Zarządzenie Nr 31/16
Wójta Gminy Żurawica
z dnia 18-04-2016

w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji w ramach Zintegrowanego Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Gminy Żurawica i powołania Administrator Systemu Informatycznego oraz Komitetu Bezpieczeństwa Informacji

Na podstawie: art. 20 ust.2 pkt 1 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 roku *w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych* (Dz. U. z 2012r. poz. 526) zarządzam, co następuje:

§1. Wprowadzam w życie Politykę Bezpieczeństwa Informacji w Urzędzie Gminy Żurawica stanowiącą załącznik nr 1 do niniejszego zarządzenia.

§2. Powołuje na Administratora Systemu Informacji Pana Sebastiana Śliwińskiego

§3. Powołuje na Komitet Bezpieczeństwa Informacji w składzie:
- Sekretarz Gminy Żurawica – przewodniczący komitetu,
- Administrator Systemu Informatycznego – członek komitetu,
- Administrator Bezpieczeństwa Informacji – członek komitetu.

§4. Wykonanie zarządzenia w zakresie wprowadzenia w życie Polityki Bezpieczeństwa Informacji w Urzędzie Gminy Żurawica powierza się Komitetowi Bezpieczeństwa Informacji.

§5. Zarządzenie wchodzi w życie z dniem jego podjęcia.

Wójt Gminy Żurawica
Krzysztof Składowski

Załącznik nr 1
do Zarządzenia nr 31/16 Wójta Gminy Żurawica z dnia 18.04.2016 r.
w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji
w ramach Zintegrowanego Systemu Zarządzania Bezpieczeństwem Informacji
w Urzędzie Gminy Żurawica
i powołania Administrator Systemu Informatycznego
oraz Komitetu Bezpieczeństwa Informacji

Polityka Bezpieczeństwa Informacji w Urzędzie Gminy Żurawica

Wójt Gminy Żurawica
Krzysztof Składowski

Opracowano na podstawie norm:
- PN-ISO/IEC 27001:2007
- PN-ISO/IEC 17799:2007
- PN-ISO/IEC 27005:2010

I. Deklaracja Wójta Gminy Żurawica

Wójt Gminy Żurawica, mając świadomość wartości posiadanych zasobów informacyjnych i konieczność ich zabezpieczenia, wprowadza do użytku i powszechnego stosowania w Urzędzie Politykę Bezpieczeństwa Informacji, w pełni akceptując i wspierając jej stosowanie.

Niniejszy dokument opisuje zasady postępowania odnoszące się do bezpieczeństwa informacji i został przygotowany z myślą o zapewnieniu standardów bezpieczeństwa w Urzędzie, ze szczególnym uwzględnieniem zgodności z obowiązującym prawem, oraz zminimalizowania skutków zagrożeń z tytułu utraty poufności, autentyczności danych, strat finansowych, jak również utraty wizerunku Urzędu.

Wójt Gminy Żurawica, podejmuje i realizuje działania w zakresie stosowania odpowiednich standardów bezpieczeństwa informacji oraz wspiera przedsięwzięcia i inicjatywy związane z ich rzeczywistą ochroną i zabezpieczaniem.

Wójt Gminy Żurawica
Krzysztof Składowski

II. Dokument Polityki Bezpieczeństwa Informacji

Polityka Bezpieczeństwa Informacji (zwana dalej Polityką) jest dokumentem określającym strategię działań, których celem jest zapewnienie efektywnego i całościowego zarządzania bezpieczeństwem informacji w Urzędzie.

Zadaniem Polityki jest określenie celu i zakresu działań mających zapewnić bezpieczeństwo informacji oraz określenie ról, podziału zadań i odpowiedzialności wiążących się z utrzymaniem bezpieczeństwa informacji w Urzędzie.

Polityka, stanowiąc również koncepcję bezpieczeństwa, zakłada postęp(fazy) dojrzałości[1] Systemu Zarządzania Bezpieczeństwem Informacji[2] w Urzędzie.

Zapisy w dokumencie Polityki występują w postaci:

1. Nakazowej - oznaczanej znakiem paragrafu i numeracją: w tym znaczeniu stanowią normę postępowania, której znajomość i obowiązek stosowania dotyczy każdego z pracowników Urzędu;
2. Preliminaryjnej - stanowiącej wytyczne oraz swego rodzaju kontekst zapisów imperatywnych.

Polityka, w celu zachowania przydatności, adekwatności i skuteczności podlega okresowym przeglądom prowadzonym przez powołanego właściciela/li niniejszej polityki.

III. Znaczenie i definicja bezpieczeństwa informacji

Zachowanie (zarządzanie) bezpieczeństwa informacji jest jednym z kluczowych elementów w procesowym podejściu do zarządzania, w którym uwzględniono ryzyko prowadzonej działalności.

Istotnym jest, że używane pojęcie informacji dotyczy wszelkiej jej postaci, niezależnie od medium; Ochronie podlegają wszelkie nośniki informacji tj. papierowe, magnetyczne, informatyczne.

Bezpieczeństwo informacji polega na zachowaniu poufności, integralności i dostępności informacji[3]. Zapewnienie tych cech osiąga się poprzez wdrożenie Systemu Zarządzania Bezpieczeństwem

---

[1] W oparciu o metodykę CobiT - Modele dojrzałości.

[2] Dalej definiowany jako SZBI.

[3] Dodatkowo mogą być brane pod uwagę inne własności, takie jak autentyczność, rozliczalność i niezawodność. Wyjaśnienia użytych pojęć zostały podane w rozdziale „Definicje".

Informacji (SZBI)[4], na który składają się zdefiniowane i określone: granice i zakresy SZBI, Polityka Bezpieczeństwa Informacji (niniejszy dokument) wraz z procedurami bezpieczeństwa, oraz podejście do szacowania i zarządzanie ryzykiem.

Działania, dokumenty i procesy SZBI powinny być dokumentowane – dokumentacja tworzona w tym celu nosi nazwę Dokumentacji Systemu Zarządzania Bezpieczeństwem Informacji.

IV. Cele bezpieczeństwa informacji

Podstawowym celem bezpieczeństwa informacji jest utrzymanie zagrożeń na poziomie akceptowalnym *(Istnieje szereg zagrożeń, np.: prawne, utrata wizerunku, naruszenie integralności czy też dostępności wskutek niewłaściwego zarządzania zasobami informacyjnymi, itp.)*.

Wdrażanie rozwiązań bezpieczeństwa niestety komplikuje większość procesów, należy jednak dążyć do minimalizacji utrudnień wprowadzonych przez zabezpieczanie *(bezpieczeństwo informacji powinno umożliwić bezpieczne funkcjonowanie Urzędu, a nie jego blokowanie)*.

Bezpieczeństwo informacji jest elementem składowym wszystkich procesów. Każdy z pracowników Urzędu powinien posiadać stosowną wiedzę gwarantującą bezpieczeństwo informacji, z którą pracuje oraz mieć możliwość skorzystania z wiedzy eksperckiej w przypadku wątpliwości, np. przy realizacji nowego projektu, zadania.

V. Struktura wyznaczania celów stosowania zabezpieczeń i zabezpieczeń, w tym struktura szacowania i zarządzania ryzykiem.

W Urzędzie przyjęto za podstawowy wykaz celów stosowania zabezpieczeń i zabezpieczeń zaprezentowany w treści załącznika A do normy PN-ISO/IEC 27001:2007.
Na tej podstawie oparto strukturę niniejszej Polityki Bezpieczeństwa Informacji, która definiuje zabezpieczenia w zidentyfikowanych obszarach w Urzędzie w oparciu o dobre praktyki określone normą PN-ISO/IEC 17799:2007 (występuje pełna korelacja między zapisami obu norm oraz rozdziałami Polityki - Poszczególne rozdziały Polityki mają swoje odniesienia do rozdziałów w normie PN-ISO/IEC 17799:2007 stanowiąc obszary zabezpieczenia).
Zidentyfikowanymi obszarami zabezpieczenia w Urzędzie są:

- Polityka Bezpieczeństwa Informacji,
- Organizacja bezpieczeństwa informacji,
- Zarządzanie aktywami,
- Bezpieczeństwo zasobów ludzkich,
- Bezpieczeństwo fizyczne i środowiskowe,
- Zarządzanie systemami i sieciami,
- Kontrola dostępu,
- Pozyskiwanie, rozwój i utrzymanie systemów informacyjnych,
- Zarządzanie incydentami związanymi z bezpieczeństwem informacji,
- Zarządzanie ciągłością działania,
- Zgodność,

Zaprezentowany katalog nie wyczerpuje wszystkich potencjalnych celów i obszarów.
Jej ewentualny rozwój zależy od wykazania takiej potrzeby w wyniku procesu zarządzania ryzykiem.
W Urzędzie przyjęto, że proces zarządzania ryzykiem prowadzony będzie zgodnie z wytycznymi normy PN-ISO/IEC 27005:2010. Polega on na:

[4] Zgodnie z normą PN-ISO/IEC 27001:2007, SZBI budowany jest w oparciu o podejście procesowe, stosuje się model „Planuj-Wykonuj-Sprawdzaj-Działaj" (PACA - Plan-Do-Check-Act).

1. Ustanowieniu kontekstu
   (przy wdrożonej Polityce: ustaleniu zakresu i granic, osób odpowiedzialnych i uczestniczących oraz przyjęciu metody szacowania ryzyka systemu zarządzania bezpieczeństwem informacji, np. wg kryteriów: oceny ryzyka, skutków, akceptowania ryzyka).
2. Szacowaniu ryzyka
   (zidentyfikowaniu ryzyk dla informacji, przypisaniu im właściciela i wartości oraz odniesieniu do kryteriów oceny)
3. Postępowaniu z ryzykiem
   (zdecydowaniu o sposobie zabezpieczenia: zredukowaniu, zachowaniu, uniknięciu lub transferze ryzyk i określeniu planu postępowania z ryzykiem)
4. Akceptowaniu ryzyka
   (formalnym udokumentowaniu i akceptacji ryzyk szczątkowych)
5. Informowaniu o ryzyku
   (poinformowaniu stron, których ryzyko dotyczy o podjętych decyzjach)
6. Monitorowaniu i przeglądzie ryzyka
   (monitorowaniu i przeglądzie ryzyk i ich czynników, -tj. wartości aktywów, skutków, zagrożeń, podatności, prawdopodobieństwa wystąpienia- w celu identyfikowania każdej zmiany w kontekście organizacji na wczesnym etapie, oraz w celu utrzymania obrazu kompletnej mapy ryzyka)

Należy uwzględnić aspekt bezpieczeństwa w każdym obszarze działalności Urzędu.
Dobór środków zabezpieczenia powinien być adekwatny do potrzeb: Powinien wynikać z analizy ryzyka i być uwzględniony w zarządzaniu ryzykiem.

Struktura i zasady dotyczące dokumentów Polityki Bezpieczeństwa Informacji:

Dokumenty Polityki Bezpieczeństwa Informacji posiadają strukturę hierarchiczną:
Głównym dokumentem jest Polityka Bezpieczeństwa Informacji.
Za opracowanie dokumentu Polityki Bezpieczeństwa Informacji oraz wynikających z niej dokumentów normatywnych, tj. określających założenia dotyczące bezpieczeństwa, odpowiedzialny jest powołany przez Wójta Gminy Żurawica Komitet Bezpieczeństwa Informacji (KBI) w skład którego wchodzi Sekretarz Gminy Żurawica, Administrator Systemu Informatycznego (ASI) i Administrator Bezpieczeństwa Informacji (ABI) który pełni dodatkowo funkcję Koordynatora Komitetu Bezpieczeństwa Informacji (KBI).

Rozszerzeniem Polityki oraz dokumentów normatywnych są wszelkie inne dokumenty, które wynikają z ww.[5] (będą to procedury, instrukcje, rejestry i inne regulacje, których powołanie jest postulowane w Polityce lub dokumentach normatywnych).

Rozszerzenia Polityki powinny być zmieniane natychmiast[6] po wprowadzeniu zmian, które skutkują dezaktualizacją poprzedniej wersji rozszerzenia.
Osobą/komórką inicjującą i koordynującą utworzenie lub modyfikację rozszerzeń(nia) jest właściciel (Gestor/Dysponent/Administrator Informacji) aktywu(ów)/zasobu.
Do opracowania lub modyfikacji ww. rozszerzeń zobligowana jest komórka (Gestor/Dysponent/Administrator Informacji) aktywu(ów)/zasobu w konsultacji z KBI. Zazwyczaj właściciel zasobu będzie merytorycznie najbardziej przygotowany do przygotowania danego

[5] Przykładowo: Administrator Bezpieczeństwa Informacji zaleca opracowanie procedury antywirusowej, określającej wymogi bezpieczeństwa, a komórka informatyki (Administrator Systemu Informatycznego) opracowuje instrukcję użycia konkretnego pakietu antywirusowego.
[6] ale tak, by nie spowodować incydentu poprzez zaniedbanie właściwego funkcjonowania systemu - priorytetem jest zapewnienie dostępności, integralności, poufności i ciągłości działania. Jeżeli zwłoka może być znaczna (powyżej 10 dni roboczych) należy o tym poinformować ABI.

rozszerzenia. Możliwa jest jednak sytuacja, w której te zadania będą rozdzielone, co zostało usankcjonowane w §8 i §9.
Opracowania niższej warstwy wynikają z dokumentów warstwy wyższej (w tych ostatnich określona zostaje komórka odpowiedzialna za opracowanie pozostałych dokumentów).

Znajomość treści oraz zasad określonych w dokumentach bezpieczeństwa obowiązują – w zakresie niezbędnym do skutecznego, adekwatnego i wydajnego świadczenia pracy wszystkich pracowników, oraz inne osoby świadczące usługi na rzecz Urzędu, w tym pracowników osób trzecich korzystających z systemów informacyjnych Urzędu, świadczących usługi na podstawie umów cywilnoprawnych.
Pracownicy, o których mowa wyżej, zobowiązani się dołożyć należytych starań, by odpowiednio wypełnić zapisy Polityki.
Nieprzestrzeganie zasad Polityki przez pracowników może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych oraz nieść za sobą skutki prawne.

Dokumenty Polityki powinny być udostępnione partnerom, z którymi Urząd współpracuje w zakresie ustalonym indywidualnie, adekwatnie do zakresu współpracy i dostępu do informacji.
Nieprzestrzeganie zasad Polityki – w zakresie udostępnionym przez Urząd - przez podwykonawców świadczących usługi na podstawie umów cywilnoprawnych może być potraktowane jako niedotrzymanie warunków umowy i nieść za sobą skutki prawne.

