ZARZĄDZENIE NR 0050.100.2021
WÓJTA GMINY LIPIE

z dnia 31 grudnia 2021 r.

w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji

Na podstawie art. 30 ust. 1 ustawy z dnia 8 marca 1990 roku o samorządzie gminnym (Dz.U. z 2020 r. poz. 713 t.j.) oraz art. 24 ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych osobowych)

Wójt Gminy Lipie
zarządza, co następuje:

§ 1. Wprowadza się w Urzędzie Gminy Lipie dokument o nazwie Polityka Bezpieczeństwa Informacji, którego treść stanowi załącznik nr 1 do zarządzenia.

§ 2. Każdy pracownik, zgodnie z wykazem, jest obowiązany zapoznać się z treścią załącznika nr 1.

§ 3. Pracodawca zobowiązuje wszystkich pracowników do przestrzegania Polityki Bezpieczeństwa Informacji pod groźbą konsekwencji służbowych, przewidzianych prawem.

§ 4. Zarządzenie wchodzi w życie z dniem ogłoszenia.

Wójt Gminy Lipie

Bożena Wieloch

Załącznik do zarządzenia Nr 0050.100.2021
Wójta Gminy Lipie
z dnia 31 grudnia 2021 r.

POLITYKA BEZPIECZEŃSTWA INFORMACJI
URZĄD GMINY LIPIE

Spis treści

1. Wprowadzenie określenie kontekstu

Informacje podobnie jak inne ważne aktywa są niezbędne do właściwego funkcjonowania każdej organizacji i z tej racji niezmiernie istotnym jest dbałość o ich odpowiednie zabezpieczenie i ochronę. Ich bezpieczeństwo oraz systemów, w których są przetwarzane jest jednym z podstawowych elementów zapewniających realizację zadań gminy. Urząd Gminy wykonuje zadania publiczne służące zaspokajaniu potrzeb mieszkańców, a wynikające z postanowień przepisów prawa. Spełnienie uzasadnionych oczekiwań klientów i wymogów przepisów prawa w zakresie zapewnienia odpowiedniego poziomu bezpieczeństwa zawartych w nich informacji jest jego zasadniczym obowiązkiem. Utrata takich jego atrybutów jak poufności, integralności, dostępności, autentyczności lub niezawodności może mieć negatywny wpływ na bieżącą działalność i wizerunek Urzędu.

Bezpieczeństwo informacji w Urzędzie Gminy oznacza jej ochronę przed szerokim spektrum zagrożeń, minimalizację ryzyka oraz zapewnienie ciągłości działania i realizację zadań na odpowiednim poziomie. Jest ono osiągane poprzez wdrożenie odpowiedniego zestawu zabezpieczeń takich jak procesy, procedury, zabezpieczenia fizyczne, rozwiązania organizacyjne oraz adekwatne funkcje oprogramowania i sprzętu.

Miarą bezpieczeństwa informacji jest poziom ryzyka naruszenia jego podstawowych atrybutów. Uznaje się, że bezpieczeństwo informacji jest zapewnione, jeżeli ryzyko nie przekracza akceptowalnych parametrów przy zachowaniu zasad sformułowanych w niniejszej Polityce.

Polityka Bezpieczeństwa Informacji (PBI) to zbiór ogólnych zasad i podstawowych wymagań, określających, w jaki sposób powinny być zarządzane, udostępniane i chronione przed nieupoważnionym wykorzystaniem, zniszczeniem lub nieautoryzowanymi zmianami materialne i informacyjne aktywa Urzędu Gminy. Określa w szczególności zasady ochrony infrastruktury, zasobów informatycznych i ludzkich. Zasady zarządzania ryzykiem, role i zadania osób uczestniczących w procesie przetwarzania informacji. Reguluje postępowanie osób korzystających z urządzeń i technologii Urzędu Gminy. Wdrożony w Urzędzie System Zarządzania Bezpieczeństwem Informacji oparty jest na międzynarodowej normie ISO/IEC 27001:2005.

System ten wdrożony został z wykorzystaniem podejścia procesowego. Bezpieczeństwo informacji w Urzędzie jest rozumiane jako:

- ochrona danych mieszkańców i interesantów, które są przetwarzane w Urzędzie,
- zapewnienie bezpieczeństwa i ciągłości świadczenia usług,
- systematyczne zarządzanie ryzykiem na podstawie przyjętej metody oceny ryzyka,

- prowadzenie analizy wprowadzanych zmian w Urzędzie i ich wpływu na bezpieczeństwo,
- zapewnienie bezpieczeństwa osobowego.

Podstawą SZBI jest opracowana i udokumentowana analizy ryzyka uwzględniająca zagrożenia i słabości mające wpływ na bezpieczeństwo informacji przetwarzanych w Urzędzie, jak również skutki związane z wystąpieniem tych zagrożeń. Szacowanie ryzyka przeprowadzane jest systematycznie a wynikiem jej realizacji jest Plan postępowania z ryzykiem, który określa szczegółowe zadania mające na celu poprawę bezpieczeństwa informacji przetwarzanych w Urzędzie.

W rozdziale „Klasyfikacja informacji" określono podział informacji przetwarzanych w Urzędzie, jak również zdefiniowano sposób przetwarzania tych informacji zarówno w formie papierowej jak i elektronicznej.

System Zarządzania Bezpieczeństwem Informacji zawiera podstawowe zasady bezpieczeństwa odnoszące się do wszystkich pracowników, a tym samy ma pośredni wpływ na wszystkie zidentyfikowane procesy. Dodatkowo opracowano szczegółowe procedury i instrukcje, które maja bezpośredni wpływ na funkcjonowanie Zintegrowanego Systemu Zarządzania.

2. Deklaracja o ustanowieniu polityki zarządzania bezpieczeństwem informacji

Misją Urzędu Gminy Lipie jest profesjonalna, skuteczna i efektywna realizacja prawnie przewidzianych i statutowo przypisanych jej zadań publicznych w sposób zgodny z prawem, oszczędny i terminowy, ukierunkowanych na promocję i rozwój społeczno-gospodarczy gminy oraz kompetentna, sprawna i uprzejma obsługa interesantów według ściśle określonych zasad. Istotnym elementem sprawnej realizacji wyżej określonej misji oraz innych obowiązujących w gminie regulacji dotyczących rozwoju i właściwego funkcjonowania gminy jest właściwe zabezpieczenie przetwarzanych tu informacji przed istniejącymi zagrożeniami w tym w szczególności niezakłócone działanie systemów informacyjnych.

Wójt Gminy oświadcza, że ma świadomość znaczenia przetwarzanych w Urzędzie Gminy informacji dla realizacji misji i celów statutowych Urzędu Gminy i wynikającej stąd potrzeby ich ochrony. Wobec powyższego zobowiązuje się do podejmowania niezbędnych działań mających na celu kompleksowe zabezpieczenie informacji jako zasobu podlegającego ochronie prawnej i niezbędnego do prawidłowego oraz sprawnego funkcjonowania struktur Urzędu Gminy poprzez budowę systemu zarządzania bezpieczeństwem informacji. Gwarancją sprawnej i skutecznej ochrony informacji będzie zapewnienie odpowiedniego poziomu kultury bezpieczeństwa oraz zastosowanie przemyślanych rozwiązań technicznych, właściwy dobór kadry pracowniczej, prawidłowe wyposażenie stanowisk i narzędzi pracy oraz dbałość o niezbędną wiedzę i świadomość pracowników.

W związku z powyższym, a również w celu spełnienia wymagań prawnych w odniesieniu do ochrony informacji Wójt Gminy ustanawia Politykę Bezpieczeństwa Informacji zgodną z rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych oraz podejmuje wysiłki związane z jej wdrożeniem oraz nieustannym doskonaleniem, deklaruje zapewnienie optymalnych warunków i niezbędnych środków finansowych dla realizacji celów zawartych w Polityce Bezpieczeństwa Informacji oraz stałą współpracę z osobami wyznaczonymi w celu jej wdrożenia, doskonalenia i nadzorowania bieżącego funkcjonowania.

