Zarządzenie Nr 443
Wojewody Dolnośląskiego
z dnia 31 grudnia 2013 r.

w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji w Dolnośląskim Urzędzie Wojewódzkim we Wrocławiu

Na podstawie art. 17 ustawy z dnia 23 stycznia 2009 r. o wojewodzie i administracji rządowej w województwie (Dz. U. Nr 31, poz. 206, z późn. zm.) [1] oraz art. 36 ust. 1 i 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.) [2], zarządza się co następuje:

§ 1. Wprowadzam w Dolnośląskim Urzędzie Wojewódzkim we Wrocławiu Politykę Bezpieczeństwa Informacji, stanowiącą załącznik do niniejszego zarządzenia.

§ 2. Zarządzenie wchodzi w życie z dniem podpisania.

WOJEWODA DOLNOŚLĄSKI
Aleksander Marek Skorupa

[1] Zmiany do wymienionej ustawy zostały ogłoszone w Dz. U. z 2010 r. Nr 40, poz. 230, Dz. U. z 2011 r. Nr 22, poz. 114, Nr 92, poz. 529, Nr 163, poz. 981, Nr 185, poz. 1092.

[2] Zmiany do wymienionej ustawy zostały ogłoszone w Dz. U. z 2002 r. Nr 153, poz. 1271, Dz. U. z 2004 r. Nr 25, poz. 219, Nr 33, poz. 285, Dz. U. z 2006 r. Nr 104, poz. 708 i 711, Dz. U. z 2007 r. Nr 165, poz. 1170, Nr 176, poz. 1238, Dz. U. z 2010 r. Nr 41, poz. 233, Nr 182, poz. 1228, Nr 229, poz. 1497, Dz. U. z 2011 r. Nr 230, poz. 1371.

Załącznik
do zarządzenia nr 443
Wojewody Dolnośląskiego
z dnia 31 grudnia 2013

DOLNOŚLĄSKI URZĄD WOJEWÓDZKI
WE WROCŁAWIU

WOJEWODA DOLNOŚLĄSKI
A. M. V
.....
Aleksander Marek Skorupa
(WOJEWODA DOLNOŚLĄSKI)

.....
(DATA)

Polityka Bezpieczeństwa Informacji

WROCŁAW **GRUDZIEŃ** **2013**

Rozdział I – Deklaracja Najwyższego Kierownictwa 3
Rozdział II – Cel Polityki Bezpieczeństwa Informacji 3
Rozdział III – Słownik terminów 4
Rozdział IV – Postanowienia ogólne 6
Rozdział V - Globalne Środowisko Bezpieczeństwa 7
Rozdział VI – Podmioty odpowiedzialne za Politykę Bezpieczeństwa Informacji 7
Rozdział VII – Użytkownicy systemu 8
Rozdział VIII – Odpowiedzialność za Politykę Bezpieczeństwa Informacji 8
Rozdział IX – Wymagania bezpieczeństwa 9
Rozdział X - Tryb bezpieczeństwa 10
Rozdział XI - Podstawowe zasady bezpieczeństwa informacji ..... 10.
Rozdział XII - Reakcja na incydenty związane z bezpieczeńsrwem informacji 15
Rozdział XIII - Przeglądy Polityki Bezpieczeństwa Informacji, audyty systemu i analizy ryzyka 15
Rozdział XIV – Odnośniki/ współzależności z inną dokumentacją związaną z bezpieczeństwem 16
Rozdział XV – Zasady dokonywania zmian w Polityce Bezpieczeństwa Informacji 18
Rozdział XVI – Zasady rozpowszechniania Polityki Bezpieczeństwa Informacji 18
Rozdział XVII – Podstawa prawna 19

Rozdział I – Deklaracja Najwyższego Kierownictwa

Mając świadomość znaczenia informacji i systemów informacyjnych dla realizacji misji i celów Dolnośląskiego Urzędu Wojewódzkiego we Wrocławiu zapewniamy, że podejmowane przez Urząd działania dążą do zapewnienia bezpieczeństwa Zasobów informacyjnych i są zgodne z wymogami obowiązującego prawa jako podstawy do realizacji zadań zapewnienia bezpieczeństwa w Urzędzie.

W celu udokumentowania realizacji Systemu Zarządzania Bezpieczeństwem Informacji przyjmuję Politykę Bezpieczeństwa Systemu Informacyjnego.