VI. Definicje:

Ogólne:

Aktywa - wszystko co ma wartość dla organizacji / Urzędu (ISO/IEC 13335-1:2004).
Zasób - składnik systemu spełniający żądaną rolę prezentacji, pamiętania, transmisji lub przetwarzania. Przykład - Kategoriami zasobów są: czas, informacja, obiekty lub procesory.
Bezpieczeństwo informacji[7] – zachowanie poufności, integralności i dostępności informacji; dodatkowo, mogą być brane pod uwagę inne własności, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność (PN-ISO/IEC 17799:2007).
Środki przetwarzania informacji – system, usługa lub infrastruktura przetwarzająca informacje lub fizyczna lokalizacja, w której się znajdują (PN-ISO/IEC 17799:2007).
Gestor danych (Dysponent) - statutowy organ, organizacja osoba/ komórka organizacyjna odpowiedzialne za szczególną kategorię informacji lub aktualne dane zawarte w informacji lub określone typy danych, do których należy sygnalizowanie użytkownikom i zarządzającym danymi, potrzeby stosowania pewnych procedur obsługi danych, związanych z zabezpieczeniem;
Ryzyko – kombinacja prawdopodobieństwa zdarzenia i jego konsekwencji;
Ryzyko związane z bezpieczeństwem informacji -potencjalna sytuacja, w której określone zagrożenie wykorzysta podatność aktywów lub grupy aktywów powodując w ten sposób szkodę dla organizacji.
Analiza ryzyka – systematyczne wykorzystanie informacji do zidentyfikowania źródeł i oszacowania ryzyka;
Szacowanie ryzyka – całościowy proces analizy i oceny ryzyka;
Ocena ryzyka – proces porównywania oszacowanego ryzyka z określonymi kryteriami w celu określenia znaczenia ryzyka.
Zarządzanie ryzykiem – skoordynowane działania kierowania i zarządzania organizacją z uwzględnieniem ryzyka. UWAGA: Zarządzanie ryzykiem zawiera zwykle szacowanie ryzyka, postępowanie z ryzykiem, akceptowanie ryzyka i informowanie o ryzyku.
Unikanie ryzyka - decyzja o nieangażowaniu się lub działanie w kierunku wycofania się z ryzykownej sytuacji.
Informowanie o ryzyku - wymiana lub dzielenie się informacjami o ryzyku między decydentami a innymi uczestnikami.

---

[7] Pojęcie informacji jest niezależne od postaci, w jakim ww. występuje: wszelkie odniesienia w dokumentach SZBI, szczególnie w Polityce, dotyczą w równym stopniu informacji znajdującej się na nośnikach tradycyjnych (papier), informatycznych jak też w każdej innej postaci (np. klisza fotograficzna, zapis audio).

Estymacja ryzyka - proces przypisywania wartości prawdopodobieństwu i następstwom.
Identyfikowanie ryzyka - proces znajdowania, zestawiania i charakteryzowania elementów ryzyka.
Ryzyko szczątkowe (residual risk) - ryzyko pozostałe po wprowadzeniu zabezpieczenia.
dopuszczalny poziom ryzyka - rozważne i staranne oszacowanie przeprowadzone przez stosowne władze, czy działanie systemu przetwarzania danych lub sieci spełnia minimalne wymagania na stosowne zalecenia dotyczące **zabezpieczenia.**
Autentyczność (authenticity) - właściwość zapewniająca, że tożsamość podmiotu lub zasobu jest taka jak deklarowana. Autentyczność dotyczy takich podmiotów jak użytkownicy, procesy, systemy i informacja
Poufność (confidentiality) - właściwość zapewniająca, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom (ISO 7498-2: 1989).
Rozliczalność (accountability) - właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi (ISO 7498-2: 1989).
Integralność danych (data integrity) - właściwość zapewniająca, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany (ISO 7498-2: 1989).
Integralność systemu (system integrity) - właściwość polegająca na tym, że system realizuje swoją zamierzoną funkcję w nienaruszony sposób, wolny od nieautoryzowanej manipulacji, celowej lub przypadkowej.
Dostępność (availability) - właściwość bycia dostępnym i możliwym do wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot (ISO 7498-2: 1989).
Niezawodność (reliability) - właściwość oznaczająca spójne, zamierzone zachowanie i skutki (ISO/IEC TR 13335-1).
Podatność (vulnerability) - obejmuje słabość zasobu lub grupy zasobów, która może być wykorzystana przez zagrożenie oraz atrakcyjność aktywów informacyjnych (ISO/IEC TR 13335-3).
Polityka – wyrażona przez kierownictwo ogólna intencja i kierunki działań.
Polityka zabezpieczenia systemu informacyjnego - spisane cele, strategie i działania, które określają, w jaki sposób aktywa systemu informacyjnego są zarządzane, chronione i rozpowszechniane w instytucji i jej systemach informacyjnych.
Zabezpieczenie – środki służące zarządzaniu ryzykiem, łącznie z politykami, procedurami, zaleceniami, praktyką lub strukturami organizacyjnymi, które mogą mieć naturę administracyjną, techniczną, zarządczą lub prawną.
Zagrożenie – potencjalna przyczyna niepożądanego incydentu, który może wywołać szkodę ryzykiem systemie lub organizacji.
Incydent związany z bezpieczeństwem informacji – jest to pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji.
Przetwarzanie danych - rozumie się przez to jakiekolwiek operacje wykonywane na danych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

Specyficzne dla zagadnień ochrony danych osobowych:
Zbiór danych - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
Przetwarzanie danych (osobowych) - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
System informatyczny - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,
Zabezpieczenie danych w systemie informatycznym - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.
Usuwanie danych - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.
Administrator danych - rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, o których mowa w art. 3, decydujące o celach i środkach przetwarzania danych osobowych.

VII. Organizacja bezpieczeństwa informacji

(Podział ról, zadań i odpowiedzialności w SZBI)

1. Administratorem danych jest Gmina Żurawica.
2. Osobą reprezentującą Administratora danych, uprawnioną do podejmowania wszelkich decyzji jest Wójt Gmina Żurawica.
3. Wszelkie zmiany w niniejszym dokumencie, jak też sposób postępowania w przypadku poważnych incydentów związanych z bezpieczeństwem informacji wymagają uzgodnienia i akceptacji Wójta Gmina Żurawica.
4. W celu koordynacji i kontrolowania SZBI w Urzędzie został powołany Komitet Bezpieczeństwa Informacji[8], (zwany dalej KBI) w skład którego wchodzą:
   - Sekretarz Gminy Żurawica,
   - Administrator Bezpieczeństwa Informacji (ABI),
   - Administrator Systemu Informatycznego (ASI).
5. KBI podlega bezpośrednio Wójtowi Gminy Żurawica.
6. KBI może czasowo włączyć do zespołu każdego pracownika, którego pomoc jest niezbędna w realizacji zadania.
7. KBI odpowiada za SZBI w zakresie:
   - Opracowanie Polityki Bezpieczeństwa Informacji i procedur bezpieczeństwa,
   - Okresową aktualizację Polityki Bezpieczeństwa Informacji i procedur bezpieczeństwa adekwatnie do zachodzących zmian zewnętrznych i wewnętrznych,
   - Prowadzenie wewnętrznych audytów z zakresu ochrony danych osobowych i bezpieczeństwa informacji,
   - Prowadzenie szkoleń z zakresu ochrony danych osobowych, bezpieczeństwa informacji oraz wdrożonych aktów normatywnych,
   - Pomoc w szacowaniu i zarządzaniu ryzykiem dla informacji, których właścicielem jest Gmina Żurawica,
   - Pomoc w nadzorowaniu przestrzegania zasad określonych w Polityce Bezpieczeństwa Informacji oraz procedurach bezpieczeństwa,
   - Pomoc w prawidłowej realizacji zarządzania upoważnieniami do przetwarzania danych osobowych oraz prowadzeniu i aktualizacji ewidencji osób upoważnionych,
   - Przygotowywanie nowych wniosków zgłoszeń rejestracyjnych do GIODO i dbanie o aktualizowanie już zarejestrowanych zbiorów danych,
   - Prowadzenie bieżącej korespondencji z GIODO.
8. Wszelki kontakt doradczy prowadzony przez KBI realizuje ABI: wszelkie zgłoszenia w tym zakresie należy kierować na adres określony w załączniku nr 1 do Polityki Bezpieczeństwa Informacji.
9. Kierownicy referatów i pracownicy na samodzielnych stanowiskach pracy zobligowani są współpracy z KBI w obszarze bezpieczeństwa informacji.
10. Kierownicy referatów i pracownicy na samodzielnych stanowiskach pracy odpowiadają za nadzór nad stosowaniem przez podległych pracowników postanowień polityki i procedur bezpieczeństwa.
11. Kierownicy referatów i pracownicy na samodzielnych stanowiskach pracy zobowiązani są do przekazywania informacji o zauważonych słabościach systemu informacyjnego do KBI (ABI).

[8] Zgodnie z zaleceniem PN-ISO/IEC 17799-2007, pkt. 6.1.1.

12. Każdy z pracowników jest zobowiązany do stosowania się do zapisów Polityki Bezpieczeństwa Informacji oraz procedur bezpieczeństwa i odpowiada za ich stosowanie.
13. Każdy z pracowników zobowiązany jest do współpracy w obszarze bezpieczeństwa informacji z KBI.

VIII. Zarządzanie aktywami

W celu osiągnięcia i utrzymania odpowiedniego poziomu ochrony aktywów Urzędu, konieczna jest ich inwentaryzacja oraz określenie właściciela (gestora), tj. osoby lub komórki, która będąc uprawniona, tworzy/zarządza aktywami zapewniając im bezpieczeństwo w Urzędzie.
Przypisanie właściciela dla aktywu(ów) następuje podczas utworzenia ww. lub podczas inwentaryzacji.
Za koordynację inwentaryzacji odpowiada KBI (ABI).
Właściciel odpowiedzialny jest za zapewnienie, że informacje i aktywa powiązane ze środkami przetwarzania informacji są poprawnie sklasyfikowane;
Przedmiotem własności może być:

- proces;
- określony zbiór działań;
- aplikacja;
- określony zbiór danych.

Szczególnie istotnym aktywem jest informacja, dla której przyjęto następującą klasyfikację:

- dane osobowe,
- dane księgowe,
- dane pracownicze,
- informacje niejawne[9],
- informacje o metodach i środowisku pracy,
- informacje dotyczące obronności kraju,
- inne, stanowiące własność Urzędu (stanowiące tajemnicę służbową). Możliwe jest, że informacja może być zakwalifikowana do kilku z ww. kategorii.

Dostęp do informacji z powyższej klasyfikacji jest reglamentowany.
Stosuje się zasadę uprzywilejowania minimalnego *(za przestrzeganie tej zasady odpowiedzialni są przełożeni pracownika)*.
Dostęp do informacji przyznawany jest przez Wójta Gminy Żurawica, lub przez osoby przez Wójta upoważnione do tej czynności (jeżeli tego wymagają osobne przepisy - w sposób wynikający z ww.).
Zakres dostępu wynika z zakresu zadań pracownika.
Ochrona zasobów dotyczy każdej ich postaci, niezależnie od medium, na którym ww. się znajdują (ochronie podlegają dokumenty, informatyczne nośniki danych, informacje przekazane ustnie).
Wyjątkiem od tej zasady są informacje wyraźnie określone jako powszechnie dostępne.
Informacjami powszechnie dostępnymi są informacje znajdujące się w oficjalnych publikacjach Urzędu, oraz dokumentach, z których treści wynika, że są przeznaczone do powszechnego dostępu.
W przypadku wykrycia aktywów, które nie zostały zinwentaryzowane, informacje o tym fakcie powinny być przekazane do ABI.
Ważnym jest, że reglamentacja informacji nie wyklucza swobody posługiwania się nią. Istotne jest tylko, by kontrolować przepływ informacji w obszarze podmiotów, dla których powyższa informacja jest przeznaczona.

[9] W rozumieniu ustawowym.

IX. Bezpieczeństwo osobowe

IX.1. Podział obowiązków i odpowiedzialności

Stanowiska pracy powinny być definiowane z uwzględnieniem podstawowej zasady rozdzielenia obowiązków i odpowiedzialności od funkcji kontrolnych z danego obszaru.
Rozdział funkcji zarządzających, wykonawczych oraz kontrolnych, zmniejsza to ryzyko niewłaściwego wykorzystywania aktywów systemu.

IX.2. Polityka kadrowa

Należy zmniejszyć ryzyko błędu, kradzieży, defraudacji, niewłaściwego użycia aktywów (w tym systemu informatycznego, urządzeń) przez użytkowników tego systemu.
Podział obowiązków i odpowiedzialności w zakresie zabezpieczenia oraz zasada najniższego poziomu przywilejów powinny być podstawą definicji stanowiska pracy związanego z dostępem do aktywów (w tym systemu informatycznego).
Za realizację tego postulatu odpowiada kierujący komórką wewnętrzną.
Zgodnie z zasadą rozdziału uprawnień i odpowiedzialności, pojedynczy pracownik nie powinien samodzielnie realizować krytycznych, z punktu widzenia systemu informacyjnego, procesów[10].
Zgodnie z zasadą najniższego poziomu przywilejów, pracownik nie powinien mieć uprawnień większych niż niezbędne do wypełnienia swoich obowiązków.
Przy definiowaniu uprawnień należy zwrócić uwagę na efektywność pracy grup pracowników *(możliwości zastępowania nieobecnych)* oraz możliwości działania w sytuacjach awaryjnych *(np. warunkowe przydzielenie uprawnień)*.
Wszyscy użytkownicy systemu informacyjnego powinni podpisać zobowiązanie nieujawniania informacji stanowiących tajemnice Urzędu, które są przetwarzane, składowane lub transmitowane za pomocą tego systemu.
Podobne jak w pkt. wyżej zastrzeżenie powinno znaleźć się także w umowach lub kontraktach zawieranych z podmiotami współpracującymi oraz stronami trzecimi.
Zobowiązania powinny podlegać rewizji w momencie zmiany warunków zatrudnienia, kontraktu lub umowy, w szczególności z uwagi na zbliżające się terminy ich zakończenia. *(Procedury związane z zakończeniem użytkowania systemu informacyjnego przez pracownika dotyczą również osób trzecich, korzystających z systemu informacyjnego czasowo, w wyniku umowy)*.
Częścią standardowego zestawu działań kończących zatrudnienie pracownika winno być odebranie wszelkich uprawnień dostępu oraz powierzonych mu aktywów.
Zwalniany pracownik powinien przekazać wszelkie dokumenty oraz informacje o aktywach systemu będących w jego dyspozycji *(np. w postaci dokumentów, dokumentacji elektronicznej, struktury katalogów, lokalizacji kopii bezpieczeństwa itp.)*. Ponadto, powinien udostępnić inne elementy systemu zabezpieczenia, takie jak tokeny uwierzytelnienia lub klucze kryptograficzne (w przypadkach uniemożliwiających przekazanie – np. certyfikaty osobiste, osobisty podpis elektroniczny – należy zadbać o działania zapewniające ciągłość działań przy jednoczesnym wykluczeniu nieuprawnionego użycia kluczy osobistych).
Wraz ze zwolnieniem pracownika musi być również zamknięte jego konto(a) jako użytkownika systemu informatycznego. Jeśli zachodzi uzasadnione podejrzenie, że zwalniany *(np. dyscyplinarnie)* pracownik dysponuje narzędziami lub informacjami, które może wykorzystać w celu naruszenia zabezpieczenia systemu informacyjnego, to należy zminimalizować prawdopodobieństwo zaistnienia tego zagrożenia. Działania sprawdzające powinny obejmować wszystkie aktywa systemu *(dostęp do dokumentów, urządzenia, aplikacje, oprogramowanie, dane, kopie bezpieczeństwa itp.)*, do których osoba ta miała dostęp.

