ZARZĄDZENIE NR 9/17

WÓJTA GMINY JAŚWIŁY

z dnia 16 marca 2017r.

o wprowadzeniu Polityki Bezpieczeństwa Informacji

Na podstawie art.31 oraz art.33 ust.3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U z 2016r. poz. 444, 1579, 1948), w związku z rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012r. 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 2016r., poz. 113 i 1744) zarządzam, co następuje:

§ 1. Wprowadzam do stosowania Politykę Bezpieczeństwa Informacji, stanowiącą załącznik do niniejszego zarządzenia.

§ 2. Wykonanie zarządzenia powierza się Administratorowi Bezpieczeństwa Informacji.

§ 3. Zarządzenie wchodzi w życie z dniem podjęcia.

WÓJT

mgr inż. Jan Joka

Załącznik
do zarządzenia nr 9/17
z dnia 16 marca 2017r.

POLITYKA BEZPIECZEŃSTWA INFORMACJI

Spis treści:

1. Słownik pojęć.

1) dostępność-właściwość bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu;
2) integralność-właściwość polegająca na zapewnieniu dokładności i kompletności aktywów;
3) incydent- pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji;
4) poufność-właściwość polegająca na tym, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom;
5) ryzyko - prawdopodobieństwo, że określone zagrożenie w połączeniu z podatnością doprowadzi do utraty lub zniszczenia zasobów;
6) rozliczalność - właściwość pozwalająca przypisać określone działanie do określonego podmiotu (osoby fizycznej, procesu, systemu) oraz umiejscowić je w czasie;
7) autentyczność - właściwość zapewniająca, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana (autentyczność dotyczy użytkowników, procesów, systemów i informacji);
8) niezawodność-właściwość oznaczająca spójne, zamierzone zachowanie i skutki.;
9) niezaprzeczalność - właściwość oznaczająca niemożność wyparcia się swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie;
10) System Zarządzania Bezpieczeństwem Informacji (SZBI) - część całościowego systemu zarządzania, oparta na podejściu wynikającym z ryzyka biznesowego, odnosząca się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji;
11) System teleinformatyczny - zespół współpracujących ze sobą według określonych reguł urządzeń, oprogramowania, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

2. Wstęp.

Informacje podobnie jak inne ważne aktywa, są niezbędne do funkcjonowania każdej organizacji i z tego powodu zaleca się ich odpowiednią ochronę.
Realizacja statutowych zadań każdej organizacji wymaga, między innymi, efektywnego dostępu do informacji oraz zapewnienia odpowiedniego poziomu bezpieczeństwa informacji. Utrata poufności, integralności, dostępności, autentyczności lub niezawodności może mieć negatywny wpływ na bieżącą działalność lub wizerunek organizacji.

Bezpieczeństwo informacji oznacza jej ochronę przed szerokim spektrum zagrożeń w celu zachowania poufności, integralności i dostępności informacji, a także minimalizacji ryzyka oraz zapewnienia ciągłości działania organizacji i realizacji jej zadań statutowych na odpowiednim poziomie.
Bezpieczeństwo informacji można osiągnąć, wdrażając odpowiedni zestaw zabezpieczeń, którymi mogą być polityki, procesy, procedury, zabezpieczenia fizyczne, struktury organizacyjne oraz funkcje oprogramowania i sprzętu.
Polityka bezpieczeństwa informacji jest zbiorem zasad i procedur, którym muszą podporządkować się osoby posiadające dostęp do zasobów informacyjnych. Określa również zasady ochrony infrastruktury, zasobów informatycznych i ludzkich.

3. Cel polityki bezpieczeństwa informacji.

Celem polityki bezpieczeństwa informacji jest zapewnienie właściwej ochrony zasobów informacyjnych w komórkach organizacyjnych Urzędu Gminy Jaświły zwanego dalej Urzędem.
Niniejszy dokument wyraża również zaangażowanie Kierownictwa Urzędu w zakresie utrzymania odpowiedniego poziomu bezpieczeństwa informacji oraz określa podstawowe przyjęte w tym obszarze cele i strategie.

Kierownictwo Urzędu aktywnie wspiera zapewnienie bezpieczeństwa informacji w całej organizacji wskazując kierunki działania, oraz przyjmując odpowiedzialność w zakresie bezpieczeństwa informacji.

4. Zakres obowiązywania polityki bezpieczeństwa informacji.

Dokument ten dotyczy wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, a także innych osób mających dostęp do chronionych informacji (np. pracowników firm zewnętrznych realizujących prace w Urzędzie). Dokument ma zastosowanie do wszystkich informacji chronionych niezależnie od formy, w jakiej są przechowywane (papierowej, elektronicznej i innej) z wyjątkiem informacji niejawnych. Należy podkreślić, że obszar ochrony informacji niejawnych posiada własne regulacje prawne i stosowne mechanizmy ochronne. Posiada także struktury organizacyjne dedykowane do ochrony informacji niejawnych wytwarzanych, przetwarzanych oraz przechowywanych w wydzielonych systemach teleinformatycznych. Podstawowym aktem prawnym jest ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2016r., poz. 1167 i 1948). Dokument dotyczy również wszystkich systemów informatycznych zlokalizowanych w budynkach Urzędu z wyjątkiem systemów służących do przetwarzania informacji niejawnych.

5. Wprowadzenie Systemu Zarządzania Bezpieczeństwem Informacji w Urzędzie Gminy Jaświły.

Zgodnie z § 20 ust. 1 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2016r., poz. 113 i 1744), Urząd jest zobowiązany zapewnić poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.
Głównymi celami są:
1) zapewnienie zgodności działań z obowiązującymi wymaganiami prawnymi;
2) ochrona systemów przetwarzania informacji przed nieuprawnionym dostępem bądź zniszczeniem;
3) zmniejszanie ryzyka utraty informacji do poziomu akceptowalnego;
4) zaangażowanie wszystkich pracowników Urzędu w ochronę informacji.

6. Organizacja Bezpieczeństwa Informacji.

W Urzędzie za bezpieczeństwo informacji, a w szczególności za opracowanie, wdrożenie i utrzymanie polityki bezpieczeństwa informacji, odpowiada Wójt Gminy Jaświły.
Sekretarz Gminy, kierownicy referatów oraz kierownicy innych komórek organizacyjnych tworzą **Zespół ds. Monitorowania Zagrożeń i Utrzymania Polityki Bezpieczeństwa Informacji.** Odpowiadają za wdrożenie i utrzymanie Polityki Bezpieczeństwa Informacji. Zobowiązani są również do natychmiastowego podjęcia działań w przypadku naruszenia zasad bezpieczeństwa informacji.
W Urzędzie działa **administrator systemów informatycznych,** który na wniosek kierowników referatów zarządza danym zasobem informacji. Odpowiedzialny jest za opracowanie, aktualizację procedur lub instrukcji danego systemu.
Administrator Bezpieczeństwa Informacji odpowiada za nadzór nad przestrzeganiem zasad ochrony przetwarzanych w Urzędzie danych osobowych oraz opracowanymi w tym celu dokumentami.
Administrator Systemu odpowiada za funkcjonowanie systemów i sieci teleinformatycznych, realizację zadań związanych z zarządzaniem systemem informatycznym Urzędu, w tym za zabezpieczenie sieci komputerowej tzn. wdrażanie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów infrastruktury informatycznej oraz ochrony danych przed nieuprawnioną modyfikacją, zniszczeniem, dostępem i ujawnieniem, a także ich utratą.
Audytor wewnętrzny odpowiada za coroczne przeprowadzanie audytu bezpieczeństwa informacji zgodnie z § 20 ust. 2 pkt 14 rozporządzenia Rady Ministrów z dnia z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2016r., poz. 113 i 1744).

7. Utrzymanie odpowiedniego poziomu bezpieczeństwa informacji.

Niezbędną praktyką po wdrożeniu mechanizmów ochrony informacji jest monitorowanie zagrożeń i zabezpieczeń, systematyczna weryfikacja i aktualizacja dokumentów Polityki Bezpieczeństwa Informacji i stosowanych zabezpieczeń. Nakłady

ponoszone na zabezpieczenia muszą być poprzedzone analizą ryzyka i kosztów, adekwatnie do potencjalnych strat spowodowanych naruszeniem bezpieczeństwa. Zadaniem Polityki Bezpieczeństwa Informacji jest zmniejszenie ryzyka płynącego z zagrożeń do akceptowalnego poziomu, to znaczy:
-zapobieganie przypadkom naruszenia bezpieczeństwa zasobów informacyjnych Urzędu,
- zminimalizowanie możliwości takiego naruszenia bezpieczeństwa,
- umożliwienie wczesnego jego wykrycia,
- zminimalizowanie strat związanych z takim naruszeniem oraz sprawne usunięcie jego skutków.
System Zarządzania Bezpieczeństwem Informacji wprowadzony w Urzędzie uwzględnia procesy utrzymania odpowiedniego poziomu bezpieczeństwa w tym:

1) zarządzanie ryzykiem;
2) zarządzania dostępem do zasobów;
3) monitorowania poziomu bezpieczeństwa;
4) zarządzania incydentem;
5) nadzoru nad dokumentacją Systemu Zarządzania Bezpieczeństwem Informacji. Dla utrzymania odpowiedniego poziomu bezpieczeństwa informacji istotne jest:

- systematyczne szkolenie oraz podnoszenie kwalifikacji zawodowych pracowników (w szczególności dotyczy to informatyków).
- Prowadzenie przez pracowników Oddziału ds. Informatyki szkoleń wewnętrznych doskonalących praktyczne umiejętności z zakresu bezpieczeństwa informacji (ochrona antywirusowa, szyfrowanie informacji)
- okresowe wykonywanie przeglądów Polityki Bezpieczeństwa Informacji
- przeprowadzanie audytów bezpieczeństwa informacji.

8. Struktura dokumentacji Polityki Bezpieczeństwa Informacji.

Zagadnienia związane z bezpieczeństwem informacji należy rozważać na następujących poziomach szczegółowości:

1) poziom organizacji,
2) poziom grupy informacji,
3) poziom systemu informatycznego,
4) poziom procedur, instrukcji i regulaminów.