Zasady, działania, kompetencje i zakresy odpowiedzialności opisane w dokumentach Polityki Bezpieczeństwa Systemu Informacyjnego obowiązują wszystkich pracowników Urzędu.

Funkcjonujący System Zarządzania Bezpieczeństwem Informacji jest w pełni zgodny z wymaganiami obowiązującego prawa i będzie nieustannie nadzorowany i doskonalony.

Rozdział II – Cel Polityki Bezpieczeństwa Informacji

Celem niniejszej Polityki jest określenie podstawowych zasad bezpiecznego przetwarzania informacji Dolnośląskiego Urzędu Wojewódzkiego we Wrocławiu. Wszelkie dokumenty określające zasady przetwarzania informacji winny być zgodne z niniejszą polityką.

Polityka Bezpieczeństwa Informacji odnosi się zarówno do pracowników Dolnośląskiego Urzędu Wojewódzkiego we Wrocławiu, jak i podmiotów zewnętrznych współpracujących z Urzędem i uzyskujących dostęp do jego Zasobów w celu świadczenia usług na rzecz Urzędu na podstawie umów, porozumień lub innych stosunków prawnych.

Rozdział III – Słownik terminów

Niniejszy dokument zawiera podstawowe definicje pojęć dotyczących polityki bezpieczeństwa informacji:

1. bezpieczeństwo informacji - zachowanie poufności, integralności i dostępności informacji; dodatkowo, mogą być brane pod uwagę inne właściwości informacji, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność (ISO/IEC 2007:2005);
2. autentyczność - właściwość zapewniająca, że tożsamość podmiotu lub Zasobu jest taka, jak deklarowana. Autentyczność dotyczy takich podmiotów jak użytkownicy, procesy, systemy i informacja;
3. dostępność - właściwość bycia dostępnym i możliwym do wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot. (ISO 7498-2: 1989);
4. niezaprzeczalność – możliwość przeprowadzenia dowodu, że działanie lub zdarzenie miało miejsce, w taki sposób, że nie można temu działaniu lub zdarzeniu później zaprzeczyć (PN-ISO/IEC 13888-1);
5. niezawodność - właściwość oznaczająca spójne, zamierzone zachowanie i skutki (PN-ISO-13335-1:1999);
6. podatność – słabość aktywu lub grupy aktywów, która może być wykorzystana przez jedno lub więcej zagrożeń (PN ISO/IEC 17799:2007);
7. poufność - właściwość zapewniająca, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom (ISO 7498-2:1989);
8. rozliczalność - właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi (ISO 7498-2:1989);
9. integralność danych - właściwość zapewniająca, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany (ISO 7498-2:1989);
10. integralność systemu - właściwość polegająca na tym, że system realizuje swoją zamierzoną funkcję w nienaruszony sposób, wolny od nieautoryzowanej manipulacji, celowej lub przypadkowej;

11. ryzyko związane z bezpieczeństwem informacji – potencjalna sytuacja, w której dane zagrożenie wykorzysta podatności aktywów lub grupy aktywów, co spowoduje szkodę dla organizacji. Ryzyko jest funkcją prawdopodobieństwa zdarzenia i jego konsekwencji (PN ISO/IEC 27005:2010);
12. zagrożenie – potencjalna przyczyna incydentu, który może spowodować stratę w systemie lub dla organizacji (PN ISO/IEC 17799:2007);
13. incydent związany z bezpieczeństwem informacji - pojedyncze lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań i zagrażają bezpieczeństwu informacji (ISO/IEC TR 18044:2004);
14. zdarzenie związane z bezpieczeństwem informacji - określony stan systemu, usługi lub sieci, który wskazuje na możliwe przełamanie bezpieczeństwa informacji, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem (ISO/IEC TR 18044:2004);
15. System Zarządzania Bezpieczeństwem Informacji (SZBI) - to część całościowego systemu zarządzania, oparta na podejściu wynikającym z ryzyka biznesowego, odnosząca się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji;
16. zarządzanie ryzykiem – skoordynowane działania kierowania i kontrolowania organizacji z uwzględnieniem ryzyka (ISO/IEC Guide 73:2002);
17. system informacyjny – system, w którym w trakcie zachodzących w nim procesów gromadzi się, przetwarza, przechowuje i udostępnia informacje, niezależnie od formy realizacji tych procesów;
18. system teleinformatyczny – zespół współpracujących ze sobą według określonych reguł urządzeń i oprogramowania;
19. Zasób (Aktywa) – wszystko, co ma wartość dla Urzędu i składa się na systemy informacyjne, a w szczególności personel, budynki, sprzęt, oprogramowanie, informacja, prawa niematerialne, wizerunek;
20. Właściciel Zasobu (WZ) – kierownik komórki organizacyjnej Urzędu, nadzorującej eksploatację, rozwój, utrzymanie, korzystanie, bezpieczeństwo i dostęp do Zasobu;