[10] Tzw. „zasada czterech oczu".

IX.3. Uświadamianie, edukacja i szkolenie

Użytkownicy systemu informacyjnego przed dopuszczeniem do pracy w systemie informacyjnym muszą posiadać świadomość konieczności zabezpieczania informacji oraz odbyć szkolenia z zakresu użytkowania systemu informacyjnego oraz stosowanych środków zabezpieczenia.
W zależności od zakresu oraz kategorii użytkowników, informacje te mogą być przekazywane na trzech poziomach: uświadamiania, szkolenia i edukacji.
Uświadomienie pracowników w zakresie zabezpieczenia systemów informacyjnych obejmuje:

- przedstawienie celów polityki zabezpieczeń prowadzonej w Urzędzie oraz pokazanie, w jaki sposób przyczynia się ona do realizacji celów działalności i ochrony aktywów,
- zrozumienie wytycznych w zakresie zabezpieczenia systemu informacyjnego.

Celem szkolenia jest przekazanie pracownikom umiejętności, które sprawią, że będą oni wykonywali swe zadania zgodnie z procedurami określonymi w Polityce Bezpieczeństwa Informacji i dokumentami związanymi z wyżej wymienioną.
Uzyskanie tego celu osiąga się poprzez wpojenie pracownikom zasad odpowiedniego postępowania z zasobami systemu informacyjnego, a w szczególności:

- zasad ochrony informacji,
- fizycznego zabezpieczenia pomieszczeń oraz zasobów systemu informacyjnego,
- ochrony haseł, kluczy lub innych środków uwierzytelnienia, umożliwiających dostęp do zasobów systemu,
- przekazywania informacji o dostrzeżonych anomaliach działania systemu, które mogą być efektem naruszenia zabezpieczenia.

Edukacja sięga głębiej niż szkolenie i jest skierowana do osób zawodowo zajmujących się zabezpieczeniami systemów informacyjnych. Ta działalność stanowi element doskonalenia zawodowego niektórych pracowników *(np. informatyk)*.
Procesy uświadamiania, szkolenia oraz edukacji w zakresie zabezpieczenia powinny mieć charakter okresowy.
Uświadamianie i szkolenia z zakresu metodyki i wytycznych organizuje ABI.
Szkolenia z zakresu zadań wykonywanych w systemie informacyjnym przeprowadza komórka wewnętrzna posiadająca największą wiedzę w przedmiocie szkolenia lub instytucja zewnętrzna.

X. Bezpieczeństwo fizyczne i środowiskowe

X.1. Strefy bezpieczeństwa (obszary bezpieczne)

Fizyczne zabezpieczenie opiera się na zdefiniowaniu stref kontrolnych, wprowadzeniu barier między tymi strefami oraz określeniu dostępu do ww. stref na podstawie uzasadnionych potrzeb.
Zdefiniowanie ww. elementów wymaga przeprowadzenia szacowania ryzyk dla wcześniej zidentyfikowanych aktywów, którą to czynność koordynuje KBI(ABI),
Stworzenie bariery dla danej strefy powinno uwzględniać wartość chronionych aktywów i usług w relacji do kosztów zabezpieczenia, a także ryzyko naruszenia zabezpieczeń oraz istniejące mechanizmy ograniczające to ryzyko. Jeśli wyodrębniono kilka poziomów fizycznego zabezpieczenia, to każdy z nich powinien mieć jednoznacznie przypisany zbiór mechanizmów kontrolujących wejście do strefy.
Chronione strefy powinny być wyposażone w mechanizmy gwarantujące upoważnionym osobom autoryzowany dostęp (elektroniczne karty dostępu, zasady użytkowania i stosowanie kluczy/ plombowania pomieszczeń).
Należy rozpatrzyć zasadność stosowania dodatkowych ograniczeń np. kontrolę dostępu gości i personelu pomocniczego oraz zapewnić niezwłoczne pozbawienie praw dostępu osób, które utraciły upoważnienie do wejścia do strefy *(np. w wyniku zwolnienia, przejścia do innego działu itp.)*

Prawa dostępu powinny podlegać okresowym przeglądom i być bezzwłocznie odbierane w przypadku, gdy nie są już niezbędne.
Zasoby (urządzenia, materiały eksploatacyjne) należy umieszczać w takich miejscach, by dostęp do nich nie wymagał nadawania uprawnień nie wynikających z zakresu obowiązków pracownika.
W zdefiniowanych obszarach osoby postronne mogą przebywać tylko pod nadzorem upoważnionych pracowników.

X.2. Zabezpieczenie infrastruktury i urządzeń systemu informacyjnego

W celu zapewnienia zabezpieczenia fizycznego infrastruktury i urządzeń należy uwzględnić:

- rozmieszczanie urządzeń systemu informacyjnego, w tym:
  - separacje urządzeń wymagających specjalnego zabezpieczenia i urządzeń chronionych na zasadach ogólnych;
  - wybór odpowiednich pomieszczeń dla tych urządzeń *(m.in. unikanie miejsc publicznych, nieumieszczanie wyraźnych oznakowań, oddzielenie od pomieszczeń, gdzie znajdują się urządzenia zapasowe oraz archiwizacyjne)*;
  - wybór takiej lokalizacji dla konsol operacyjnych, urządzeń z wymiennymi nośnikami danych *(pamięci taśmowych, napędów dyskowych, wyjmowalnych dysków)* oraz drukarek, faksów, aby utrudnić dostęp do nich nieuprawnionym osobom;
- zapewnienie pewnego zasilania:
  - powinny być opracowane i wykonane szczegółowe plany wszystkich instalacji zasilających budynku *(zasilanie elektryczne, instalacje: wodna, gazowa, kanalizacyjna, telefoniczna, alarmowa itp.)*;
  - komputery uczestniczące w przetwarzaniu informacji należącej do systemu informatycznego muszą być zasilane z wydzielonej sieci elektrycznej, zabezpieczonej co najmniej urządzeniem UPS *(wskazany również agregat prądotwórczy)*, dla pozostałych komputerów i innych urządzeń warunek ten powinien być spełniony;
  - należy przestrzegać obowiązujących norm zasilania urządzeń elektrycznych zalecanych przez producentów tych urządzeń;
  - jeśli nie ma odpowiedniego zabezpieczenia budynku, to należy zorganizować ochronę najważniejszych urządzeń systemu *(m.in. serwery, urządzenia aktywne)*;
- zabezpieczenie przeciwpożarowe:
  - w pomieszczeniach w których znajduje się kluczowe wyposażenie (w tym teleinformatyczne) należy zapewnić obecność systemów przeciwpożarowych (alarmujących o pożarze i gaszących),
  - pomieszczenia (i sprzęt) powinny być dobrane pod kątem zapewnienia możliwie wysokiego poziomu bezpieczeństwa ogniowego; Ściany powinny być o odpowiedniej odporności ogniowej – zależnej od strefy zagrożenia Z.L,[11]
  - w pomieszczeniach nie należy przechowywać materiałów łatwopalnych.
- Inne środki zabezpieczenia:
  - pomieszczenia w których znajdują się kluczowe elementy systemu teleinformatycznego powinno być klimatyzowane, a urządzenia powinny być zabezpieczone przed zalaniem (np. serwer nie powinien znajdować się w bezpośrednim sąsiedztwie wylotu klimatyzatora, czy też kaloryferów).
- zabezpieczenie okablowania:
  - kable zasilające i łącza zapewniające transmisję danych lub realizujące inne usługi systemu informacyjnego powinny być chronione przed zniszczeniem lub przechwyceniem przesyłanej informacji;

[11] ZL - klasa zagrożenia ludzi. Dz.U. z 2002 r. Nr 75 poz. 690

- trasy kabli powinny być wybierane ze szczególną starannością *(np. biorąc pod uwagę łatwość dostępu przez nieuprawnione osoby)*;

- zasady zabezpieczania urządzeń znajdujących się poza siedzibą Urzędu:
  - użytkowanie urządzeń systemu informacyjnego powinno odbywać się pod kontrolą; dotyczy to zwłaszcza nośników zawierających dane będące tajemnicą służbową;
  - należy przestrzegać zasad użytkowania przenośnych komputerów osobistych;
  - należy przedsięwziąć odpowiednie środki zabezpieczenia urządzeń składowania danych przed kradzieżą lub uszkodzeniem w czasie transportu, *(tj. zabezpieczenie transportowanych urządzeń, zabezpieczenie danych – kopie bezpieczeństwa)*.
- zasady bezpiecznego zbywania urządzeń:
  - zaleca się sprawdzenie wszystkich składników sprzętu zawierającego nośniki informacji, aby przed jego zbyciem upewnić się, że wszelkie informacje wrażliwe fizycznego licencjonowane oprogramowanie zostały usunięte lub bezpiecznie nadpisane.
- zasady dotyczące wynoszenia mienia:
  - zaleca się, aby sprzęt, informacje (dokumenty) lub oprogramowanie nie było wynoszone bez uprzedniego zezwolenia.

X.3. Zasady fizycznego zabezpieczenia aktywów

Za realizację zadań z §57 i §58 odpowiada osoba, której aktywa zostały powierzone pod opiekę.
Należy tak organizować przestrzeń pracy, by osoba postronna nie miała sposobności do zapoznania się z informacją, do posiadania której nie została upoważniona: należy odpowiednio ustawić meble, monitory komputerów itp.
Za realizację tego zadania odpowiada kierownik wewnętrznej komórki/referatu.[12]
Zasady regulujące postępowanie z nośnikami danych stanowią odrębny dokument Polityki Bezpieczeństwa Informacji.

Postępowanie z dokumentami oraz nośnikami danych (takimi jak np.: wyjmowalne dyski, CD-ROM-y, taśmy magnetyczne, pendrive`y) musi być oparte na sformalizowanych zasadach postępowania uwzględniających: warunki przechowywania, transportowania i niszczenia oraz fizyczne ograniczenia dostępu do tych nośników oraz zasady opuszczania przez nie siedziby Urzędu.

XI. Zarządzanie systemami i sieciami

XI.1. Zasady bezpiecznego korzystania z systemów informatycznych

Systemy informatyczne narażone są na działania niepożądane (w tym: 1- oprogramowanie szkodliwe typu wirus, keyloger, trojan, rotkit, bomba logiczna, robak itp. 2- uszkodzenia danych czy systemu).
Wszyscy użytkownicy powinni być świadomi tych zagrożeń i w miarę swych możliwości przeciwdziałać zagrożeniu stosując mechanizmy kontroli dostępu, profilaktykę antywirusową czy też w sposób odpowiedzialny zabezpieczać dane (kopie danych), jeżeli te nie są wykonywane automatycznie[13].

Dokonywanie zmian w korporacyjnym systemie informatycznym możliwe jest tylko przez pracowników komórki informatyki(ASI), którzy do tych celów, oprócz zwykłych kont użytkowników posiadają konta uprzywilejowane – tzw. administracyjne.

---

[12] Jeżeli realizacja tego zadania jest niemożliwa, należy taką informację przekazać do ABI. Stanowi ona jedno ze źródeł do szacowania ryzyka.
[13] Za zabezpieczenie systemu informatycznego poprzez tworzenie kopii bezpieczeństwa odpowiada pion informatyki.

Komórka informatyki(ASI) odpowiada za aktualność zainstalowanego w systemie oprogramowania antywirusowego oraz bezpieczne skonfigurowanie środowiska (aktualizacje systemowe, aktywacja zabezpieczeń, bezpieczna topologia sieci[14] itp.).
Wszelkie nośniki zewnętrzne powinny być przed ich użyciem wcześniej sprawdzone programem antywirusowym – w przypadku wykrycia programu szkodliwego należy o tym fakcie niezwłocznie powiadomić pracownika komórki informatyki(ASI).
Zabronione jest świadome wprowadzanie do środowiska korporacyjnego oprogramowania szkodliwego, mającego cechy powielania się, destabilizującego pracę systemu lub służącego do nieautoryzowanej zmiany uprawnień w systemie czy też wykradania danych z ww.
Wszelka dokumentacja systemowa powinna być przechowywana w sposób bezpieczny, a dostęp do ww. powinien być ograniczony do osób uprawnionych.

XI.2. Wycofywanie sprzętu i niszczenie nośników informacji

Jedynie osoby upoważnione przez Administratora danych (Wójta Gminy) mogą zbywać lub utylizować wyposażenie komputerowe oraz nośniki informacji stanowiące własność Urzędu.
W przypadku tymczasowego (np. w celach serwisowych) lub trwałego przekazania osobom trzecim sprzętu komputerowego, albo w przypadku jego likwidacji wszelkie nośniki danych powinny zostać ze sprzętu usunięte. Alternatywą dla usunięcia nośników jest bezpieczne usunięcie danych z ww.
Za wykonanie tej czynności odpowiada komórka informatyki (ASI).

XI.3. Dokumentacja

W skład dokumentacji wchodzi:

- dokumentacja systemu, w tym jego konfiguracja,
- dokumentacja aplikacji użytkowych,
- funkcjonujące procedury dotyczące systemu *(w tym procedury awaryjne)*,
- dokumentacja zabezpieczenia systemu (plany zabezpieczenia, polityka zabezpieczenia, dziennik, itp.).

Za obecność aktualnej dokumentacji odpowiada właściciel aktywów.
Za opracowanie aktualnej dokumentacji odpowiada komórka merytoryczna posiadająca największy zasób wiedzy z przedmiotu opracowania.
Dostęp do poszczególnych części dokumentacji wynika z zakresu dostępu do systemu.