Na politykę bezpieczeństwa informacji organizacji składają się zasady bezpieczeństwa obowiązujące w Urzędzie zawarte w niniejszym dokumencie.
Polityka bezpieczeństwa grupy informacji powinna odzwierciedlać zasady bezpieczeństwa i zarządzania wynikające z polityki bezpieczeństwa jednostki organizacyjnej oraz zasady wynikające ze specyfiki danej grupy informacji (np. dane osobowe, płacowo - kadrowe, informacje niejawne).
Poziom grupy informacji reprezentuje Polityka Bezpieczeństwa dla przetwarzanych w Urzędzie danych osobowych wraz z dokumentami związanymi - załącznik nr8.
Polityka bezpieczeństwa systemu informatycznego powinna odzwierciedlać zasady bezpieczeństwa i zarządzenia zawarte w Polityce Bezpieczeństwa Informacji w zakresie systemów informatycznych oraz zasady wynikające ze specyfiki informacji przetwarzanych w danym systemie informatycznym. Powinna także zawierać szczegółowe wymagania w dziedzinie bezpieczeństwa oraz opisy zabezpieczeń, które mają być zastosowane, a także sposoby ich użycia w celu zapewnienia odpowiedniego poziomu bezpieczeństwa. Ważne jest, aby zastosowane podejście było efektywne i racjonalne. Polityka bezpieczeństwa systemu informatycznego powinna być zatwierdzona. Wykaz zatwierdzonych polityk bezpieczeństwa systemów informatycznych zawiera załącznik nr 8.
Procedury, instrukcje i polityki szczegółowe regulują szczegółowe zasady korzystania z zasobów informacyjnych, a także użytkowania systemów informatycznych. Poziom procedur, instrukcji i polityk szczegółowych reprezentują następujące dokumenty:
Polityka Kontroli Dostępu do Informacji - załącznik nr 1.
Zawiera zasady kontroli dostępu do informacji w Urzędzie, a w szczególności zapewniania dostępu uprawnionymi użytkownikom i zapobiegania nieuprawnionemu dostępowi, zarządzania uprawnieniami i przywilejami, loginami i hasłami, kontroli dostępu do sieci, w tym zdalnego dostępu spoza Urzędu oraz postępowania ze sprzętem przenośnym.
Polityka Tworzenia Kopii Zapasowych - załącznik nr 2.
Określa zasady tworzenia, przechowywania i testowania kopii zapasowych danych.

Procedura zarządzania ryzykiem w bezpieczeństwie informacji - załącznik nr 3.
Określa metodykę i zasady zarządzania ryzykiem w Urzędzie
Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji - załącznik nr 4.
Określa zasady postępowania z incydentami bezpieczeństwa informacji, zgłaszania zdarzeń, zgłaszania słabości systemu bezpieczeństwa, odpowiedniego reagowania na incydenty, analizy przyczyn, podejmowania działań naprawczych, wyciągania wniosków z incydentów i gromadzenia materiału dowodowego
Ewidencja i klasyfikacja systemów informatycznych - załącznik nr 5.
Określa zasady ewidencjonowania i klasyfikowania systemów informatycznych.
Instrukcja w zakresie profilaktyki antywirusowej - załącznik nr 6. Określa zasady ochrony przed wirusami i innym złośliwym kodem.
Instrukcja pracy na stanowisku - załącznik nr 7.
Określa zasady pracy na stanowisku wyposażonym w monitor ekranowy i drukarkę.
Pozostałe dokumenty związane z funkcjonowaniem Systemu Zarządzania Bezpieczeństwem informacji w Urzędzie to:
- schemat postępowania z incydentami związanymi z bezpieczeństwem informacji
- rejestr incydentów związanych z bezpieczeństwem informacji
- rejestr przeglądów PBI

9. Odpowiedzialność za ochronę informacji.

Skuteczna ochrona zasobów informacyjnych Urzędu wymaga wspólnego działania i zaangażowania wszystkich pracowników. Zarówno kierownictwo jak i wszyscy pracownicy są zobowiązani, odpowiednio do swoich obowiązków i zajmowanych stanowisk, do przestrzegania Polityki Bezpieczeństwa Informacji, a zwłaszcza zasad zawartych w procedurach, instrukcjach i innych dokumentach Polityki. Pracownicy w szczególności zobowiązani są do przestrzegania procedur opisujących zasady korzystania z haseł, procedur ochrony antywirusowej oraz procedur eksploatacji systemów informatycznych, a także do przestrzegania zakazu udostępniania hasła do swojego komputera, zakazu korzystania z nielegalnego oprogramowania oraz zakazu instalowania jakiegokolwiek oprogramowania bez zgody administratora systemu informatycznego. Pracownicy są zobowiązani do używania zasobów informacyjnych Urzędu wyłącznie do celów służbowych.
Ponadto wszyscy pracownicy są zobowiązani do przestrzegania zasad ochrony informacji prawnie chronionej np.: danych osobowych i informacji niejawnych.
Całokształt obsługi informatycznej i utrzymania sieci komputerowej w Urzędzie realizuje informatyk.
W przypadku osób z którymi Urząd zawiera umowy cywilno-prawne, z których wynika, że będą korzystali z zasobów informacyjnych Urzędu należy w zawieranej umowie wprowadzić klauzulę dot. obowiązku przestrzegania postanowień Polityki Bezpieczeństwa Informacji.
Polityka Bezpieczeństwa Informacji obowiązuje wszystkich dostawców usług i oprogramowania, jednostki zewnętrzne i ich pracowników, o ile w trakcie realizacji umowy otrzymują dostęp do zasobów informatycznych Urzędu, w tym przypadku należy w zawieranej umowie wprowadzić klauzulę dot. obowiązku przestrzegania postanowień Polityki Bezpieczeństwa Informacji. W uzasadnionych przypadkach należy przeprowadzić szkolenie w zakresie PBI obowiązującej w Urzędzie.
Odpowiedzialność za bezpieczeństwo informacji Urzędu obejmuje nie tylko siedzibę Urzędu, ale także wszelkie sytuacje, w których informacje związane z działalnością Urzędu są przetwarzane poza jej siedzibą. Obejmuje to w szczególności zdalny dostęp do sieci komputerowej Urzędu.

10. Podstawowe zasady bezpieczeństwa informacji.

1. Skuteczna ochrona zasobów informacyjnych Urzędu wymaga wspólnego działania i zaangażowania wszystkich pracowników.
2. W sytuacjach kryzysowych, ujawnienie informacji wrażliwych pod względem poufności uznawane jest jako zagrożenie mniejsze od zniszczenia tych informacji.
3. Obowiązek ochrony zasobów Urzędu, w przypadku współpracy z kontrahentami i jednostkami zewnętrznymi określany jest w ramach umów zawartych z tymi podmiotami.
4. Pracownicy Urzędu zobowiązani są do używania zasobów informacyjnych Urzędu wyłącznie do celów służbowych, chyba, że regulacje szczegółowe stanowią inaczej. W związku z tym wszyscy użytkownicy zasobów informacyjnych podlegają kontroli dostępu do

nich.
5. W celu zapewnienia bezpieczeństwa zasobów Urzędu stosuje się następujące ogólne zasady:
a) zasada przywilejów koniecznych - każdy pracownik posiada prawa dostępu do zasobów Urzędu ograniczone wyłącznie do tych, które są konieczne do wykonywania powierzonych mu obowiązków,
b) zasada wiedzy koniecznej - pracownicy posiadają wiedzę o zasobach Urzędu ograniczoną wyłącznie do zagadnień, które są konieczne do realizacji powierzonych im zadań,
c) zasada asekuracji zabezpieczeń - ochrona zasobów winna opierać się na co najmniej dwóch mechanizmach zabezpieczenia,
d) zasada rozliczalności - Urząd dąży do zapewnienia jednoznacznej odpowiedzialności pracowników za powierzone im zasoby; wszyscy użytkownicy zasobów informacyjnych ponoszą odpowiedzialność za zaniedbanie swoich obowiązków w zakresie bezpieczeństwa informacji.
e) zasada czystego biurka - należy unikać pozostawiania dokumentów na biurku bez opieki. Po zakończeniu pracy należy uprzątnąć biurko z dokumentów papierowych oraz informatycznych nośników danych. Zaleca się przechowywanie pod zamknięciem (najlepszym rozwiązaniem jest sejf, szafa lub inna forma zabezpieczenia) dokumentów i nośników zawierających wrażliwe lub krytyczne informacje służbowe.
f) zasada czystego ekranu - zamykanie sesji lub blokowanie komputera i terminala pozostawionego bez opieki lub czasowo nieużywanego (za pomocą mechanizmu blokowania ekranu i klawiatury kontrolowanego hasłem lub innym podobnym mechanizmem). Po zakończonym dniu pracy komputer powinien zostać wyłączony.

11. Dobór zabezpieczeń.

Urząd dobiera cele stosowania zabezpieczeń i zabezpieczenia odpowiednio do wymagań prawnych i wyników analizy ryzyka dla bezpieczeństwa informacji. Zabezpieczenia fizyczne, techniczne i organizacyjne powinny uzupełniać się wzajemnie zapewniając wspólnie wymagany poziom bezpieczeństwa informacji.

12. Sankcje za naruszenie zasad bezpieczeństwa informacji.

Nieprzestrzeganie zasad zawartych w dokumentach Polityki Bezpieczeństwa Informacji Urzędu, jest naruszeniem obowiązków pracowniczych wynikających w szczególności z Kodeksu pracy i może pociągnąć za sobą skutki dyscyplinarne oraz spowodować pociągnięcie do odpowiedzialności wynikającej z przepisów prawa. Naruszenie zasad ochrony informacji może spowodować pociągnięcie do odpowiedzialności karnej wynikającej z przepisów:

- ustawy o ochronie danych osobowych
- kodeksu karnego dot. przestępstw przeciwko ochronie informacji
- przepisów chroniących tajemnice zawodowe.