21. Kierownictwo – Wojewoda, Dyrektor Generalny, Kierownicy komórek organizacyjnych Urzędu ;
22. Administrator Bezpieczeństwa Informacji (ABI) – osoba nadzorująca przestrzeganie stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych;
23. Zespół ds. Monitorowania Zagrożeń i Utrzymania Polityki Bezpieczeństwa – zespół powołany Zarządzeniem Nr 387a Wojewody Dolnośląskiego z dnia 6 listopada 2013 roku.
24. Urząd – Dolnośląski Urząd Wojewódzki we Wrocławiu.

Rozdział IV – Postanowienia ogólne

Polityka Bezpieczeństwa Informacji jest zgodna z prawem Rzeczpospolitej Polskiej oraz prawem Unii Europejskiej i opiera się na Polskich Normach.

Każdy pracownik Urzędu przyjmuje na siebie obowiązek ochrony Zasobów Urzędu w zakresie uzyskanych uprawnień. Obowiązek ochrony Zasobów nie kończy się z chwilą ustania stosunku pracy lub innego stosunku prawnego stanowiącego podstawę wykonywania pracy na rzecz Urzędu w takim zakresie, jaki ustanawiają przepisy prawa. Obowiązek ochrony Zasobów w przypadku współpracy z podmiotami zewnętrznymi określany jest w ramach zawartych z nimi umów.

Niniejszą Polityką Bezpieczeństwa nie jest objęta ochrona informacji niejawnych w rozumieniu ustawy o ochronie informacji niejawnych, których ochrona odbywa się na odrębnych zasadach.

Rozdział V – Globalne Środowisko Bezpieczeństwa

Przetwarzanie informacji odbywa się we wszystkich lokalizacjach Urzędu to jest:

- we Wrocławiu pl. Powstańców Warszawy 1,
- w Legnicy ul. F. Skarbka 3,
- w Wałbrzychu ul. Słowackiego 23a,
- w Jeleniej Górze ul. Wiejska 29.

Rozdział VI – Podmioty odpowiedzialne za Politykę Bezpieczeństwa Informacji

- Wojewoda Dolnośląski,
- Dyrektor Biura Informatyki i Obsługi Urzędu,
- Przewodniczący Zespołu ds. Monitorowania Zagrożeń i Utrzymania Polityki Bezpieczeństwa,
- Administrator Bezpieczeństwa Informacji,
- użytkownicy systemu.

Rozdział VII – Użytkownicy systemu

Każdy użytkownik systemu teleinformatycznego dysponuje indywidualnym kontem i hasłem, za pośrednictwem którego może korzystać z udostępnianych Zasobów i usług. Mechanizmy uwierzytelniania, rejestrowania zdarzeń i monitorowania zdarzeń gwarantują rozliczalność użytkowników zarejestrowanych w tym systemie. Przydzielanie dostępu oraz nadawanie uprawnień do systemów teleinformatycznych reguluje „Procedura nadawania, zmiany i cofania uprawnień" oraz „Polityka Bezpieczeństwa Ochrony Danych Osobowych i Instrukcja Zarządzania Systemem Informatycznym". Kierownik komórki organizacyjnej jest odpowiedzialny za aktualny stan ilościowy i status kont podległych pracowników oraz przyznany im poziom uprawnień.

Rozdział VIII – Odpowiedzialność za Politykę Bezpieczeństwa Informacji

1. Wojewoda Dolnośląski powołuje Zespół ds. Monitorowania Zagrożeń i Utrzymania Polityki Bezpieczeństwa. Do zadań zespołu należy:
    - przeprowadzenie audytu sprzętu teleinformatycznego i oprogramowania,
    - opracowanie Polityki Bezpieczeństwa Dolnośląskiego Urzędu Wojewódzkiego we Wrocławiu,
    - opracowywanie rocznego harmonogramu audytów wewnętrznych z zakresu bezpieczeństwa,
    - przeprowadzanie audytów wewnętrznych z zakresu bezpieczeństwa.

