Zarządzenie Nr 103/2015
WOJEWODY ŚWIETOKRZYSKIEGO
z dnia 10 listopada 2015 r.

zmieniające zarządzenie 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. W zarządzeniu Nr 65/2014 Wojewody Świętokrzyskiego z dnia 11 sierpnia 2014 r. w sprawie wprowadzenia Polityki Bezpieczeństwa Informacji dla Świętokrzyskiego Urzędu Wojewódzkiego w Kielcach ulegają zmianie następujące załączniki do Polityki Bezpieczeństwa Informacji :

1) Polityka Kontroli Dostępu do Informacji - załącznik nr 1
2) Polityka Tworzenia Kopii Zapasowych - załącznik nr 2
3) Procedura Zarządzania Incydentami Związanymi z Bezpieczeństwem Informacji - załącznik nr 4
4) Instrukcja w zakresie profilaktyki antywirusowej - załącznik nr 6

§ 2. Zarządzenie wchodzi w życie z dniem podpisania.

WOJEWODA ŚWIĘTOKRZYSKI

Bożentyna Pałka-Koruba

UZASADNIENIE

Zmiana zarządzenia jest zgodna z § 20 ust. 2 pkt 1 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z dnia 16 maja 2012 r. poz. 526), na podstawie którego kierownictwo podmiotu publicznego zobowiązane jest do zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia. W Świętokrzyskim Urzędzie Wojewódzkim zadanie to jest realizowane poprzez okresowy przegląd Polityki Bezpieczeństwa Informacji w wyniku którego dokonano zmian w treści załączników wymienionych w zarządzeniu.

DYREKTOR
Wydziału Organizacji i Kadr
mgr Edyta Suchoń

Załącznik nr 1
Polityki Bezpieczeństwa Informacji
Świętokrzyskiego Urzędu
Wojewódzkiego

POLITYKA KONTROLI DOSTĘPU DO INFORMACJI

Listopad 2015

Definicje pojęć stosowanych w polityce.

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. **Konto** - to zbiór zasobów i uprawnień mający unikalny identyfikator w systemie informatycznym lub sieci komputerowej.

7. **Użytkownik** - to byt (osoba lub inny system) korzystający z systemu komputerowego. Użytkownicy mogą być identyfikowani w celach zliczania czasu pracy, bezpieczeństwa, czy też zarządzania zasobami. Aby użytkownik został zidentyfikowany, użytkownik posiada konto (konto użytkownika), do którego przypisana jest nazwa (nazwa użytkownika) i hasło (lub inny sposób autentykacji – np. informacje biometryczne). Użytkownicy uzyskują dostęp do systemów przez interfejs użytkownika, a sam proces identyfikacji jest nazywany logowaniem (od angielskiego *logging in*).

1. Cel polityki.

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

2. Zakres stosowania.

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

3. Odpowiedzialność.

Wszyscy użytkownicy uzyskujący dostęp do zasobów sieci komputerowej Urzędu jak również użytkownicy stanowisk nie podłączonych do sieci ale zainstalowanych na terenie Urzędu, odpowiedzialni są za przestrzeganie zasad opisanych w polityce w zakresie ochrony haseł. Administrator systemu odpowiedzialny jest za zakładanie i usuwanie kont w systemie, przydzielanie i odbieranie dostępu do zasobów użytkownikom stanowisk, generowanie użytkownikom pierwszych haseł dostępowych, przechowywanie wniosków o uruchomienie stanowiska.

Dyrektorzy wydziałów/biur Urzędu oraz inne komórki organizacyjne korzystające 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 polityce.

4. Udzielanie dostępu do zasobów informatycznych.

4.1. Procedura przydzielania stanowisk roboczych

4.1.1. Dyrektor wydziału/biura oraz inne komórki organizacyjne składają wniosek do Wydziału Organizacji i Kadr o zainstalowanie/zmianę przeznaczenia stanowiska w sieci komputerowej ŚUW w Kielcach.
Wzór wniosku stanowi ZAŁĄCZNIK NR1.

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.

4.1.3. W przypadku braku akceptacji Kierownika Oddziału ds. Informatyki, wniosek jest odsyłany wnioskodawcy z określeniem przyczyny uniemożliwiającej zainstalowanie stanowiska roboczego użytkownika.

