Z A R Z Ą D Z E N I E Nr 37 /2013
WOJEWODY ŚWIĘTOKRZYSKIEGO
z dnia 4 kwietnia 2013 r.

w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji dla Świętokrzyskiego Urzędu Wojewódzkiego w Kielcach

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.) w związku z § 20 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. poz. 526) zarządza się, co następuje:

§ 1. Wprowadzam Politykę Bezpieczeństwa Informacji dla Świętokrzyskiego Urzędu Wojewódzkiego w Kielcach, stanowiącą załącznik nr 1 do niniejszego zarządzenia.

§ 2. 1. Polityka Bezpieczeństwa Informacji jest podstawowym dokumentem zawierającym zasady i wymagania ochrony posiadanych informacji, zwłaszcza przechowywanych i przetwarzanych w ramach systemów informatycznych.

2. Każdy pracownik Świętokrzyskiego Urzędu Wojewódzkiego, stażysta, praktykant inna osoba fizyczna uzyskująca dostęp do zasobów informacyjnych Urzędu musi zostać zapoznana z Polityką Bezpieczeństwa Informacji, fakt ten potwierdza pisemnym oświadczeniem (wzór załącznik nr 2 do niniejszego zarządzenia) złożonym w Oddziale Zarządzania Zasobami w Wydziale Organizacji i Kadr.

§ 3. Nadzór nad wykonaniem niniejszego zarządzenia sprawuje Informatyk Wojewódzki.

§ 4. Zarządzenie wchodzi w życie z dniem podpisania.

WOJEWODA ŚWIĘTOKRZYSKI
Bożentyna Pałka-Koruba

Załącznik nr 1

do zarządzenia Wojewody Świętokrzyskiego nr 37/2013

z dnia 4 kwietnia 2013r.

POLITYKA BEZPIECZEŃSTWA INFORMACJI

Spis treści:

SŁOWNIK TERMINÓW

Opracowany w oparciu o obowiązujące normy

Analiza ryzyka - to proces identyfikacji ryzyka, określenia jego wielkości i wyodrębnienia obszarów wymagających zabezpieczeń

Autentyczność - właściwość polegająca na tym, że pochodzenie lub zawartość obiektu informatycznego są takie jak deklarowane

Bezpieczeństwo informacji - zachowanie poufności, integralności i dostępności informacji; dodatkowo mogą być brane pod uwagę inne własności, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność

Dostępność - zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów wtedy, gdy jest to potrzebne

Integralność - zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania

Hasło dostępu - ciąg znaków wykorzystywany w celu autoryzacji dostępu do danych

Koń trojański - program, najczęściej szkodliwy, instalujący się na komputerze bez wiedzy użytkownika, który umożliwia nieuprawnione gromadzenie, fałszowanie lub niszczenie danych

Monitorowanie - proces weryfikacji stosowanych metod i zasad bezpieczeństwa oraz kontrola ich przestrzegania

Naruszenie bezpieczeństwa - odstępstwo od obowiązujących procedur postępowania lub bezprawne naruszenie zasobów bez względu na skutki

Niezawodność - właściwość oznaczająca spójne, zamierzone zachowanie i skutki

Polityka bezpieczeństwa - zestaw efektywnych, udokumentowanych zasad i procedur bezpieczeństwa wraz z ich planem wdrożenia i egzekwowania

Poufność - zapewnienie, że informacja jest dostępna jedynie osobom upoważnionym

Ryzyko - prawdopodobieństwo, że określone zagrożenie w połączeniu z podatnością doprowadzi do utraty lub zniszczenia zasobów

System informatyczny - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych

Utrzymanie ciągłości działania – zapewnienie na określonym poziomie, nieprzerwanej realizacji zadań statutowych Urzędu na wypadek wystąpienia incydentu związanego z bezpieczeństwem informacji

Zasada czystego biurka – zasada stanowiąca, że osoba opuszczająca miejsce pracy nie pozostawia na biurku lub innym miejscu używanym przez niego do pracy, w sposób dostępny dla innych osób, dokumentów i nośników zawierających informacje wrażliwe