XI.4. Monitorowanie dostępu

Powinny *(jeżeli system daje taką możliwość)* być prowadzone rejestry zapisu *(logi)* wszystkich prób dostępu do aktywów systemu zarówno zakończonych sukcesem, jak i niepowodzeniem.
Rejestry kontroli dostępu powinny być analizowane w procesie audytu lub procedurach wykrywania naruszenia zabezpieczenia.
Podczas analizy powyższych logów należy zwrócić uwagę na:

- próby dostępu zakończone niepowodzeniem;
- charakterystykę wykorzystywania uprzywilejowanego dostępu;
- użytkowanie aktywów zawierających wrażliwą informację;
- analizę statystyczną procesu rejestrowania się użytkowników systemu w celu wykrycia nienormalnych zachowań.

[14] Np. wyłączenie nieużywanych gniazd sieciowych oraz inne działania wykluczające możliwości podłączenia „obcego" komputera do sieci korporacyjnej.

XII. Kontrola dostępu

XII.1. Zarządzanie dostępem użytkowników

1. Prawo dostępu do systemu informacyjnego *(lub jego cofnięcie)* nadaje Administrator danych (Wójt Gminy) lub osoba przez niego upoważniona.
2. Kierujący wewnętrzną komórką/referatem wnioskuje o przyznanie/cofnięcie dostępu do systemu informatycznego dla pracownika na podstawie zatwierdzonego przez Administratora danych (Wójta Gminy) wniosku, który przekazywany jest do realizacji Administratorowi Systemu Informatycznego wraz z realizacją wniosku o:

a) dostęp: pracownik staje się użytkownikiem systemu informatycznego.
b) cofnięcie dostępu: pracownik traci prawa dostępu.

Pracownik, któremu zostaje przyznane prawo dostępu musi być przeszkolony w zakresie bezpieczeństwa informacji.
Wymóg ten jest konieczny ze względu na fakt, iż:
bezpośrednio za bezpieczeństwo przetwarzanych informacji oraz za prawidłową eksploatację systemu i sprzętu informatycznego w przypisanym mu zakresie odpowiada użytkownik.
Za organizację procesu przetwarzania informacji odpowiedzialni są kierownicy komórek organizacyjnych/referatu.

XII.2. Dostęp do urządzeń drukujących i powielających

W przypadku drukowania/kopiowania lub oczekiwania na wydrukowanie/skopiowanie informacji określonej jako chroniona, użytkownik zobligowany jest zapewnić, by osoby nieuprawnione nie uzyskały dostępu do przetwarzanej przez niego informacji (np. być obecnym przy urządzeniu drukującym, po uzyskaniu wydruku zabezpieczyć wydruk z drukarki, po wykonaniu kopii musi zabezpieczyć kopię i oryginał).
Osoba, która oczekuje na wydruk/kopię musi być uprawniona do jej przeglądania.
Wszystkie zbędne kopie/wydruki powinny być w sposób bezpieczny zniszczone.

XII.3. Polityka haseł

Identyfikacja i uwierzytelnienie mają na celu zapewnienie autentyczności użytkowników systemu, rozliczalności wszystkich działań i zdarzeń zachodzących w systemie.

Przy wyborze hasła są możliwe dwie sytuacje:

- generacja hasła przez użytkownika:
  jeśli hasło jest wybierane przez użytkownika, to powinno być trudne do odgadnięcia, tzn. nie zawierać imion własnych, charakterystycznych liczb i dat, składać się zarówno z małych, jak i dużych liter, cyfr i znaków przestankowych;
- generacja hasła automatyczna:
  w przypadku automatycznego generowania hasła należy ustawić minimalną długość hasła i eliminować trywialne rozwiązania.

Wszystkie standardowe hasła *(np. ustawione przez producenta)* należy zastąpić innymi, wybranymi indywidualnie hasłami.
Wszystkie hasła administracyjne[15] występujące w systemie informacyjnym muszą być składowane celem zapewnienia ciągłości funkcjonowania.
Hasło administracyjne niezdeponowane jest hasłem nielegalnymi stosowanie go stanowi naruszenie bezpieczeństwa systemu. Za składowanie hasła odpowiada użytkownik tego hasła.

[15] Dotyczy haseł umożliwiających działania administracyjne, tj.: zakładanie, usuwanie haseł użytkowników, w tym innych haseł administracyjnych.

Hasła powinny być regularnie zmieniane (Jeżeli częstotliwość zmiany nie została ustalona inaczej, przyjmuje się domyślnie okres jednego miesiąca); Za zmianę hasła w systemie odpowiada użytkownik.
W przypadku utraty lub ujawnienia hasła należy je niezwłocznie zmienić oraz poinformować o tym fakcie pion informatyki (ASI).
Nieużywane konta/hasła muszą być blokowane.

XII.4. Karty elektroniczne*(o ile są w Urzędzie stosowane)*

Ogólne zasady korzystania z kart elektronicznych opierają się na stosowaniu poniższych reguł:

- Należy prowadzić rejestr wydanych kart elektronicznych. Jeżeli ilość kart jest znaczna *(np. są stosowane do identyfikacji w systemie kontroli dostępu w jednostce organizacyjnej)* to powinna istnieć procedura wydawania, rejestrowania, blokady, wymiany i niszczenia kart elektronicznych;
- Kopie kart elektronicznych pełniące podobną funkcję jak klucze mechaniczne czy też dostępowi do komputerów powinny być składowane w miejscu osobno ustalonym.
- Zaleca się by przy wyborze czytników kart oraz samych kart zapewnić by urządzenia te spełniały międzynarodowe standardy opracowane dla urządzeń tego typu w zakresie parametrów technicznych oraz zabezpieczenia przed uszkodzeniem.

XII.5. Kontrola dostępu do sieci

Dostęp do zasobów sieci jest ograniczony do osób uprawnionych.
Osobami uprawnionymi są:
-pracownik, którego przyznany zakres zadań wymaga dostępu do sieci,
-przedstawiciel firmy zewnętrznej (zakres czynności jest ujęty w umowie / porozumieniu zawartym między Urzędem a firmą zewnętrzną).
Uwierzytelnienie (weryfikacji tożsamości) może być realizowane na poziomie systemu, sieci lub komputerów.
Niedopuszczalna jest praca w systemie informatycznym na identyfikatorze innym niż własny.
Odstępstwo od tej zasady skutkuje m.in. odpowiedzialnością osoby udostępniającej za czyny popełnione na ww. identyfikatorze.
Zakres dostępu ograniczony jest do minimalnego poziomu umożliwiającego wykonanie zadań określonych zakresem zadań pracownika w systemie.
Za ciężkie naruszenie obowiązków pracowniczych należy uznać świadome uzyskanie przez użytkownika nieuprawnionego dostępu do systemu. *(np.: uzyskanie dostępu do dysku innego użytkownika bez jego wiedzy i zgody jest traktowane jako incydent informatyczny).*

Ze względu na fakt, iż informatyk (ASI) pracując z uprawnieniami administratora nie podlega żadnym ograniczeniom, muszą funkcjonować organizacyjne ramy zakresu i sposobu wykonywania obowiązków, tak aby maksymalnie ograniczyć ryzyko błędów lub nadużyć z jego strony *(np.: logi systemowe, dzienniki, rejestry, procedury postępowania, których przykładem może być wymóg nie pozostawiania bez opieki aktywnego terminala z logowaniem z prawami administratora).*
Powyższa zasada, tj. sformalizowane czynności realizowane w systemie dotyczą (choć może mniej jaskrawiej się to przejawia) wszystkich użytkowników systemu.

XII.6. Zarządzanie komputerami

Zarządzanie komputerami opiera się na następujących zasadach:
Dostęp do komputerów z wyłączeniem komputerów powszechnie dostępnych jest ograniczony. Własność tą uzyskuje się poprzez aktywację dostępnych zabezpieczeń *(np.: hasło BIOS, login do konta indywidualnego, blokada klawiatury, wygaszasz ekranowy z hasłem, oraz inne dostępne zabezpieczenia sprzętowe).*

Dostęp do komputera może mieć więcej niż jedna osoba – wtedy konieczne jest wyznaczenie osoby administrującej, odpowiedzialnej za bezpieczeństwo tego komputera *(zmiana hasła, brak aktualnej wersji oprogramowania antywirusowego, informowanie o nieprawidłowościach w funkcjonowaniu zabezpieczeń)*.
Do każdego komputera musi być prowadzona dokumentacja prowadzona np.w postaci dziennika komputerowego, w której zawarte są wszystkie istotne zmiany dotyczące sprzętu, zainstalowanego oprogramowania, przeprowadzonych działań (np.: konserwacje, przeglądy, naprawy, zmiany osoby administrującej), lokalizacji oraz osoby administrującej. Prawo do wpisu mają osoby uprawnione (np.: informatyk, elektronik, konserwujący sprzęt informatyczny).
W celu zapewnienia integralności systemu i zawartych w nim danych należy:

- aktywować kontrolę antywirusową, zapewniając regularnie aktualizacje bazy sygnatur programów szkodliwych,
- regularnie tworzyć kopie bezpieczeństwa istotnych danych.

Zabezpieczyć kopie posiadanego oprogramowania.
Za wdrożenie mechanizmów bezpieczeństwa (aktywację zabezpieczeń, obecność oprogramowania antywirusowego na komputerze, zgodność zainstalowanego oprogramowania z wykazem zawartym w dzienniku komputerowym oraz kopie bezpieczeństwa składowane na serwerze) odpowiada pion informatyki (ASI).
Za stosowanie mechanizmów zabezpieczeń odpowiada użytkownik (w tym za wykonanie kopii bezpieczeństwa – jeżeli nie jest ona czyniona zdalnie/automatycznie).
Należy zapewnić fizycznie odseparowane składowanych kopii od innych aktywów systemu informatycznego.
Obowiązek nadzoru stosowania zabezpieczeń przez użytkowników przypisany jest kierownikom wewnętrznych komórek organizacyjnych. Powyższy obowiązek ma charakter działań ciągłych.

XII.7. Kontrola dostępu do aplikacji i informacji

Obowiązujące są następujące założenia:

- prawa dostępu do aplikacji, części aplikacji lub informacji powinny być udzielane użytkownikom, którzy pełnią odpowiednie funkcje *(np. administratorom aplikacji, użytkownikom, zgodnie z zasadą separacji obowiązków i odpowiedzialności)*;
- definiowanie praw dostępu na podstawie grupy użytkowników lub profilów nie powinno uniemożliwiać rozliczenia poszczególnych użytkowników;
- nie należy udzielać praw dostępu ponad niezbędne minimum, wynikające z prawidłowego funkcjonowania aplikacji oraz konieczności zachowania poufności (informacji);

XII.8. Zarządzanie zabezpieczeniem komputerów przenośnych *(transportowanych)*

Na bezpieczeństwo danych zawartych w komputerze składa się zarówno fizyczna ochrona obiektu *(kontrola ruchu osobowego, kontrola dostępu do pomieszczeń poprzez stosowanie zabezpieczeń technicznych)* jak i uwierzytelnienie w systemie *(hasła na BIOS, system/ sieć, aplikację, plik)*. Ze względu na brak możliwości ciągłego zabezpieczenia fizycznego komputerów przenośnych należy szczególną uwagę zwrócić na zapewnienie możliwie wysokiego poziomu zabezpieczenia urządzenia z wykorzystaniem mechanizmów uwierzytelniania. Powyższe założenia sprowadzają się do następujących zasad:

- obowiązkiem użytkownika jest bezpośredni nadzór nad komputerem przenośnym w trakcie transportu (dopuszcza się transport bezpośredni przez użytkownika lecz dla komputerów zawierających dane stanowiące dużą wartość dla Urzędu, wskazane jest zapewnienie bezpiecznego transportu, tj. takiego który zmniejszy ryzyko m.in. kradzieży. Alternatywą jest zapewnienie zabezpieczenia kryptograficznego danych).

- obowiązkiem użytkownika jest bezpośredni nadzór nad komputerem przenośnym znajdującym się poza Urzędem;
- obowiązkiem użytkownika jest właściwe zabezpieczenie komputera na terenie macierzystej jednostki organizacyjnej/Urzędu lub oddanie urządzenia do przechowania do komórki Informatyki (ASI), którego obowiązkiem jest zabezpieczyć przekazany sprzęt;
- w celu zapewnienia awaryjnego dostępu do komputera i zawartych w nim danych użytkownik obowiązany jest do przekazania przełożonemu kompletu środków zabezpieczenia (np. przekazać w kopertach haseł dostępu do komputera/plików/aplikacji), których odtworzenie bez użytkownika jest niemożliwe lub uciążliwe;
- jeżeli są stosowane inne zabezpieczenia – dalej zwane żetonami dostępu - należy zapewnić awaryjny dostęp poprzez zwielokrotnienie dostępu i zabezpieczenie jednego z żetonów na wypadek w sytuacji naruszenia własności dostępności zasobów;
- za uaktywnienie dostępnych zabezpieczeń odpowiada informatyk (ASI);
- za stosowanie dostępnych zabezpieczeń odpowiada użytkownik (np.: odpowiada za aktywowanie blokowania klawiatury, stosowanie wygaszaczy ekranowych);

W przypadku przekazania komputera innemu użytkownikowi, użytkownik pierwotny zobligowany jest po konsultacji z przełożonym do usunięcia przetwarzanych przez siebie danych z przekazywanego komputera. Jeżeli czynność leży poza jego możliwościami zobligowany jest do zwrócenia się o pomoc do informatyka, który w obecności użytkownika usunie wskazane dane.

XII.9. Bezpieczeństwo komunikacji – INTERNET

Ryzyko, jakie niesie ze sobą udostępnienie aktywów systemu informacyjnego na zewnątrz, powinno być minimalizowane.

Zabrania się działań które mogą negatywnie wpłynąć na obraz Urzędu (rozsyłanie spamu, pobieranie nielegalnych lub nieetycznych treści).
Za stworzenie bezpiecznych warunków komunikacji odpowiada pion informatyki (ASI).

XIII. Zarządzanie incydentami związanymi z bezpieczeństwem informacji

Celem zdefiniowania tego obszaru zabezpieczenia jest zminimalizowanie negatywnych skutków niepożądanych zdarzeń w systemie informacyjnym, będących następstwem działań na szkodę tego systemu.

XIII.1. Zgłaszanie zdarzeń związanych z bezpieczeństwem

Najczęstszym naruszeniem zabezpieczenia jest:

- utrata usługi[16], urządzenia lub funkcjonalności[17];
- przeciążenie lub niepoprawne działanie systemu;
- błędy ludzkie;
- niezgodność z politykami, procedurami lub zaleceniami;
- naruszenie ustaleń związanych z bezpieczeństwem fizycznym;
- niekontrolowane zmiany systemu;
- niepoprawne działanie oprogramowania lub sprzętu;
- naruszenia dostępu.