4.1.4. Administrator systemu na podstawie wniosku ustanawia parametry stanowiska roboczego oraz udostępnia zasoby.

4.1.5. W porozumieniu z administratorem systemu, pracownik Oddziału ds. Informatyki dokonuje końcowej konfiguracji stanowiska roboczego.

Uwaga!

1. Dyrektorzy wydziału/biura oraz inne komórki organizacyjne są zobowiązane 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. Dyrektor wydziału/biura oraz inne komórki organizacyjne są zobowiązane:

4.2.1.1 Złożyć nowy wniosek w przypadku zmiany danych podanych we wniosku w terminie 7 dni od wystąpienia zdarzenia powodującego zmianę.

4.2.1.2 4.2.1.2 Złożyć wniosek o likwidację konta w terminie 7 dni od wystąpienia zdarzenia powodującego likwidację konta.

Wzór wniosku stanowi ZAŁĄCZNIK NR2.

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, 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 wydziału/biura oraz inne komórki organizacyjne są zobowiązane:

   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)
- Hasło nie może się powtarzać

5.3. Hasła nie wolno nigdzie zapisywać ani na papierze, ani w postaci elektronicznej - należy je zapamiętać. Niedopuszczalne jest zwłaszcza zapisywanie haseł na kartkach przyklejonych do monitora, klawiatury, czy biurka. Hasło należy zmieniać co najmniej raz na miesiąc.

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.

5.5. Hasła do kont o wysokich uprawnieniach są przechowywane w zaklejonych kopertach w zabezpieczonej szafie pancernej. Na każdej kopercie powinna być informacja o przeznaczeniu konta oraz data umieszczenia hasła w kopercie. Informacje o fizycznej lokalizacji haseł przechowuje administrator systemu.

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

W przypadku, gdy pracownicy Urzędu używają w pracy systemu informatycznego udostępnianego przez zewnętrzną instytucję (np.: ministerstwo) ochronie podlegają jedynie dane i programy umożliwiające uwierzytelnienie i dostęp do ww. systemu (np.: loginy, hasła,

certyfikaty). Należy wtedy oprócz stosowania się do zasad opisanych w niniejszej polityce stosować się do zaleceń i polityki bezpieczeństwa instytucji udostępniającej system.

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

7. Kontrola dostępu do sieci komputerowej.

Każda stacja użytkownika podłączona do sieci ma z góry określoną politykę dostępu do Internetu i pozostałych sieci. Każda droga połączenia z Internetem przechodzi przez zaporę urządzenia UTM, które filtruje ruch sieciowy. Dla systemów zawierających dane wrażliwe tworzone są sieci VLAN, co pozwala na dokładniejszą kontrolę drogi połączeń. Na hostach udostępniających usługi sieciowe zablokowany jest dostęp do innych usług niż te uzupełniane. Usługi takie jak WWW czy DNS, wystawione na dostęp zewnętrzny, należy umieszczać w bezpiecznej strefie zdemilitaryzowanej (DMZ). Użytkownicy powinni mieć bezpośredni dostęp tylko do zasobów określonych we wniosku.

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

Zdalny dostęp do systemów informatycznych realizowany jest przez szyfrowaną wirtualną sieć prywatną VPN tylko i wyłącznie po poprawnej identyfikacji i uwierzytelnieniu zdalnego użytkownika. Dostęp do sieci VPN ograniczony jest tylko do tych użytkowników, którym ten dostęp jest niezbędny do realizacji powierzonych zadań. Podstawą do uzyskania zdalnego dostępu jest wniosek dyrektora wydziału/biura złożony w Wydziale Organizacji i Kadr oraz zapis w umowie jeśli sprawa dotyczy podmiotu zewnętrznego. Zgoda po uzyskaniu opinii informatyka wojewódzkiego. Oddział ds. Informatyki prowadzi rejestr użytkowników VPN.

Komputery przenośne wykorzystywane poza siedzibą są zabezpieczone dodatkowo poprzez hasło BIOS.

