Załącznik nr 1

do zarządzenia Wojewody Świętokrzyskiego nr 99 **/2016**

z dnia 21 lipca 2016r.

POLITYKA BEZPIECZEŃSTWA INFORMACJI

ŚWIĘTOKRZYSKIEGO URZĘDU WOJEWÓDZKIEGO W KIELCACH

WYDANIE - 1

Wersja – 1

Opracował:

INFORMATYK WOJEWÓDZKI

Marek Rak

(data i podpis)

Zatwierdził:

WOJEWODA ŚWIĘTOKRZYSKI

21.07.2016r. Agata Wojtyszek

(data i podpis)

DYREKTOR
Wydziału Organizacyjno-Kadrowego
mgr Paweł Lubieniecki

Wykaz zmian w Polityce Bezpieczeństwa Informacji

Nr wydania	Nr wersji	Dokument - Rozdział - strona	Data	Opis zmiany Data obowiązywania	Opracował
2	1	wszystkie	17.05.2016	Wydanie pierwsze 25.05.2016 r.	Marek Rak

Spis treści

1. Słownik pojęć.

1) dostępność informacji – właściwość polegającą na tym, że informacja jest możliwa do wykorzystania przez uprawniony podmiot na jego żądanie, w założonym czasie
2) integralność informacji – właściwość polegającą na tym, że informacja nie została zmodyfikowana w sposób nieuprawniony
3) Incydent – pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań statutowych organizacji i zagrażają bezpieczeństwu informacji (na podstawie PN-ISO/IEC 17799),
4) Poufność – właściwość polegająca na tym, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom (na podstawie PN-ISO/IEC 27001),
5) Rozliczalność – właściwość pozwalająca przypisać określone działanie do określonego podmiotu (osoby fizycznej , procesu, systemu) oraz umiejscowić je w czasie
6) Autentyczność – właściwość zapewniająca, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana (autentyczność dotyczy użytkowników, procesów, systemów i informacji)
7) Niezawodność – właściwość oznaczająca spójne, zamierzone zachowanie i skutki.
8) Niezaprzeczalność – właściwość oznaczająca niemożność wyparcia się swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie
9) 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
10) System teleinformatyczny – zespół współpracujących ze sobą według określonych reguł urządzeń, oprogramowania, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych
11) Administrator systemu – pracownik Świętokrzyskiego Urzędu Wojewódzkiego (ŚUW) w Kielcach, odpowiedzialny za realizację zadań związanych z zarządzaniem systemem informatycznym ŚUW, w tym za zabezpieczenie sieci komputerowej tzn. wdrażanie stosownych środków administracyjnych, technicznych i fizycznych w ŚUW w celu zabezpieczenia zasobów infrastruktury informatycznej oraz ochrony danych przed nieuprawnioną modyfikacją, zniszczeniem, dostępem i ujawnieniem, a także ich utratą.
12) Stanowisko – pojedynczy komputer osobisty lub terminal przeznaczony do określonych zadań związanych między innymi z dostępem do sieci komputerowej ŚUW.
13) 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.
14) Konto - to zbiór zasobów i uprawnień mający unikalny identyfikator w systemie informatycznym lub sieci komputerowej.
15) 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).