2. Administrator Bezpieczeństwa Informacji:
    - pełni rolę Administratora Bezpieczeństwa Informacji w rozumieniu art. 36 ust. 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych;
    - zapewnia, że zadania z zakresu bezpieczeństwa są realizowane zgodnie z Polityką Bezpieczeństwa Informacji;
    - określa postępowanie w przypadku niezgodności z obowiązującymi aktami normatywnymi oraz dokumentacją techniczną;

- przedkłada do zatwierdzenia metodykę i procesy związane z bezpieczeństwem informacji, w tym dotyczącą klasyfikacji informacji, szacowania ryzyka, systemu mierników poziomu zabezpieczeń;
- rozpoznaje znaczące zmiany zagrożeń i stopień narażenia informacji lub środków do przetwarzania informacji na zagrożenia;
- szacuje adekwatność i koordynuje wdrożenie oraz okresowe testowanie zabezpieczeń;
- skutecznie promuje w organizacji kształcenie, szkolenia i uświadamianie w zakresie bezpieczeństwa informacji;
- ocenia informacje uzyskane z monitorowania i przeglądu incydentów związanych z bezpieczeństwem informacji oraz zaleca odpowiednie działania w stosunku do zidentyfikowanych incydentów związanych z bezpieczeństwem informacji.

3. Przełożeni wszystkich szczebli, odpowiadają za nadzór nad realizacją zadań wynikających z Polityki Bezpieczeństwa Informacji, w stosunku do podległych pracowników.

Rozdział IX – Wymagania bezpieczeństwa

Organizacja Urzędu oraz systemy informacyjne służące do przetwarzania danych, muszą spełniać następujące wymagania bezpieczeństwa:

- integralności, autentyczności i dostępności danych, na podstawie których jest prowadzona działalność statutowa Urzędu,
- niezawodności, dostępności i integralności istotnych systemów informacyjnych Urzędu,
- integralności i poufności informacji dotyczących Klientów Urzędu,
- rozliczalności działań i zdarzeń zachodzących w systemach informacyjnych Urzędu,

- poufności i ochrony dostępu do informacji wrażliwych, w szczególności wynikających z odnośnych przepisów prawa.

Dobór odpowiednich środków ochrony uzależniony jest od wyniku analizy ryzyka. Każde ryzyko inne niż szczątkowe wymaga zastosowania dodatkowych zabezpieczeń bezpieczeństwa fizycznego, osobowego, obiegu dokumentów redukujących poziom ryzyka do oczekiwanego poziomu.

Rozdział X – Tryb bezpieczeństwa

W Urzędzie zastosowany został tryb bezpieczeństwa wielopoziomowy.

Rozdział XI – Podstawowe zasady bezpieczeństwa informacji

1. W celu zapewnienia bezpieczeństwa informacji stosuje się następujące ogólne zasady:
    - „przywilejów koniecznych" – każdy użytkownik systemów informacyjnych Urzędu ma prawa dostępu do Zasobów ograniczone wyłącznie do tych, które są niezbędne do wykonywania powierzonych mu obowiązków;
    - rozliczalności – Urząd dąży do zapewnienia jednoznacznej odpowiedzialności pracowników za Zasoby im powierzone; wszyscy użytkownicy Zasobów muszą być świadomi swej odpowiedzialności i konsekwencji, które poniosą, jeżeli zaniedbają swoje obowiązki; przekazywanie własnych praw dostępu do Zasobów innym osobom jest zabronione; odstępstwo od zasady rozliczalności musi być uzasadnione, odnotowane oraz zatwierdzone przez osoby odpowiedzialne za bezpieczeństwo;

- „separacji obowiązków", polegającej na tym, że zadania krytyczne z punktu widzenia bezpieczeństwa systemu nie mogą być realizowane przez jedną osobę.
- „domniemanej odmowy", to jest przyjęcia jako standardowych najbardziej restrykcyjnych ustawień, które można zwolnić jedynie w określonych sytuacjach („to, co nie jest dozwolone, jest zabronione").