Zasada czystego ekranu – zasada stanowiąca, że osoba opuszczająca miejsce pracy nie pozostawia na swoim stanowisku pracy stacji roboczej (inne przenośne urządzenia IT) w stanie umożliwiającym innym osobom korzystanie z niej

Zasada wiedzy uzasadnionej – pracownik lub inne osoby (umowa o dzieło, zlecenie, staż, praktyki) powinny mieć dostęp tylko do tych informacji, które są mu niezbędne w pracy

Wirus - program, najczęściej szkodliwy, instalujący się na komputerze bez wiedzy użytkownika, który potrafi się sam powielać, często przez sieci komputerowe, przez dołączanie swojej kopii do innych programów; dokonuje niepożądanych zmian w systemie uszkadzając dane, programy a nawet sprzęt komputerowy

1. Cel polityki bezpieczeństwa informacji

Zapewnienie bezpieczeństwa informacji jest normą, koniecznością oraz obowiązkiem wynikającym z obowiązujących przepisów prawa.

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.

Realizacja statutowych zadań każdej jednostki organizacyjnej 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 jednostki.

Niniejszy dokument wyraża świadomość Kierownictwa Urzędu w zakresie potrzeb bezpieczeństwa informacji oraz określa podstawowe przyjęte w tym obszarze cele i strategie.

Celem Polityki Bezpieczeństwa Informacji jest zapewnienie, że aktywa informacyjne, posiadane przez Świętokrzyski Urząd Wojewódzki w Kielcach zwany dalej Urzędem, są zabezpieczone w stopniu właściwym dla ich wrażliwości i krytyczności. Niewłaściwa ochrona informacji, zwłaszcza przetwarzanych w ramach systemu informatycznego Urzędu, może doprowadzić do braku dostępu do informacji, naruszenia ich integralności lub nieautoryzowanego ujawnienia, a w rezultacie do naruszenia obowiązujących regulacji prawnych lub pogorszenia wizerunku Urzędu, a w krytycznych przypadkach nawet strat finansowych.

W Urzędzie informacje podlegają ochronie zgodnie z następującymi wymogami prawa:

1. Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (j.t. Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.),
2. Ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228, z późn. zm.),
3. Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. Nr 112, poz. 1198, z późn. zm.),
4. Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. Nr 130, poz. 1450, z późn. zm.),
5. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. Nr 64, poz. 565, z późn. zm.),
6. Ustawa z dnia 21 listopada 2008 r. o służbie cywilnej (Dz. U. Nr 227, poz. 1505 z późn. zm.),
7. Ustawa z dnia 16 września 1982 r. o pracownikach urzędów państwowych (j.t. Dz.U. z 2001 r. Nr 86, poz. 953 z późn. zm.),
8. Ustawa z dnia 26 czerwca 1974 r. - Kodeks pracy (t.j. Dz. U. z 1998 r. Nr 21, poz. 94 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. Nr 100, poz. 1024),

10. Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie określenia podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych (Dz. U. 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 2012 r. poz. 526),

Niniejszy dokument dotyczy pracowników Urzędu, a także innych osób mających dostęp do informacji chronionej w ŚUW (np. stażystów, praktykantów, innych osób fizycznych realizujących zadania oraz pracowników firm zewnętrznych realizujących prace na rzecz Urzędu). Dokument ma zastosowanie do wszystkich informacji chronionych niezależnie od formy, w jakiej są przechowywane (papierowej, elektronicznej i innej).

2. Struktura dokumentów Polityki Bezpieczeństwa Informacji

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

- Poziom jednostki organizacyjnej,
- Poziom grupy informacji,
- Poziom systemu informatycznego,
- Poziom procedur, instrukcji i regulaminów.

Na **politykę bezpieczeństwa informacji jednostki organizacyjnej** składają się zasady bezpieczeństwa obowiązujące w Urzędzie oraz specyficzne dla jednostki.

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).

Polityka bezpieczeństwa systemu informatycznego (która może być 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 1.

Procedury, instrukcje i regulaminy regulują szczegółowe zasady korzystania z zasobów informacyjnych, a także użytkowania systemów informatycznych.