16) Zespół ds. monitorowania zagrożeń i utrzymania Systemu Zarządzania Bezpieczeństwem Informacji – wyznaczeni przez Dyrektora Generalnego pracownicy Urzędu, którzy zajmują się zarządzaniem incydentami związanymi z bezpieczeństwem informacji w Urzędzie zgodnie z Zarządzeniem Nr 6 Dyrektora Generalnego Urzędu z dnia 8 kwietnia 2016 r. w sprawie powołania Zespołu ds. monitorowania zagrożeń i utrzymania Systemu Zarządzania Bezpieczeństwem Informacji.
17) Zasoby informatyczne - ogół systemów informatycznych wykorzystywanych przez daną organizację
18) Kopia zapasowa – kopia danych lub oprogramowania. Celem jej wykonywania jest odtworzenie systemu po awarii.
19) Zasoby - to, co stanowi wartość, aktywa Urzędu;
20) akceptacja ryzyka – decyzja uprawnionej osoby o zaniechaniu działań mających na celu zmianę poziomu ryzyka
21) analiza ryzyka – systematyczne podejście mające na celu zidentyfikowanie w systemie źródeł ryzyka i przypisanie zidentyfikowanym ryzykom wartości
22) estymacja ryzyka – proces przypisywania wartości poziomowi ryzyka
23) identyfikowanie ryzyka – proces znajdowania, zestawiania i charakteryzowania przyczyn ryzyka w systemie
24) informowanie o ryzyku – wymiana lub dzielenie się informacjami o ryzyku między interesariuszami systemu
25) interesariusz – osoba lub organizacja, która może wpływać, na którą można wpływać lub która postrzega siebie jako zależną od podejmowanych decyzji lub działań
26) końcowy poziom ryzyka – poziom ryzyka pozostający po procesie postępowania z ryzykiem
27) materializacja zagrożenia – stan, w którym zagrożenie oddziałuje na system
28) ocena ryzyka – proces porównywania wartości ryzyka z określonymi kryteriami w celu określenia znaczenia ryzyka
29) podatność – słabość aktywu (zasobu) lub zabezpieczenia, która może być wykorzystana przez co najmniej jedno zagrożenie
30) postępowanie z ryzykiem – proces wyboru i wdrażania środków sterowania ryzykiem mających na celu zmianę wartości poziomu ryzyka
31) poziom ryzyka – produkt operacji na wartości przypisanej skutkowi i wartości związanej z prawdopodobieństwem zaistnienia zdarzenia powodującego skutek
32) poufność informacji – właściwość polegająca na tym, że informacja nie jest udostępniana ani ujawniana nieautoryzowanym osobom, podmiotom lub procesom
33) ryzyko – skutek niepewności w odniesieniu do ustalonego celu
34) ryzyko szczątkowe – ryzyko, którego poziom nie przekracza akceptowanej wartości

35) skutek – negatywna zmiana w odniesieniu do zaplanowanego poziomu miernika celu w wyniku oddziaływania zagrożenia
36) szacowanie ryzyka – całościowy proces analizy i oceny ryzyka
37) właściciel ryzyka – osoba odpowiedzialna za zarządzanie danym ryzykiem w systemie
38) zagrożenie – potencjalna przyczyna niepożądanego oddziaływania na system
39) zarządzanie ryzykiem – skoordynowane działania mające na celu kierowanie i sterowanie ryzykiem w systemie
40) zdarzenie – wystąpienie lub zmiana konkretnego zestawu okoliczności

2. Bezpieczeństwo informacji.

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 zachowana 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.

Pojęcie polityka rozumiane jest często jako zorganizowane działanie prowadzące do osiągnięcia celu. Celem polityki bezpieczeństwa informacji jest taki opis struktury oraz sposobu funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) funkcjonującego w Świętokrzyskim Urzędzie Wojewódzkim w Kielcach zwanym dalej Urzędem aby zapewnić właściwą ochronę zasobów informacyjnych w komórkach organizacyjnych Urzędu.

4. Deklaracja Kierownictwa Urzędu.

Niniejszy dokument wyraża 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.

5. Zakres obowiązywania polityki bezpieczeństwa informacji.

Dokument ten dotyczy wszystkich pracowników w rozumieniu w szczególności ustawy o służbie cywilnej oraz 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 2010 r., Nr 182, poz. 1228). Dokument dotyczy również wszystkich systemów informatycznych zlokalizowanych w budynkach Urzędu z wyjątkiem systemów służących do przetwarzania informacji niejawnych.

6. System Zarządzania Bezpieczeństwem Informacji w Świętokrzyskim Urzędzie Wojewódzkim w Kielcach.

Zgodnie z § 20 ust. 1 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 2016 r., poz. 113), Urząd opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali System Zarządzania Bezpieczeństwem Informacji zwany dalej SZBI zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

Głównymi celami stawianymi przed SZBI 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.

SZBI wprowadzony w Urzędzie opiera się o procesy w celu utrzymania odpowiedniego poziomu bezpieczeństwa.