13. Zasady rozpowszechniania dokumentu oraz tryb wprowadzania zmian.

Do zapoznania się z Polityką Bezpieczeństwa Informacji Urzędu i dokumentami związanymi zobligowana jest kadra kierownicza oraz wszyscy pracownicy. Niniejszy dokument winien być udostępniony również uprawnionym podmiotom zewnętrznym w celu zapoznania się i postępowania w zgodzie z postanowieniami niniejszego dokumentu. Osoba odpowiedzialna za sprawy kadrowe przekazuje, do zapoznania się, nowo zatrudnionym pracownikom oraz stażystom i praktykantom Politykę Bezpieczeństwa Informacji wraz z dokumentami związanymi. Nowo zatrudniony pracownik oraz stażysta czy praktykant jest zobowiązany zapoznać się z zasadami, regułami i postanowieniami zawartymi w w/w dokumentach.
Dokumentacja PBI powinna być przeglądana i weryfikowana:

1) na polecenie Wójta, Sekretarza Urzędu, kierowników referatów;
2) w przypadku wystąpienia poważnych incydentów związanych z bezpieczeństwem informacji;
3) w celu realizacji zaleceń wynikających z przeprowadzonych audytów i kontroli;
4) w przypadku wejścia w życie nowych przepisów dotyczących bezpieczeństwa informacji;
5) przypadku poważnych modyfikacji infrastruktury teleinformatyczne

6) w przypadku zawarcia umów, z których wynikają zobowiązania związane z bezpieczeństwem informacji.

Zmiany w dokumentach wprowadza Zespół ds. Monitorowania Zagrożeń i Utrzymania Polityki Bezpieczeństwa Informacji na podstawie okresowych przeglądów. Zmieniony dokument zatwierdza Wójt i wprowadza w drodze zarządzenia.

WÓJT
mgr inż. Jan Joka

Załącznik nr 1
do Polityki Bezpieczeństwa Informacji
Urzędu Gminy Jaświły

POLITYKA
KONTROLI DOSTĘPU DO INFORMACJI

Definicje pojęć stosowanych w polityce.

1. **Administrator systemu** - pracownik Urzędu Gminy Jaświły, odpowiedzialny za realizację zadań związanych z zarządzaniem systemem informatycznym, w tym za zabezpieczenie sieci komputerowej tzn. wdrażanie stosownych środków administracyjnych, technicznych i fizycznych w Urzędzie w celu zabezpieczenia zasobów infrastruktury informatycznej oraz ochrony danych przed nieuprawnioną modyfikacją, zniszczeniem, dostępem i ujawnieniem, a także ich utratą.
2. **Stanowisko** - pojedynczy komputer osobisty lub terminal przeznaczony do określonych zadań związanych między innymi z dostępem do sieci komputerowej Urzędu.
3. **System informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
4. **Zasoby informatyczne** - ogół systemów informatycznych wykorzystywanych przez daną organizację
5. **Spam** - niechciane wiadomości elektroniczne. Najbardziej rozpowszechniony jest spam wysyłany za pośrednictwem poczty elektronicznej. Zwykle (choć nie zawsze) jest wysyłany masowo. Istotą spamu jest rozsyłanie dużej liczby informacji komercyjnych o jednakowej treści do nieznanych sobie osób. Nie ma znaczenia, jaka jest treść tych wiadomości.
6. **Konto** - to zbiór zasobów i uprawnień mający unikalny identyfikator w systemie informatycznym lub sieci komputerowej.
7. **Użytkownik** - to byt (osoba lub inny system) korzystający z systemu komputerowego. Użytkownicy mogą być identyfikowani w celach zliczania czasu pracy, bezpieczeństwa, czy też zarządzania zasobami. Aby użytkownik został zidentyfikowany, użytkownik posiada konto (konto użytkownika), do którego przypisana jest nazwa (nazwa użytkownika) i hasło (lub inny sposób autentykacji - np. informacje biometryczne). Użytkownicy uzyskują dostęp do systemów przez interfejs użytkownika, a sam proces identyfikacji jest nazywany logowaniem (od angielskiego *logging in).*

1. Cel polityki.

Celem polityki jest określenie zasad udzielania dostępu użytkowników do danych zgromadzonych w sieci komputerowej Urzędu oraz uniemożliwienie dostępu osobom niepowołanym. Dostęp do określonych zasobów informatycznych jest przydzielany na podstawie udokumentowanych potrzeb użytkowników.

2. Zakres stosowania.

Działania opisane w niniejszej polityce obowiązują, we wszystkich referatach i pozostałych komórkach organizacyjnych Urzędu oraz innych jednostkach korzystających z sieci komputerowej Urzędu. Niniejsza polityka jest elementem Polityki Bezpieczeństwa Informacji ustanowionej w Urzędzie.

3. Odpowiedzialność.

Wszyscy użytkownicy uzyskujący dostęp do zasobów sieci komputerowej Urzędu jak również użytkownicy stanowisk nie podłączonych do sieci ale zainstalowanych na terenie Urzędu, odpowiedzialni są za przestrzeganie zasad

opisanych w polityce w zakresie ochrony haseł. Administrator systemu odpowiedzialny jest za zakładanie i usuwanie kont w systemie, przydzielanie i odbieranie dostępu do zasobów użytkownikom stanowisk, generowanie użytkownikom pierwszych haseł dostępowych.
Kierownicy referatów Urzędu oraz inne komórki organizacyjne korzystające z sieci komputerowej Urzędu odpowiedzialni są za analizę celowości uruchomienia stanowiska, za przygotowanie i przekazanie do referatu Organizacyjnego wniosków o skonfigurowanie stanowiska oraz przydzielenie lub zlikwidowanie konta użytkownikowi, a także zapoznanie podległych im pracowników z treścią tej polityki.

4. Udzielanie dostępu do zasobów informatycznych.

1) kierownicy referatów wnioskują do Sekretarza Gminy o założenie zmianę/likwidację) konta użytkownika zasobów informatycznych Urzędu.
2) Sekretarz Gminy sprawdza wniosek m.in. pod względem zgodności z wymogami ustawy o ochronie danych osobowych i ustawy o ochronie informacji niejawnych, a następnie przekazuje zaakceptowany wniosek administratorowi systemu, który ustala z użytkownikiem nazwę konta.
3) Administrator systemu na podstawie wniosku zakłada konto lub zmienia parametry konta i przekazuje użytkownikowi wszystkie dane niezbędne do korzystania z niego, w tym hasło do pierwszego zalogowania.
4) W przypadku likwidacji konta, administrator usuwa lub blokuje konto w terminie określonym w treści wniosku.
5) W porozumieniu z administratorem systemu, informatyk dokonuje końcowej konfiguracji poczty elektronicznej na komputerze użytkownika (jeżeli wniosek tego dotyczy) i innych niezbędnych elementów potrzebnych użytkownikowi do wykonywania zadań określonych w regulaminie stanowiska pracy.

5. Określenie sposobu przydziału haseł dla użytkowników i częstotliwość ich zmiany oraz wskazanie osoby/osób odpowiedzialnej/odpowiedzialnych za te czynności.

1. Użytkownicy stanowisk roboczych są zobowiązani zapoznać się z „Polityką Bezpieczeństwa Informacji" oraz chronić przed nieuprawnionym wykorzystaniem wszelkie znane im lub będące w ich posiadaniu dane umożliwiające dostęp do zasobów sieci komputerowej Urzędu. Oznacza to m.in. zakaz ujawniania haseł umożliwiających dostęp do kont lub innych zasobów, np. do plików zawierających hasła, klucze szyfrujące, itp.
2. Po otrzymaniu haseł umożliwiających dostęp do konta użytkownik powinien niezwłocznie zmienić te hasła na inne, znane tylko sobie. Hasła powinny spełniać następujące wymagania:
- minimalna długość hasła powinna wynosić 8 znaków;
- hasło powinno zawierać duże i małe litery, znaki specjalne oraz cyfry;
- nie należy używać wyrazów występujących we wszelkiego rodzaju słownikach, nawet jeśli zostaną uzupełnione innymi znakami;
- nie należy też używać żadnych wyrazów lub liczb występujących w danych personalnych użytkownika.
- nie należy używać haseł wynikających z układu klawiatury (np.: qwerty)
- hasło nie może się powtarzać

3. Hasła nie wolno nigdzie zapisywać ani na papierze, ani w postaci elektronicznej -

należy je zapamiętać. Niedopuszczalne jest zwłaszcza zapisywanie haseł na kartkach przyklejonych do monitora, klawiatury, czy biurka. Hasło należy zmieniać co najmniej raz na miesiąc.
4. Posługiwanie się danymi identyfikującymi lub uwierzytelniającymi należącymi do innego użytkownika w celu dostępu do zasobów sieci komputerowej Urzędu na jego konto lub podejmowania jakichkolwiek innych działań (a zwłaszcza wykorzystanie podpisu elektronicznego) w jego imieniu jest zabronione.

6. Zasady postępowania dotyczące dostępu pracowników Urzędu do systemów informatycznych udostępnianych do celów służbowych przez zewnętrzne instytucje poprzez sieć Internet lub inną sieć rozległą.

W przypadku, gdy pracownicy Urzędu używają w pracy systemu informatycznego udostępnianego przez zewnętrzną instytucję (np. ministerstwo) ochronie podlegają jedynie dane i programy umożliwiające uwierzytelnienie i dostęp do ww. systemu (np.: loginy, hasła, certyfikaty). Należy wtedy oprócz stosowania się do zasad opisanych w niniejszej polityce stosować się do zaleceń i polityki bezpieczeństwa instytucji udostępniającej system.

Pracownicy Urzędu korzystają z systemu udostępnionego przez zewnętrzne instytucje wyłącznie w siedzibie Urzędu i w godzinach pracy Urzędu, na sprzęcie komputerowym przeznaczonym do celów służbowych, chyba, że ustalenia z instytucją udostępniającą system stanowią inaczej lub specyfika pracy w tym systemie wymaga odstąpienia od tej zasady.