Wdrożony system określa kierunek działania Urzędu Gminy w celu zapewnienia systemowego nadzoru nad gromadzeniem, przetwarzaniem, przechowywaniem i udostępnianiem informacji, niezależnie od sposobu realizacji tych procesów.

3. Zakres obowiązywania

Zakres Polityki Bezpieczeństwa Informacji odnosi się do:

1. Komórek organizacyjnych znajdujących się w strukturze organizacyjnej, która zamieszczona jest w Regulaminie Organizacyjnym Urzędu Gminy.
2. Pomieszczeń, w których przetwarzane są informacje podlegające ochroną zlokalizowanych w budynku Urzędu Gminy.
3. Zasobów informacyjnych (aktywów) zaangażowanych w realizację zadań publicznych, a w szczególności:
   a) potencjału ludzkiego, czyli wszystkich pracowników Urzędu Gminy w rozumieniu przepisów Kodeksu Pracy, stażystów, praktykantów, wolontariuszy oraz inne osoby i instytucje mające dostęp do informacji podlegających ochronie;
   b) dokumentów papierowych i elektronicznych będących własnością Urzędu Gminy lub klientów Urzędu Gminy, o ile zostały przekazane na podstawie przepisów prawnych lub umów;
   c) sprzętu komputerowego oraz innych nośników danych (np. pamięci przenośne, optycznych - CD-R, DVD-R), na których znajdują się informacje podlegające ochranie.
4. Technologii służących pozyskiwaniu, selekcjonowaniu, analizowaniu, przetwarzaniu, zarządzaniu i udostępnianiu informacji, do których zalicza się systemy elektroniczne wspomagające realizację zadań publicznych.

Wyłączenia w SZBI dotyczą:

Obszar przetwarzania informacji niejawnych.

Zgodnie z zasadami obowiązującymi w Urzędzie Gminy każdy pracownik jest zobowiązany do ochrony przetwarzanych tu informacji w tym informacji powierzonych przez klientów i kontrahentów poprzez przestrzegania niniejszej polityki, a wszelkie przypadki naruszenia jej zasad mogą skutkować podjęciem kroków dyscyplinarnych.

Ponadto przełożeni są odpowiedzieli za nadzorowanie przestrzegania niniejszej polityki przez podlegających im pracowników.

Obowiązek informowania o naruszeniach

Każdy pracownik ma obowiązek natychmiastowego poinformowania Sekretarza Urzędu Gminy o przypadkach możliwej utraty informacji, danych, uzyskania dostępu do nich przez nieupoważnione osoby trzecie lub też ich ujawnienia w innych okolicznościach.

Polityka Zarządzania Bezpieczeństwem Informacji jest dokumentem nadrzędnym nad wszystkimi dokumentami dotyczącymi bezpieczeństwa informacji i stanowi dokument poziomu pierwszego.

Kolejny poziom stanowi przede wszystkim Polityka bezpieczeństwa danych osobowych i Plan ochrony informacji niejawnych, Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, opracowywane zgodnie z ogólnymi wymaganiami i zasadami ochrony informacji określonymi w niniejszej Polityce Zarządzania Bezpieczeństwem Informacji.

4. Cel wprowadzenia systemu zarządzania bezpieczeństwem informacji

Zgodnie z § 20 ust. 1 Rozporządzenia rady Ministrów z dnia 12 kwietnia 2O12r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych każda organizacja realizująca zadania publiczne jest zobowiązać ustanowią wdrożyć, eksploatować, monitorować, przeglądać, utrzymywać i doskonalić system zarządzania bezpieczeństwem informacji gwarantujący ich autentyczność rozliczalność, niezaprzeczalność i niezawodność.

Celem wdrożenia systemu bezpieczeństwa informacji jest zapewnienie wymaganego zaangażowania pracowników w utrzymanie bezpieczeństwa informacji, w szczególność przetwarzanej w systemach informatycznych, określenie kierunków rozwoju zarządzani* bezpieczeństwem tych systemów, przy jednoczesnym spełnieniu wszelkich wymogów obowiązującego prawa oraz zagwarantowanie sprawnego funkcjonowania struktur administracyjnych Urzędu Gminy.

Wdrożony system zarządzania bezpieczeństwem informacji winien zapewnić osiągnięcie takiego poziomu organizacyjnego i technicznego, który:

- będzie gwarantem pełnej ochrony informacji oraz ciągłości procesu ich przetwarzania poprzez tworzenie, utrzymywanie i testowanie planów zachowania ciągłości działania;
- zapewni zachowanie poufności, integralności i dostępności informacji chronionych oraz jawnych,
- zagwarantuje odpowiedni poziom bezpieczeństwa informacji, bez względu na jej postać, we wszystkich systemach jej przetwarzania,
- zapewni zgodność z przepisami prawnymi, wymaganiami kontraktowymi i innymi wymaganiami obowiązującymi Urząd Gminy, a odnoszącymi się do bezpieczeństwa informacji;
- maksymalnie ograniczy występowanie zagrożeń dla bezpieczeństwa informacji, które wynikają z celowej bądź przypadkowej działalności człowieka oraz ich ewentualni
- wykorzystania na szkodę Urzędu Gminy,
- zapewni poprawne i bezpieczne funkcjonowanie Wszystkich systemów przetwarzania informacji,
- zapewni gotowość do podjęcia działań w sytuacjach kryzysowych dla bezpieczeństwa Urzędu Gminy, jego interesów oraz posiadanych i powierzonych mu informacji.

Powyższe cele realizowane są poprzez:

- wdrożenie struktury organizacyjnej zapewniającej optymalny podział oraz koordynację zadań i odpowiedzialności związanych z zapewnieniem bezpieczeństwa informacji,
- wyznaczenie osób odpowiedzialnych za kluczowe aktywa przetwarzających informację, którzy zobowiązani są do zapewnienia im możliwie jak najwyższego poziomu bezpieczeństwa,
- zidentyfikowanie wszelkich aktywów w rozumieniu systemu zarządzania bezpieczeństwem informacji oraz określenie ich wartości i znaczenia dla Urzędu Gminy poprzez przeprowadzenie oceny ryzyka, według kryteriów przyjętych w procesie zarządzania ryzykiem, zrozumienie ich podatności praż zagrożeń, które mogą narazić je na ryzyko;
- wdrożenie systemu zarządzania incydentami naruszającymi bezpieczeństwo informacji oraz słabościami systemu;
- przyjęcie za obowiązujące przez wszystkich pracowników polityki i procedur bezpieczeństwa obowiązujących w Urzędzie,
- podział informacji na klasy i przyporządkowanie im zasad postępowania,
- określenie zasad przetwarzania informacji, w tym stref, w których może się ono odbywać,
- przegląd i aktualizację polityk i procedur postępowania dokonywanych przez odpowiedzialne osoby w celu jak najlepszej reakcji na zagrożenia i incydenty,
- ciągłe doskonalenie systemu zapewniającego bezpieczeństwo informacji, funkcjonującego w Urzędzie zgodnie z wymaganiami

Polityka Bezpieczeństwa Informacji podlega regularnym przeglądom, będzie weryfikowana i dostosowywana w celu zapewnienia odpowiedniego poziomu bezpieczeństwa, dokumentacji PBI odbywają się raz w roku.

W zależności od potrzeb mogą zostać przeprowadzone dodatkowe przeglądy po stwierdzeniu istotnego naruszenia bezpieczeństwa, pojawieniu się zasadniczych zmian w Urzędzie, jego strukturze lub jego otoczeniu (nowe zagrożenia, technologie).

Celem przeglądów polityki jest zapewnienie jej stosowalności w stosunku do realizowanych zadań publicznych oraz możliwości obsługi interesantów w każdych warunkach niezależnie od okoliczności i zmian w Urzędzie Gminy.

Za zapewnienie warunków niezbędnych do ustanowienia, wdrożenia, eksploatowania, monitorowania, przeglądania, utrzymywania i doskonalenia systemu czyni się odpowiedzialnym Sekretarza Gminy.