8.1. Wynoszenie urządzeń przenośnych będących własnością Urzędu poza jego siedzibę może występować wyłącznie w ramach wykonywania obowiązków służbowych po wyrażeniu zgody przez Dyrektora Wydziału Organizacji i Kadr i po wpisaniu ich do rejestru.

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

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

8.4. Wprowadza się obowiązek aktualizacji rejestru przez wydziały co pół roku.

8.5. Użytkownik może mieć prawa administratora na wynoszonym urządzeniu jedynie wtedy jeżeli jest to niezbędne w celu umożliwienia podłączenia się do sieci w kontrolowanej jednostce.

9. Kontrola dostępu do pomieszczeń serwerowni.

Wydziela się strefę bezpieczeństwa w pomieszczeniach serwerowni Urzędu. Znajdują się tam wszystkie serwery, które przechowują zasoby informatyczne Urzędu. Dostęp do tych pomieszczeń mają tylko uprawnieni pracownicy Oddziału ds. Informatyki. Inne osoby mogą przebywać w tych pomieszczeniach tylko w obecności osób uprawnionych. Dostęp do strefy wydzielonej jest udzielany na podstawie upoważnienia Kierownika Oddziału ds. Informatyki. Dostęp do strefy wydzielonej jest możliwy za pomocą indywidualnych kart zbliżeniowych, wejścia do strefy są monitorowane. Strefa bezpieczeństwa obejmuje pokoje 310, 311,312,313,314. W strefie wydzielonej stosuje się następujące mechanizmy bezpieczeństwa:

a) Drzwi antywłamaniowe,
b) Plombowanie drzwi,
c) Alarm,
d) Monitoring warunków klimatycznych.
e) Klucze do strefy w zaplombowanym worku.

Strefa bezpieczeństwa jest obszarem ograniczonego dostępu nie przeznaczonym do ciągłej pracy ludzi. W związku z tym zabrania się przechowywania tam innych sprzętów lub rzeczy nie związanych z wykonywaniem zadań.

Dopuszcza się instalowanie urządzeń należących do zewnętrznych podmiotów w pomieszczeniach serwerowni ŚUW pod warunkiem, że zasady ich umieszczania i użytkowania będą szczegółowo określone w porozumieniach zawieranych z tymi podmiotami.

Zasady te nie mogą stać w sprzeczności z postanowieniami niniejszej polityki. Podmioty zewnętrzne, których urządzenia znajdują się w serwerowni Urzędu powinny się zapoznać z treścią Polityki Bezpieczeństwa Informacji ŚUW i zaakceptować jej postanowienia, składając stosowne oświadczenie.

10. Procedura przeglądu uprawnień do systemów.

W celu utrzymania efektywnej kontroli nad dostępem do danych i systemów informatycznych Administrator Systemu dokonuje przeglądu praw użytkowników do systemów Przegląd uprawnień do systemów jest wykonywany 2 razy do roku na dzień 30 czerwca i 31 grudnia oraz w wypadku dużych zmian kadrowych, a także w dowolnym czasie na wniosek Zespołu ds. monitorowania zagrożeń i utrzymania PBI lub audytora wewnętrznego. Przegląd musi obejmować zarówno konta zwykłych użytkowników, jak i konta o wysokich uprawnieniach. Danymi wejściowymi są informacje o zmianach kadrowych. Wynikiem przeglądu jest aktualizacja danych o uprawnieniach potwierdzona sporządzeniem notatki przez Administratora Systemu.

Załącznik nr 2
Polityki Bezpieczeństwa Informacji
Świętokrzyskiego Urzędu
Wojewódzkiego

POLITYKA TWORZENIA KOPII ZAPASOWYCH

Listopad 2015

Definicje pojęć stosowanych w polityce.

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. **Kopia zapasowa** – kopia danych lub oprogramowania. Celem jej wykonywania jest odtworzenie systemu po awarii.