7. Kontrola dostępu do sieci komputerowej.

Użytkownicy winni mieć bezpośredni dostęp tylko do zasobów określonych we wniosku.

8. Zasady postępowania dotyczące pracy na odległość oraz urządzeń przenośnych i nośników danych wynoszonych poza siedzibę Urzędu.

Komputery przenośne wykorzystywane poza siedzibą są zabezpieczone dodatkowo poprzez hasło BIOS oraz zaszyfrowanie danych zapisanych na twardym dysku.
1. Wynoszenie urządzeń przenośnych będących własnością Urzędu poza jego siedzibę może występować wyłącznie w ramach wykonywania obowiązków służbowych po wyrażeniu zgody przez kierownika referatu.
2. Urządzenia przenośnie i nośniki danych wynoszone poza siedzibę Urzędu winne zapewniać możliwość szyfrowania danych w celu ochrony przed dostępem osób nieupoważnionych w wypadku zagubienia lub kradzieży urządzenia. W szczególności dotyczy to laptopów, notebooków , netbooków, dysków przenośnych i pendrive'ów.
3. Urządzenia nie spełniające powyższych wymagań będą sukcesywnie wymieniane.
4. W przypadku utraty urządzenia należy niezwłocznie powiadomić przełożonych oraz Sekretarza Gminy.

9. Kontrola dostępu do pomieszczeń serwerowni.

Dostęp do serwerowni mają tylko uprawnieni pracownicy – informatycy

Urzędu. Inne osoby mogą przebywać w tych pomieszczeniach tylko w obecności osób uprawnionych.

10. Procedura przeglądu uprawnień do systemów.

W celu utrzymania efektywnej kontroli nad dostępem do danych i systemów informatycznych Administrator Systemu dokonuje przeglądu praw użytkowników do systemów. Przegląd uprawnień do systemów jest wykonywany w ramach przeglądu i aktualizacji Polityki Bezpieczeństwa Informacji. Przegląd musi obejmować zarówno konta zwykłych użytkowników jak i konta o wysokich uprawnieniach. Wynikiem przeglądu jest aktualizacja danych o uprawnieniach potwierdzona sporządzeniem notatki przez Administratora Systemu.

WÓJT
mgr inż. Jan Joka

Załącznik
Polityki Kontroli Dostępu

Wniosek o założenie / zmianę / likwidację konta w* zasobach informatycznych

Dane wnioskodawcy:
Imię i nazwisko:.....
Stanowisko służbowe:.....
Jednostka organizacyjna:.....
Dane osoby, która jest/będzie użytkownikiem konta:
Imię i nazwisko:.....
Stanowisko służbowe:.....
Jednostka organizacyjna:.....
Oddział w jednostce:.....
Nazwa konta:.....
Przeznaczenie konta (wpodpunktach a), b),c),d) wpisać słowo „ TAK" lub" NIE"):
a) Sieć komputerowa SUW.....
b) Poczta elektroniczna wewnętrzna:.....
c) Poczta elektroniczna zewnętrzna (INTERNET):.....
d) System EZD:.....
e) Inne usługi (podać jakie wraz z uzasadnieniem celowości):
1. Termin likwidacji konta *(w przypadku konta czasowego lub wniosku o likwidację konta)*:
2. Miejsca korzystania z konta:

Lp	Lokalizacja stanowiska roboczego (budynek, piętro, pokój)

Data Pieczątka i podpis
Wnioskodawcy

* - niepotrzebne skreślić

WÓJT
mgr inż. Jan Joka

Załącznik nr 2
Polityki Bezpieczeństwa Informacji
Urzędu Gminy Jaświły

POLITYKA
TWORZENIA KOPII ZAPASOWYCH

Definicje pojęć stosowanych w polityce.

1. **Administrator systemu** - pracownik Urzędu Gminy Jaświły, odpowiedzialny za realizację zadań związanych z zarządzaniem systemem informatycznym, w tym za zabezpieczenie sieci komputerowej tzn. wdrażanie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów infrastruktury informatycznej oraz ochrony danych przed nieuprawnioną modyfikacją, zniszczeniem, dostępem i ujawnieniem, a także ich utratą.
2. **Stanowisko** - pojedynczy komputer osobisty lub terminal przeznaczony do określonych zadań związanych między innymi z dostępem do sieci komputerowej.
3. **System informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
4. **Zasoby informatyczne** - ogół systemów informatycznych wykorzystywanych przez daną organizację
5. **Kopia zapasowa** - kopia danych lub oprogramowania. Celem jej wykonywania jest odtworzenie systemu po awarii.

1. Cel polityki.

Polityka Tworzenia Kopii Zapasowych określa zasady tworzenia, przechowywania i testowania kopii zapasowych oraz odzyskiwania z nich danych i systemów informatycznych, w celu zapewnienia integralności i dostępności informacji oraz środków przetwarzania informacji.

2. Zakres stosowania.

Działania opisane w niniejszej polityce obowiązują, we wszystkich referatach i pozostałych komórkach organizacyjnych Urzędu oraz innych jednostkach korzystających z sieci komputerowej Urzędu. Niniejsza polityka jest elementem Polityki Bezpieczeństwa Informacji ustanowionej w Urzędzie.

3. Wykonywanie kopii systemów informatycznych.

Na potrzeby zachowania ciągłości działania systemów informatycznych i utrzymania integralności danych wykonuje się kopie zapasowe zbiorów danych. Zadanie to realizowane jest codziennie w dni robocze. Kopie tworzone są przyrostowo, tzn. kopiowane są pliki nowe i te których zawartość uległa zmianie. Kopie zapasowe sporządza się również w następujących przypadkach:
a) przed dokonaniem istotnej zmiany konfiguracyjnej (np. aktualizacji oprogramowania, ustawień systemowych),
b) po przeprowadzeniu zmiany konfiguracyjnej (np. aktualizacji oprogramowania, ustawień systemowych, zmianie praw dostępu).

Kopie zapasowe, wykonane w danym dniu przechowywane są przez okres 2 miesięcy a po ustaniu użyteczności kopii zapasowej jest ona niezwłocznie usuwana. Kopie zapasowe konfiguracji systemów operacyjnych serwerów wykonuje administrator systemu po każdej zmianie konfiguracji oprogramowania (np. po utworzeniu, rekonfiguracji lub usunięciu konta użytkownika w systemie, zmianie praw dostępu itp.)
Za prawidłowość tworzenia kopii zapasowych odpowiada administrator systemu.

4. Wykonywanie kopii zapasowych danych roboczych użytkowników sieci komputerowej Urzędu przechowywanych na serwerach

1. Administrator systemu odpowiada za wykonywanie kopii zapasowych danych roboczych użytkowników (kopie robocze) przechowywanych na serwerach zlokalizowanych w sieci komputerowej Urzędu (bazy danych, katalogi użytkowników, katalogi grup).
2. Za wykonywanie kopii zapasowych danych znajdujących się na poszczególnych stacjach roboczych poza serwerownią odpowiadają użytkownicy tych stacji roboczych. Częstotliwość tworzenia kopii zapasowych na stacjach roboczych zależy od ilości i wagi przetwarzanych informacji. Niedopuszczalne jest przechowywanie kopii zapasowych na tych samych nośnikach, na których są one przetwarzane. Użytkownicy mogą zlecać administratorowi systemu wykonanie kopii przetwarzanych przez nich danych (np. kopii folderów osobistych skrzynek pocztowych). Zlecenie należy złożyć w formie elektronicznej za pomocą systemu EZD.

5. Testowanie kopii zapasowych.

Kopie zapasowe sprawdzane są okresowo pod kątem ich dalszej przydatności przez administratora systemu nie rzadziej niż raz na miesiąc. Polega to na testowym odtworzeniu zawartości kopii na innym urządzeniu. Administrator systemu sporządza notatkę po każdym teście. Po stwierdzeniu nieprzydatności kopii zapasowych zbiorów nośnik zostaje pozbawiony danych lub wybrakowany w inny sposób uniemożliwiający dalszy odczyt informacji.

6. Odzyskiwanie danych i systemów informatycznych z kopii zapasowych.

Odzyskiwanie danych z kopii zapasowych jest wykonywane w następujących przypadkach:

a) utraty całości lub części danych na serwerze;
b) utraty integralności całości lub części danych na serwerze;
c) w celu odtworzenia poprzedniej wersji danych przekazany w systemie EZD;
d) na wniosek organu kontrolnego (np.: NIK);
e) przy przenoszeniu danych na nowy serwer.

Odzyskiwanie całego systemu informatycznego jest wykonywane w wypadku awarii sprzętowej lub systemowej nośników danych na których jest on zlokalizowany, uniemożliwiającej korzystanie z danego systemu.
Za odzyskiwanie danych z kopii zapasowych odpowiada administrator systemu.

W.O. J.T.
mgr inż. Jan Joka

Załącznik nr 3
Polityki Bezpieczeństwa Informacji
Urzędu Gminy Jaświły

Procedura zarządzania ryzykiem w bezpieczeństwie informacji

Opracowana na podstawie przygotowanej przez Ministerstwo Administracji i Cyfryzacji metodyki oceny ryzyka, o której mowa w przyjętej przez Radę Ministrów w czerwcu 2013 r. Polityce Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej

Definicje pojęć i skrótów stosowanych w procedurze

Zasoby - to, co stanowi wartość, aktywa Urzędu;
Zagrożenie - zdarzenie, które może wywołać negatywne skutki, czynnik ryzyka;
Podatność - aspekty, które mogą być wykorzystane przez/ sprzyjać powstaniu zagrożenia, słabość, przyczyna, słaby punkt;
Skutek - efekt wystąpienia zagrożenia, następstwo;
Zmaterializowanie się ryzyka - sytuacja, w której ryzyko zaistniało, wystąpienie ryzyka;
Zabezpieczenia - rozwiązania, które zmniejszają ryzyko, mechanizmy kontroli, środki kontroli;
Ryzyko rezydualne - ryzyko uwzględniające zabezpieczenia i ich skuteczność, ryzyko szczątkowe;
Ryzyko nieodłączne - ryzyko nieuwzględniające zabezpieczeń
STI - system teleinformatyczny.
KZTI - krytyczne zasoby teleinformatyczne
Polityka - Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej

Cel ustanowienia procedury

Celem Procedury Zarządzania Ryzykiem w bezpieczeństwie informacji jest wsparcie PBI, w zakresie ograniczania do minimum ryzyka dla bezpieczeństwa informacji w Urzędzie, a w szczególności określenie metodyki i zasad zarządzania ryzykiem w Urzędzie.