Szczególnie: w systemach informatycznych:

- atak oprogramowania szkodliwego *(np. wirus, koń trojański)*,
- uszkodzenie systemu informatycznego,

[16] Np.: utrata dostępności, np. do katalogu sieciowego.
[17] Np.: wyczerpanie baterii w zamku elektronicznym - zamek przestaje działać.

- luki zabezpieczeń w systemie teleinformatycznym *(np. pliki na kopiach awaryjnych tracą zabezpieczenie wynikające z praw dostępu określonych w systemie operacyjnym)*,
- niewłaściwe skonfigurowanie systemu, którego skutkiem jest udostępnienie zasobów podmiotowi nieuprawnionemu *(np. brak hasła, brak aktywowanej funkcji blokady klawiatury czy wygaszacza ekranowego, czy obecność trwale aktywnych standartowych haseł)*,
- świadoma lub nieświadoma nieuprawniona ingerencja w system teleinformatyczny osób trzecich, tj.:
  - nieświadome – wynikające z braku wiedzy użytkownika dotyczącej obsługi,
  - nieświadome – wynikające z nieświadomego przekazania *(np. podpatrzenie przez osobę trzecią, atak socjontechniczny)* uprawnień dostępu podmiotowi nieuprawnionemu,
  - świadome – udostępnienie podmiotowi nieuprawnionemu dostępu do zasobów,
  - świadome – naruszenia poufności lub integralności systemu informatycznego *(udostępnienie plików, wydruków, lub ich uszkadzanie)*.

Ta lista nie wyczerpuje wszystkich możliwości, wskazuje jedynie kierunki na które należy zwrócić uwagę podczas codziennej pracy. Warto dodać, iż ok. 80% naruszenia zabezpieczeń spowodowane jest przez użytkownika. Dlatego też należy zmierzać w kierunku segmentowania dostępu/działań w systemie informacyjnym, tak, by maksymalnie utrudnić szkodliwe działania *(osobnym, wcześniej omawianym zagadnieniem jest odpowiednia polityka kadrowa)*.

Wiele przypadków naruszenia bezpieczeństwa w systemach informatycznych związana jest z oprogramowaniem złośliwym.

Informacje związane z obecnością takiego oprogramowania należy traktować jako chronioną.

1. Ogólny schemat postępowania na wypadek stwierdzenia naruszenia w systemie informacyjnym przedstawia się następująco:

a) **Użytkownik informuje kierującego komórką oraz pracownika komórki merytorycznie odpowiedzialnej za obszar zdarzenia[18] o nieprawidłowościach w funkcjonowaniu systemu;**
b) **Komórka merytorycznie odpowiedzialna za obszar zdarzenia szacuje wstępnie typ i zakres naruszenia;**
c) **Jeżeli sytuacja tego wymaga, tzn. zdarzeniu towarzyszą negatywne następstwa na skalę całego Urzędu, KBI (ABI) informuje o zdarzeniu Wójta Gminy, który po konsultacji z KBI podejmuje decyzję o sposobie dalszego działania (ustala sposób i rodzaj działań naprawczych).**
d) **Komórka merytorycznie odpowiedzialna za obszar zdarzenia przystępuje do przywrócenia systemu do stanu przed zdarzeniem.**
e) **Po przywróceniu stanu stabilnego komórka merytorycznie odpowiedzialna za obszar zdarzenia udostępnia system użytkownikowi oraz informuje (w formie potwierdzanej i zabezpieczonej kryptograficznie[19]: tj. e`mail wraz z podaniem numeru kontaktowego[20]) o przebiegu zdarzenia ABI.**
f) **Bezpośredni przełożony w porozumieniu z komórką merytorycznie odpowiedzialną za obszar zdarzenia decyduje o ewentualnej sankcji dla osoby odpowiedzialnej za wywołanie incydentu.**

[18] Np.: jeżeli zdarzenie dotyczy systemu informatycznego, należy poinformować informatyka (ASI).
[19] Poprzez wysyłkę pliku skompresowanego (np. zip, rar) z użyciem hasła co najmniej 10 znakowego.
[20] Po skontaktowaniu się przez ABI, tą drogą zostanie przekazane hasło.

2. W celu oszacowania typu i zakresu naruszenia należy ustalić:

- miejsce wystąpienia naruszenia (w przypadku systemów informatycznych np. aplikację lub komputer),
- zakres zdarzenia (w przypadku systemów informatycznych np. liczbę komputerów dotkniętych następstwami zdarzenia),
- rodzaj ujawnionej/uszkodzonej informacji,
- punkt, w którym nastąpiło zdarzenie,
- poziom oszacowanych szkód,
- szacunkowy czas, po którym naruszenie zostało(zostanie) zlikwidowane,
- aktywa systemu informacyjnego niezbędne w działaniach związanych z naruszeniem zabezpieczeń,
- implikacje organizacyjne i prawne.

Od momentu wykrycia naruszenia powinny być zabezpieczone wszystkie rejestry dokumentujące użytkowanie systemu.

XIII.2. Zgłaszanie słabości systemu bezpieczeństwa

Każdy z użytkowników (w tym pracownicy i użytkownicy zewnętrzni, np. wykonawcy) jest zobligowany do informowania o dostrzeżonych lub podejrzewanych słabościach systemu przełożonemu, który informuje o słabościach systemu KBI.

XIII.3. Zarządzanie incydentami związanymi z bezpieczeństwem informacji oraz udoskonaleniami

Zgłoszone incydenty bądź słabości systemu stanowią materiał źródłowy, który wykorzystywany jest w procesie zarządzania ryzykiem.

KBI (ABI) reagując na zgłaszane oraz wykryte w toku działań audytorskich słabości tworzy stosowne regulacje, które po konsultacji z kierownikami komórek/Referatów, których regulacje dotyczą, wdraża do stosowania.

W przypadku modyfikacji Polityki Bezpieczeństwa KBI(ABI) przekazuje dokument do zatwierdzenia Wójtowi Gminy.

XIV. Utrzymanie ciągłości działania

Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania

Nie każde częściowe lub całkowite uszkodzenie systemu informacyjnego wymaga uaktywnienia planów awaryjnych. Często uszkodzenia te można usunąć w krótkim czasie, zgodnie z rutynowymi procedurami. Sytuacja awaryjna lub katastrofalna pojawia się wtedy, gdy przywrócenie normalnego stanu pracy systemu informacyjnego w wymaganym czasie nie jest możliwe. Istotne jest by w planach awaryjnych uwzględniony został aspekt bezpieczeństwa informacji.

Osobą podejmującą decyzję o uruchomieniu planów awaryjnych jest Administrator danych (Wójt Gminy). Decyzję swoją podejmuje na podstawie informacji uzyskanych od kierujących komórkami, których zdarzenie dotyczy oraz KBI.

Za obecność aktualnych planów awaryjnych odpowiada właściciel aktywów.

Za opracowanie aktualnych planów awaryjnych odpowiada komórka merytoryczna posiadająca największy zasób wiedzy z przedmiotu opracowania.

Po przywróceniu systemu do stanu normalnego funkcjonowania, komórka merytorycznie odpowiedzialna za obszar zdarzenia udostępnia system użytkownikom oraz informuje o tym komórki, których zdarzenie dotyczyło.

XV. Działania testowe w systemie informatycznym

Działania testowe oraz rozwojowe mogą spowodować niezamierzone zmiany w systemie informatycznym. Dlatego też zaleca się, jeżeli jest to możliwe od strony technicznej dążyć do tego, by powyższe działania przeprowadzać z wykorzystaniem komputerów wydzielonych z zastosowań codziennego środowiska pracy do celów testowych.
Należy dążyć do tego, by podczas testów korzystać z danych fikcyjnych. Jeżeli jest to niemożliwe, po przeprowadzeniu testów wykorzystujących dane autentyczne, należy powyższe usunąć z systemu. Za wykonanie tej czynności odpowiada testujący (organizujący testy). Parametry komputerów testowych oraz oprogramowanie na nich zainstalowane (system operacyjny, oprogramowanie antywirusowe) powinny być takie same jak stosowane w codziennym środowisku pracy.

XVI. Zarządzanie zmianami

Wszystkie zmiany w systemie informacyjnym powinny być kontrolowane i dokumentowane przez Gestora i wskazani przez niego użytkownicy.
Chodzi przede wszystkim o to, aby zminimalizować ryzyko naruszenia bezpieczeństwa systemu informacyjnego poprzez naruszenie jego integralności i/lub ciągłości.
Obowiązek formalnego nadzoru dotyczy zmian w systemach operacyjnych, oprogramowaniu, urządzeniach i procedurach.
Należy więc:

1. Dokonywać tylko autoryzowane zmiany;
2. Prowadzić rejestr istotnych zmian w systemie informacyjnym *(prowadzi komórka wprowadzająca zmianę lub wskazana w osobnej procedurze)*;
3. Informować o wprowadzonych zmianach wszystkie zainteresowane komórki – zakres przekazanych informacji musi być adekwatny do zapotrzebowania poszczególnych komórek.

XVII. Audyt systemu zabezpieczenia

Pojęcie audytu jest definiowane w dwojaki sposób:
Zgodnie z pierwszą definicją, audyt oznacza przegląd rejestrów *(sekwencji rekordów)* zawierających informacje o zdarzeniach w systemie operacyjnym, aplikacjach oraz działaniach użytkowników. Rejestry te zapewniają systemowi rozliczalność. Należy podkreślić, że audyt rejestrów systemowych to także podstawowe źródło informacji przy wykrywaniu incydentów i rekonstrukcji zdarzeń.

Według drugiej definicji, audyt jest pojęciem szerszym i obejmuje przegląd dokumentacji i analizę mechanizmów zabezpieczeń w obszarze zarządzania, eksploatacji i techniki.
Audyt jest wtedy elementem procesu szacowania poziomu zabezpieczenia systemu informacyjnego.

Pierwsza z definicji dotyczy działań audytorskich prowadzonych przez komórkę informatyki i zamyka się w codziennych czynnościach sprawdzających rejestry, poprawność implementacji mechanizmów bezpieczeństwa, poprawność automatycznie tworzonych kopii bezpieczeństwa itp. Druga definicja stanowi podstawę działań kontrolnych osób kontrolujących np. zewnętrznych audytów/specjalistów ds. bezpieczeństwa

Audyt prowadzony przez ABI dotyczy spełniania w Urzędzie istniejących regulacji z zakresu bezpieczeństwa informacji.
Działania audytorskie oraz kontrolne przeprowadzane są zgodnie z obowiązującymi w Urzędzie regulacjami dotyczącymi tych działań.

XVIII. Zgodność przyjętych rozwiązań z obowiązującymi uregulowaniami / przepisami prawnymi:

Na projektowanie, eksploatowanie, używanie i zarządzanie systemami informacyjnymi mogą mieć wpływ wymagania bezpieczeństwa wynikające z ustaw, regulacji wewnętrznych i umów. W celu uniknięcia naruszeń przepisów prawa, zobowiązań wynikających z ustaw, regulacji wewnętrznych, umów oraz jakichkolwiek wymagań bezpieczeństwa, Gestorzy/Dysponenci odpowiadają za zidentyfikowanie ww. wymagań (określenie odpowiednich przepisów prawnych) oraz zapewnienie (zgodnie z obowiązującymi wewnętrznymi regulacjami w tym zakresie, przy współpracy w zakresie pomocy prawnej), by ryzyka związane z naruszeniem w tym obszarze były zminimalizowane do poziomu akceptowalnego.

Wójt Gminy Żurawica
Krzysztof Składowski

Załącznik nr 1
do Polityki Bezpieczeństwa Informacji
w Urzędzie Gminy Żurawica

Procedura nr 1
Zarządzanie systemem informatycznym
w Urzędzie Gminy Żurawica

Spis treści:

I. Zarządzanie dostępem do systemu informatycznego w Urzędzie

1. Do ochrony zasobów systemu informatycznego w Urzędzie stosuje się systemy kontroli dostępu oparte na mechanizmach uwierzytelniania[1] użytkownika.

Zarządzanie dostępem odbywa się w kilku obszarach, tj.:

a) zarządzania kontami użytkowników w systemie operacyjnym,
b) zarządzania dostępem do poczty elektronicznej,
c) zarządzania dostępem do zasobów sieciowych (katalogów sieciowych),
d) zarządzania dostępem do sieci INTERNET,
e) zarządzania dostępem do systemów informatycznych,

Niniejsza procedura określa zarządzanie systemem we wszystkich podanych wyżej kategoriach z wykluczeniem zarządzania dostępem do poszczególnych systemów informatycznych (konkretnych aplikacji), których sposób użytkowania oraz zarządzania dostępem określają opracowane indywidualnie procedury[2].

2. Systemowe konto użytkownika, indywidualne konto pocztowe oraz uprawnienie dostępu do sieci INTERNET są dalej nazywane uprawnieniami podstawowymi.
3. Warunkiem wnioskowania o przyznanie użytkownikowi dostępu do systemu informatycznego Urzędu jest jego znajomość przyjętych w Urzędzie rozwiązań z zakresu bezpieczeństwa informacji;

II. Szkolenie:

1. Dla użytkowników będących pracownikami Urzędu wymaganym trybem zapoznania się z zasadami bezpieczeństwa informacji jest uczestnictwo w szkoleniu organizowanym przez KBI, potwierdzone podpisem przeszkolonego na „liście osób przeszkolonych"[3].
2. Przy okresowych szkoleniach grupowych, organizowanych przez KBI, kierujący wewnętrzną komórką organizacyjną uzgadnia z KBI terminy szkoleń, które zapewnią możliwie dużą frekwencję.
3. W sytuacji, w której pracownik nie uczestniczył w organizowanych przez KBI szkoleniach okresowych (np. jest to nowozatrudniony pracownik), kierujący wewnętrzną komórką uzgadnia z KBI indywidualny termin szkolenia.
4. Kierujący na szkolenie (kierownik Referatu, bezpośredni przełożony)kontaktuje się z KBI i zgłasza potrzebę organizacji szkolenia.
5. Dla użytkowników, którzy dostęp do systemu uzyskują wskutek realizacji umowy, której są stroną, znajomość ww. zasad i ich zakres adekwatny do realizowanych dla Urzędu zadań, powinna zostać określona w treści umowy.

III. Zarządzanie kontami (utworzenie, zawieszenie, usunięcie) oraz dostępem do sieci INTERNET odbywa się za pomocą wniosków 1a – 1c niniejszej procedury.

Za wyjątkiem przypadków szczególnie umotywowanych (vide zał. nr 1a) dla każdego z użytkowników generowane jest konto systemowe z uprawnieniami podstawowymi (tj. bez możliwości dokonywania zmian w ustawieniach systemowych).