2. Ochrona Urzędu – budynek zabezpieczany jest przez służbę ochrony budynku, która ma za zadanie utrzymanie bezpieczeństwa i porządku na terenie obiektu oraz jego otoczenia za pomocą całodobowego monitoringu, systemów alarmowych oraz cyklicznych patroli. Wejście na teren budynku i do pomieszczeń biurowych po godzinach urzędowania wymaga zezwolenia kierownika Urzędu, natomiast osoby postronne są legitymowane w celu ustalenia zasadności pobytu na terenie budynku. Zasady kontroli wejść do budynku oraz procedury związane z bezpieczeństwem osób przebywających na terenie obiektu oraz jego ochroną zostały zawarte w załącznikach „Instrukcji Ochrony Obiektu" (zarządzenie Nr 9 Dyrektora Generalnego Dolnośląskiego Urzędu Wojewódzkiego we Wrocławiu z dnia 2 marca 2012 r.)
3. System ochrony ppoż. w budynku Urzędu – postępowanie pracowników w przypadku wystąpienia zagrożeń pożarowych oraz przeciwdziałania tym zagrożeniom (sposoby postępowania na wypadek pożaru lub miejscowego zagrożenia oraz zasad ewakuacji) w budynku zostało opisane w załącznikach do „Instrukcji Ochrony Obiektu" (zarządzenie Nr 9 Dyrektora Generalnego Dolnośląskiego Urzędu Wojewódzkiego we Wrocławiu z dnia 2 marca 2012 r.)
4. Bezpieczeństwo fizyczne infrastruktury systemów teleinformatycznych jest zapewnione poprzez umiejscowienie jej w obszarze szczególnie chronionym, którym jest serwerownia. Dostęp do serwerowni reguluje „Instrukcja postępowania dla pracowników Oddziału Sieci i Systemów Informatycznych, dotycząca wejścia do serwerowni" oraz „Instrukcja postępowania na wypadek wystąpienia problemów z klimatyzatorami w serwerowni Urzędu i możliwości przegrzania się urządzeń".
5. Systemy teleinformatyczne Urzędu są zabezpieczone przed nieupoważnionym dostępem, modyfikacją lub zniszczeniem. Infrastruktura systemów teleinformatycznych jest zabezpieczona przed nieupoważnionym dostępem z zewnątrz poprzez system zabezpieczeń sprzętowych i programowych typu Firewall.

6. W celu wykonywania czynności służbowych, pracownik korzysta z powierzonego mu sprzętu komputerowego. Wyniesienie sprzętu poza obszar użytkowania wymaga zgody przełożonego oraz spełnienia zasad określonych w „Instrukcji Gospodarowania składnikami majątku w Dolnośląskim Urzędzie Wojewódzkim we Wrocławiu" (zarządzenie Nr 59a Dyrektora Generalnego Dolnośląskiego Urzędu Wojewódzkiego we Wrocławiu z dnia 1 października 2013 r.)
7. Dostęp do komputera, jest zabezpieczony za pomocą procesu uwierzytelnienia z wykorzystaniem unikalnego identyfikatora użytkownika oraz hasła. Pracownik jest odpowiedzialny za wszystkie czynności wykonane przy pomocy identyfikatora, którym się posługuje lub posługiwał. Pracownik jest zobowiązany do zachowania poufności hasła oraz do nieudostępniania go osobom trzecim. W przypadku podejrzenia lub stwierdzenia ujawnienia hasła, należy je niezwłocznie zmienić.
8. Administratorzy sieci komputerowej i serwerów, wykonują swoje zadania korzystając z kont o wysokich uprawnieniach. Zasady dotyczące tych kont reguluje „Instrukcja postępowania dla pracowników Oddziału Sieci i Systemów Informatycznych, dotycząca tworzenia i przechowywania haseł do kont o wysokich uprawnieniach".
9. Urządzenia wielofunkcyjne - drukujące i powielające - są instalowane na serwerze wydruków oraz konfigurowane przez pracownika Biura Informatyki i Obsługi Urzędu. W celu uniemożliwienia wydruku, skanu bądź kopii przez osoby nieuprawnione dostęp do urządzeń wielofunkcyjnych odbywa się poprzez autoryzację użytkownika za pomocą kodu pin lub karty zbliżeniowej oraz dodanie konta użytkownika i nadanie mu kodu pin na urządzeniu (realizuje pracownik Biura Informatyki i Obsługi Urzędu) po zgłoszeniu w systemie HELPDESK. Istnieje możliwość raportowania i kontrolowania liczby wydruków, skanów i wykonanych kopii w odniesieniu do danego użytkownika.
10. Pracownicy Urzędu, w czasie wykonywania czynności służbowych mogą korzystać z Intranetu, Internetu oraz poczty elektronicznej, na zasadach określonych w „Regulaminie pracy Urzędu".
11. Na wypadek katastrofy lub rozległej awarii technicznej są opracowywane, oraz okresowo testowane plany ciągłości działania dla systemów istotnych z punktu widzenia działalności statutowej Urzędu.