Metodyka zarządzania ryzykiem.

W Urzędzie Gminy Jaświły do zarządzania ryzykiem w bezpieczeństwie informacji wybrana została metodyka zaproponowana przez Ministerstwo Administracji i Cyfryzacji w celu wykonania oceny ryzyka zgodnie z „Polityką Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej".
Zgodnie z tą Polityką, jak również powszechnie stosowanymi metodykami i systemami zarządzania bezpieczeństwem, w tym bezpieczeństwem teleinformatycznym dla zaplanowania i realizowania adekwatnych działań zapewniających bezpieczeństwo teleinformatyczne niezbędne jest:
a) dokonanie inwentaryzacji zasobów;
b) określenie zasobów kluczowych;
c) przeprowadzenie oceny ryzyka;
d) podjęcie działań będących następstwem oceny ryzyka.

Ocena ryzyka obejmuje:
- identyfikację ryzyka,

- analizę ryzyka,
- ewaluację ryzyka.

Postępowanie z ryzykiem - to działania podejmowane w następstwie oceny ryzyka. Zarządzanie ryzykiem obejmuje m.in. ocenę ryzyka i postępowanie z ryzykiem.

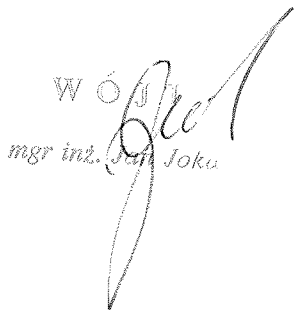
1. Założenia do działań związanych z zarządzaniem ryzykiem oraz sprawozdawczością wynikającą z Polityki

1) W analizie nie należy uwzględniać przetwarzania informacji niejawnych w rozumieniu ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2016r., poz. 1167 i 1948).
2) Ocena ryzyka oraz działania z niej wynikające nie ograniczają się jedynie do zagrożeń natury technicznej i uwzględniają również zagrożenia generowane przez użytkowników oraz inne strony zainteresowane.
3) Na potrzeby oceny ryzyka i przygotowania sprawozdania zidentyfikowane ryzyka dzieli się na:
- ryzyko wewnętrzne - ryzyko, które jest związane z wystąpieniem zagrożenia wewnętrznego lub takiego, na które jednostka ma wpływ (działanie albo zaniechanie pracownika, dostawcy, awaria urządzenia spowodowana złą eksploatacją itp.);
- ryzyko zewnętrzne - ryzyko, które jest związane z wystąpieniem zagrożenia zewnętrznego (działanie cyberprzestępcy, działanie sił przyrody itp.).

2. Odpowiedzialność

Odpowiedzialność za przeprowadzenie oceny ryzyka i przygotowanie sprawozdania podsumowującego wyniki oceny ryzyka ponosi informatyk.
Odpowiedzialność za podejmowanie określonych działań w stosunku do zidentyfikowanych ryzyk ponoszą użytkownicy.

3. Sposób przeprowadzania oceny ryzyka 3.3.1. Identyfikacja systemów teleinformatycznych



Wybór krytycznych zasobów teleinformatycznych (KZTI)

Zidentyfikowane zagrożenia dzielone są na dwie kategorie: krytyczne i pozostałe.
Na wybór KZTI ma wpływ istotność/znaczenie KZTI. Przez istotność/znaczenie rozumie się to, do jakich usług używany jest sprzęt i jakie jest znaczenie tych usług z punktu widzenia zadań i roli Państwa. Uwzględniane jest, jak brak funkcjonowania albo nieprawidłowe funkcjonowanie wpłynie na:
- bezpieczeństwo Państwa i obywateli, w tym ich życia i zdrowia, jak również porządek publiczny (pomimo że niniejsza metodyka nie dotyczy działań stosowanych do przetwarzania informacji niejawnych, jest prawdopodobne, że część może mieć wpływ na bezpieczeństwo Państwa i obywateli);

1. Identyfikacja zagrożeń związanych z KZTI.

Dla każdego z KZTI należy zidentyfikować związane z nim zagrożenia, które mogą spowodować m.in.:
a) niedostępność usług,
b) nieuprawniony dostęp do danych / kradzież danych,
c) nieuprawnioną modyfikację danych,
d) zniszczenie danych.

Na etapie identyfikacji zagrożeń sporządzana jest lista zidentyfikowanych zagrożeń. Przy Identyfikacji zagrożeń wykorzystywane są m.in.:
- ilość incydentów,
- wyniki audytów i kontroli,
- fachowa literatura,
- specjalistyczne fora internetowe,
- informacje udostępniane przez producentów oprogramowania i sprzętu.

Przykładowe zagrożenia dotyczące bezpieczeństwa teleinformatycznego wymieniono w załączniku nr 1 do niniejszej Procedury.

2. Wybór kluczowych zagrożeń

W celu skoncentrowania oraz efektywnego wykorzystania sił i środków wybierane są w Urzędzie zagrożenia kluczowe, których liczba waha się od kilku do kilkunastu. Dokonanie selekcji zagrożeń odbywa się przez podjęcie arbitralnej decyzji osoby odpowiedzialnej za KZTI.

3. Przeanalizowanie zagrożeń pod względem ich skutków i prawdopodobieństwa wystąpienia

Analiza skutków zagrożeń uwzględnia:
- skutki związane z życiem lub zdrowiem ludzi;
- skutki finansowe;
- skutki związane z nierealizowaniem funkcji i zadań;
- skutki związane z zaufaniem obywateli do władzy publicznej.

Analiza prawdopodobieństwa wystąpienia zagrożeń, tam gdzie ma to zastosowanie, uwzględnia:
- dane historyczne (informacje o zmaterializowaniu ryzyka w jednostce i otoczeniu);
- zabezpieczenia i ich skuteczność (w tym przeciwdziałające, detekcyjne, dające możliwość skutecznej reakcji po wykryciu);
- podatności (występujące słabości);
- ekspozycję (czas dostępności, liczba użytkowników, liczba operacji, dostępność przez internet);
- atrakcyjność zasobu (m.in. korzyść materialna, prestiż, korzyść polityczna dla potencjalnego cyberprzestępcy związana z naruszeniem bezpieczeństwa);
- cyberprzestępcę (potencjalny agresor, jego wiedza, motywacja i zasoby).

WÓJT
mgr inż. Jan Joka

Analiza ryzyka

1. Ocena skutków zagrożeń i prawdopodobieństwa ich wystąpienia

Zgromadzone dane na temat skutków i prawdopodobieństwa, oceniane są z zastosowaniem poniższej skali punktowej.

Skala oceny skutków

Poniżej znajduje się macierz, która ma ułatwić ocenę skutku na właściwym poziomie. Każde zagrożenie analizowane jest pod kątem skutków w czterech aspektach (krok 5: życie lub zdrowie, finanse, funkcje i zadania, zaufanie). W celu ułatwienia i zapewnienia obiektywnej i wyważonej oceny skutków, dla poszczególnych aspektów przyjęto charakterystyki przypisane do odpowiednich poziomów punktowych. Ocena punktowa skutku wyrażana jest jako jedna wartość w przedziale od 1 do 5, co oznacza odpowiednio skutek oceniony jako nieznaczny (1) do bardzo duży (5).

Możliwe jest wystąpienie zagrożenia, które nie będzie oddziaływało na wszystkie cztery aspekty, przykładowo nie będzie oddziaływało na aspekt finansowy, ale jego wpływ np. na życie lub zdrowie spowoduje wysoką (4 albo 5 punktów) ocenę skutków. Może również wystąpić sytuacja, w której dane zagrożenie będzie niosło za sobą skutki, dla których opis trzech aspektów będzie wskazywał na ocenę na poziomie 1 (np. straty poniżej 100 000, krótkie i nieznaczne zakłócenia w realizacji funkcji i zadań Państwa, nieznaczna utrata zaufania obywateli do władzy publicznej), natomiast bardzo wysoka ocena w jednym aspekcie (np. utrata życia) spowoduje całościową ocenę skutków na poziomie 4 czy nawet 5 punktów.

Ocenę skutków można przeprowadzić stosując metody matematyczne np. dokonanie oceny punktowej w poszczególnych aspektach i wyliczenia średniej. Jednakże wyrażona punktowo ocena jest wynikiem analizy, zaś poniższa macierz ma charakter jedynie wspomagający. Określając wartość skutku, zakładany jest możliwy, ale najbardziej negatywny scenariusz wystąpienia zagrożenia.