---

[1] Uwierzytelnienie polega na weryfikacji przedstawionej tożsamości.
[2] Osobą inicjującą i prowadzącą zadanie zgodnie z uprawnieniami jest KBI.
[3] Kierownicy wewnętrznych komórek organizacyjnych są zobowiązani do zapewnienia (poprzez skierowanie na szkolenie do KBI) podległym pracownikom przeszkolenia z tego zakresu, oraz do prowadzenia w podległej komórce „listy osób przeszkolonych" – wzór listy: zał. nr.4.

IV. Konta podstawowe

1. Ze względów bezpieczeństwa konfiguracja podstawowego systemowego konta użytkownika zakłada, że pięciokrotne błędne wprowadzenie hasła powoduje jego blokadę.
2. Składowanie haseł do kont podstawowych jest zbędne;
3. W przypadku zablokowania konta, użytkownik zawiadamia o zdarzeniu informatyka (ASI), który po stwierdzeniu, że przyczyną blokady nie jest incydent bezpieczeństwa, odblokowuje konto użytkownika (w przeciwnym wypadku nie odblokowując konta podejmuje działania określone dla obsługi incydentu).
4. Hasło użytkownika dla konta systemowego powinno być zmieniane co najmniej co 30 dni.
5. W celu zapewnienia odpowiedniego poziomu bezpieczeństwa należy zapewnić by długość hasła miała co najmniej 8 znaków, oraz by hasło było kombinacją literowo cyfrową (zaleca się, by w wyraz{y} tworzący{e} hasło włączyć cyfry, np.: zka21mys – chodzi o to by hasło było łatwo odtwarzalne metodą mnemotechniczną, przy jednoczesnej odporności na przełamanie).
6. Konfiguracja systemu powinna wymuszać realizację wymogów: zapewnienia złożoności hasła, oraz wymuszenia zmiany hasła z określoną częstotliwością.
7. Hasło do konta pocztowego powinno być zmieniane nie rzadziej niż raz na pół roku oraz w przypadku podejrzenia, że zostało skompromitowane. Sposób tworzenia hasła do konta pocztowego jest identyczny z przedstawionym wyżej dla konta systemowego.

V. Konta uprzywilejowane (administratora)

1. Pracownikiem szczególnie uprawnionym jest Administrator Systemu Informatycznego (ASI), który oprócz kont z uprawnieniami podstawowymi, posiada konta uprzywilejowane (konta administracyjne).
2. Konto administratora powinno być używane tylko podczas czynności administracyjnych – przy innych działaniach administrator powinien używać systemowego konta podstawowego.
3. Niedopuszczalne jest pozostawienie stacji z aktywnym kontem administracyjnym bez nadzoru – za naruszenie tej zasady pełną odpowiedzialność ponosi właściciel konta.
4. Funkcja administratora nie upoważnia do zapoznania się z treścią zawartą w zasobach użytkowników.
   Sytuacja taka może mieć miejsce jedynie w przypadku uzgodnienia takiego działania z właścicielem zasobów, Wójtem Urzędu, przy formalnym potwierdzeniu takiej zgody.
   Naruszenie tej zasady jest równoważne naruszeniu obowiązków pracowniczych i po wykryciu stanowi podstawę do wszczęcia postępowania wyjaśniającego i nałożenia kary za ww. czyn.
5. Częstotliwość zmiany haseł kont administracyjnych ustala Administrator Systemu Informatycznego (ASI) w sposób zapewniający bezpieczeństwo systemu.
6. Hasła administratora muszą być składowane i opisane w sposób jednoznacznie identyfikujący: system, konto, właściciela konta, oraz datę zdeponowana.
7. Częstotliwość zmiany haseł oraz sposób deponowania haseł musi zostać określona w instrukcji składowania haseł administracyjnych, za opracowanie której odpowiada Administrator danego systemu (ASI).

VI. Konta pocztowe

1. W Urzędzie mogą występować dwa rodzaje elektronicznych kont pocztowych:
   a) indywidualne (przypisane do osoby, np. Jana Kowalskiego)
   b) funkcyjne (przypisane do zadania, np. działalności sekretariatu)

2. Nazwa konta indywidualnego tworzona jest wg reguły:
   [pierwsza litera imienia][nazwisko]@.....

UWAGA: w nazwie nie stosuje się polskich znaków diakrytycznych
(zostają zamienione wg reguły: ń →n)

3. W przypadku ewentualnego dublowania nazw skrzynki przy stosowaniu ww. reguły należy nowotworzoną skrzynkę uzupełnić o kolejną literę imienia. Przy wyczerpaniu tej metody należy zastosować indeksy cyfrowe (np. w Urzędzie pracuje 2-ch Janów Kowalskich, więc zgodnie z podaną zasadą utworzone zostaną konta: j.kowalski@..... oraz ja.kowalski@.....
4. Nazwa konta funkcyjnego tworzona jest wg reguły:
   [nazwa]@....., gdzie nazwą może być np. „sekretariat".

UWAGA: w nazwie nie stosuje się polskich znaków diakrytycznych
(zostają zamienione wg reguły: ń →n)

5. Konto funkcyjne przypisane jest do konkretnej osoby (określonej we wniosku o utworzenie kont podstawowych użytkownika).
6. W przypadku nieobecności tej osoby i konieczności zapewnienia dostępu do konta funkcyjnego, kierujący komórką organizacyjną w dyspozycji którego znajduje się ww. konto realizuje wniosek o utworzenie kont podstawowych użytkownika, zmieniając właściciela skrzynki (opcja „Zmiana właściciela funkcyjnego konta pocztowego");
7. Standardowy rozmiar konta pocztowego to 100 MB. Potrzebę zwiększenia rozmiaru skrzynki wraz z uzasadnieniem należy przedstawić we Wniosku o nadanie uprawnień podstawowych użytkownika, w polu: „Szczegółowy, umotywowany opis uprawnień w systemie, jeżeli inny niż standardowy".

VII. <u>Zarządzanie zasobami znajdującymi się na dyskach sieciowych (utworzenie i usunięcie grupy, dodanie i usunięcie użytkownika do grupy) odbywa się za pomocą wniosków 2 – 3b.</u>

1. Każda komórka organizacyjna może mieć utworzoną dowolną strukturę własnych katalogów sieciowych.
2. Dostęp do tak zdefiniowanych zasobów realizowany jest poprzez tzw. grupę (np. kilku pracowników danej komórki organizacyjnej), której przysługują zadane prawa, np.: prawo do odczytu, prawo do zapisu[4] lub pełne prawa[5].
   Zarządzanie zasobami realizowane jest za pomocą wniosku 2, natomiast zarządzanie grupami za pomocą wniosków 3a i 3b.
3. Zakłada się, że Administrator Systemu Informatycznego (ASI) posiada pełne prawa do wszystkich katalogów sieciowych – tworzenie dla tej grupy użytkowników wniosków oraz ewidencjonowanie jest zbędne.
4. Kierownicy komórek organizacyjnych mają prawo wnioskowania o dostęp tylko do zasobów, dla których są właścicielami.

A. *Czynności podejmowane w celu uzyskania dostępu użytkownika do kont podstawowych*:

1) Przełożony użytkownika wypełnia „Wniosek o utworzenie kont podstawowych użytkownika", którego wzór stanowi załącznik nr 1a do niniejszych zasad, oraz przekazuje ww. do realizacji Administrator Systemu Informatycznego (ASI).

---

[4] W tych uprawnieniach mieści się prawo do wykonywania i modyfikacji.

[5] Odczyt, zapis, kasowanie danych, tworzenie podkatalogów wraz z nadawaniem uprawnień.

a) Administrator Systemu Informatycznego (ASI) realizuje wniosek w systemie, zakładając dla użytkownika tzw., hasła techniczne, którego zmiana zostanie wymuszona przy pierwszym logowaniu użytkownika.
b) Administrator Systemu Informatycznego (ASI) informuje użytkownika o utworzeniu kont(a) i konieczności zmiany hasła przy pierwszym logowaniu.
c) Użytkownik niezwłocznie wykonuje pierwsze logowanie i zmianę hasła na własne.
d) Administrator Systemu Informatycznego (ASI) przechowuje wniosek oraz uzupełnia ewidencję użytkowników[6].

B. Czynności podejmowane w celu cofnięcia dostępu użytkownika do kont podstawowych:

a) W przypadku ustania stosunku pracy z pracownikiem Pracownik ds. kadr przekazuje kopię karty obiegowej do Administratora Systemu Informatycznego (ASI), na podstawie której Administrator Systemu Informatycznego (ASI) usuwa wszelkie konta użytkownika[7].
b) Jeżeli przyczyna wniosku o cofnięcie dostępu jest inna niż ustanie stosunku pracy, za wypełnienie i przekazanie do realizacji „Wniosku o usunięcie kont podstawowych użytkownika", (według wzoru z załącznika nr 1b do niniejszych zasad), odpowiada przełożony użytkownika.
c) Administrator Systemu Informatycznego (ASI) realizuje wniosek w systemie.
d) Administrator Systemu Informatycznego (ASI) przechowuje wniosek.

C. *Czynności podejmowane w celu zablokowania dostępu użytkownika do kont podstawowych*[8]:

a) Przełożony użytkownika wypełnia „Wniosek o zablokowanie kont podstawowych użytkownika", którego wzór stanowi załącznik nr 1c do niniejszych zasad, oraz przekazuje ww. do realizacji Administratorowi Systemu Informatycznego (ASI).
b) Administrator Systemu Informatycznego (ASI) realizuje wniosek w systemie.
c) Administrator Systemu Informatycznego (ASI) przechowuje wniosek oraz uzupełnia ewidencję użytkowników.

D. *Czynności podejmowane w celu utworzenia lub usunięcia zasobów*:

a) Kierownik komórki organizacyjnej/referatu/bezpośredni przełożony pracownika wypełnia „Wniosek o utworzenie/usunięcie zasobów", którego wzór stanowi załącznik nr 2 do niniejszych zasad, oraz przekazuje ww. do realizacji Administratorowi Systemu Informatycznego (ASI).
b) Administrator Systemu Informatycznego (ASI) realizuje wniosek w systemie.
c) Administrator Systemu Informatycznego (ASI) informuje przedstawiciela Gestora (kierującego wew. kom.) o realizacji wniosku.
d) Administrator Systemu Informatycznego (ASI) przechowuje wniosek oraz uzupełnia ewidencję zasobów[9].

---

[6] Forma prowadzonej ewidencji jest dowolna (może być prowadzona w formie elektronicznej). Sposób prowadzenia ww. określa ASI w osobnej instrukcji.
[7] Należy zapewnić, by w przyszłości nie zostały użyte nazwy kont, które kiedyś były przyznane innemu użytkownikowi.
[8] Wniosek przydatny np. w przypadku dłuższej nieobecności użytkownika w pracy.
[9] Forma prowadzonej ewidencji jest dowolna (może być prowadzona w formie elektronicznej). Sposób prowadzenia ww. określa ASI w osobnej instrukcji.

E. *Czynności podejmowane w celu utworzenia lub modyfikacji grupy użytkowników*:

a) Kierownik komórki organizacyjnej/referatu/bezpośredni przełożony pracownika wypełnia „Wniosek o utworzenie/modyfikację grupy użytkowników", którego wzór stanowi załącznik nr 3a do niniejszych zasad, oraz przekazuje ww. do realizacji Administratorowi Systemu Informatycznego (ASI).
b) Administrator Systemu Informatycznego (ASI) realizuje wniosek w systemie.
c) Administrator Systemu Informatycznego (ASI) przechowuje wniosek oraz uzupełnia ewidencję grupy użytkowników[10].

F. *Czynności podejmowane w celu usunięcia grupy użytkowników*:

a) Kierownik komórki organizacyjnej/referatu/bezpośredni przełożony pracownika wypełnia „Wniosek o usunięcie grupy użytkowników", którego wzór stanowi załącznik nr 3b do niniejszych zasad, oraz przekazuje ww. do realizacji Administratorowi Systemu Informatycznego (ASI).
b) Administrator Systemu Informatycznego (ASI) realizuje wniosek w systemie. Jeżeli do zasobu nie jest uprawniony żaden użytkownik, to po konsultacji z właścicielem zasobu podejmowana jest decyzja o jego archiwizacji lub usunięciu.
c) Administrator Systemu Informatycznego (ASI) przechowuje wniosek oraz uzupełnia ewidencję grupy użytkowników.

VIII. Zasady użytkowania systemu informatycznego

1. Pracownik, któremu oddano do użytku sprzęt komputerowy (dalej zwany użytkownikiem) jest zobowiązany do:
   a) zabezpieczania dostępu do komputera poprzez nadzór nad powierzonym sprzętem oraz stosowanie loginów, haseł i praw dostępu do zasobów.
   b) zabezpieczania dostępu do pomieszczeń w których znajduje się sprzęt komputerowy pod nieobecność użytkownika.
   c) Zwracanie uwagi na niewłaściwe działanie systemu informatycznego i zgłaszanie takich stanów do Administratora Systemu Informatycznego (ASI) (szczególnie dotyczy to zdarzeń związanych z działaniem programów szkodliwych, np. wirusów komputerowych).
   d) podłączania swoich komputerów i urządzeń peryferyjnych wyłącznie do gniazdek zasilających komputerów z uziemieniem (zerowaniem)[11].
   e) wyłączania komputera oraz urządzeń peryferyjnych po zakończeniu pracy.
   f) dbania o czystość (czyszczenie z kurzu i innych zanieczyszczeń) powierzonego mu sprzętu, a w szczególności obudów, monitorów, klawiatur i myszy komputerowych.
2. System informatyczny jest przeznaczony do wykorzystania wyłącznie w zakresie działalności prowadzonej przez Urząd przy zastosowaniu oprogramowania, którego użycie jest zgodne z prawem[12]. W związku z powyższym:
   a) osobą uprawnioną do zmian w systemie (instalacja oprogramowania, zmiany konfiguracji, itp.) jest Administrator Systemu Informatycznego (ASI). Użytkownik dokonując działań nieuprawnionych (np. instalując własne oprogramowanie) ponosi pełną odpowiedzialność za swe działanie: zarówno z tytułu naruszenia obowiązków pracowniczych, jak też odpowiedzialność cywilną i karną z tytułu naruszenia prawa (np. Ustawy o prawie autorskim i prawach pokrewnych -Dz. U. Nr 24 z dnia 23 lutego 1994 r. z późn. zmianami).

---

[10] Jak wyżej.
[11] Niestosowanie tej zasady może spowodować zniszczenie sprzętu komputerowego lub porażenie prądem
[12] Szczególnie z Ustawą o prawie autorskim i prawach pokrewnych (Dz. U. Nr 24 z dnia 23 lutego 1994 r. z późn. zmianami).

b) Urząd, jako właściciel swych zasobów ma prawo do wglądu i użytkowania[13] do wszelkich treści znajdujących się w zasobach administrowanych przez użytkowników (katalogi sieciowe, konta pocztowe, zasoby dyskowe).