12. Pracownicy, wykonujący czynności służbowe na komputerach przenośnych są zobowiązani do zachowania szczególnej ostrożności. Komputery przenośnie powinny być przechowywane z zamykanych na klucz szafach lub sejfach. Zasady użycia komputerów przenośnych do przetwarzania danych osobowych są określone w „Polityce Bezpieczeństwa Ochrony Danych Osobowych i Instrukcji Zarządzania Systemem Informatycznym".

13. W sieci komputerowej Urzędu, istnieje techniczna możliwość zdalnego dostępu do wybranych Zasobów, poprzez bezpieczne połączenie typu VPN. Użytkownicy, korzystający z Zasobów sieci Urzędu poprzez zdalny dostęp, są zobowiązani do zachowania szczególnej ostrożności. Uprawnienia w zakresie zdalnego dostępu są nadawane zgodnie z „Procedurą nadawania uprawnień zdalnego dostępu do sieci Urzędu".

14. Zakupy sprzętu komputerowego i oprogramowania są realizowane zgodnie z zapotrzebowaniem komórek organizacyjnych Urzędu stosownie do możliwości finansowych Urzędu.

    Pracownicy Biura Informatyki i Obsługi Urzędu dokonują odbioru nowo zakupionego sprzętu komputerowego i oprogramowania pod względem ilościowo-jakościowym i na zgodność z fakturą lub SIWZ. Przed przekazaniem do użytkownika sprzęt i oprogramowanie są wprowadzane do ewidencji i oznakowywane. Instalacja sprzętu/oprogramowania odbywa się przez uprawnionych pracowników Biura Informatyki i Obsługi Urzędu w porozumieniu z użytkownikami, dla których jest przeznaczony.

    Naprawy i konserwacje są wykonywane wyłącznie przez upoważnionych pracowników Biura Informatyki i Obsługi Urzędu lub zewnętrznych dostawców usług serwisowych. Podstawą do wykonywania w/w czynności są zgłoszenia HELPDESK – dotyczące problemów technicznych oraz konieczności wykonania konserwacji sprzętu.

15. Wymiana lub modernizacja sprzętu komputerowego odbywa się w miarę potrzeb oraz z uwzględnieniem możliwości finansowych Urzędu. Podstawą do ewentualnej wymiany/ modernizacji sprzętu są: zgłoszenia HELPDESK pracowników Urzędu, pisma z Wydziałów/Biur Urzędu wskazujące potrzeby w zakresie wymiany/modernizacji sprzętu komputerowego, ocena sprawności i przydatności sprzętu, zgłoszenie zapotrzebowania na zakupy nowego sprzętu komputerowego do rocznych Planów Zamówień Publicznych i zakupy z uwzględnieniem dostępnych środków finansowych Urzędu. Zasady wycofywania z użycia sprzętu komputerowego reguluje „Instrukcja gospodarowania zbędnymi lub zużytymi składnikami majątku" oraz „Procedura wycofywania sprzętu i niszczenia nośników informacji".
16. Pracownicy Urzędu mają możliwość przechowywania plików, związanych z wykonywaniem czynności służbowych, nie tylko na dysku komputera lokalnego, ale także na przydzielonych im osobistych Zasobach sieciowych. Ponadto, w celu usprawnienia wspólnej pracy z tymi samymi dokumentami, pracownicy Urzędu mogą korzystać z Zasobów sieciowych współdzielonych z innymi pracownikami oddziału. Zasady korzystania z Zasobów sieciowych Urzędu reguluje „Instrukcja korzystania z Zasobów sieciowych Urzędu".
17. W celu zapewnienia ciągłości działania, w Urzędzie funkcjonuje centralny system tworzenia kopii bezpieczeństwa, w skład którego wchodzi dedykowany serwer backupowy wraz z programem archiwizującym oraz urządzenie archiwizujące-biblioteka taśmowa. Zasady tworzenia kopii bezpieczeństwa reguluje „Procedura tworzenia kopii bezpieczeństwa i ich przechowywania".
18. Okresowo są przeprowadzane szkolenia dla pracowników Urzędu, dotyczące bezpieczeństwa informacji oraz ochrony innych Zasobów Urzędu.

Rozdział XII – Reakcja na incydenty związane z bezpieczeństwem informacji.