Podstawowym dokumentem Polityki Bezpieczeństwa Informacji na poziomie procedur, instrukcji i regulaminów w Urzędzie jest instrukcja *„Zasady przetwarzania danych w sieci komputerowej Świętokrzyskiego Urzędu Wojewódzkiego w Kielcach"* – załącznik nr 2.

3. Odpowiedzialność za bezpieczeństwo informacji

W Urzędzie za bezpieczeństwo informacji, a w szczególności za opracowanie, wdrożenie i utrzymanie polityki bezpieczeństwa informacji, odpowiada Wojewoda Świętokrzyski.

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

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

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, wnioskowanie o wydawanie stosownych upoważnień.

Pełnomocnik ds. Ochrony Informacji Niejawnych odpowiada za zapewnienie przestrzegania przepisów o ochronie informacji niejawnych.

Administrator Bezpieczeństwa Informacji odpowiada za nadzór nad opracowanymi dokumentami dla przetwarzanych w Urzędzie danych osobowych.

Administrator Systemu odpowiada za funkcjonowanie systemów lub sieci teleinformatycznych oraz za przestrzeganie zasad i wymagań bezpieczeństwa systemów i sieci teleinformatycznych dla informacji niejawnych.

Inspektor Bezpieczeństwa Teleinformatycznego odpowiada za bieżącą kontrolę zgodności funkcjonowania sieci lub systemu teleinformatycznego ze szczególnymi wymaganiami bezpieczeństwa oraz kontrolę przestrzegania procedur bezpiecznej eksploatacji dla informacji niejawnych.

Wszyscy pracownicy są zobowiązani, odpowiednio do swoich obowiązków i zajmowanych stanowisk, do przestrzegania Polityki Bezpieczeństwa Informacji, a zwłaszcza zasad zawartych w procedurach, regulaminach 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. W związku z tym wszyscy użytkownicy podlegają monitoringowi. Powyższe zasady dotyczą stażystów, praktykantów oraz innych osób fizycznych, które realizują powierzone im zadania. Pracownicy są zobowiązani również chronić sprzęt wykorzystywany do przetwarzania, przesyłania i przechowywania informacji, pomieszczenia w których znajduje się sprzęt oraz oprogramowanie wykorzystywane w Urzędzie.

Ponadto **wszyscy pracownicy są zobowiązani** do przestrzegania zasad ochrony informacji prawnie chronionej.

Nie wolno instalować wszelkiego rodzaju oprogramowania w całej infrastrukturze. Oddział ds. Informatyki kontroluje i sam instaluje dopuszczone oprogramowanie. W przypadku wykrycia nielegalnego oprogramowania pracownicy są zmuszenie poinformować o tym fakcie Dyrektora Generalnego Urzędu.

W przypadku korzystania ze sprzętu mobilnego np. laptopów, notebooków, pendrive pracowników obowiązują te same zasady jak przy korzystaniu ze sprzętu na miejscu w Urzędzie,

czyli nie wolno instalować nielegalnego oprogramowania a przede wszystkim należy wykorzystywać otrzymany sprzęt do celów służbowych.

Całokształt obsługi informatycznej i utrzymania sieci w Urzędzie realizuje Oddział ds. Informatyki.

Skuteczna ochrona zasobów informacyjnych Urzędu wymaga wspólnego działania i zaangażowania Kierownictwa Urzędu oraz pracowników.

Polityka Bezpieczeństwa Informacji obowiązuje wszystkich kontrahentów, jednostki zewnętrzne i pracowników, o ile w trakcie realizacji umowy otrzymują dostęp do zasobów informatycznych. Dostęp do zasobów otrzymują po wcześniejszym wydaniu stosownego upoważnienia i zapoznaniu się z Polityką.

Obowiązek ochrony zasobów Urzędu, w przypadku współpracy z jednostkami i podmiotami zewnętrznymi określony jest w ramach zawieranych umów. Umowy winny być parafowane przez Informatyka Wojewódzkiego.

W przypadku stażystów, praktykantów lub innych 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.

4. 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
- ✓ chroniących tajemnice zawodowe.