5. Podstawowe definicje

Zapewnienie bezpieczeństwa informacji	zapewnienie ich poufności, integralności i dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka dotyczącego zasobów stanowiących przedmiot niniejszej Polityki.
Poufność	definiowana jest jako zapewnienie, że chroniona informacja dostępna jest jedynie dla osób upoważnionych
Integralność	to zapewnienie, że informacje są kompletne i dokładne oraz że są przetwarzane w kontrolowany sposób.
Dostępność	gwarantuję, żę osoby, które są upoważnione i którym informacje są potrzebne, mają do nich dostęp w odpowiednim miejscu i czasie.
Autentyczność informacji	zapewnienie, że informacja jest zgodna z prawdą, oryginalna
Rozliczalność działań	zapewnienie, że wszystkie istotne czynności wykonane przy przetwarzaniu informacji zostały zarejestrowane i jest możliwe zidentyfikowanie osoby, która daną czynność wykonała
Niezawodność działań	zapewnienie, że wykonywane czynności prowadzą do zamierzonych skutków
Zarządzanie ryzykiem	skoordynowane postępowanie, którego celem jest identyfikacja, kontrolowanie i minimalizowanie ryzyka związanego z bezpieczeństwem informacji i ciągłością działania

6. Klasyfikacja informacji

Wszystkie informacje wytwarzane i przetwarzane w Urzędzie Gminy nieoznakowane jako należące do osób trzecich stanowią własność Urzędu Gminy i podlegają ochronie.

Wszelkie aktywa informacyjne powstające w Urzędzie Gminy oraz do niego dostarczane muszą zostać przypisane do określonego właściciela. W tym celu prowadzi się rejestr zasobów informacyjnych, Polityka umożliwia przypisanie każdej tworzonej lub otrzymywanej informacji do określonej grupy, Wszystkie informacje przetwarzane w Urzędzie Gminy dzieli się na następujące grupy:

Informacje niejawne, których ochrona realizowana jest w oparciu o przepisy zawarte w ustawie z 5 sierpnia 2010r. o ochronie informacji niejawnych. Posiadają one własny, niezależny od określanego przez niniejszą politykę system ochrony zgodnie z wymaganiami ustawy. Za organizację systemu ochrony informacji niejawnych odpowiada merytoryczny pracownik posiadający uprawnienia do dostępu do informacji niejawnych

Informacje prawnie chronione (do użytku wewnętrznego) są to informację chronione na podstawie powszechnie obowiązujących aktów prawnych.

Do tej grupy kwalifikowane są informacje o istotnym znaczeniu dla funkcjonowania Urzędu, do których dostęp mają jedynie osoby zatrudnione w Urzędzie. Udostępnienie tych informacji osobom (zarówno fizycznym, jak i prawnym), które nie pozostają w takim związku wymaga formalnej autoryzacji i zgody osób zarządzających.

Atrybuty jakości informacji zakwalifikowanych do tej określa się następująco:

1. Dostępność-ograniczona do osób posiadających odpowiednie autoryzacje, dystrybucja informacji jedynie do osób uprawnionych,
2. Integralność - weryfikacja integralności informacji jest obowiązkowa,
3. Poufność - nie jest wymagana, lecz odbiorcy informacji są zobowiązani do ochrony otrzymywani informacji należących do tej grupy.

Do grupy tej kwalifikuje się wszelkie informacje niezbędne do sprawnego działania Urzędu - obowiązujące procedury, zarządzenia, materiały szkoleniowe, okólniki, raporty, kontrakty i porozumienia z podmiotami zewnętrznymi, wewnętrzne listy mailingowe i książki telefoniczne, dokumentacje projektowe i wykonawcze, dokumenty wymieniane z innymi podmiotami (wydawane decyzje itp.), dane osobowe Itp. kadrowe, finansowo-księgowe, dokumentacja postępowań z zakresu zamówień publicznych.

Dodatkowe mechanizmy ochrony

Właściciel informacji dokonuje klasyfikacji informacji oraz określa listę osób, którym informacja ma być udostępniona.

Odbiorca informacji jest odpowiedzialny za odpowiednie zabezpieczenie informacji podczas

jej przetwarzania oraz przechowywania, niezależnie od formy i nośnika, na którym informacja jest przechowywana.

Zarządzanie kopiami

Kopie informacji „do użytku wewnętrznego" mogą być wykonywane jedynie przez pracowników Urzędu lub przez współpracujące z nim podmioty, których upoważnieni Kopia informacji „do użytku wewnętrznego" podlega takim samym zasadom ochrony jak jej oryginał.

Dystrybucja informacji „do użytku wewnętrznego"

Wewnątrz Urzędu:

1. w przypadku przekazywania informacji na nośniku należy go umieścić w odpowiedniej kopercie poczty wewnętrznej,
2. do dystrybucji w postaci elektronicznej dopuszczalne jest jedynie wykorzystywanie wewnętrznego systemu poczty elektronicznej wyposażonego w mechanizm zapobiegający przypadkowemu lub zamierzonemu wysłaniu informacji na adres zewnętrzny.

Na zewnątrz Urzędu:

1. Na nośnikach-odpowiednio zabezpieczony list polecony za potwierdzeniem odbioru lub przesyłka kurierska,
2. W postaci elektronicznej - poczta elektroniczna wyposażona w działający mechanizm szyfrowania przesyłek.
3. Telefaxem - pod warunkiem uwierzytelnienia numeru odbiorcy.

Usuwanie informacji „do użytku wewnętrznego"

Należy zastosować mechanizmy uniemożliwiające odzyskanie usuwanej informacji „do użytku wewnętrznego". Informacja i wszystkie jej kopie muszą być bezwarunkowo usunięta po upływie terminu jej ważności lub na udokumentowane polecenie jej Właściciela. Za archiwizację informacji „do użytku wewnętrznego" odpowiada jej Właściciel,

1. Dokumenty w postaci papierowej - należy użyć niszczarki dokumentów,
2. Dokumenty na nośnikach elektronicznych - w przypadku wycofania nośnika (np. krążka *CD/DVD) z dalszego użycia* należy przeprowadzić jego fizyczną likwidację. Nośniki, na których niemożliwe jest skasowanie danych (np. CD Read Only) należy przed przekazaniem uszkodzić *fizycznie. Z* nośników, na których możliwe jest kasowanie danych należy przed przekazaniem do likwidacji skasować wszelkie informacje stosując standardowe mechanizmy systemu operacyjnego (np. procedurę formatowania).
3. Jeśli nośnik (np. komputer), na którym znajduje się informacja „do użytku wewnętrznego" *podlegająca* usunięciu będzie w dalszym ciągu wykorzystywany przez tego samego użytkownika należy skasować tą informację posługując się standardowymi mechanizmami systemu operacyjny W przypadku przekazywania nośnika (komputera, dysku przenośnego

itp.) innemu użytkownikowi należy skasować wszelkie zawarte na nim informacje „do użytku wewnętrznego" i przekazać go wyznaczonemu pracownikowi w celu zakończenia procedury kasowania zawartych na nim informacji

Pozostałe informacje przetwarzane w Urzędzie (ogólnodostępne- publiczne) w tym min informacje, których zakres i tryb udostępniania określa ustawa o dostępie do informacji publicznej. Są to min. publikacje na stronie www, informacje udostępniane na wniosek lub zamieszczone w BIP.

Do grupy tej należy kwalifikować informacje spełniające następujące warunki:

Informacja jest przeznaczona do powszechnego wykorzystywania. Okresowa utrata dostępność informacji nie stanowi zagrożenia dla ciągłości działania Urzędu i ryzyko z tym związane określono jako akceptowalne.

Zachowanie integralności informacji posiada ograniczone (np. wizerunkowe) znaczenie dla Urzędu Utrata integralności nie rodzi skutków finansowych lub prawnych dla Urzędu.