Zakres SZBI obejmuje następujące procesy:

1) Nadzór nad dokumentacją SZBI.
2) Analiza i monitorowanie zagrożeń związanych z przetwarzaniem informacji.
3) Analiza ryzyka.
4) Inwentaryzacja sprzętu i oprogramowania informatycznego.
5) Zarządzanie uprawnieniami do pracy w systemach informatycznych.
6) Szkolenia pracowników zaangażowanych w proces przetwarzania informacji.
7) Nadzór nad pracą na odległość i mobilnym przetwarzaniem danych.
8) Serwis sprzętu informatycznego i oprogramowania.
9) Procedury zgłaszania i obsługi incydentów.
10) Audyt wewnętrzny z zakresu bezpieczeństwa informacji.
11) Zarządzanie kopiami zapasowymi.
12) Zabezpieczenia techniczno-organizacyjne dostępu do informacji.
13) Zabezpieczenia techniczno-organizacyjne systemów informatycznych.
14) Zapewnienie rozliczalności działań w systemach informatycznych.

Na funkcjonowanie SZBI mają wpływ potrzeby i cele działania, wymagania bezpieczeństwa, realizowane procesy oraz wielkość i struktura organizacji.

W Urzędzie za ustanowienie wdrożenie, eksploatowanie, monitorowanie, przeglądanie, utrzymywanie i doskonalenie SZBI odpowiada Wojewoda Świętokrzyski.

Zadaniem Dyrektora Generalnego Urzędu jest zapewnienie warunków niezbędnych do ustanowienia wdrożenia, eksploatowania, monitorowania, przeglądania, utrzymywania i doskonalenia SZBI.

Polityka Bezpieczeństwa Informacji jest podstawowym dokumentem SZBI.

7. Organizacja Bezpieczeństwa Informacji.

W Urzędzie za nadzór nad bezpieczeństwem informacji, a w szczególności za opracowanie, wdrożenie i utrzymanie SZBI, odpowiada Wojewoda.

Dyrektor Generalny Urzędu, dyrektorzy wydziałów/biur oraz kierownicy innych komórek organizacyjnych odpowiadają za przestrzeganie zapisów Polityki Bezpieczeństwa Informacji.

Dyrektor Generalny Urzędu, powołuje Zespół ds. Monitorowania Zagrożeń i Utrzymania Systemu Zarządzania Bezpieczeństwem Informacji, który zobowiązany jest do natychmiastowego podjęcia działań określonych w odpowiednich procedurach w przypadku naruszenia zasad bezpieczeństwa informacji.

Zespół ds. Monitorowania Zagrożeń i Utrzymania Systemu Zarządzania Bezpieczeństwem Informacji odpowiada za monitorowanie funkcjonowania mechanizmów bezpieczeństwa informacji, właściwe postępowanie z incydentami związanymi z bezpieczeństwem informacji i przypadkami naruszenia zasad bezpieczeństwa informacji, dokonywanie corocznych przeglądów PBI i SZBI i opracowywanie zmian w stosownych dokumentach, procedurach i infrastrukturze technicznej. Zespół powoływany jest zarządzeniem Dyrektora Generalnego Urzędu.

W Urzędzie działają **administratorzy systemów informatycznych**, którzy na wniosek dyrektorów wydziałów zarządzają danym zasobem informacji. Odpowiedzialni są 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 ŚUW, w tym za zabezpieczenie sieci komputerowej tzn. wdrażanie stosownych środków administracyjnych, technicznych i fizycznych w ŚUW 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.

8. 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:

Aktualne dokumenty PBI znajdują się na portalu pracownika w sekcji „Dokumenty Strategiczne", „Ochrona Informacji"

- 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.

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.

Audyt wewnętrzny w zakresie bezpieczeństwa informacji

Zgodnie z decyzją kierownictwa Urzędu audyt wewnętrzny w zakresie bezpieczeństwa informacji, o którym mowa w *§20 ust. 2 pkt 14 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*, prowadzony jest przez Zespół Audytu Wewnętrznego.