1. Cel polityki.

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

2. Zakres stosowania.

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

3. Wykonywanie kopii systemów informatycznych.

Na potrzeby zachowania ciągłości działania systemów informatycznych i utrzymania integralności danych wykonuje się kopie zapasowe zbiorów danych. Zadanie to realizowane jest codziennie w dni robocze. Kopie awaryjne są wykonywane automatycznie przez dedykowane oprogramowanie poza godzinami pracy Urzędu według ustalonego harmonogramu. Harmonogram zawiera również określenie jakie zasoby i systemy są kopiowane. Kopie tworzone są przyrostowo, tzn. kopiowane są pliki nowe i te których zawartość uległa zmianie. Kopie trafiają do biblioteki taśmowej zarządzanej przez ww. oprogramowanie. Wyniki tworzenia kopii zapasowych są rejestrowane. Zakres tworzenia kopii zapasowych obejmuje:

a) Bazy danych zlokalizowane na serwerach;
b) Pliki i katalogi na serwerach;
c) Systemy operacyjne serwerów.

Kopie zapasowe sporządza się również w następujących przypadkach:

a) przed dokonaniem istotnej zmiany konfiguracyjnej (np. aktualizacji oprogramowania, ustawień systemowych),
b) po przeprowadzeniu zmiany konfiguracyjnej (np. aktualizacji oprogramowania, ustawień systemowych, zmianie praw dostępu).

Kopie zapasowe, wykonane w danym dniu przechowywane są przez okres 2 miesięcy oraz zabezpieczone są przed nieumyślnym skasowaniem i przechowywane w bibliotece taśmowej. Po zapełnieniu taśmy kopie przechowywane są w metalowym sejfie zamykanym na klucz. Po ustaniu użyteczności kopii zapasowej jest ona niezwłocznie usuwana. Informacje o fizycznej lokalizacji kopii zapasowych przechowuje administrator systemu.

Kopie zapasowe konfiguracji systemów operacyjnych serwerów wykonuje administrator systemu po każdej zmianie konfiguracji oprogramowania (np. po utworzeniu, rekonfiguracji lub usunięciu konta użytkownika w systemie, zmianie praw dostępu itp.)

Za prawidłowość tworzenia kopii zapasowych odpowiada administrator systemu.

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

4.1. Administrator systemu odpowiada za wykonywanie kopii zapasowych danych roboczych użytkowników (kopie robocze) przechowywanych na serwerach zlokalizowanych w sieci komputerowej Urzędu (bazy danych, katalogi użytkowników, katalogi grup).

4.2. Kopie danych są wykonywane automatycznie według procedury opisanej w punkcie 3.

4.3. Za wykonywanie kopii zapasowych danych znajdujących się na poszczególnych stacjach roboczych poza serwerownią odpowiadają użytkownicy tych stacji roboczych. Częstotliwość tworzenia kopii zapasowych na stacjach roboczych zależy od ilości i wagi przetwarzanych informacji. Niedopuszczalne jest przechowywanie kopii zapasowych na tych samych nośnikach na których są one przetwarzane. Użytkownicy mogą zlecać administratorowi systemu wykonanie kopii przetwarzanych przez nich danych (np. kopii folderów osobistych skrzynek pocztowych). Zlecenie należy złożyć w formie elektronicznej za pomocą systemu EZD.

5. Testowanie kopii zapasowych.

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

6. Odzyskiwanie danych i systemów informatycznych z kopii zapasowych.

Odzyskiwanie danych z kopii zapasowych jest wykonywane w następujących przypadkach:

a) utraty całości lub części danych na serwerze;

b) utraty integralności całości lub części danych na serwerze;

c) w celu odtworzenia poprzedniej wersji danych na wniosek z wydziału podpisany przez dyrektora danego wydziału przekazany w systemie EZD;

d) na wniosek organu kontrolnego (np.: NIK);

e) przy przenoszeniu danych na nowy serwer.

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

Za odzyskiwanie danych z kopii zapasowych odpowiada administrator systemu.

Załącznik nr 4
Polityki Bezpieczeństwa Informacji
Świętokrzyskiego Urzędu
Wojewódzkiego

Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji

Listopad 2015

Definicje pojęć stosowanych w procedurze.