Poufność nie jest zachowywana. W grupie tej znajdą się więc wszelkie informacje marketingowe, broszury, zawartość publicznych stron WWW (łączenie z BIP - Biuletynem Informacji Publicznej), publicznie dostępne dane finansowe, katalogi i wszelkie inne informacje udostępniane bez *konieczności* spełnienia przez ich odbiorcę jakichkolwiek warunków - np. automatycznie generowane odpowiedzi na pocztę elektroniczną w okresie urlopu pracownika. W pewnych przypadkach może być konieczne zachowanie integralności informacji przeznaczonych do udostępniania publicznego (np. aktów prawnych lub ich projektów, dokumentacji zamówień publicznych, protokoły kontroli itp.).

<u>Zarządzanie kopiami informacji udostępnianych publicznie</u>

Informacje zakwalifikowane do tej grupy mogą być powielane bez ograniczeń w dowolnej formie

Odpowiedzialność za zarządzanie kopią informacji (w szczególności za jej aktualność) spoczywa na odbiorcy informacji, który tą kopię wykonał.

Dystrybucja informacji udostępnianych publicznie

Nie podlega ograniczeniom, jeśli nie narusza ogólnych przepisów prawa.

Usuwanie informacji udostępnianych publicznie

Nie określa się żadnych dodatkowych wymagań ~ w przypadku informacji w formie elektronicznej w postaci pliku wystarcza standardowe skasowanie go z wykorzystaniem standardowej funkcji systemu operacyjnego, nośniki zawierające informacje zakwalifikowane do tej grupy (papier, tworzywa sztuczne, urządzenia elektroniczne itp.) mogą być przekazywane do recyklingu.

7. Podstawowe zasady bezpieczeństwa informacji

Skuteczna ochrona zasobów informacyjnych Urzędu Gminy wymaga wspólnego działania i zaangażowania wszystkich pracowników.

- Każdy pracownik jest zapoznany z regułami oraz z kompletnymi i aktualnymi procedurami ochrony informacji obowiązującymi w swojej jednostce organizacyjnej.
- Pracownicy zobowiązani są do używania zasobów informatycznych wyłącznie do celów służbowych.

W celu zapewnienia bezpieczeństwa zasobów Urzędu Gminy na każdym stanowisku pracy stosuje się następujące zasady ogólne:

- wiedzy koniecznej - każdy pracownik posiada wiedzę o systemie, do którego ma dostęp, ograniczoną wyłącznie do zagadnień, które są konieczne do realizacji powierzonych mu zadań.
- zasada ograniczonego dostępu - każdy pracownik posiada prawa dostępu do informacji, ograniczone wyłącznie do tych, które są konieczne do wykonywania powierzonych mu zadań.
- asekuracji zabezpieczeń - każdy mechanizm zabezpieczający musi być ubezpieczony drugim, innym (podobnym). W przypadkach szczególnych może być dodatkowe (trzecie) niezależne zabezpieczenie.
- zasada rozliczalności — dąży się do zapewnienia jednoznacznej odpowiedzią^ pracowników za powierzone im zasoby, pracownik ponosi odpowiedzialność a świadome lub zaistniałe w wyniku zaniedbania przekazanie swoich uprawnień innym osobom.
- czystego biurka — po zakończeniu pracy z biurka należy uprzątnąć dokumenty papiery poprzez umieszczenie ich w zamykanych szafach, szufladach. Zbędne dokumenty papierowe zniszczyć przy pomocy niszczarki. Taką samą zasadę stosować do nośnik informacji elektronicznej.
- czystego ekranu - każdy komputer musi mieć ustawiony wygaszasz ekranu po podanie hasła lub wyłączający się automatycznie po określonym czasie bezczynne; użytkownika. Dodatkowo przed pozostawieniem włączonego komputera bez op» użytkownicy powinni zablokować go (włączając wygaszasz ekranu) lub w przypał dłuższej nieobecności wylogować się z systemu

Dostęp do informacji przetwarzanych i przechowywanych w Urzędzie Gminy jest podda kontroli wynikającej z obowiązujących przepisów prawa powszechnego oraz dodatkowy: wymagań bezpieczeństwa.

Kontrola polega na:

- wydzieleniu obszarów przeznaczonych do przechowywania oraz przetwarzał poszczególnych zestawów danych i zapewnieniu odpowiednich barier fizycznych przeciwdziałających nieuprawnionemu dostępowi
- zarządzaniu uprawnieniami poszczególnych użytkowników w sposób zapewniający dostęp wyłącznie do danych wymaganych do wykonywania obowiązków służbowych jeśli ta dane podlegają ochronie z jakiejkolwiek przyczyny
- stosowaniu bezpiecznych systemów przetwarzania informacji
- bieżącym informowaniu pracowników o wszelkich zmianach w zakresie reguł dotyczących przechowywania, przetwarzania i udostępniania informacji

Adekwatność i skuteczność stosowanych w Urzędzie Gminy środków kontroli dostępu do informacji podlega bieżącej weryfikacji w ramach audytów wewnętrznych.

Identyfikacja zasobów

Zasoby informacyjne są to zasoby materialne i niematerialne, w tym wszelkiego rodzaju użyteczne dane (informacje), niezbędne do skutecznego i zgodnego z przepisami prawa podejmowania decyzji.

Zasoby informacyjne dzielimy na:

- informacje np.: bazy danych i pliki z danymi, kontrakty, umowy, dokumentacja systemowa, podręczniki użytkownika, materiały szkoleniowe, procedury, ślady audytowe, informacje zarchiwizowane, akta spraw;
- system teleinformatyczny: współdziałające ze sobą aplikacje, programy, urządzenia komputerowe, urządzenia telekomunikacyjne, nośniki informacji i inne;
- zasoby lokalowe, np.: budynki, pomieszczenia, biura i in. w których przetwarza się informacje;
- usługi np.: teleinformatyczne, telekomunikacyjne, ogrzewanie, zasilanie, klimatyzacja, itp.;
- ludzkie: ludzie, ich kwalifikacje, umiejętności i doświadczenie;
- wartości niematerialne np.: reputacja, wizerunek Urzędu Gmin

7.1. Zasady ogólne

- Wszyscy pracownicy są świadomi konieczności ochrony zasobów **informatycznych** i aktywnie uczestniczą w tym procesie
- Każdy pracownik przeszedł szkolenie z zasad ochrony informacji, spełnia dopuszczenia do informacji i podpisał stosowne oświadczenie o zachowaniu poufny
- Stosuje się zasadę: nie zawsze i wszędzie trzeba mówić, co się wie, ale zawsze trzeba wiedzieć co, gdzie i do kogo się mówi.
- Prawo przebywania w określonych miejscach mają tylko osoby upoważnione.
- Obowiązek ochrony zasobów Urzędu Gminy w przypadku współpracy z kontrahentami i jednostkami zewnętrznymi określony jest w ramach umów zawartych z podmiotami.
- System informatyczny jest przygotowany na wszelkie zagrożenia. Niedopuszczalne tymczasowe wyłączanie mechanizmów zabezpieczających.
- Przyjęto zasadę, iż skuteczne zabezpieczenie jest tylko wtedy, gdy stosuje się podejście kompleksowe, uwzględniające wszystkie stopnie i ogniwa ogólnie pojętego procesu przetwarzania informacji.
- W sytuacja kryzysowych, ujawnienie informacji wrażliwych pod względem poufności uznawane jest jako zdarzenie mniejszej wagi niż zniszczenie informacji
- W praktyce realizuje się zasadę dostosowywania mechanizmów wewnętrznych każdego systemu do zmieniających się warunków zewnętrznych.
- Używane mechanizmy są adekwatne do sytuacji.
- Podejmowane środki zaradcze nie mogą przekraczać poziomu akceptacji.

7.2. Środki bezpieczeństwa

Środki bezpieczeństwa stosowane w Urzędzie Gminy w ramach systemu bezpieczeństwa informacji grupuje się w trzy kategorie: dotyczące zabezpieczeń fizycznych, zabezpieczeń technicznych oraz proceduralno - organizacyjnych.

Zabezpieczenia fizyczne są podstawową funkcją polityki bezpieczeństwa i zawierają takie elementy jak ochrona poszczególnych wybranych pomieszczeń, ochrona sprzętu informatycznego, wydzielenie stref bezpieczeństwa i administracyjnych, dozór fizyczny, systemy alarmowe, systemy wizyjne, systemy kontroli dostępu. Itd. Każda z form ochrony fizycznej jest tak dostosowana do wartości chronionej, aby nakłady przeznaczone na wdrożenie zabezpieczeń nie były wyższe niż wartość chroniona.