Ocena	**Poziom (S)**	**Skutki związane z życiem lub zdrowiem ludzi**	**Skutki finansowe dla Państwa, w tym gospodarki**	**Skutki związane z nierealizowaniem funkcji i zadań**	**Skutki związane z zaufaniem obywateli do władzy publicznej**
1	Nieznaczny	Nieznaczne obrażenia	Straty poniżej 100 000	Krótkotrwałe i nieznaczne zakłócenia w realizacji funkcji i zadań	Nieznaczna utrata zaufania obywateli do władzy publicznej
2	Mały	Niewielkie obrażenia	Straty od 100 000 do 300 000	Niewielkie zakłócenia w realizacji funkcji i zadań	Niewielka utrata zaufania obywateli do władzy publicznej
3	Średnie	Poważne obrażenia	Straty od 300 000 do 500 000	Poważne zakłócenia w realizacji funkcji i zadań	Poważna utrata zaufania obywateli do władzy publicznej

4	Duży	Poważne i trwałe obrażenia	Straty od 500 000 do 1 000 000	Poważne i trwałe zakłócenia w realizacji funkcji i zadań	Poważna i trwała utrata zaufania obywateli do władzy publicznej
5	Bardzo duży	Utrata życia	Straty powyżej 1 000 000	Poważny i długotrwały brak realizacji funkcji i zadań	Poważna i długotrwała utrata zaufania obywateli do władzy publicznej

WÓJ
mgr inż. Jan Jok

Przy ocenie skutków uwzględniane są zabezpieczenia, które mają zastosowanie do zmniejszenia skutków.
Skala oceny prawdopodobieństwa
Przy ocenie prawdopodobieństwa, analizowane jest zagrożenie, uwzględniające charakterystyki umieszczone w kolumnie „Opis wspomagający". W przypadku wystąpienia sytuacji, w której poszczególne charakterystyki występują w różnych przedziałach punktowych, ocena oparta jest na osądzie oceniających prawdopodobieństwo. W przypadku oceny danych historycznych, uwzględniane są dane posiadane w Urzędzie, jak również informacje z otoczenia. Analiza podatności uwzględnia znane i występujące w rzeczywistości podatności. W sytuacji, w której jedna albo więcej charakterystyk nie ma miała zastosowania nie jest uwzględniana, np. zagrożenie może nie być wywołane celowym działaniem pracownika lub innej strony zainteresowanej (nie ma zastosowania charakterystyka -cyberprzestępca).

Ocena	**Poziom (P)**	**Opis wspomagający**
1	Bardzo mało prawdopodobne	Dane historyczne: Nie występuje Zabezpieczenia: Liczne i bardzo skuteczne Podatności: Brak Atrakcyjność: Bardzo mała Ekspozycja: Nieistotna Cyberprzestępca: Przypadkowy
2	Mało prawdopodobne	Dane historyczne: Bardzo nieliczne wystąpienia Zabezpieczenia: Liczne i skuteczne Podatności: Bardzo nieliczne Atrakcyjność: Mała Ekspozycja: Bardzo małe znaczenie Cyberprzestępca: Nieprofesjonalny, mający małą wiedzę
o J	Prawdopodobne	Dane historyczne: Nieliczne wystąpienia Zabezpieczenia: Liczne i częściowo skuteczne Podatności: Nieliczne Atrakcyjność: Średnia Ekspozycja: Małe znaczenie Cyberprzestępca: Profesjonalny, mający odpowiednią wiedzę

4	Bardzo prawdopodobne	Dane historyczne: Wystąpienia Zabezpieczenia: Nieliczne i mało skuteczne Podatności: Liczne Atrakcyjność: Duża Ekspozycja: Duże znaczenie Cyberprzestępca: Profesjonalny, mający odpowiednią wiedzę i zmotywowany
5	Pewne	Dane historyczne: Liczne wystąpienia Zabezpieczenia: Brak albo nieliczne i nieskuteczne Podatności: Bardzo liczne Atrakcyjność: Bardzo duża Ekspozycja: Bardzo duże znaczenie Cyberprzestępca: Profesjonalny, mający odpowiednią wiedzę, zmotywowany i wyposażony w niezbędne zasoby, w tym finansowe

WÓJT

mgr inż. Jan Joka

2. Ustalenie poziomu ryzyka

Poziom ryzyka (PR) jest obliczany jako iloczyn skutków (S) i prawdopodobieństwa (P)

PR=S P

3. Ewaluacja ryzyka

Ewaluacja ryzyka dokonywana jest według poniższej tabeli:

Kryteria		Ewaluacja ryzyka
Wartość punktowa PR	Poziom ryzyka	
1-5	Małe	Akceptowalne
6-9	Średnie	Akceptowalne, wymagające decyzji osoby odpowiedzialnej
10- 16 oraz 5 gdzie P = 1 a S = 5	Duże	Nieakceptowalne, wymagające decyzji osoby odpowiedzialnej w zakresie dalszego postępowania z ryzykiem
	Bardzo duże	Nieakceptowalne, wymagające decyzji kierownika jednostki w zakresie dalszego postępowania z ryzykiem

4. Podjęcie decyzji dotyczącej postępowania z ryzykiem.

W stosunku do ryzyk podejmowane są następujące decyzje:

- zapobieganie, czyli działania polegające na zmniejszeniu poziomu ryzyka;
- przeniesienie ryzyka na inną jednostkę (przenosząc ryzyko, należy pamiętać, że jego przeniesienie najczęściej nie zmniejsza odpowiedzialności za jego wystąpienie, co ma istotne znaczenie z punktu widzenia działania Państwa);
- unikanie, czyli m.in. zaprzestanie działań powodujących ryzyko;
- tolerowanie (akceptowanie) ryzyka w przypadku, gdy istnieją określone trudności w przeciwdziałaniu ryzykom lub gdy koszty planowanych działań doskonalących mogą przekroczyć przewidywane korzyści.

Zgodnie z powyższą metodyką realizowane jest monitorowanie ryzyka.

4. Monitorowanie ryzyka

Podstawowym celem monitorowania ryzyka jest uzyskanie potwierdzenia, że wdrożona procedura jest skuteczna. Równie ważne jest wykrywanie sytuacji, gdy środki ochrony są niewystarczające bądź funkcjonowanie procedury jest poniżej przyjętych standardów. W obu przypadkach konieczne jest podejmowanie zdecydowanych działań doskonalących.

Proces monitorowania ryzyka składa się z następujących elementów:

1.Wejście: wszystkie uzyskane informacje z systemu zarządzania ryzykiem,

2.Działanie: obserwacja ryzyka i czynników ryzyka,

3.Wyjście: ciągłe dostrajanie systemu zarządzania ryzykiem.

Proces monitorowania ryzyka ma charakter ciągły.

Podczas etapu monitorowania powinny być zbierane również informacje o tym, jak zmieniają się ryzyka:

Czy zmieniły się zagrożenia?

Czy zmieniły się podatności?

Czy zmieniło się prawdopodobieństwo wystąpienia ryzyka?
Czy zmienił się wpływ skutków zaistniałego ryzyka?
Czy działania dla złagodzenia ryzyka są nadal odpowiednie?

5. Informowanie o ryzyku.
Komunikowanie ryzyka polega na wzajemnej wymianie informacji dotyczących ryzyka, między odpowiedzialnymi za zarządzanie ryzykiem, a zainteresowanymi stronami. Powinno prowadzić do wzrostu świadomości ryzyka wśród pracowników Urzędu, co może wspierać naturalne mechanizmy kontroli wewnętrznej.

6. Działania związane z zarządzaniem ryzykiem.
Na podstawie przedstawionej powyżej metodyki przynajmniej raz w roku podczas przeglądu PBI oraz po każdej istotnej zmianie w Urzędzie mogącej mieć wpływ na ryzyko, dokonuje się identyfikacji i oceny ryzyka oraz określa metody przeciwdziałania ryzyku. Wykonywany jest także przegląd procesu zarządzania ryzykiem w celu jego usprawnienia. Na podstawie wyników powyższych działań sporządza się arkusz sprawozdania podsumowującego wyniki analizy ryzyka zgodnie z wzorem stanowiącym załącznik nr 2 do niniejszej Procedury. Jednocześnie stale realizowany jest proces monitorowania ryzyka. Podstawowym źródłem danych do monitorowania ryzyka jest proces zarządzania incydentami związanymi z bezpieczeństwem informacji.

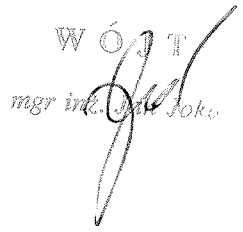
WÓJT
mgr inż. [illegible]

Załącznik nr 1
do Procedury zarządzania ryzykiem
w bezpieczeństwie informacji

Przykładowe zagrożenia dotyczące bezpieczeństwa teleinformatycznego

1. Zainstalowanie złośliwego oprogramowania (m.in. wirusy, robaki, bomby logiczne, konie trojańskie) przez korespondencję elektroniczną
2. Zainstalowanie złośliwego oprogramowania (m.in. wirusy, robaki, bomby logiczne, konie trojańskie) przez stronę www
3. Zainstalowanie złośliwego oprogramowania (m.in. wirusy, robaki, bomby logiczne, konie trojańskie) przez nośniki zewnętrzne
4. Zainstalowanie złośliwego oprogramowania (m.in. wirusy, robaki, bomby logiczne, konie trojańskie) w instalowanym oprogramowaniu
5. Zainstalowanie złośliwego oprogramowania (m.in. wirusy, robaki, bomby logiczne, konie trojańskie) w trakcie naprawy lub serwisu
6. Wykorzystanie luk w systemach urządzeń mobilnych
7. Atak zewnętrzny ograniczający dostęp typu DDoS
8. Przejęcie informacji przesyłanych pocztą elektroniczną
9. Podsłuchanie informacji przesyłanych siecią radiową
10. Podsłuchanie informacji przesyłanych siecią tradycyjną
11. Włamanie do STI
12. Atak socjotechniczny w celu przejęcia danych (phishing)
13. Przekierowanie - pharming
14. Nieuprawniony fizyczny dostęp do urządzeń
15. Nieuprawniony dostęp do nośników danych (m.in. optycznych, magnetycznych)
16. Brak zasilania energetycznego
17. Zalanie wodą lub innymi substancjami z instalacji wewnętrznych
18. Pożar
19. Powódź
20. Przegrzanie sprzętu
21. Awaria sprzętu
22. Zły stan techniczny sprzętu
23. Niewydolne urządzenia (zbyt wolne, nieodpowiadające wymaganiom programowym)
24. Niestabilność łącza w usłudze dostępu do internetu
25. Niewystarczająca przepustowość łącza w usłudze dostępu do internetu
26. Używanie oprogramowania niemającego wsparcia producenta
27. Kradzież sprzętu z siedziby jednostki
28. Kradzież sprzętu mobilnego
29. Podejrzenie informacji w siedzibie jednostki
30. Podejrzenie informacji przetwarzanej na sprzęcie mobilnym
31. Błędy uprawnionych użytkowników - niezapisanie danych
32. Błędy uprawnionego użytkownika - skasowanie danych
33. Błąd uprawnionego użytkownika - wysłanie informacji pocztą elektroniczną do nieuprawnionej osoby
34. Błąd uprawnionego użytkownika - administratora - błędna konfiguracja dająca nadmierne uprawnienia
35. Celowe działanie uprawnionych użytkowników - zniszczenie informacji
36. Celowe działanie uprawnionych użytkowników - sprzedaż informacji
37. Celowe działanie uprawnionych użytkowników - sabotaż
38. Celowe działanie uprawnionych użytkowników - nadużycie uprawnień
39. Celowe działanie - zniszczenie sprzętu
40. Brak świadomości użytkowników STI na temat ryzyk (zagrożeń, podatności, skutków)