5. Zagrożenia dla bezpieczeństwa informacji

Konieczność wdrożenia Polityki Bezpieczeństwa Informacji w celu zapewnienia właściwej ochrony informacji wynika z istnienia zagrożeń dla poufności, autentyczności, dostępności, integralności informacji w Urzędzie. Zagrożenia można sklasyfikować na wiele sposobów; poniżej przyjęto następującą klasyfikację:

- Zagrożenia losowe – wszystkie zagrożenia, które nie są powodowane celowym działaniem (np. klęski żywiołowe, przerwy w zasilaniu, awarie sprzętowe, błędy oprogramowania, niezamierzone pomyłki użytkowników, administratora, niezamierzone wprowadzanie złośliwego oprogramowania jak wirusy, konie trojańskie, itp.).
- Zagrożenia zamierzone, czyli świadome i celowe, np.:
  - nieuprawniony dostęp do systemu (włamanie) z zewnątrz lub z jego wnętrza,
  - nieuprawniony dostęp, przekaz lub ujawnienie informacji (np. na skutek zastosowania metod socjotechnicznych, kradzieży, podsłuchu, odzyskania informacji z kosza na śmieci),
  - użycie złośliwego oprogramowania (wirusy, konie trojańskie),
  - bezpośrednie zagrożenie zasobów systemu (np. uszkodzenie sprzętu, usunięcie lub modyfikacja programu lub danych).

Analiza oraz stałe monitorowanie zagrożeń są ważnym elementem procesu zarządzania bezpieczeństwem informacji.

6. 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 zminimalizowanie możliwości naruszenia bezpieczeństwa zasobów informacyjnych Urzędu,

umożliwienie wczesnego wykrycia takiego naruszenia, zminimalizowanie strat związanych z takim naruszeniem oraz sprawne usunięcie jego skutków.

Istotne jest systematyczne szkolenie oraz podnoszenie kwalifikacji zawodowych pracowników.

Odpowiednie zarządzanie zasobami Urzędu wymaga rejestracji i dokonywania ich rocznych przeglądów. Przeglądy przeprowadzają Dyrektorzy wydziałów /biur, którzy posiadają odpowiednie zasoby. Analizy wyników przeglądu zasobów informacyjnych dokonuje audytor wewnętrzny, który swoje wnioski w sprawozdaniu z audytu przekazuje Wojewodzie i Dyrektorowi Generalnemu Urzędu.

Załącznik nr 1
do Polityki Bezpieczeństwa Informacji
Świętokrzyskiego Urzędu Wojewódzkiego w Kielcach

Wykaz polityk bezpieczeństwa systemów informatycznych w Świętokrzyskim Urzędzie Wojewódzkim w Kielcach

L.p.	Nazwa
1	Polityka bezpieczeństwa systemu informatycznego EZD PUW - WERSJA 3.11 – do celów służbowych
2	Polityka bezpieczeństwa dla przetwarzanych w Świętokrzyskim Urzędzie Wojewódzkim w Kielcach zbiorów danych osobowych – wprowadzona odrębnym zarządzeniem

Załącznik nr 2
do Polityki Bezpieczeństwa Informacji
Świętokrzyskiego Urzędu Wojewódzkiego
w Kielcach

INSTRUKCJA

ZASADY PRZETWARZANIA DANYCH W SIECI KOMPUTEROWEJ ŚWIĘTOKRZYSKIEGO URZĘDU WOJEWÓDZKIEGO W KIELCACH

Definicje pojęć stosowanych w instrukcji

1. **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.

2. **Stanowisko** – pojedynczy komputer osobisty lub terminal przeznaczony do określonych zadań związanych między innymi z dostępem do sieci komputerowej ŚUW.

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. **Netykieta** – to zbiór zasad przyzwoitego zachowania w Internecie, swoista etykieta obowiązująca w Sieci. Zasady netykiety wynikają wprost z ogólnych zasad przyzwoitości lub są odzwierciedleniem niemożliwych do ujęcia w standardy ograniczeń technicznych wynikających z natury danej usługi Internetu.

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*).

Instrukcja
Zasady przetwarzania danych w sieci komputerowej Świętokrzyskiego Urzędu Wojewódzkiego w Kielcach zwanego „Urzędem"

1. Cel instrukcji

Celem instrukcji jest określenie zasad przetwarzania danych w sieci komputerowej Urzędu, a w szczególności udzielania dostępu do danych zgromadzonych w sieci komputerowej Urzędu oraz ich ochrony.