Zabezpieczenia techniczne są bezpośrednio zintegrowane ze sprzętem informatycznym i oprogramowaniem i oznaczają np. szyfrowanie danych, sprzętową lub programową detekcję intruzów w systemie, weryfikację' integralności danych, czy bezpieczeństwo kanałów transmisyjnych

Zabezpieczania organizacyjne zawierają procedury tworzenia użytkowników, generowania haseł, pracy w systemie, przestrzegania i dbałości o poufność informacji, postępowania w sytuacjach kryzysowych, nakładania klauzuli tajności, generowania kopii zapasowych, przeprowadzania analizy ryzyka przeprowadzania prób odtwarzania systemu itd. Żaden ze środków bezpieczeństwa z różnych kategorii zabezpieczeń nie może funkcjonować w Urzędzie Gminy samodzielnie. Możliwie pełną ochronę w Urzędzie Gminy uzyskuje się w wyniku stosowania kompilacji wszystkich dostępnych form, które wzajemnie się uzupełniają. Dla każdej wartości chronionej konieczna jest osobna analiza stosowanych środków bezpieczeństwa.

7.3. Bezpieczeństwo fizyczne i środowiskowe

Urząd Gminy, dba o zapewnienie wysokiego poziomu bezpieczeństwa fizycznego i środowiskowego. Celem takiego postępowania jest zapewnienie bezpieczeństwa informacji przed dostępem osób niepowołanych, uszkodzeniem lub innymi zakłóceniami w odniesieniu do informacji. W przypadku danych od naszych Klientów najistotniejsze jest zapewnienie wszystkich trzech podstawowych aspektów bezpieczeństwa poufności danych oraz ich dostępności i integralności. Podobnie sytuacja wygląda w przypadku danych własnych. Skuteczna realizacja postawionego celu możliwa jest dzięki ustanowionym praktykom i podziałowi odpowiedzialności związanemu z wyznaczeniem stref bezpieczeństwa, zasadami pracy oraz administrowaniem prawami dostępu do nich. Kluczowe systemy techniczne i informatyczne wyposażone są w systemy podtrzymujące zasilanie. Urząd Gminy kieruje się następującą zasadą: „Blokuj dostęp do wszystkich miejsc przetwarzania informacji poza wyraźnie dozwolonymi, bo od tego zależy bezpieczeństwo również Twoich chroniony informacji".

Ochronę fizyczną w Urzędzie Gminy stanowią zamykane na patentowe zamki drzwi, metalowe szafy, oraz systemy alarmowe traktowane jako podstawowe elementy systemu bezpieczeństwa informacji. Ograniczają możliwość kradzieży dokumentów, bezpośredni dostęp do urządzeń przetwarzających informacje oraz nośników przechowujących je.

Wszystkie pomieszczenia biur Urzędu Gminy kwalifikuje się jako obszary o średnim poziomi bezpieczeństwa, co powodowane jest brakiem informacji o klauzulach niejawności, natomiast powszechnym występowaniem informacji zawierających dane osobowe. Do każdego typu obszaru dobiera się odpowiednie zabezpieczenia techniczne zgodnie zaleceniami ustawy o ochronie danych osobowych i wydanych na jej podstawie rozporządzeń wykonawczych.

Istotnym aspektem ochrony fizycznej jest zabezpieczenie przed pożarem. Pomieszczenia Urzędu Gminy są one właściwe zabezpieczone przed pożarem I na wypadek powstania pożaru.

7.4. Bezpieczeństwo sprzętu

Bezpieczeństwo sprzętu zapewniane jest poprzez takie warunki pracy sprzętu, które minimalizują ryzyko ich uszkodzenia lub nieautoryzowanego dostępu, zapewniając równocześnie ochronę przed awariami systemów wspomagających (instalacja elektryczna, wodno-kanalizacyjna itp.). Te same zasady dotyczą instalacji kablowych. Dla zapewnienia ciągłej dostępności i integralności sprzętu zaleca się prawidłową jego konserwację. Użytkowanie sprzętu poza siedzibą organizacji jest możliwe po autoryzacji przez kierownictwo i przy uwzględnieniu dodatkowych ryzyk. Zbycie sprzętu następuje po uprzednim upewnieniu się iż nie zawiera istotnych dla organizacji informacji.

Bezpieczeństwo fizyczne, sprzętu i okablowania, konfiguracji i eksploatacji sieci uzyskuje się w Urzędzie Gminy poprzez określenie kierunkowych standardów w zakresie:

- bezpieczeństwa fizycznego (parametr bezpieczeństwa fizycznego, kontrola fizycznych wejść, zabezpieczenie biur, pokoi i urządzeń, ochrona przed zagrożeniami zewnętrznymi i środowiskowymi, praca w obszarach zabezpieczonych, obszary ogólnie dostępne);
- bezpieczeństwo sprzętu i okablowania (rozmieszczenie i ochrona sprzętu, urządzenia wspomagające, bezpieczeństwo okablowania, utrzymanie sprzętu, bezpieczeństwo sprzętu znajdującego się poza terenem Urzędu Gminy, bezpieczne usuwanie sprzętu, wynoszenie majątku)
- konfiguracja i eksploatacja sieci (środki kontroli przeciwko kodowi złośliwemu i mobilnemu, środki kontroli sieci, bezpieczeństwo usług sieciowych, polityki i procedury dotyczące wymiany informacji, przesyłanie wiadomości drogą elektroniczną, polityka korzystania z usług sieciowych, identyfikacja sprzętu w sieciach ochrona portu służącego do zdalnego diagnozowania i konfiguracji, segregacja w sieciach, kontrola połączeń w sieci, nadzorowanie słabości technicznych)

Z uwagi na to, że standardy zawieraj a informacje, których ujawnienie nieuprawnionym stronom trzecim mogłoby w istotnym stopniu obniżać bezpieczeństwa informacji, są udostępniane tylko pracownikom wykonującym zadania określone w standardach.

Kontrola dostępu według normy musi odzwierciedlać potrzeby biznesowe i wymogi bezpieczeństwa. Przyznawanie i odbieranie uprawnień dostępu do wszystkich systemów i aplikacji odbywa się na podstawie formalnej procedury. Korzystanie z przywilejów (zasobów) musi być ograniczone i kontrolowane. Hasła użytkowników podlegają kontroli zgodnie z założoną polityką bezpieczeństwa a ich użytkowanie z powszechnymi sprawdzonymi praktykami. Użytkownicy zabezpieczają sprzęt pozostawiony bez opieki. Prowadzą też politykę czystego biurka i ekranu. Kontrolowany jest dostęp do sieci zarówno od wewnątrz jak

i od zewnątrz. Użytkownicy mają dostęp jedynie do tych usług sieciowych, do których mają autoryzację. Przy połączeniach zewnętrznych identyfikowani są ludzie i sprzęt. Zalecana jest fizyczna i logiczna kontrola dostępu do portów diagnostycznych i konfiguracyjnych. Zaleca się ograniczenie i ścisłe kontrolowanie dostępu do programów narzędziowych pozwalających na obejście zabezpieczeń systemowych. Logowanie przebiegać musi wedle udokumentowanych procedur a czas trwania sesji i połączenia jest ograniczony

Pozyskiwanie, rozwój i utrzymanie systemów informacyjnych obejmuje:

- wymagania bezpieczeństwa systemów informacyjnych,
- poprawne przetwarzanie w aplikacjach,
- zabezpieczenia kryptograficzne,
- bezpieczeństwo plików systemowych,
- bezpieczeństwo w procesach rozwojowych i obsługi informatycznej,
- Zarządzanie podatnościami technicznymi,

7.5. Zarządzanie aktywami i ryzykami

Urząd Gminy zarządza swoimi aktywami Informatycznymi poprzez zapewnienie im wymaganego poziomu bezpieczeństwa. Identyfikowane są aktywa informatyczne i klasyfikowane zgodnie ze stawianymi im wymaganiami w zakresie ochrony.