41. Brak znajomości zasad i procedur bezpieczeństwa
42. Zbyt rzadko zmieniane hasła
43. Zbyt słabe hasła
44. Zbyt często zmieniane hasła
45. Nieprzestrzeganie przez użytkowników STI zasad i procedur bezpieczeństwa
46. Nieprawidłowe zarządzanie uprawnieniami użytkowników - nadanie nadmiernych uprawnień
47. Nieprawidłowe zarządzanie uprawnieniami użytkowników - brak cofnięcia albo bardzo opóźnione cofnięcie uprawnień
48. Źle skonfigurowane, w tym otwarte porty
49. Źle skonfigurowane systemy operacyjne
50. Brak zabezpieczeń protokołów komunikacyjnych



Załącznik nr 2 do Procedury
zarządzania ryzykiem
w bezpieczeństwie informacji

Sprawozdanie podsumowujące wyniki oceny ryzyka za.....rok

1. Informacje o ocenie ryzyka

Lp.	KZTI	**Identyfikacja ryzyka**			**Analiza ryzyka**			**Ewaluacja ryzyka**	**Sposób postępowania z ryzykiem przyjęty w jednostce**
		Rodzaj ryzyka	Zdarzenie (dodatkowo można krótko opisać jego skutki i prawdopodobieństwo)	Podatności	Ocena (S)	Ocena (P)	Poziom ryzyka = SxP		

2. Proponowane przez jednostkę działania zmniejszające ryzyko, o charakterze systemowym i horyzontalnym:
3. Informacje o zmaterializowaniu się ryzyka w roku.....o poziomie „Bardzo duże":
.....
4. Informacje dodatkowe:.....

WÓJT
mgr inż. Jan Joka

Załącznik nr 4
Polityki Bezpieczeństwa Informacji
Urzędu Gminy Jaświły

Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji

Definicje pojęć stosowanych w procedurze.

1. **Administrator systemu** – pracownik Urzędu Gminy Jaświły, odpowiedzialny za realizację zadań związanych z zarządzaniem systemem informatycznym SUW, w tym za zabezpieczenie sieci komputerowej tzn. wdrażanie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów infrastruktury informatycznej oraz ochrony danych przed nieuprawnioną modyfikacją, zniszczeniem, dostępem i ujawnieniem, a także ich utratą.
2. **Stanowisko** - pojedynczy komputer osobisty lub terminal przeznaczony do określonych zadań związanych między innymi z dostępem do sieci komputerowej.
3. **System informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
4. **Zasoby informatyczne** - ogół systemów informatycznych wykorzystywanych przez daną organizację
5. **Incydent związany z bezpieczeństwem informacji** - pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań statutowych organizacji i zagrażają bezpieczeństwu informacji
6. **Podatność** - słabość systemu informatycznego, która może być wykorzystana przez co najmniej jedno zagrożenie
7. **Zespól ds. Monitorowania Zagrożeń i Utrzymania Polityki Bezpieczeństwa Informacji** -

wyznaczeni przez Wójta Gminy Jaświły pracownicy Urzędu, którzy zajmują się zarządzaniem incydentami związanymi z bezpieczeństwem informacji w Urzędzie.

1. Cel procedury.

Celem Procedury Zarządzania Incydentami Związanymi z Bezpieczeństwem Informacji jest zapewnienie że zdarzenia związane z bezpieczeństwem informacji oraz słabości systemów informacyjnych, są zgłaszane w sposób umożliwiający szybkie podjęcie działań korygujących.

2. Zakres stosowania.

Działania opisane w niniejszej procedurze obowiązują, we wszystkich referatach i pozostałych komórkach organizacyjnych Urzędu oraz innych jednostkach korzystających z sieci komputerowej Urzędu. Niniejsza procedura jest elementem Polityki Bezpieczeństwa Informacji ustanowionej w Urzędzie.

3. Odpowiedzialność.

Odpowiedzialność za prawidłowe zgłoszenie incydentów dotyczących bezpieczeństwa infrastruktury informatycznej spoczywa na pracownikach Urzędu dokonujących zgłoszeń. Każdy pracownik odpowiedzialny za rozwiązanie problemu lub zapobieżenie incydentowi działa zgodnie z niniejszą procedurą.
Zespół ds. Monitorowania Zagrożeń i Utrzymania Polityki Bezpieczeństwa Informacji jest odpowiedzialny za:
1) Niezwłoczne reagowanie na incydenty bezpieczeństwa informacji w określony i z góry ustalony sposób;
2) Ocenę istniejących i potencjalnych zagrożeń w zakresie bezpieczeństwa informacji;

3) Ocenę przyczyn i skutków incydentów naruszenia bezpieczeństwa informacji w tym gromadzenie materiału dowodowego;
4) Przygotowywanie propozycji działań korygujących i naprawczych oraz nadzór nad ich wprowadzaniem;
5) Dokonywanie okresowego przeglądu i aktualizacji Polityki Bezpieczeństwa Informacji;
6) Prowadzenie działań zmierzających do wzrostu świadomości w zakresie zapewnienia bezpieczeństwa informacji w Urzędzie;

4. Klasyfikacja incydentów.

Podział zdarzeń:
1) Zdarzenia losowe zewnętrzne (np.: klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej, ciągłość pracy systemów zostaje zakłócona, nie dochodzi do naruszenia poufności danych.

2) Zdarzenia losowe wewnętrzne (np.: niezamierzone pomyłki operatorów, administratorów, awarie sprzętowe, błędy w oprogramowaniu), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych.

3) Zdarzenia zamierzone, świadome i celowe - stanowią najpoważniejsze zagrożenie naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zdarzenia te możemy podzielić na:
- nieuprawniony dostęp do danych z zewnątrz (włamanie do systemu), nieuprawniony dostęp do danych z sieci wewnętrznej,
- nieuprawniony transfer danych,
- pogorszenie funkcjonowania sprzętu i oprogramowania (np.: działanie wirusów),
- bezpośrednie zagrożenie materialnych składników systemu (np.: kradzież sprzętu).

Przykłady zdarzeń które mogą być zakwalifikowane jako uzasadnione podejrzenie naruszenia bezpieczeństwa informacji:
1) Sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na infrastrukturę teleinformatyczną jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.
2) Niewłaściwe parametry środowiska jak zbyt wysoka temperatura lub nadmierna wilgotność (w szczególności dotyczy to serwerowni).
3) Awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie systemu, a w tym sam fakt pozostawienia serwisantów bez nadzoru.
4) Pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu.
5) Jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikacje w systemie.

6) Nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie.
7) Stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji).
8) Nastąpiła niedopuszczalna manipulacja danymi w systemie.
9) Ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą elementy systemu zabezpieczeń.
10) Praca w systemie lub w sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych, np.: praca w systemie lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.
11) Ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. „bocznej furtki", itp.
12) Podmieniono lub zniszczono nośniki z danymi bez odpowiedniego upoważnienia lub w niedozwolony sposób skasowano lub kopiowano dane osobowe.
13) Rażąco naruszono dyscyplinę pracy w zakresie przestrzegania PBI (nie wylogowanie się, pozostawienie włączonego komputera po zakończeniu pracy, nie zamknięcie pokoju z komputerem, nie wykonywanie w ustalonych terminach kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.)
14) Stwierdzenie nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych, w tym także osobowych (otwarte szafy, regały, biurka).

5. Zgłaszanie incydentów

Pracownicy Urzędu mają obowiązek zgłaszać zauważone przez siebie incydenty oraz notować wszystkie szczegóły związane z incydentem.
Zgłaszający incydent nie powinien podejmować działań na własną rękę jednak w miarę możliwości powinien zabezpieczyć materiał dowodowy, np.: robiąc zdjęcie ekranu komputera co do którego zaistniało podejrzenie, że jego działanie odbiega od normy. W przypadku podejrzenia istnienia wirusa komputerowego należy postępować zgodnie z Instrukcją w zakresie profilaktyki antywirusowej, zał. nr 6 do PBI.
Informacji ocenia poziom istotności incydentu dla Urzędu kierując się następującymi kryteriami:

- wpływ incydentu na ciągłość działania Urzędu i wypełnianie jego zadań statutowych;
- krytyczność systemów dotkniętych skutkami incydentu bezpieczeństwa;
- wrażliwość informacji, których poufność, integralność czy dostępność naruszono (na przykład czy naruszono bezpieczeństwo informacji prawnie chronionej - np.: danych osobowych, informacji niejawnych);
- rozległość wpływu incydentu na działanie systemów (np. nie działa jeden komputer, cała sieć itp.);
- rozmiar szkód powstałych na skutek incydentu;
- koszt usunięcia i naprawy skutków incydentu bezpieczeństwa;
- szacowany czas przywrócenia ciągłości działania dotkniętego incydentem bezpieczeństwa systemu;
- zasoby wymagane do przywrócenia ciągłości działania systemu (personel, wsparcie firm zewnętrznych, wymagane dodatkowe czy zamienne urządzenia oraz oprogramowanie, czas odtwarzania systemów z kopii zapasowych itp.);

6. Postępowanie z incydentami

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

1) Informatyk, który przyjął zgłoszenie, powiadamia niezwłocznie kierownika referatu lub osobę go zastępującą o fakcie i treści zgłoszenia.