2. Zakres stosowania

Działania opisane w niniejszej Instrukcji obowiązują we wszystkich wydziałach, biurach i pozostałych komórkach organizacyjnych Urzędu oraz innych jednostkach korzystających z sieci komputerowej Urzędu. Niniejsza instrukcja 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 instrukcji w zakresie ochrony haseł, profilaktyki antywirusowej, wykonywania kopii bezpieczeństwa własnych zasobów oraz ich ochrony.

Administrator systemu odpowiedzialny jest za zakładanie kont, przydzielanie zasobów użytkownikom stanowisk, wykonywanie okresowych kopii danych serwerów, generowanie użytkownikom pierwszych haseł dostępowych, przechowywanie wniosków o uruchomienie stanowiska i założenie konta oraz ochronę antywirusową zasobów sieci komputerowej Urzędu zgromadzonych na serwerach.

Dyrektorzy wydziałów/biur oraz kierownicy innych komórek organizacyjnych Urzędu korzystających z sieci komputerowej Urzędu odpowiedzialni są za analizę celowości uruchomienia stanowiska, za przygotowanie i przekazanie do Wydziału Organizacji i Kadr wniosków o skonfigurowanie stanowiska oraz przydzielenie lub zlikwidowanie konta użytkownikowi, a także zapoznanie podległych im pracowników z treścią tej instrukcji.

4. Udzielanie dostępu do zasobów informatycznych

4.1. Procedura przydzielania stanowisk roboczych

4.1.1. Dyrektor wydziału/biura oraz kierownicy innych komórek organizacyjnych składają wniosek do Wydziału Organizacji i Kadr o zainstalowanie/zmianę przeznaczenia stanowiska w sieci komputerowej ŚUW w Kielcach.
Wzór wniosku stanowi ZAŁĄCZNIK NR 1.

4.1.2. Dyrektor WOiK przekazuje wniosek Kierownikowi Oddziału ds. Informatyki.

4.1.3. Kierownik Oddziału ds. Informatyki akceptuje wniosek i przekazuje go administratorowi systemu.

4.1.4. W przypadku braku akceptacji Kierownika Oddziału ds. Informatyki, wniosek jest odsyłany wnioskodawcy z określeniem przyczyny uniemożliwiającej zainstalowanie stanowiska roboczego użytkownika.
4.1.5. Administrator systemu na podstawie wniosku ustanawia parametry stanowiska roboczego oraz udostępnia zasoby.
4.1.6. W porozumieniu z Administratorem systemu, pracownik Oddziału ds. Informatyki dokonuje końcowej konfiguracji stanowiska roboczego.

Uwaga!

1. Dyrektorzy wydziałów/biur oraz kierownicy innych komórek organizacyjnych są zobowiązani złożyć nowy wniosek w przypadku zmiany danych podanych we wniosku.
2. Administrator systemu ma prawo zablokować dostęp do funkcji i zasobów systemu w przypadku stwierdzenia niewłaściwego, niezgodnego z treścią wniosku wykorzystywania stanowiska roboczego

4.2. Procedura uzyskiwania kont

4.2.1. Dyrektorzy wydziałów/biur oraz kierownicy innych komórek organizacyjnych przesyłają do Wydziału Organizacji i Kadr wniosek o założenie/zmianę/likwidację konta użytkownika zasobów informatycznych Urzędu.
Wzór wniosku stanowi ZAŁĄCZNIK NR 2.
4.2.2. Dyrektor WOiK przekazuje wniosek Kierownikowi Oddziału ds. Informatyki. W przypadku braku akceptacji Kierownika Oddziału ds. Informatyki, udzielana jest wnioskodawcy odpowiedź z określeniem przyczyny uniemożliwiającej realizację wniosku.
4.2.3. Kierownik Oddziału ds. Informatyki 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.
4.2.4. 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.
4.2.5. W przypadku likwidacji konta, Administrator usuwa lub blokuje konto w terminie określonym w treści wniosku.
4.2.6. W porozumieniu z Administratorem systemu, pracownik Oddziału ds. Informatyki 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.

Uwaga!