Każdy pracownik Urzędu lub podmiotu zewnętrznego, ma obowiązek natychmiastowego informowania o wystąpieniu incydentu związanego z bezpieczeństwem informacji lub bezpieczeństwem Zasobów, bezpośredniego przełożonego oraz Przewodniczącego Zespołu ds. Monitorowania Zagrożeń i Utrzymania Polityki Bezpieczeństwa, a w przypadku incydentu związanego z bezpieczeństwem danych osobowych także Administratora Bezpieczeństwa Informacji w sposób określony w szczegółowych instrukcjach.

Zespół ds. Monitorowania Zagrożeń i Utrzymania Polityki Bezpieczeństwa lub Administrator Bezpieczeństwa Informacji podejmuje natychmiastowe działania mające na celu minimalizację ryzyka wystąpienia negatywnych efektów wystąpienia incydentu.

W przypadku wystąpienia incydentu związanego z bezpieczeństwem informacji, Zespół ds. Monitorowania Zagrożeń i Utrzymania Polityki Bezpieczeństwa może przeprowadzić analizę zdarzenia związanego z bezpieczeństwem informacji oraz podjąć działania zaradcze w celu zmniejszenia potencjalnych strat oraz zredukowania ryzyka ponownego wystąpienia podobnego incydentu.

Rozdział XIII – Przeglądy Polityki Bezpieczeństwa Informacji, audyty systemu i analizy ryzyka.

Polityka Bezpieczeństwa powinna być poddawana przeglądowi przynajmniej raz na rok. W razie istotnych zmian dotyczących przetwarzania danych osobowych Przewodniczący Zespołu ds. Monitorowania Zagrożeń i Utrzymania Polityki Bezpieczeństwa może zarządzić przegląd polityki bezpieczeństwa stosownie do potrzeb.
Zespół ds. Monitorowania Zagrożeń i Utrzymania Polityki Bezpieczeństwa analizuje, czy Polityka Bezpieczeństwa Informacji i pozostała dokumentacja jest adekwatna do:

- zmian w budowie systemu,
- zmian organizacyjnych,

- zmian w obowiązującym prawie.

Przewodniczący Zespołu ds. Monitorowania Zagrożeń i Utrzymania Polityki Bezpieczeństwa może, stosownie do potrzeb, przeprowadzić wewnętrzny audyt zgodności. Zakres, przebieg i rezultaty audytu dokumentowane są w formie pisemnej.
Przewodniczący Zespołu ds. Monitorowania Zagrożeń i Utrzymania Polityki Bezpieczeństwa po uzgodnieniu z najwyższym kierownictwem, może zlecić przeprowadzenie audytu zewnętrznego przez wyspecjalizowany podmiot.

Zespół ds. Monitorowania Zagrożeń i Utrzymania Polityki Bezpieczeństwa przeprowadza proces szacowania ryzyka w oparciu o gotową macierz opracowaną w oparciu o metodę CRAMM (Crisis Risk Management Metodology). W tym podejściu ryzyko szacowane jest jakościowo w oparciu o wybrany poziom wymagań bezpieczeństwa, związany z ochroną poufności, integralności i dostępności informacji w skali 10-cio stopniowej. W rzędach macierzy wyszczególniane są zasoby systemu podlegające ochronie; kolumny przedstawiają ryzyka, jakie zagrażają integralności, poufności i dostępności tych zasobów. W poszczególne komórki macierzy wpisywane są rezultaty oszacowania skutków utraty atrybutów bezpieczeństwa informacji (poufności, integralności, dostępności), podatność zasobów na zidentyfikowane dla systemu zagrożenia i wielkość obliczonego dla każdego zasobu ryzyka, będącego iloczynem skutków i podatności.

Rozdział XIV – Odnośniki/ współzależności z inną dokumentacją związaną z bezpieczeństwem

Celem Polityki Bezpieczeństwa Informacji jest określenie zasad funkcjonowania Systemu Zarządzania Bezpieczeństwem Informacji.

Dokumenty ustanawiają metody zarządzania oraz wymagania niezbędne dla zapewnienia skutecznej i spójnej ochrony przetwarzanych informacji.

Dokumenty Polityki Bezpieczeństwa Informacji podzielone zostały na dwa poziomy:

1) dokumenty opisujące ogólne zasady bezpieczeństwa informacji,
2) dokumenty opisujące zasady bezpieczeństwa systemów przetwarzania.