Ważnym elementem zarządzania aktywami i bezpieczeństwem informacji jest przeprowadzenie okresowej analizy ryzyka i opracowywanie planów postępowania z ryzykiem. Analiza jej wyników stanowi podstawę podejmowania wszelkich działań w zakresie doskonalenia ochrony zasobów Urzędu Gminy. Na podstawie wyników analizy ryzyka opracowywane są plany postępowania z ryzykiem dla aktywów o ryzykach większych niż ustalony poziom ryzyka akceptowalnego.

Analiza ryzyk jest dokonywana przez Kierownictwo podczas przeglądów systemu zarządzania bezpieczeństwem oraz po zmianach mających wpływ na system bezpieczeństwa informacji.

7.6. Zarządzanie incydentami

W przypadku wszelkich incydentów w Urzędzie Gminy, powiadamiany jest Sekretarz. Z jego udziałem dokonywana jest wstępna analiza incydentu, po czym podejmowane są działania zgodne z zasadami reakcji na zdarzenia.

Po wystąpieniu incydentu natychmiast podejmowane są działania mające usunąć ewentualne skutki zaistnienia incydentu, a następnie wszystkie incydenty są szczegółowo analizowane i podejmowane są dalsze decyzje właściwe dla danej sytuacji. Incydenty są zapisywane w rejestrze zbiorczym, a następnie analizowane.

7.7. Zarządzanie ciągłością działania

Kierownictwo Urzędu Gminy dba o zapewnienie ciągłości funkcjonowania usług związanych z przetwarzaniem danych. Celem takiego postępowania jest przeciwdziałanie przerwom w działalności oraz ochrona krytycznych procesów przed rozległymi awariami lub katastrofami, realizacja postawionego celu możliwa jest dzięki ustanowionym praktykom i podziałowi odpowiedzialności związanemu z zarządzaniem ciągłością działania tak, aby ograniczyć do akceptowalnego poziomu skutki wypadków i awarii.

Reagowanie na zdarzenia mogące prowadzić do zaburzenia procesów przetwarzania informacji jest przedmiotem stosownych rozwiązań, w tym instrukcji i planów awaryjnych. Plany awaryjne podlegają systematycznemu testowaniu.

Kierownictwo mając na uwadze konieczność szybkiego dostosowania się do wymagań klienta i otoczenia, ciągłe zmiany przepisów prawnych oraz dążenie do wzrostu efektywności i wydajności pracy, dostosowuje metody postępowania dla skutecznej i terminowej obsługi zmian w infrastrukturze teleinformatycznej przy utrzymaniu pożądanego poziomu bezpieczeństwa przetwarzanych danych i ograniczeniu ryzyka negatywnego wpływa na obsługę teleinformatyczną Urzędu Gminy.

Proces zarządzania zmianą w Urzędzie Gminy przebiega w następujących etapach:

- ustalenie celu zmiany
- rozważenie wielkości i ważności zmiany dla Urzędu Gminy
- określenie momentów krytycznych we wdrożeniu zmiany
- zainicjowanie zmiany, przeprowadzenie testów, wdrożenie w systemie produkcyjnym
- aktywne włączenie pracowników Urzędu Gminy w proces zmiany
- monitorowanie i raportowanie kolejnych kroków wdrożenia zmiany.

7.8. Zarządzanie systemami i sieciami

Kierownictwo Urzędu Gminy dba o przestrzeganie zasad związanych z utrzymywaniem i użytkowaniem systemów informatycznych I sieci. Celem takiego postępowania jest zapewnienie poufności, integralności i dostępności przetwarzanej przez nie informacji własnych.

Skuteczna realizacja postawionego celu możliwa jest dzięki:

- kompetencjom i świadomości pracowników oraz podpisanym umowom ze specjalistycznymi firmami administrującymi zasobami informatycznymi;
- opracowanym zasadom konserwacji urządzeń w celu zapewnienia ich ciągłej pracy;
- kontrolowaniu wszelkich zmian do infrastruktury technicznej;
- prowadzeniu prac rozwojowych i testowych na oddzielnych urządzeniach lub środowiskach w celu zapewnienia bezpieczeństwa systemów produkcyjnych;
- nadzorowaniu usług dostarczanych przez strony trzecie w szczególności odbieraniu ich i akceptowaniu w sposób świadomy uwzględniający ich wpływ na istniejący system bezpieczeństwa;
- wdrożeniu zabezpieczeń chroniących przed oprogramowaniem złośliwym i mobilnym, systematycznemu tworzeniu i testowaniu kopii bezpieczeństwa;
- przestrzeganiu opracowanych zasad postępowania z nośnikami
- bieżącym monitorowaniu zasobów informacyjnych

Kierownictwo monitoruje możliwość wystąpienia incydentów bezpieczeństwa i posiada mechanizmy reagowania przypadkach ich wystąpienia. Szczegółowy sposób postępowania zawierają stosowne procedury.

Bezpieczeństwo fizyczne, sprzętu i okablowania, konfiguracji i eksploatacji sieci w Urzędzie Gminy poprzez określenie kierunkowych standardów w zakresie:

- bezpieczeństwa fizycznego (parametr bezpieczeństwa fizycznego fizycznych wejść, zabezpieczenie biur, pokoi i urządzeń, ochrona przędza^ zewnętrznymi i środowiskowymi, praca w obszarach zabezpieczonych $_{t}$ ogólnie dostępne)
- bezpieczeństwo sprzętu i okablowania (rozmieszczenie i ochrona sprzętu, urządzenia wspomagające, bezpieczeństwo okablowania, utrzymanie sprzętu, bezpieczeństwo sprzętu znajdującego się poza terenem Urzędu Gminy, bezpieczne usuwanie sprzętu, wynoszenie majątku)
- konfiguracja i eksploatacja sieci (środki kontroli przeciwko kodowi złośliwemu i mobilnemu, środki kontroli sieci, bezpieczeństwo usług sieciowych, polityki i procedury dotyczące wymiany informacji, przesyłanie wiadomości drogą

elektroniczną, polityka korzystania z usług sieciowych, identyfikacja sprzętu w sieciach, ochrona portu służącego do zdalnego diagnozowania i konfiguracji, segregacja w sieciach, kontrola połączeń w sieci, nadzorowanie słabości technicznych)

8. Infrastruktura systemu informacyjnego Urzędu Gminy

Przetwarzanie informacji, w tym informacji osobowych, odbywa się we wszystkich pomieszczeniach Urzędu Gminy tj.

Infrastrukturę systemu informatycznego w Urzędzie Gminy stanowią integralnie działające komputery stacjonarne klasy PC wyposażone w oprogramowanie tzw. pakiety biurowe i korzystające z łączności z zewnętrzną siecią Internet poprzez współpracę z lokalnymi sieciami znajdującymi się w obiektach, gdzie zlokalizowane są poszczególne biura.