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. **Incydent związany z bezpieczeństwem informacji** – pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań statutowych organizacji i zagrażają bezpieczeństwu informacji

6. **Podatność** – słabość systemu informatycznego, która może być wykorzystana przez co najmniej jedno zagrożenie

7. **Zespół ds. Monitorowania Zagrożeń i Utrzymania Polityki Bezpieczeństwa Informacji** – wyznaczeni przez Dyrektora Generalnego pracownicy Urzędu, którzy zajmują się zarządzaniem incydentami związanymi z bezpieczeństwem informacji w Urzędzie zgodnie z Zarządzeniem Nr 9 Dyrektora Generalnego Urzędu z dnia 18 kwietnia 2014 r w sprawie powołania Zespołu ds. monitorowania zagrożeń i utrzymania Polityki Bezpieczeństwa Informacji.

1. Cel procedury.

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

2. Zakres stosowania.

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

3. Odpowiedzialność.

Odpowiedzialność za prawidłowe zgłoszenie incydentów dotyczących bezpieczeństwa infrastruktury informatycznej spoczywa na pracownikach Urzędu dokonujących zgłoszeń. Każdy pracownik Oddziału ds. Informatyki odpowiedzialny za rozwiązanie problemu lub zapobieżenie incydentowi działa zgodnie z niniejszą procedurą.
Zespół ds. Monitorowania Zagrożeń i Utrzymania Polityki Bezpieczeństwa Informacji jest odpowiedzialny za:

1) Niezwłoczne reagowanie na incydenty bezpieczeństwa informacji w określony i z góry ustalony sposób;
2) Ocenę istniejących i potencjalnych zagrożeń w zakresie bezpieczeństwa informacji;
3) Ocenę przyczyn i skutków incydentów naruszenia bezpieczeństwa informacji w tym gromadzenie materiału dowodowego;
4) Przygotowywanie propozycji działań korygujących i naprawczych oraz nadzór nad ich wprowadzaniem;
5) Dokonywanie okresowego przeglądu i aktualizacji Polityki Bezpieczeństwa Informacji;
6) Prowadzenie działań zmierzających do wzrostu świadomości w zakresie zapewnienia bezpieczeństwa informacji w Urzędzie;
7) Współpracę z Rządowym Zespołem Reagowania na Incydenty Komputerowe CERT.

4. Klasyfikacja incydentów.

Podział zdarzeń:

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

2) Zdarzenia losowe wewnętrzne (np.: niezamierzone pomyłki operatorów, administratorów, awarie sprzętowe, błędy w oprogramowaniu), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu, może nastąpić naruszenie poufności danych.
3) Zdarzenia zamierzone, świadome i celowe – stanowią najpoważniejsze zagrożenie naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zdarzenia te możemy podzielić na:
   - nieuprawniony dostęp do danych z zewnątrz (włamanie do systemu),
   - nieuprawniony dostęp do danych z sieci wewnętrznej,
   - nieuprawniony transfer danych,
   - pogorszenie funkcjonowania sprzętu i oprogramowania (np.: działanie wirusów),
   - bezpośrednie zagrożenie materialnych składników systemu (np.: kradzież sprzętu).

Przykłady zdarzeń które mogą być zakwalifikowane jako uzasadnione podejrzenie naruszenia bezpieczeństwa informacji:

1) Sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na infrastrukturę teleinformatyczną jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.
2) Niewłaściwe parametry środowiska jak zbyt wysoka temperatura lub nadmierna wilgotność (w szczególności dotyczy to serwerowni).
3) Awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie systemu, a w tym sam fakt pozostawienia serwisantów bez nadzoru.
4) Pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu.
5) Jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikacje w systemie.
6) Nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie.
7) Stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji).
8) Nastąpiła niedopuszczalna manipulacja danymi w systemie.
9) Ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą elementy systemu zabezpieczeń.
10) Praca w systemie lub w sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych, np.: praca w systemie lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.
11) Ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. „bocznej furtki", itp.
12) Podmieniono lub zniszczono nośniki z danymi bez odpowiedniego upoważnienia lub w niedozwolony sposób skasowano lub kopiowano dane osobowe.
13) Rażąco naruszono dyscyplinę pracy w zakresie przestrzegania PBI (nie wylogowanie się, pozostawienie włączonego komputera po zakończeniu pracy, nie zamknięcie pokoju z komputerem, nie wykonywanie w ustalonych terminach kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.)

14) Stwierdzenie nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych, w tym także osobowych (otwarte szafy, regały, biurka).