3. Użytkownik powinien korzystać z systemu informatycznego zgodne z obowiązującym prawem, normami społecznymi i obyczajowymi. Za naruszenie ww. ponosi odpowiedzialność osobiście.
4. W związku z koniecznością dokonywania okresowych przeglądów stanu funkcjonowania oprzyrządowania sieci ustala się godziny serwisowe na poniedziałki od 7:30 do 9:30. Zasoby sieciowe są w tym czasie niedostępne dla użytkowników.

IX. Zarządzanie sprzętem informatycznym i programami

1. Administrator Systemu Informatycznego (ASI) prowadzi bieżącą ewidencję komputerów użytkowanych w Urzędzie wraz z ich konfiguracją wewnętrzną w formie Kart Technicznych (załącznik nr 5).
2. W razie zmiany konfiguracji, np. po awarii lub modernizacji, Administrator Systemu Informatycznego (ASI) wystawia nową zaktualizowaną Kartę Techniczną.
3. Sprzęt komputerowy i jego konfiguracja podlega okresowym inwentaryzacjom.
4. Administrator Systemu Informatycznego (ASI) prowadzi bieżącą ewidencję legalnego oprogramowania zainstalowanego na komputerach Urzędu w formie Kart Oprogramowania (załącznik nr 6).
5. W razie jakichkolwiek zmian w zakresie oprogramowania, Administrator Systemu Informatycznego (ASI) wystawia nową zaktualizowaną Kartę Oprogramowania.
6. Licencje na używane w Urzędzie oprogramowanie przechowuje Administrator Systemu Informatycznego (ASI) wraz z oryginalnymi nośnikami. Administrator Systemu Informatycznego (ASI) odpowiada za okresowe inwentaryzowanie oprogramowania i licencji.
7. Pomieszczenie, w którym zlokalizowane są serwery musi być zabezpieczone dostępowo i objęte nadzorem systemu przeciw włamaniowego. (Zdalne konsole dostępowe oraz stacje monitorujące muszą być zabezpieczone dostępowo).
8. Klucze do ww. pomieszczeń muszą być plombowane.
9. Za właściwe zabezpieczenie pomieszczeń, w którym zlokalizowane są serwery oraz zdalne konsole i stacje monitorujące odpowiada Administrator Systemu Informatycznego (ASI).
10. Wszelkie zgłoszenia dotyczące zmian w konfiguracji sprzętu, oprogramowania, sieci, jak również zgłoszenia niewłaściwej pracy ww. elementów należy zgłaszać do Administratora Systemu Informatycznego (ASI), która realizuje obsługę w tym zakresie.
11. W przypadku obsługi dotyczącej naprawy/modernizacji, Administrator Systemu Informatycznego (ASI) dokumentuje swe działanie poprzez sporządzenie „Protokołu naprawy/modernizacji komputera" (załącznik nr 7) w 2 egz., z których po jednym otrzymują użytkownik oraz Administrator Systemu Informatycznego (ASI).
12. W razie zmiany konfiguracji sprzętu sporządzana jest także nowa Karta Techniczna Komputera.

X. Zabezpieczenie danych

1. Zaleca się[14], by użytkownicy przechowywali ważne dane w katalogach sieciowych, które podlegają okresowej archiwizacji (zalecenie wynika również z tego, że dostęp do zasobu

---

[13] Za wyjątkiem zasobów, których sposób wykorzystania zdefiniowano w odrębnych umowach (np. uwzględniających prawa własności {współ-}twórcy).

[14] W przypadku uszkodzenia komputera stacjonarnego istnieje wysokie prawdopodobieństwo bezpowrotnego utracenia danych składowanych tylko na tym komputerze – bez kopii bezpieczeństwa.

mają wszyscy użytkownicy danej grupy, więc ewentualna nieobecność jednego z członków grupy nie wpłynie na efektywność pracy zespołu).

2. Administrator Systemu Informatycznego (ASI) zapewnia archiwizację zasobów systemowych (katalogów aplikacji wraz z konfiguracją i danymi, zasobów służących do bieżącej działalności Urzędu), oraz archiwizację danych zawartych w katalogach sieciowych grup użytkowników z częstotliwością zależną od możliwości systemu informatycznego.
3. Sposób realizacji zadania wykonania kopii oraz harmonogram wykonywanych kopii określa Administrator Systemu Informatycznego (ASI) w osobnej instrukcji.
4. Wszelkie dane przesyłane w formie elektronicznej (np. za pośrednictwem poczty elektronicznej), dla których istotne jest zapewnienie poufności, powinny być przesyłane z wykorzystaniem środków kryptograficznych. Do czasu wdrożenia rozwiązania systemowego przez Administratora Systemu Informatycznego (ASI) wymaganym sposobem zabezpieczania przesyłanych plików jest stosowanie przez użytkowników narzędzi do kompresji danych (zależnie od narzędzia zainstalowanego w systemie) z opcją zabezpieczania hasłem[15].

XI. Zarządzanie zasobami

1. Zgodnie z Polityką Bezpieczeństwa Informacji, rozdział VIII – Zarządzanie aktywami, każda udostępniana w sieci komputerowej usługa lub zasób posiadają swoich gestorów/dysponentów.
2. Gestorem/dysponentami mogą być:
   a) Osoby posiadające prawo dysponowania wskazanymi usługami i zasobami.
   b) Administrator Systemu Informatycznego (ASI) w części dotyczącej usług i zasobów nie posiadających innych dysponentów.
3. Na dzień wejścia w życie zarządzenia, dysponentów poszczególnych usług i zasobów określa załącznik nr 8.
4. Użytkownik sieci może korzystać z usług i zasobów sieciowych za zgodą i w zakresie określonym przez dysponenta poszczególnych zasobów – wg zatwierdzonych wniosków dostępowych.

[15] Hasło powinno być odpowiednio złożone – zgodnie z zasadami dla kont podstawowych.

XII. Postępowanie w przypadku wykrycia oprogramowania szkodliwego

Jednym z istotnych zagrożeń dla systemu informatycznego w Urzędzie jest zagrożenie wynikające z działania oprogramowania szkodliwego: „wirusów", „trojanów", „rootkitów", „bomb logicznych", „keylogerów" itp.;

Szkodliwość tego typu programów, oprócz oczywistych strat polegających na uszkodzeniu, czy kradzieży danych, wiąże się również ze stratą czasu, jaka potrzebna jest na przywrócenie systemu do prawidłowego funkcjonowania – szczególnie w środowisku sieciowym, gdzie możliwa jest propagacja szkodliwego kodu na inne elementy systemu informatycznego.

Czas potrzebny na przywrócenie systemu do pracy może przekroczyć wartość krytyczną, tj. uniemożliwić skorzystanie z ww. systemu, dlatego też, konieczne jest wprowadzenie zasad, które zniwelują do tolerowanego minimum zagrożenia związane z oprogramowaniem szkodliwym.

Zostaje określone:

a) Postępowanie w przypadku wykrycia programu szkodliwego w systemie informatycznym,
b) Postępowanie z nośnikami zewnętrznymi,
c) Podział zadań związanych z profilaktyką antywirusową,

A. Postępowanie w przypadku wykrycia programu szkodliwego w systemie informatycznym

1. W przypadku wykrycia programu szkodliwego na nośniku zewnętrznym, niedozwolone jest korzystanie z tego nośnika do czasu potwierdzonego przez program antywirusowy usunięcia wykrytego oprogramowania szkodliwego (wszelkie wątpliwości w zakresie spełnienia tego warunku użytkownik ma obowiązek konsultować z Administratorem Systemu Informatycznego (ASI)).
2. Jeżeli program szkodliwy został wykryty, należy bezzwłocznie:
   a) **zaprzestać pracy w systemie do czasu usunięcia zagrożenia** (o czym poinformuje pracownik Administrator Systemu Informatycznego (ASI)),
   b) wstrzymać obieg nośników informatycznych, które były użytkowane na stanowisku, na którym pojawił się komunikat o obecności programu szkodliwego do czasu sprawdzenia nośników i przyzwolenia użycia nośników przez Administratora Systemu Informatycznego (ASI),
   c) **poinformować o wykryciu programu szkodliwego Administratora Systemu Informatycznego (ASI).**
3. Jeżeli w wyniku działania oprogramowania szkodliwego doszło do naruszenia bezpieczeństwa systemu informatycznego, szczególnie jeżeli uszkodzeniu lub zniszczeniu uległy istotne dane, np. dane osobowe, dane księgowe, Administrator Systemu Informatycznego (ASI) informuje o tym fakcie KBI (ABI) –zgodnie z §116 Polityki Bezpieczeństwa Informacji (dalsze działania wynikają z §116).
4. Po przywróceniu systemu do stanu bezpiecznego, Administrator Systemu Informatycznego (ASI) informuje użytkowników systemu o możliwości podjęcia pracy.

B. Postępowanie z nośnikami zewnętrznymi

1. Za nośnik zewnętrzny traktuje się każdy nośnik, który był wprowadzony/włączony do innego systemu informatycznego lub nie był kontrolowany przez oprogramowanie antywirusowe w Urzędzie, np.:
   a) pendrive włożony do gniazda USB na komputerze domowym,
   b) reklamowy nośnik z danymi, np. CD/DVD/Blu-ray dostarczona do Urzędu (np. w celach marketingowych),

c) komputer/dysk przenośny.

2. Każdy nośnik zewnętrzny należy[16] przed użyciem w systemie informatycznym sprawdzić programem antywirusowym poprzez pełne skanowanie nośnika.

W przypadku wykrycia programu szkodliwego należy zastosować zasady określone w §1, tj.: "Postępowanie w przypadku wykrycia programu szkodliwego w systemie informatycznym".

C. Podział zadań związanych z profilaktyką antywirusową

1. Każdy z pracowników odpowiada za kontrolę antywirusową nośników, które włącza do środowiska korporacyjnego oraz reagowanie w sytuacji pojawienia się oprogramowania szkodliwego w systemie (np. w sytuacji zgłoszenia infekcji przez program antywirusowy).
2. Kierujący wewnętrzną komórką organizacyjną zapewnia, by każdy z pracowników posiadający dostęp do systemu informatycznego był przeszkolony z zakresu bezpieczeństwa systemu informacyjnego[17].
3. Administrator Systemu Informatycznego (ASI) odpowiada za:

a) obecność i aktualność oprogramowania antywirusowego oraz odpowiednią jego konfigurację (wszędzie, gdzie jest to technicznie możliwe należy zapewnić zdalną aktualizację programu i sygnatur oraz raportowanie pracy programu[18]),
b) okresowe przeglądanie logów programu antywirusowego[19],
c) odpowiednią konfigurację aktywnych urządzeń sieciowych, programów pocztowych, przeglądarek internetowych, Firewall`i itp.
d) Zarządzanie poziomami uprawnień dostępu do systemu informatycznego w sposób zapewniający możliwie wysoki poziom bezpieczeństwa (dla zwykłych użytkowników za wystarczające uznaje się uprawnienia podstawowe, za pomocą których użytkownik nie jest w stanie dokonać zmian w konfiguracji systemu).
e) działania naprawcze w przypadku wykrycia oprogramowania szkodliwego.
f) opracowanie instrukcji użytkowania programu antywirusowego dla użytkowników.

XIII. Ustalenia końcowe

W celu zachowania spójności zapisów należy zapewnić obecność podsumowania stanu systemu na dzień wdrożenia niniejszego załącznika (wykazy użytkowników i ich uprawnienia dostępowe do systemu i zasobów). Za realizację zadania odpowiada Administrator Systemu Informatycznego (ASI).

XIV. Przepisy przejściowe

(Obowiązują do czasu wdrożenia indywidualnych procedur dla poszczególnych systemów informatycznych)

1. W przypadku nawiązania stosunku pracy z pracownikiem, który powinien mieć dostęp do wewnętrznej sieci komputerowej, bezpośredni przełożony tego pracownika, po uprzednio uzyskanej akceptacji ze strony Wójta Gminy, powinien wystąpić do Administratora Systemu Informatycznego (ASI) ze zleceniem (Karta uprawnień pracownika) dotyczącym

---

[16] W celu wykluczenia obecności programów szkodliwych.

[17] Szkolenie organizuje KBI; Jeżeli pracownik nie uczestniczył w szkoleniu organizowanym grupowo, Kierujący konsultuje z KBI termin szkolenia indywidualnego.
(Dostęp do systemu informacyjnego możliwy jest po potwierdzeniu odbycia przeszkolenia.)

[18] Raportowanie daje możliwość bieżącego nadzoru nad zdarzeniami w systemie antywirusowym, w tym reakcji na permanentne próby zainfekowania systemu np. z wybranej stacji.

[19] W celu monitorowania skuteczności wdrożonych rozwiązań i ustalenia najczęstszych źródeł (prób) infekcji a także w celach dokumentacyjnych.

udostępnienia pracownikowi praw korzystania z sieci. Zlecenie powinno zawierać imię i nazwisko pracownika, nazwę referatu i zajmowane przez niego stanowisko, zasoby sieciowe oraz usługi, z których pracownik będzie mógł korzystać, a także zakres czasu (dobowy i tygodniowy) w którym zasoby mają być udostępnione.

2. W przypadku rozwiązania z pracownikiem umowy o pracę (bez względu na jej rodzaj) lub jej wygaśnięcie (bez względu na jej przyczynę) Pracownik ds. kadr winien niezwłocznie przekazać pisemne zlecenie do Administratora Systemu Informatycznego (ASI) o odebranie pracownikowi praw dostępu do sieci. Wniosek powinien zawierać imię i nazwisko pracownika, dział i zajmowane stanowisko oraz termin (datę) odebrania praw dostępu do sieci.
3. Administrator Systemu Informatycznego (ASI) zobowiązany jest do nadawania, usuwania oraz prowadzenia ewidencji i praw dostępu do sieci komputerowej dla poszczególnych pracowników zgodnie z otrzymywanymi zleceniami.

Data.....

Wniosek o nadanie uprawnień podstawowych użytkownika

Wypełnia przełożony użytkownika

DOTYCZY:

☐ **Utworzenia konta systemowego**
☐ **Utworzenia konta pocztowego**
☐ **Zmiany właściciela funkcyjnego konta pocztowego**
☐ **Nadania uprawnień dostępu do sieci INTERNET**

Imię i nazwisko użytkownika	
Budynek/Pokój	
Nr telefonu	
Komórka organizacyjna	
Nazwa konta pocztowego *(obowiązkowe tylko w przypadku zmiany właściciela konta funkcyjnego)*	
Szczegółowy, umotywowany opis uprawnień w systemie, jeżeli inny niż standardowy:	

Użytkownik oświadcza, że znane mu są zasady dostępu do zasobów systemu informatycznego Urzędu i zobowiązuje się do ich przestrzegania.