1. Dyrektorzy wydziałów/biur oraz kierownicy innych komórek organizacyjnych są zobowiązani:
   1.1. złożyć nowy wniosek w przypadku zmiany danych podanych we wniosku,
   1.2. złożyć wniosek o likwidację konta.
2. Administrator systemu ma prawo zablokować konto, w przypadku stwierdzenia niewłaściwego, niezgodnego z treścią wniosku wykorzystywania konta.

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

5.1. 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.

5.2. Po otrzymaniu z WOiK 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).

5.3. Hasła nie wolno nigdzie zapisywać ani na papierze, ani w postaci elektronicznej - należy je zapamiętać. Hasło należy zmieniać co najmniej raz na miesiąc.

5.4. 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. Instrukcja pracy na stanowisku

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

Uwaga!

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 ww. parametrów mogą dokonywać wyłącznie uprawnieni pracownicy Oddziału ds. Informatyki po uzgodnieniu z administratorem systemu.

3. 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.

7. Wykonywanie kopii systemów informatycznych

Kopie awaryjne konfiguracji systemu wykonuje Administrator systemu po każdej zmianie konfiguracji oprogramowania (np. po utworzeniu, rekonfiguracji lub usunięciu konta użytkownika w systemie, zmianie praw dostępu itp.).

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

8.1. Administrator systemu wykonuje kopie zapasowe danych roboczych użytkowników (kopie robocze) zlokalizowanych w sieci komputerowej Urzędu (bazy danych, katalogi użytkowników, katalogi grup).

8.2. Kopie danych mogą być wykonywane automatycznie według określonego harmonogramu.

9. Metody i częstotliwość działań związanych z profilaktyką antywirusową w systemach informatycznych użytkowanych w sieci komputerowej Urzędu

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

9.2. Ochrona zasobów sieci komputerowej z wykorzystaniem funkcji systemowych.
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.

9.3. Ochrona zasobów sieci komputerowej z wykorzystaniem programów antywirusowych.

9.3.1 Ochrona antywirusowa zasobów informatycznych jest realizowana przez system antywirusowy posiadający następujące funkcje:

- zabezpieczenie zasobów informatycznych przed wirusami komputerowymi za pomocą modułu rezydentnego, skanującego na bieżąco wszystkie zasoby komputera,
- aktualizację baz sygnatur wirusów na bieżąco,
- możliwość automatycznego podejmowania działań w przypadku pojawienia się nowych, nieznanych wirusów (np. zablokowanie komunikacji z zawirusowanym komputerem).

9.3.2. 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.

9.3.3. 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.

9.3.4. Użytkownicy sieci komputerowej prowadzą profilaktykę antywirusową zgodnie z *„Instrukcją w zakresie profilaktyki antywirusowej”* – ZAŁĄCZNIK NR 3.

10. Metody postępowania w sytuacjach nadzwyczajnych.

W przypadku:

- podejrzenia naruszenia lub stwierdzenia próby naruszenia bezpieczeństwa informacji (np. przełamania zabezpieczeń systemu informatycznego),
- podejrzenia utraty integralności zasobów informatycznych lub utraty danych,
- podejrzenia próby podszycia się innej osoby pod użytkownika systemu,

należy niezwłocznie zawiadomić Administratora systemu.

W przypadku podejrzenia działania szkodliwego oprogramowania (wirus, trojan) należy postępować zgodnie z *„Instrukcją w zakresie profilaktyki antywirusowej”* – ZAŁĄCZNIK NR 3.

W przypadku:

- podejrzenia awarii stanowiska lub urządzenia zewnętrznego (np. drukarka),
- utraty dostępu do sieci komputerowej przez stanowisko,
- zaobserwowania zachowania się komputera, które odbiega od normy

należy niezwłocznie zawiadomić Oddział ds. Informatyki, które zajmuje się serwisem sprzętu. Zabrania się użytkownikom dokonywania napraw we własnym zakresie.

11. Wymagania oraz zasady postępowania dotyczące urządzeń przenośnych i nośników danych wynoszonych poza siedzibę Urzędu w ramach wykonywania obowiązków służbowych

11.1. Wynoszenie urządzeń przenośnych będących własnością Urzędu poza jego siedzibę może występować wyłącznie w ramach wykonywania obowiązków służbowych.