Zapis o prowadzeniu corocznych audytów w zakresie bezpieczeństwa zawarty został w §9 pkt 4 aktualnego Regulaminu wewnętrznego Wydziału Organizacji i Kadr, w którym usytuowana jest komórka audytu wewnętrznego.

Audyt bezpieczeństwa informacji powinien obejmować w szczególności badanie zgodności z wymogami *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.*

Audyt prowadzony jest Urzędzie w formie zadań zapewniających, z uwzględnieniem wymogów określonych w:

- *ustawie z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2013 r., poz. 885 ze zm.),*

- *rozporządzeniu Ministra Finansów z dnia 4 września 2015 r. w sprawie audytu wewnętrznego oraz informacji o pracy i wynikach tego audytu (Dz. U. z 2015 r., poz. 1480)*

- *Standardach audytu wewnętrznego dla jednostek sektora finansów publicznych (Komunikat Nr 2 Ministra Finansów z dnia 17 czerwca 2013 r. – Dz. Urz. Min. Fin., poz. 15).*

Ponadto cel, uprawnienia i odpowiedzialność odnoszące się do działania audytu wewnętrznego w Urzędzie zostały określone w Karcie Audytu Wewnętrznego w Świętokrzyskim Urzędzie Wojewódzkim w Kielcach, stanowiącej Załącznik do Zarządzenia Nr 31/2013 Wojewody Świętokrzyskiego z dnia 22 marca 2013 r.

Audyt w zakresie bezpieczeństwa informacji:

- ujmowany jest corocznie w planie audytu wewnętrznego, po przeprowadzeniu analizy ryzyka;
- prowadzony jest na podstawie przygotowanego programu zadania zapewniającego, w którym każdorazowo określany jest cel, zakres przedmiotowy, metodologia i techniki przeprowadzania zadania;
- dokumentowany jest jak zadanie zapewniające, a wyniki zadania prezentowane są w formie sprawozdania; prowadzony jest monitoring oraz czynności sprawdzające wdrożenie wydanych zaleceń.

Audyty są przeprowadzane w oparciu o szczegółowe zasady organizacji i metodologii wykonywania audytu wewnętrznego w Świętokrzyskim Urzędzie Wojewódzkim zawarte w *Podręczniku audytu wewnętrznego*.

W przypadku, gdy Zespół Audytu Wewnętrznego nie będzie posiadał uprawnień, specjalistycznej wiedzy i umiejętności do realizacji zakresu danego zadania audytowego, należy skorzystać przy jego realizacji z pomocy specjalistów z wewnątrz lub z zewnątrz Urzędu.

9. Struktura dokumentacji Polityki Bezpieczeństwa Informacji.

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

- Poziom organizacji,
- Poziom grupy informacji,
- Poziom systemu informatycznego,
- 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 Świętokrzyskim Urzędzie Wojewódzkim w Kielcach danych osobowych wraz z dokumentami związanymi – załącznik nr 8 .

Polityka bezpieczeństwa systemu informatycznego (opracowana dla konkretnego 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 w stosunku do potrzeb danej jednostki organizacyjnej. 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:

Procedura 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, kontroli dostępu do pomieszczeń serwerowni, w tym zdalnego dostępu spoza Urzędu oraz postępowania ze sprzętem przenośnym.

Procedura Tworzenia Kopii Zapasowych – załącznik nr 2.

Określa zasady tworzenia, przechowywania i testowania kopii zapasowych danych.

Procedura Zarządzania Ryzykiem w Systemie Zarządzania Bezpieczeństwem Informacji – załącznik nr 3.

Określa metodykę i zasady zarządzania ryzykiem w Systemie Zarządzania Bezpieczeństwem Informacji w Urzędzie w zakresie zagrożeń pochodzących z cyberprzestrzeni.

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 SZBI w Urzędzie to:

- Schemat postępowania z incydentami związanymi z bezpieczeństwem informacji
- Rejestr incydentów związanych z bezpieczeństwem informacji
- Rejestr przeglądów PBI

10. 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 Oddział ds. Informatyki.