Podpis użytkownika	Podpis przełożonego użytkownika
.....	.....

Wypełnia informatyk realizujący wniosek

Przyznany identyfikator logowania	
Przyznana nazwa konta pocztowego	
Data realizacji wniosku	
Imię i nazwisko osoby realizującej wniosek	
Podpis osoby realizującej wniosek	

Data.....

Wniosek o usunięcie uprawnień podstawowych użytkownika

Wypełnia przełożony użytkownika
lub, w przypadku ustania stosunku pracy – Pracownik ds. kadr

DOTYCZY:

☐ **Usunięcia konta z komputerowej sieci korporacyjnej**
☐ **Usunięcia konta pocztowego**
☐ **Cofnięcia dostępu do sieci INTERNET**

Imię i nazwisko użytkownika	
Budynek/Pokój	
Nr telefonu	
Nazwa konta sieciowego (podać tylko w przypadku istniejących kilku kont użytkownika)	
Nazwa konta pocztowego (podać tylko w przypadku istniejących kilku kont użytkownika)	
Komórka organizacyjna	

Podpis przełożonego
użytkownika

.....

Wypełnia informatyk realizujący wniosek

Data realizacji wniosku	
Imię i nazwisko osoby realizującej wniosek	
Podpis osoby realizującej wniosek	

Data.....

Wniosek o zablokowanie uprawnień podstawowych użytkownika

Wypełnia przełożony użytkownika

DOTYCZY:

☐ **Zablokowania konta w komputerowej sieci korporacyjnej**

☐ **Zablokowania konta pocztowego**

Imię i nazwisko użytkownika	
Budynek/Pokój	
Nr telefonu	
Nazwa konta sieciowego (podać tylko w przypadku istniejących kilku kont użytkownika)	
Nazwa konta pocztowego (podać tylko w przypadku istniejących kilku kont użytkownika)	
Komórka organizacyjna	

Podpis przełożonego użytkownika

.....

Wypełnia informatyk realizujący wniosek

Data realizacji wniosku	
Imię i nazwisko osoby realizującej wniosek	
Podpis osoby realizującej wniosek	

Data.....

Wniosek o utworzenie☒/usunięcie☐[20] zasobów

Wypełnia komórka wnioskująca

Komórka organizacyjna (Gestor zasobów)	
Imię i nazwisko osoby wnioskującej (Kierownik komórki organizacyjnej)	
Nr telefonu do kontaktu	
Nazwa zasobu 1(nazwa katalogu sieciowego)	
Nazwa zasobu 2(nazwa katalogu sieciowego)	
Nazwa zasobu 3(nazwa katalogu sieciowego)	
Nazwa zasobu 4(nazwa katalogu sieciowego)	
Nazwa zasobu 5(nazwa katalogu sieciowego)	

Podpis wnioskującego

.....

Wypełnia informatyk realizujący wniosek

Data realizacji wniosku	
Imię i nazwisko osoby realizującej wniosek	
Podpis osoby realizującej wniosek	

[20] Zaznaczyć właściwe pole.

Data .....

Wniosek o utworzenie☒/modyfikację☐[21] grupy użytkowników

Wypełnia komórka wnioskująca

Komórka organizacyjna (Gestor zasobów)	
Imię i nazwisko osoby wnioskującej (Kierownik komórki organizacyjnej)	
Nr telefonu do kontaktu	
Nazwa grupy	
Nazwa zasobu (nazwa katalogu sieciowego) **Uprawnienia**	..... Odczyt ☐ Zapis ☐ Pełne prawa ☐
Lista osób wchodzących w skład grupy:	

Podpis wnioskującego

.....

Wypełnia informatyk realizujący wniosek

Data realizacji wniosku	
Imię i nazwisko osoby realizującej wniosek	
Podpis osoby realizującej wniosek	

[21] Zaznaczyć właściwe pole.

Data.....

Wniosek o usunięcie grupy użytkowników

Wypełnia komórka wnioskująca

Komórka organizacyjna (Gestor zasobów)	
Imię i nazwisko osoby wnioskującej (Kierownik komórki organizacyjnej)	
Nr telefonu do kontaktu	
Nazwa grupy	
Decyzja dotycząca sposobu postępowania z zasobami grupy (dotyczy tylko sytuacji, kiedy do zasobów nie ma już przypisanej żadnej grupy)	Archiwizacja ☐ Usunięcie ☐

Podpis wnioskującego

.....

Wypełnia informatyk realizujący wniosek

Data realizacji wniosku	
Imię i nazwisko osoby realizującej wniosek	
Podpis osoby realizującej wniosek	

Wzór

Lista osób przeszkolonych
oraz oświadczenie pracowników

Ja niżej podpisany oświadczam, że:

1) Zostałem przeszkolony w zakresie bezpieczeństwa systemów informacyjnych, w szczególności zostałem zapoznany z Polityką Bezpieczeństwa Informacji oraz Procedurami do ww.,
2) Zapoznano mnie z treścią przepisów dotyczących ochrony danych osobowych, a w szczególności z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.), oraz rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.
3) Poinformowano mnie o odpowiedzialności wynikającej z Ustawy o prawie autorskim i prawach pokrewnych (Dz. U. Nr 24 z dnia 23 lutego 1994 r. z późn. zmianami).
4) Poinformowano mnie o obowiązku zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę (obowiązek ten wynika z art. 11 ust. 4 ustawy z 16 kwietnia 1993r. o zwalczaniu nieuczciwej konkurencji (Dz.U. z 2003 r. Nr 153, poz. 1503 ze zm.)) lub których ochrona wynika z odrębnych przepisów.

Treści z którymi zostałem(am) zapoznany(a) są dla mnie zrozumiałe i zobowiązuję się do ich przestrzegania przy pełnej świadomości konsekwencji wynikających z naruszenia ww. przepisów.

Lp.	Nazwisko i imię	Data przeszkolenia	Podpis osoby przeszkolonej	Komórka organizacyjna

Karta techniczna komputera Nr. .....

1. KOMPUTER: _____
   /nr inwentarzowy/
2. OBUDOWA: _____
3. MODEL (płyta gł. + procesor): _____
4. PAMIĘĆ RAM: _____
5. DYSK TWARDY: _____
6. STACJE DYSKIETEK: _____
7. KARTA GRAFIKI: _____
8. MONITOR: _____
9. KLAWIATURA: _____
10. MYSZKA: _____
11. WYPOSAŻENIE DODATKOWE:

1.	Karta dźwiękowa
2.	Karta sieciowa
3.	CD ROM
4.	INNE
5.	Drukarka

12. MIEJSCE INSTALACJI: _____
13. UŻYTKOWNIK: _____
    /imię i nazwisko/
14. DATA ZAKUPU: _____
15. CENA EWIDENCYJNA: _____
16. UWAGI: _____

Żurawica, dnia ..... 20.....r.

..... /sporządził/

..... /podpis użytkownika/

Karta oprogramowania komputera Nr. .....

1. KOMPUTER: ST-491/ 0
   /nr inwentarzowy/
2. MIEJSCE INSTALACJI: | 0
   /Oddział/ /dział/
3. UŻYTKOWNIK:
   /imię i nazwisko/
4. SYSTEM OPERACYJNY:

-DOS	1.		
-WINDOWS	2.		
-inny system operacyjny	3.		

4. NAKŁADKA:

1.	

2. WIELKOŚĆ HDD:

1.	

2. DOSTĘP DO PROGRAMÓW SIECIOWYCH:

1.	
2.	
3.	
4.	
5.	
6.	

7. PROGRAMY INDYWIDUALNE W KOMPUTERZE:

1.	
2.	
3.	
4.	
5.	
6.	
7.	
8.	
9.	
10.	
11.	
12.	
13.	
14.	
15.	
16.	
17.	
18.	
19.	
20.	

Żurawica, dnia ..... 20.....r.

....
/sporządził/ /podpis użytkownika/

Protokół naprawy/modernizacji nr ...../20.....

z dnia ..... 20.... r.

Dotyczy komputera nr : ..... nr inwent.: .....
Miejsce lokalizacji:..... Użytkownik: .....

Rodzaj naprawy/modernizacji: 1. .....

2. .....

Części zdemontowane:

Lp.	Nazwa części:	Stan techniczny:	Przeznaczenie:
1.			
2.			
3.			
4.			
5.			

Części zamontowane:

Lp.	Nazwa części:	Pochodzenie:	Data nabycia:	Przeznaczenie:
1.				
2.				
3.				
4.				
5.				

Podpisy:

..... /Informatyk/

..... /Użytkownik/

Wykaz Gestorów/Dysponentów usług i zasobów sieciowych Urzędu

wg stanu na dzień: .....r.

I.	USŁUGI	
Lp.	**Nazwa usługi**	**Gestor/Dysponent**
1.	Dostęp do Internetu	...
2.	Adres e-poczty	...
3.	Dostęp do serwera FTP (wpisy)	...

II.	ZASOBY	
Lp.	**Nazwa usługi**	**Gestor/Dysponent**
1.	Umowy, zamówienia, zlecenia	...
2.	Bank	
3.	Planowanie i budżetowanie	...
4.	Deklaracje elektroniczne	
5.	Sprzedaż	...
6.	Fakturowanie sprzedaży z magazynów	
7.	Kasa	...
8.		
9.	Automatyczna dekretacja księgowa	...
10.	Relacje z kontrahentami	
11.	Księgowość	
12.	Automatyczne księgowania w księgowości	
13.		
14.	Kadry i płace	...
15.	Rozliczenia finansowe	
16.	Rezerwa emerytalna	
17.	Rezerwa jubileuszowa	
18.	Środki trwałe	
19.	Kalkulacje	
20.	Wyposażenie	
21.	Zamówienia publiczne	
22.	Zakup	
23.	Rozliczenie VAT	
24.		
31.		

35.	Statystyki eksploatacyjne:	
	Czynsze	...
	Ekwiwalenty (odzież rob.)	
	Ekwiwalenty (śr. czystości)	
	Telefony komórkowe	
	Telefony TP	
	Transport	
	Rozliczenie paliwa	

URZĄD GMINY ŻURAWICA

UPRAWNIENIA DO SIECIOWYCH PROGRAMÓW KOMPUTEROWYCH

KARTA UPRAWNIEŃ PRACOWNIKA

.....	.....	.....	.....
imię i nazwisko	konto sieciowe	komórka organizacyjna	kierownik kom. organizacyjnej

DOSTĘP DO SIECIOWYCH PROGRAMÓW KOMPUTEROWYCH

PROGRAM		**RODZAJ UPRAWNIEŃ**		
Nazwa programu	Odczyt	Zapis	Modyfikacja	Kasowanie
1.	.....	.....	.....	.....
2.	.....	.....	.....	.....
3.	.....	.....	.....	.....
4.	.....	.....	.....	.....
5.	.....	.....	.....	.....
6.	.....	.....	.....	.....
7.	.....	.....	.....	.....
8.	.....	.....	.....	.....
9.	.....	.....	.....	.....
10.	.....	.....	.....	.....

CZAS DOSTĘPU

Dni tygodnia:	**Godziny:**
Poniedziałek:	.....
Wtorek:	.....
Środa:	.....
Czwartek:	.....
Piątek:	.....
Sobota:	.....
Niedziela:	.....

Żurawica, dnia ....
wypełnił

Procedura nr 3
Cykl rozwoju zbiorów informacyjnych oraz systemów informatycznych w Urzędzie Gminy Żurawica

§ 1. Zarządzanie bezpieczeństwem zbiorami informacyjnymi oraz systemami informatycznymi, dalej zwanymi systemem informacyjnym, obejmuje pełny cykl rozwoju: od fazy wstępnej, gdzie określone zostają wymagania, do wycofania z użycia.

1.1. Cykl rozwoju systemu informacyjnego dzieli się na następujące fazy:
- wstępną, której celem jest opracowanie założeń i wymagań bezpieczeństwa (w tym określenie akceptowalnego poziomu ryzyka bezpieczeństwa)
- budowy/wdrożenia, której celem jest bezpieczne wdrożenie systemu informacyjnego w Urzędzie Gminy;
- eksploatacji, której celem jest zapewnienie poprawnego i bezpiecznego funkcjonowania systemu informacyjnego;
- wycofania z eksploatacji, której celem jest przygotowanie systemu informacyjnego do zakończenia jego funkcjonowania.

1.2. W fazie wstępnej, powołany Dysponent (Gestor) systemu wraz z KBI określa wymogi, które są niezbędne dla właściwego i zgodnego z prawem wdrożenia i funkcjonowania systemu[1] oraz jego późniejszego skutecznego wycofania z eksploatacji.

Konieczne jest pisemne zdefiniowanie[2]:
- celu i zakresu przetwarzanych danych,
- przepisów prawa lub umów, na mocy których informacja w systemie ma być przetwarzana i chroniona,
- zbiorów danych i relacji między nimi w systemie,
- rodzaju informacji przetwarzanej w systemie i powiązania z innymi systemami,
- koniecznych funkcji w systemie (np.: administrator, użytkownik, informatyk) i zakresu realizowanych przez ww. zadań,
- obszarów przetwarzania,
- szacunkową wielkość strat dla Urzędu, jakie mogłyby powstać, na skutek utraty przez informacje przetwarzane w systemie poufności, dostępności lub integralności.

1.3. W fazie budowy/wdrożenia istotne jest poprawne wdrożenie ustaleń, które miały miejsce w fazie pierwszej. Na etapie wdrożenia, Właściciel (Gestor) wyznacza użytkowników i administratorów aplikacji w sposób określony w fazie wstępnej.

1.4. W fazie eksploatacji działania zorientowane są na prawidłowe, zgodne z obowiązującymi procedurami użytkowanie systemu.

1.5. Faza wycofania systemu wiąże się z likwidacją systemu informacyjnego zgodnie z określonymi w fazie wstępnej zasadami. Jeżeli istnieje taka możliwość[3], dane z systemu oraz sam system zostają usunięte.

---

1 Szczególnie należy zwrócić uwagę na Rozporządzenie rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych(Dz. U. z 2012r. poz. 526) i na Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. 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 2004r. Nr 100, poz.1024).

2 Zdefiniowanie tych obszarów stanowi element dokumentacji bezpieczeństwa systemu informacyjnego.

3 Zazwyczaj natychmiastowe usunięcie jest niemożliwe ze względu na obowiązujące przepisy, np. Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach, jak też przepisy wykonawcze do ww.