Poszczególne komputery mają uruchomione zapory systemowe oraz aktywne programy antywirusowe zabezpieczające przed ingerencją z zewnątrz

9. Identyfikacja zagrożeń

Zagrożenia można podzielić ze względu na lokalizację ich *źródła na:*
wewnętrzne (powstające wewnątrz organizacji), obejmujące zagrożenie związane uszkodzeniem lub brakiem dostępu do danych spowodowane błędem, przypadkowym albo celowym działaniem nieuczciwych użytkowników, zewnętrzne (powstające poza organizacją), które obejmują zagrożenie utratą, uszkodzeniem danych lub pozbawieniem możliwości obsługi przez celowe i przypadkowe działanie ze strony osób trzecich w stosunku do sieci lub systemy fizyczne, w których utrata, uszkodzenie danych lub brak możliwości obsługi następuje z powodu wypadku, awarii, katastrofy lub innego nieprzewidzianego zdarzenia wpływającego na system informacyjny bądź urządzenie sieciowe

Najbardziej prawdopodobne z nich to:

Awarie sieci elektrycznej - zagrożenie to kojarzone jest najczęściej z przestojami związanymi brakiem dostępu do systemu teleinformatycznego. Szacując ich koszt należy wziąć pod uwagę utratę zysków, koszty okresu bezproduktywności pracowników Jak również obniżenie satysfakcji klientów. Są one bezpośrednio powiązane z czasem jaki trwa przerwa w dostawie energii elektrycznej. Jednakże nawet niewielkie przerwy czy niestabilności mogą doprowadź do awarii elementów systemu i konieczności jego ponownego uruchomienia. Źródłem wspomnianych niestabilności są awarie linii przesyłowych wysokiego napięcia lub samej elektrowni po których operator musi włączyć generatory w celu utrzymania stabilności całego systemu elektroenergetycznego. Przyjmuje się, że systemy informatyczne są narażone średnio na kilkanaście przerw w dostawie energii w skali roku. Około 90% trwa krócej niż 5 minut Zarówno liczba awarii jak i ich długość mogą w dającej się przewidzieć przyszłości ulec znacznemu zwiększeniu, spowodowanemu kryzysem energetycznym, stanem technicznym polskich elektrowni oraz zmianom klimatycznym. Zagrożenie spowodowane awariami sieci energetycznej jest jak widać dość duże lecz także ogólnie znane.

Awarie sprzętu - przez awarię rozumie się niezdolność produktu Jako całości lub tylko jego elementów do wykonywania wymaganych funkcji. Definicję tę można uzupełnić o warunek stawiany przez firmy ubezpieczeniowe mówiący o awarii jako uszkodzeniu nie spowodowanym bezpośrednim działaniem człowieka ani eksploatacją niezgodną z zaleceniami producenta. Tak rozumiane awarie wiążą się ściśle z niezawodnością, czyli zespołem właściwości odnoszących się do zdolności poprawnej pracy w czasie ustalonego okresu czasu.

Fizyczna kradzież dokumentów - przez fizyczną kradzież dokumentów, rozumiane jest bezprawne przywłaszczenie zarówno dokumentów w formie papierowej jak i cyfrowej. Najczęściej dokonywana jest przez pracowników odchodzących z firmy. Pozostałe kradzieże dokumentów także spowodowane są pośrednio przez pracowników a ściślej przez ich zaniedbania. Pozostawianie niezabezpieczonych dokumentów po zakończeniu pracy czy wydruków bądź kserokopii na tackach odbiorczych urządzeń to sytuacja nagminna w organizacjach. Odpowiedzią na te problemy jest odpowiednia polityka personalna oraz wprowadzenie, przestrzeganie oraz kontrole polityki bezpieczeństwa. Pomocny może być też odpowiedni system obiegu dokumentów, który znakowałby dokumenty, kopie i wydruki w sposób umożliwiający identyfikację ich źródła. Pozwoliłoby to na detekcję sposobu w jaki dokumenty wydostały się poza organizację oraz wyciągnięcie sankcji wobec winnych. Stosunkowo rzadkie lecz najbardziej groźne, są kradzieże dokumentów w skutek włamań do pomieszczeń firmowych. Zazwyczaj pozostawiają ślady i skutkują powiadomieniem organów ścigania. Kierownictwo organizacji, stosuje zabezpieczenia w postaci alarmów, monitoringu czy ochrony fizycznej. Pomimo małej skali, zagrożenia utratą dokumentów poprzez włamania nie można lekceważyć. Podjęcie tak dużego ryzyka w celu nielegalnego uzyskania informacji świadczy iż planowane jest ich wykorzystanie a nie jedynie zaspokojenie ciekawości.

Kradzieże sprzętu - niebezpieczeństwo to dotyczy przede wszystkim urządzeń przenośnych, które często wynoszone są poza siedzibę organizacji przez co tracą ochronę poprzez stosowane techniczne i fizyczne zabezpieczenia. Powstające w ten sposób straty materialne, zrekompensowane mogą być w wyniku realizacji polis ubezpieczeniowych. Nie obejmują one jednak danych zawartych na nośnikach informacji. Zaleca się aby wszystkie istotne dane umieszczone były w pamięciach masowych, które znajdują się w serwerowniach, czyli miejscach podlegających szczególnej ochronie. Nie jest jednak w wielu przypadkach możliwe. Coraz większą popularnością cieszą się laptopy, które pozwalają na prace poza środowiskiem sieciowym firmy Zabezpieczenia stosowane dla sprzętu przenośnego możemy podzielić na klasy:

1. Zapobiegające kradzieżom,
2. Pozwalające na odzyskanie skradzionego,
3. Uniemożliwiające niepowołany dostęp do danych,

Klasa pierwsza obejmuje wykorzystanie gniazda Kensington Lock. Większość obecnie produkowanych modeli laptopów jest w nie standardowo wyposażonych. W gniazdo to wpinana jest linka z zamkiem na klucz lub szyfrowym, która przymocowana również do

stabilnego elementu uniemożliwia kradzież sprzętu. Innym rozwiązaniem jest alarm wyposażony w przypinany czujnik ruchu o regulowanej czułości np. IC Gear Notebook.
Alarm. Szansę na odzyskanie skradzionego sprzętu zwiększymy poprzez podanie organom ścigania numerów seryjnych. Warto też fakt kradzieży zgłosić producentowi sprzętu, który przekazuje informacje do swoich autoryzowanych serwisów. Dostęp do danych w skradzionym sprzęcie uniemożliwiają stosowane w laptopach czytniki biometryczne.
Pomyłki użytkowników systemu informatycznego, Nawet najdoskonalszy system informatyczny nie jest w stanie absolutnie wykluczyć błędów czynnika ludzkiego Choć błędów ludzkich uniknąć nie można to istnieją mechanizmy pozwalające na ograniczenie a często na wyeliminowanie ich skutków. Są to np. kopie migawkowe, rozpraszanie zasobów, systematycznie wykonywane kopie bezpieczeństwa tzw. backup.
Pożar, zalanie, inne zdarzenia losowe Z samej definicji zdarzenia losowe są nieprzewidywalne, nie należą jednak do rzadkości. Ponieważ stosowanie zabezpieczeń poprzez odpowiednie elementy konstrukcyjne budynku oraz systemy alarmowe, jest niezwykle kosztowne nie obejmuje zazwyczaj wszystkich elementów systemu informacyjnego organizacji pozostaje zatem właściwe ubezpieczenie od skutków takiego zdarzenia.
Wirusy.
Ochronę przed mailware zapewnia oprogramowanie antywirusowe. Zastosowane odpowiednie oprogramowanie, oprócz podstawowej funkcji jaką jest ochrona przed wszystkimi rodzajami mailware, powinno cechować się możliwością zdalnej, centralnej administracji. Należy zwrócić uwagę na fakt iż nieliczne z oferowanych na polskim rynku antywirusów chronią systemy przed rootkit-ami oraz spamem. Prostota instalacji i konfiguracji to cecha drugorzędna, gdyż zazwyczaj zajmuje się tym wykwalifikowana kadra.
Inną, rzadko braną pod uwagę przy zakupie cechą jest wpływ jaki działający w tle antywirus ma na wydajność systemu.
Włamania do systemu informatycznego, Najprostszym a zarazem najskuteczniejszym sposobem nielegalnego dostania się do systemu jest odgadnięcie lub zdobycie hasła i nazwy użytkownika. Często nazwy użytkowników przyznawane są według określonych zasad np. pierwsza litera imienia, znak kropki i nazwisko. Informacja o sposobie ich generowania jest powszechnie znana wśród kadry pracowniczej i nie uznawana jest za szczególnie chronioną. Do rzadkości należy również usuwanie standardowych nazw użytkowników administrujących systemem takich jak „admin", „administrator'* czy „manager". Stąd odgadnięcie ich nie jest zadaniem trudnym, szczególnie w jednostkach publicznych, w których nazwiska urzędników są jawne i często wypisane na drzwiach biur. Duży problem stanowi proceder zapisywania haseł przez pracowników i pozostawiania ich w dostępnym dla innych miejscu. Ponieważ pamięć

ludzka jest zawodna, poza zapisywaniem, panuje też tendencja do konstruowania najprostszych i najkrótszych haseł.