11.2. Urządzenia przenośne i nośniki danych wynoszone poza siedzibę Urzędu powinny 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.

11.3. Urządzenia nie spełniające powyższych wymagań będą sukcesywnie wymieniane.

11.4. W przypadku utraty urządzenia należy niezwłocznie powiadomić przełożonych oraz Kierownika Oddziału ds. Informatyki.

11.5. Oddział ds. Informatyki prowadzi ewidencję urządzeń przenośnych, które można wynosić poza siedzibę Urzędu.

12. 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 instrukcji oraz 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.

Załącznik nr 1
do Instrukcji „Zasady przetwarzania danych w sieci komputerowej Świętokrzyskiego Urzędu Wojewódzkiego w Kielcach"

Kielce, dnia .....

Wniosek
o zainstalowanie / zmianę przeznaczenia stanowiska* w sieci komputerowej ŚUW w Kielcach

1. Wnioskodawca:

Imię i nazwisko: .....
Stanowisko służbowe: .....
Jednostka organizacyjna: .....

2. Główny użytkownik stanowiska:

Imię i nazwisko: .....
Stanowisko służbowe: .....
Oddział: .....
Jednostka organizacyjna: .....

3. Lokalizacja stanowiska *(budynek, piętro, pokój):*

---

4. Przeznaczenie stanowiska *(należy podać wszystkie zasoby sieci komputerowej, do których stanowisko ma mieć dostęp. Jeśli nowe stanowisko – dodatkowo wpisać słowo „NOWE") :*

---

*- niepotrzebne skreślić

Załącznik nr 2
Instrukcji „Zasady przetwarzania danych w sieci komputerowej Świętokrzyskiego Urzędu Wojewódzkiego w Kielcach"

Kielce, dnia.....

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

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 (w podpunktach a), b),c),d) wpisać słowo „TAK" lub" NIE"):

a) Sieć komputerowa ŚUW .....
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)

* - niepotrzebne skreślić

Załącznik nr 3
do Instrukcji „Zasady przetwarzania danych
w sieci komputerowej Świętokrzyskiego Urzędu Wojewódzkiego w Kielcach"

Instrukcja w zakresie profilaktyki antywirusowej

1. Zabrania się umieszczania w urządzeniach odczytujących dane na stanowisku (stacje dyskietek, czytniki CD-ROM, DVD, porty USB itp.) nośników rozprowadzanych z różnego rodzaju czasopismami, materiałami reklamowymi itp.
2. Zabrania się bez zgody Wydziału Organizacji i Kadr 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 Wydziału Organizacji i Kadr innych, niż dopuszczony w ŚUW, 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 MAKRO.
7. Należy systematycznie przeprowadzać kontrolę antywirusową stanowiska programem dostarczonym przez Wydział Organizacji i Kadr.
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 CD-ROM,USB itp.), wyraźnie oznaczyć i przekazać nośnik administratorowi sieci komputerowej. 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 administratorowi sieci komputerowej (WOiK).
4. Użytkownik ma obowiązek zgłaszania do WOiK wszelkich zauważonych niestandardowych zachowań systemu antywirusowego.

Załącznik nr 2
do zarządzenia Wojewody Świętokrzyskiego nr 31 /2013
z dnia 4 kwietnia 2013r.

Kielce, ...

.....
imię i nazwisko
.....
stanowisko
.....
wydział/ biuro

OŚWIADCZENIE

o zapoznaniu się z Polityką Bezpieczeństwa Informacji

Ja niżej podpisana/y oświadczam, że zapoznałam/em się oraz zrozumiałam/em Politykę Bezpieczeństwa Informacji Świętokrzyskiego Urzędu Wojewódzkiego i zobowiązuję się do przestrzegania zawartych w niej zasad, reguł i postanowień. Jednocześnie oświadczam, że jestem świadoma/y tego, iż wszelkie wykonywane przeze mnie operacje w sieci komputerowej ŚUW www (z pocztą elektroniczną włącznie), w szczególności dotyczące zasobów wrażliwych pod względem poufności, mogą być monitorowane.

.....
(imię i nazwisko, podpis)