Zestaw dokumentów Polityki Bezpieczeństwa Informacji składa się z następujących rodzajów dokumentów:

1) niniejszego dokumentu Polityki Bezpieczeństwa Informacji opisującego:

- cele działań dotyczących zapewnienia bezpieczeństwa informacji,
- przyjęte strategie osiągnięcia celów ochrony informacji,
- opis struktury Polityki Bezpieczeństwa Informacji,
- opis struktury odpowiedzialności za bezpieczeństwo informacji,
- podstawy prawne i normatywne Polityki Bezpieczeństwa Informacji,
- zakres stosowania Polityki Bezpieczeństwa Informacji,
- zakres rozpowszechniania niniejszego dokumentu.

2) dokumentów opisujących zasady bezpieczeństwa:

a. Regulaminu Pracy Urzędu,

b. Instrukcji gospodarowania składnikami majątku w Dolnośląskim Urzędzie Wojewódzkim we Wrocławiu,

c. Instrukcji postępowania dla pracowników Oddziału Sieci i Systemów Informatycznych, dotycząca wejścia do serwerowni Urzędu,

d. Instrukcji postępowania na wypadek wystąpienia problemów z klimatyzatorami w serwerowni Urzędu i możliwości przegrzania się urządzeń sieciowych,

e. Procedury nadawania uprawnień zdalnego dostępu dla pracowników Urzędu i podmiotów zewnętrznych współpracujących z Urzędem,

f. Instrukcji korzystania z Zasobów sieciowych Urzędu,

g. Procedury tworzenia kopii bezpieczeństwa i ich przechowywania,

h. Instrukcji postępowania dla pracowników Oddziału Sieci i Systemów Informatycznych, dotycząca tworzenia i przechowywania haseł do kont o wysokich uprawnieniach,

i. Procedury nadawania, zmiany i cofania uprawnień w systemach informatycznych Urzędu,

j. Instrukcji ochrony obiektu,

k. Instrukcji bezpieczeństwa pożarowego.

Poszczególne dokumenty wymienione powyżej, będą tworzone sukcesywnie i wprowadzane w życie w formie odrębnych dokumentów wydanych na podstawie stosownych upoważnień.

Rozdział XV – Zasady dokonywania zmian w Polityce Bezpieczeństwa Informacji

Niniejszy dokument i inne dokumenty z nim związane, będą modyfikowane w przypadku:

- ogłoszenia nowych lub modyfikacji istniejących przepisów prawa;
- przekazania uwag przez odbiorców Polityki Bezpieczeństwa Informacji;
- powstania zaleceń poaudytowych;
- w wyniku przeprowadzenia corocznych przeglądów Polityki Bezpieczeństwa Informacji;
- zmian organizacyjnych w Urzędzie.

Zespół ds. Monitorowania Zagrożeń i Utrzymania Polityki Bezpieczeństwa po dokonaniu analizy sprawozdania rocznego z przeprowadzonych audytów przez Kierownictwo Urzędu, podejmuje decyzję o ewentualnym wprowadzeniu zmian w Polityce Bezpieczeństwa Informacji.

Każda zmiana Polityki Bezpieczeństwa Informacji powinna być odzwierciedleniem efektów szacowania ryzyka lub audytów prowadzonych przez Zespół ds. Monitorowania Zagrożeń i Utrzymania Polityki Bezpieczeństwa.

Rozdział XVI – Zasady rozpowszechniania Polityki Bezpieczeństwa Informacji

Z treścią niniejszego dokumentu są zapoznawani wszyscy pracownicy Urzędu oraz podmioty zewnętrzne uczestniczące w realizacji działań statutowych Urzędu.

Z treścią polityk szczegółowych, instrukcji, regulaminów i procedur zawartych w dokumentach związanych, są zapoznawani pracownicy Urzędu lub podmioty zewnętrzne w zakresie niezbędnym do wykonania swoich obowiązków służbowych.

Rozdział XVII – Podstawa prawna

Podstawę egzekwowania od pracowników Urzędu przestrzegania zasad niniejszej Polityki Bezpieczeństwa Informacji stanowią przepisy prawa oraz stosunek prawny będący podstawą wykonywania pracy na rzecz Urzędu.

Podstawą egzekwowania przestrzegania zasad ochrony informacji od podmiotów zewnętrznych uczestniczących w procesach związanych z działalnością Urzędu są przepisy prawa lub stosowne zapisy umów, decyzji i porozumień.

Listę dobrych praktyk w zakresie bezpieczeństwa informacji zawiera Polska Norma PN-ISO/IEC 27001:2007P.