Wyłudzenie informacji. Wyłudzenie informacji często bazuje na elementach socjotechniki.

Utrata wsparcia technicznego. Utrata wsparcia technicznego jest szczególnie groźna w przypadku oprogramowania niestandardowego, wykonywanego na potrzeby konkretnej organizacji. W przeciwieństwie do sprzętu, którego podzespoły zazwyczaj dostępne są na rynku i który można łatwo zastąpić innym o zbliżonych lub nawet tych samych parametrach wymiana oprogramowania może być niezwykle trudna. Wiąże się często z koniecznością przeprowadzenia długotrwałego wdrożenia i konwersji danych z jednego systemu do drugiego. Najczęściej problem ten występuje w przypadku: upadłości lub likwidacji właściciela oprogramowania, zmiany formy prawnej lub organizacyjnej organizacji, wygaśnięcia dotychczasowych umów, zaprzestania wsparcia oprogramowania w związku z wprowadzeniem nowych wersji

10. Odpowiedzialność za bezpieczeństwo informacji

1. Za bezpieczeństwo informacji odpowiedzialny jest każdy pracownik Urzędu Gminy w szczególności odpowiada on za przestrzeganie zasad bezpieczeństwa wynikających z polityki oraz zgłaszanie incydentów bezpieczeństwa.
2. We wszystkich umowach zawieranych w Urzędzie Gminy, które mogą dotyczyć przetwarzania danych w jednostce, należy uwzględnić zapisy zobowiązujące drugą stronę do przestrzegania odpowiednich zapisów PBI.
3. Za nadzór nad przestrzeganiem postanowień PBl odpowiada Sekretarz, który w szczególności odpowiedzialny jest za:
   - określanie jakiego rodzaju informacje mogą być przetwarzane w jednostce;
   - identyfikację grup informacji podlegających ochronie
   - określanie, czy jednostka jest właścicielem danej grupy informacji, czy też naleją innego podmiotu;
   - ustalanie wykazu informacji stanowiących tajemnicę
   - przygotowanie dokumentu głównego PBl oraz nadzór i akceptację dokumentów bezpieczeństwa grup informacji chronionych, polityk bezpieczeństwa systemów przetwarzania, procedur i regulaminów;
   - analizę raportów o wszelkich zdarzeniach związanych z bezpieczeństwem informacji chronionych

Kierownictwo Urzędu Gminy zapewnia kompetentną kadrę pracowniczą do wykonywania wyznaczonych żądań. Celem takiego postępowania jest ograniczenie ryzyka błędu ludzkiego, kradzieży, nadużycia lub niewłaściwego użytkowania zasobów. Realizacja postanowień możliwa jest dzięki ustanowionym praktykom i podziałowi odpowiedzialności związanych z weryfikacja do pracy podczas naboru, zasadom zatrudniania pracowników oraz ustalonej procedurze rozwiązywania umów o pracę.

10.1. Odpowiedzialność za systemy Informatyczne

Rolę Administratora Systemu (AS) pełni Informatyk.

Administrator Systemów odpowiedzialny jest za:

- zapewnianie ciągłości działania systemu Informatycznego i optymalizację wydajności;
- instalację i konfigurację sprzętu I oprogramowania;
- konfigurację i administrację oprogramowaniem systemowym i sieciowym;
- przydzielanie praw dostępu do systemu osobom upoważnionym.
- przygotowywanie danych analitycznych opisujących działanie systemów teleinformatycznych w kontekście zarządzania bezpieczeństwem informacji,
- okresowe raportowanie o stanie bezpieczeństwa systemów teleinformatycznych,
- odnotowanych incydentach bezpieczeństwa oraz statusie podejmowanych działań w odpowiedzi na incydenty,
- przygotowanie procedur bezpieczeństwa danego system u przetwarzania informacji chronionych,
- przygotowanie dokumentów procedur zarządzania kontami użytkowników,
- przygotowanie dokumentów procedur kryzysowych związanych z incydentami w systemach przetwarzania informacji,
- koordynację działań zapewniających sprawne funkcjonowanie i zabezpieczenie
- systemów teleinformatycznych Urzędu przed niepowołanym dostępem,
- nadzór nad wdrożeniem nowych aplikacji,
- zapewnienie, że do informacji chronionych mają dostęp wyłącznie osoby upoważnione i że mogą one wykonywać wyłącznie uprawnione operacje,
- kontrolę procesu przyznawania praw dostępu,
- przeciwdziałanie próbom naruszenia bezpieczeństwa informacji,

Praca Administratora Systemu jest nadzorowana pod względem bezpieczeństwa przez Sekretarza.

11. Zakres stosowania i rozpowszechniania Polityki Bezpieczeństwa Informacji

1. Niniejszy dokument Polityki Bezpieczeństwa Informacji jest dokumentem nadrzędnym nad wszystkimi dokumentami dotyczącymi bezpieczeństwa informacji w Urzędzie Gminy.
2. Zasady określone przez dokumenty Polityki Bezpieczeństwa Informacji

zastosowanie do, w szczególności do:

- wszystkich systemów informatycznych oraz papierowych, w których są przetwarzane informacje podlegające ochronie,
- informacji będących w dyspozycji lub innych podmiotów, o ile zostały przekazy podstawie umów,
- wszystkich nośników papierowych, magnetycznych, optycznych i innych, na jakim są lub będą znajdować się informacje podlegające ochronie,
- wszystkich lokalizacji - budynków i pomieszczeń, w których są lub k przetwarzane informacje podlegające ochronie.

3. Do stosowania zasad określonych przez dokumenty Polityki Bezpieczeństwa Informacji zobowiązani są wszyscy pracownicy w rozumieniu przepisów Kodeksu Pracy, konsultanci, stażyści i inne osoby mające dostęp do informacji podlegających ochronie.
4. Z treścią niniejszego dokumentu oraz właściwymi dokumentami niższego rzędu mają zapoznać się wszyscy pracownicy i inne osoby mające dostęp do informacji przetwarzanej w jednostce, przed przystąpieniem do przetwarzania danych.
5. Niniejszy dokument może być przedstawiany podmiotom, z którymi Urząd Gminy związany jest umowami, lub innym jednostkom współpracującym.

12. Podstawy prawne

1. Ustawa z dnia 5 sierpnia 2010 r. o ochronie Informacji niejawnych (Dz. U. z 2010 r. Nr 182, poz. 1228) wraz z mającymi zastosowanie aktami wykonawczymi.
2. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2014 r. , poz. 1182).
3. Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (t.j. Dz. U. z 2014 r., poz. 782).
4. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2007 r. w sprawie Biuletynu informacji publicznej (Dz. U. z 2007 r. Nr 10, poz. 68).
5. Ustawa z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2013 r. poz. 907).
6. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2013 r. poz. 235) wraz z mającymi zastosowanie aktami wykonawczymi.
7. Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2002 r. Nr 144, poz. 1204 z późn. zm.).
8. Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych (Dz. U. z 2001 r. Nr 128, poz. 1402 z późn. zm.).
9. Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. z 2013 r. poz. 262)
10. Ustawa z dnia 29 czerwca 1995 r. o statystyce publicznej (Dz. U. z 2012 r. poz. 591 z późn. zm.)
11. Ustawa z dnia 26 czerwca 1974 r. - Kodeks pracy (Dz. U. z 1998 r. Nr 21, poz. 94, z późn. zm.).
12. Ustawa z dnia 23 kwietnia 1964 r. - Kodeks cywilny (Dz. U, z 1964 r. Nr 16, poz. 93, z późn.) zm.).
13. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji *w* postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych Dz. U. 2012, poz. 526).
14. Polska Norma *PN - ISO* / IEC 27001 : 2007 Technika informatycy bezpieczeństwa - Systemy *zarządzania* bezpieczeństwem informacji – Wymagaj.
15. Polska Normy *PN - ISO* / IEC 17799 : 2007 Technika informatyczna, bezpieczeństwa - Praktyczne zasady zarządzania bezpieczeństwem informacji;