.....

(data, podpis Administratora Bezpieczeństwa Informacji)

WYKAZ OSÓB, KTÓRE ZAPOZNANO Z „POLITYKĄ BEZPIECZEŃSTWA" ORAZ „INSTRUKCJĄ ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH"

URZĘDZIE GMINY W ŚWIERZNIE

Lp.	nazwisko i imię	stanowisko	data	Podpis