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 oraz klauzulę o możliwości przeprowadzenia audytu bezpieczeństwa informacji w jednostce zewnętrznej . Dostęp do zasobów informatycznych i pomieszczeń Urzędu uzyskują po wcześniejszym otrzymaniu stosownego upoważnienia i zapoznaniu się z Polityką Bezpieczeństwa Informacji. Dostęp do zasobów

jest ograniczony do okresu zdefiniowanego w umowie. 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.

11. 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, tokenem lub innego podobnego mechanizmu). Po zakończonym dniu pracy komputer powinien zostać wyłączony;

12. 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. W doborze celów stosowania zabezpieczeń i zabezpieczeń należy kierować się zaleceniami Polskiej Normy PN-ISO/IEC 17799.

13. Sankcje za naruszenie zasad bezpieczeństwa informacji.

Nieprzestrzeganie zasad zawartych w dokumentach Polityki Bezpieczeństwa Informacji Urzędu, jest naruszeniem obowiązków pracowniczych wynikających w szczególności z ustaw o służbie cywilnej, o pracownikach urzędów państwowych oraz 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.

14. 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.

Komórka odpowiedzialna za sprawy kadrowe udostępnia, 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 i złożyć pisemne oświadczenie potwierdzające znajomość zasad, reguł i postanowień zawartych w w/w dokumentach.

Dokumentacja PBI powinna być przeglądana i weryfikowana:

- Na polecenie Wojewody/Dyrektora Generalnego
- W przypadku wystąpienia poważnych incydentów związanych z bezpieczeństwem informacji
- W celu realizacji zaleceń wynikających z przeprowadzonych audytów i kontroli
- W przypadku wejścia w życie nowych przepisów dotyczących bezpieczeństwa informacji
- W przypadku poważnych modyfikacji infrastruktury teleinformatycznej
- W przypadku zawarcia umów, z których wynikają zobowiązania związane z bezpieczeństwem informacji
- Okresowo, nie rzadziej niż raz w roku

Zmiany w dokumentach wprowadza Zespół ds. Monitorowania Zagrożeń i Utrzymania Systemu Zarządzania Bezpieczeństwem Informacji na podstawie okresowych przeglądów. Zmieniony dokument zatwierdza Wojewoda Świętokrzyski i wprowadza w drodze zarządzenia.

15. Przepisy prawne i polskie normy.

W Urzędzie informacje podlegają ochronie zgodnie z następującymi wymogami prawa:

1. Ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (j.t. Dz. U. z 2016 r. poz. 922),
2. Ustawą o ochronie informacji niejawnych z dnia 5 sierpnia 2010 r. (Dz. U. z 2010 r., Nr 182, poz. 1228),
3. Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (j.t. Dz. U. z 2015 r., poz.2058 ze zm.),
4. Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym (j.t. Dz. U. z 2013 r., poz. 262),
5. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (j.t. Dz. U. z 2014 r., poz. 1114)
6. Ustawa z dnia 21 listopada 2008r o służbie cywilnej (Dz. U. z 2014 r. poz. 1111 z późn. zm.),
7. Ustawa z dnia 16 września 1982 r. o pracownikach urzędów państwowych (j.t. Dz. U. z 2013 r., poz. 269),
8. Ustawa z dnia 26 czerwca 1974 r. - Kodeks pracy (j.t. Dz. U. z 2014 r. poz. 1502 z późn. zm.),
9. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r., Nr 100, poz. 1024).
10. Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. z 2011 r., Nr 159, poz. 948)
11. Rozporządzenie 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 2016 r., poz. 113)

12. Rozporządzenie Ministra Pracy i Polityki Społecznej z dnia 1 grudnia 1998 r. w sprawie bezpieczeństwa i higieny pracy na stanowiskach wyposażonych w monitory ekranowe (Dz. U. z 1998 r., Nr 148, poz. 973, z późn. zm.).

Podstawą normalizacyjną dokumentu Polityki Bezpieczeństwa Informacji są niżej wymienione polskie normy:

1. PN ISO/IEC 27001:2007 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania.
2. PN ISO/IEC 27005 Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji.
3. PN-ISO/IEC 17799:2007 Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zarządzania bezpieczeństwem informacji.