2) Po analizie zdarzenia i okoliczności z nim związanych informatyk zabezpiecza materiał dowodowy. Zawiadamia członków Zespołu ds. Monitorowania Zagrożeń i Utrzymania Polityki Bezpieczeństwa Informacji.

3) Zespół zbiera się niezwłocznie, dokonuje analizy materiału dowodowego i podejmuje decyzję o sposobie dalszego postępowania. Gromadzenie materiału dowodowego:

- dla dokumentów papierowych: oryginał jest bezpiecznie przechowywany wraz z informacją, kto znalazł dokument, gdzie, kiedy i kto by był świadkiem tego zdarzenia; każde śledztwo może wykazać, że oryginał nie został naruszony
- dla dokumentów na nośnikach komputerowych zaleca się: utworzenie obrazu lub kopii (zależnie od stosownych wymagań) wszelkich nośników wymiennych; zaleca się zapisanie informacji znajdujących się na dyskach twardych lub w pamięci komputera, aby zapewnić ich dostępność, zaleca się zachowanie zapisów wszelkich działań podczas procesu kopiowania oraz aby proces ten odbywał się w obecności świadków; zaleca się przechowywanie oryginalnego nośnika i dziennika zdarzeń w sposób bezpieczny i nienaruszony (jeśli to niemożliwe, to co najmniej jeden obraz lustrzany lub kopię).

4) W przypadku stwierdzenia działań umyślnych i ustaleniu sprawcy incydentu zespół przekazuje wyniki analizy wraz z zabezpieczonym materiałem dowodowym Wójtowi Gminy Jaświły w celu wyciągnięcia konsekwencji dyscyplinarnych wobec sprawcy lub podjęcia kroków prawnych wobec osób trzecich.

5) Zespół ds. Monitorowania Zagrożeń i Utrzymania Polityki Bezpieczeństwa Informacji wyciąga wnioski z każdego incydentu i określa jeśli to możliwe działania korygujące i zapobiegawcze w celu uniknięcia ponownego wystąpienia incydentu.

7. Szkolenia.

Brak wiedzy i umiejętności poprawnego rozpoznania i klasyfikacji oraz oceny poziomu istotności incydentu po stronie zgłaszającego nie może być przyczyną zaniechania powiadomienia jednostek odpowiedzialnych w przedsiębiorstwie o zaistniałym incydencie lub podejrzeniu wystąpienia takowego.

Dlatego należy przeprowadzać szkolenia pracowników Urzędu w zakresie zarządzania incydentami co najmniej raz do roku.

WÓJT

mgr inż. Jan [illegible]

Załącznik nr 5
Polityki Bezpieczeństwa Informacji

Instrukcja w zakresie profilaktyki antywirusowej

Metody i działania związane z profilaktyką antywirusową w systemach informatycznych użytkowanych w sieci komputerowej Urzędu.

Osobą prowadzącą działania profilaktyczne mające na celu ochronę zasobów sieci komputerowej Urzędu przed atakami wirusów komputerowych jest administrator systemu.

1. Administrator systemu wykorzystuje następujące funkcje systemowe:
a) rejestracja i śledzenie informacji o dostępach lub próbach dostępu do zasobów i usług danego systemu.
b) rejestracja i śledzenie komunikatów o błędach w pracy systemu.
c) szyfrowanie i uwierzytelnianie informacji przesyłanych w sieci.
d) wykrywanie obecności fałszywego oprogramowania w danych wpływających do systemu z sieci.
e) kontrola integralności oprogramowania zainstalowanego w systemie.
2. Ochrona antywirusowa zasobów informatycznych jest realizowana przez system antywirusowy posiadający następujące funkcje:
a) zabezpieczenie zasobów informatycznych przed wirusami komputerowymi za pomocą modułu rezydentnego, skanującego na bieżąco wszystkie zasoby komputera,
b) aktualizację baz sygnatur wirusów na bieżąco,
c) możliwość automatycznego podejmowania działań w przypadku pojawienia się nowych, nieznanych wirusów (np.: zablokowanie komunikacji z zawirusowanym komputerem).
3. Aktualizacja baz sygnatur wirusów
a) Bazy sygnatur wirusów dla serwera są aktualizowane bezpośrednio z serwera producenta systemu antywirusowego.
b) Bazy sygnatur wirusów dla stanowisk roboczych są aktualizowane bezpośrednio z serwera producenta systemu antywirusowego.
c) Aktualizacja baz sygnatur wirusów odbywa się nie rzadziej niż jeden raz każdego dnia roboczego.
4. Kontrola antywirusowa.
a) Zasoby informatyczne są skanowane na bieżąco za pomocą modułu rezydentnego. Kontroli podlegają wszystkie pliki (odczytywane i zapisywane) w tym poczta elektroniczna;
b) System antywirusowy jest zaprogramowany do wykonywania okresowych kontroli antywirusowych całego systemu plików. Kontrole te są wykonywane przez program automatycznie nie rzadziej niż jeden raz w tygodniu;
c) Zabrania się korzystania ze stanowiska bez aktywnego programu antywirusowego;

Zalecenia dla użytkowników stacji roboczych.

1. Zabrania się umieszczania w urządzeniach odczytujących dane na stanowisku (czytniki CD-ROM, DVD, porty USB itp.) nośników rozprowadzanych - z różnego rodzaju czasopismami, materiałami reklamowymi itp.
2. Zabrania się bez zgody kierownika referatu używania na stanowisku pracy urządzeń do gromadzenia i przenoszenia danych, takich jak pamięci „flash" dołączane przez porty USB, karty radiowe, urządzenia „bluetooth", dyski wymienne, modemy nie będących własnością Urzędu.
3. Zabrania się wykorzystywania do celów służbowych bez zgody kierownika referatu innych, niż dopuszczonych w Urzędzie, systemów poczty elektronicznej.
4. Z uwagi na próby ataków na systemy użytkowników poprzez zainfekowanie poczty elektronicznej zaleca się zachowanie szczególnej ostrożności przy otwieraniu otrzymanych tą drogą załączników. W przypadku otrzymania nieoczekiwanej przesyłki pocztowej, która zawiera załącznik lub odsyła do treści bezpośrednio do strony www zaleca się aby nie otwierać załącznika ani nie korzystać bezpośrednio z przesłanych odnośników.
5. Zaleca się wyłączenie opcji autopodglądu załącznika w programie pocztowym Outlook.
6. Korzystając z programów MS Office (Word, Excel itp.) i podobnych należy, jeśli to możliwe, uaktywnić ich wewnętrzny system ochrony przed wirusami.
7. Należy systematycznie przeprowadzać kontrolę antywirusową stanowiska programem dostarczonym przez informatyka Urzędu.
8. Każdy nośnik danych, używany do przenoszenia danych pomiędzy stanowiskami komputerowymi, przed odczytaniem danych należy sprawdzić programem antywirusowym.

Postępowanie w przypadku ujawnienia lub podejrzenia istnienia wirusa:

1. Gdy zachowanie systemu komputerowego odbiega od normy (komunikaty o błędach, nieoczekiwane zniknięcie lub pojawienie się plików lub katalogów, spowolniona praca systemu, dziwne lub niezrozumiałe informacje pojawiające się na ekranie itp.) należy również przeprowadzić kontrolę antywirusową systemu.
2. Jeśli program antywirusowy stwierdził istnienie wirusa na nośniku danych taki nośnik należy natychmiast wyjąć z czytnika (stacji dyskietek, czytnika DVD-ROM,USB itp.), wyraźnie oznaczyć i przekazać nośnik administratorowi systemu. Następnie należy sporządzić notatkę służbową ze zdarzenia i przeprowadzić kontrolę antywirusową całego systemu.
3. Po stwierdzeniu obecności wirusa w systemie przez program antywirusowy, jeśli to możliwe, należy zezwolić programowi antywirusowemu na usunięcie wirusów. Jeśli program antywirusowy nie będzie mógł usunąć wirusów nie niszcząc części lub całości zbioru zainfekowanego wirusem, należy przerwać działanie programu antywirusowego i natychmiast zgłosić ten fakt informatykowi.
4. Użytkownik ma obowiązek zgłaszania wszelkich zauważonych niestandardowych zachowań systemu antywirusowego.

WÓJT

mgr inż. Jan Joko

Załącznik nr 6
Polityki Bezpieczeństwa Informacji

INSTRUKCJA PRACY NA STANOWISKU WYPOSAŻONYM W MONITOR I DRUKARKĘ.

Szczegółowe zasady pracy na stanowisku określa „Instrukcja BHP na stanowisku pracy z komputerem i drukarką".

1. Użytkownikom nie wolno dopuszczać osób nieuprawnionych do pracy na ich stanowiskach. Zaleca się stosowanie wygaszaczy ekranu zabezpieczonych hasłem, które uruchamiają się po czasie nie dłuższym niż 5 minut.
2. Zabrania się użytkownikom samowolnego zmieniania parametrów konfiguracyjnych ich komputerów, a w szczególności tych dotyczących sieci komputerowej, gdyż może to zakłócić pracę całej sieci komputerowej Urzędu. Zmiany w/w parametrów mogą dokonywać wyłącznie uprawnieni informatycy po uzgodnieniu z administratorem systemu.
3. Zabrania się użytkownikom samodzielnego instalowania oprogramowania na ich komputerach, a w zwłaszcza oprogramowania nielegalnego i nie zaakceptowanego przez informatyka.
4. Zabrania się użytkownikom wykorzystywania sieci komputerowej Urzędu do rozpowszechniania:
a) spamu;
b) treści pornograficznych;
c) treści, które mogą uniemożliwić lub utrudnić korzystanie z komputera lub wywołać szkodę (np. wirusy, łańcuszki);
d) treści, które w jakikolwiek sposób łamią prawo Rzeczpospolitej Polskiej, wewnętrzne akty prawne, niniejsze zasady lub etykietę, a w szczególności prawo autorskie;
e) treści, które budzą odrazę bądź naruszają dobra osobiste lub materialne.

WÓJT
mgr inż. Jan Soko