5. Zgłaszanie incydentów

Pracownicy Urzędu mają obowiązek zgłaszać zauważone przez siebie incydenty oraz notować wszystkie szczegóły związane z incydentem. Punktem kontaktowym jest Oddział ds. Informatyki. Incydenty można zgłaszać na portalu dla pracowników na mac0 w formularzu do zgłaszania awarii, mailem do Kierownika Oddziału ds. Informatyki lub telefonicznie pod numery 13-80, 17-52, 18-51. Zgłoszenie musi zawierać:

- imię i nazwisko zgłaszającego,
- miejsce i datę wystąpienia incydentu,
- opis zdarzenia.

Zgłaszający incydent nie powinien podejmować żadnych działań na własną rękę jednak w miarę możliwości powinien zabezpieczyć materiał dowodowy, np.: robiąc zdjęcie ekranu komputera co do którego zaistniało podejrzenie, że jego działanie odbiega od normy. W przypadku podejrzenia istnienia wirusa komputerowego należy postępować zgodnie z Instrukcją w zakresie profilaktyki antywirusowej, zał nr 6 do PBI.
Zespół ds. Monitorowania Zagrożeń i Utrzymania Polityki Bezpieczeństwa Informacji ocenia poziom istotności incydentu dla Urzędu kierując się następującymi kryteriami:

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

6. Postępowanie z incydentami

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

1) Pracownik Oddziału ds. Informatyki , który przyjął zgłoszenie, powiadamia niezwłocznie kierownika oddziału lub osobę go zastępującą o fakcie i treści zgłoszenia.

2) Po analizie zdarzenia i okoliczności z nim związanych kierownik oddziału ds. Informatyki wprowadza dane o incydencie do rejestru incydentów oraz zabezpiecza materiał dowodowy. Zawiadamia członków Zespołu ds. Monitorowania Zagrożeń i Utrzymania Polityki Bezpieczeństwa Informacji.
3) Zespół zbiera się niezwłocznie, dokonuje analizy materiału dowodowego i podejmuje decyzję o sposobie dalszego postępowania. Gromadzenie materiału dowodowego:
   • dla dokumentów papierowych: oryginał jest bezpiecznie przechowywany wraz z informacją, kto znalazł dokument, gdzie, kiedy i kto by był świadkiem tego zdarzenia; każde śledztwo może wykazać, że oryginał nie został naruszony
   • dla dokumentów na nośnikach komputerowych zaleca się: utworzenie obrazu lub kopii (zależnie od stosownych wymagań) wszelkich nośników wymiennych; zaleca się zapisanie informacji znajduj znajdujących się na dyskach twardych lub w pamięci komputera, aby zapewnić ich dostępność, zaleca się zachowanie zapisów wszelkich działań podczas procesu kopiowania oraz aby proces ten odbywał się w obecności świadków; zaleca się przechowywanie
   oryginalnego nośnika i dziennika zdarzeń w sposób bezpieczny i nienaruszony (jeśli to niemożliwe, to co najmniej jeden obraz lustrzany lub kopię).
4) W przypadku stwierdzenia działań umyślnych i ustaleniu sprawcy incydentu zespół przekazuje wyniki analizy wraz z zabezpieczonym materiałem dowodowym Dyrektorowi Generalnemu w celu wyciągnięcia konsekwencji dyscyplinarnych wobec sprawcy lub podjęcia kroków prawnych wobec osób trzecich.
5) Zespół ds. Monitorowania Zagrożeń i Utrzymania Polityki Bezpieczeństwa Informacji wyciąga wnioski z każdego incydentu i określa jeśli to możliwe działania korygujące i zapobiegawcze w celu uniknięcia ponownego wystąpienia incydentu.

7. Szkolenia.

Brak wiedzy i umiejętności poprawnego rozpoznania i klasyfikacji oraz oceny poziomu istotności incydentu po stronie zgłaszającego nie może być przyczyną zaniechania powiadomienia osób odpowiedzialnych w jednostce o zaistniałym incydencie lub podejrzeniu jego wystąpienia Dlatego w miarę posiadanych zasobów, co najmniej raz do roku należy przeprowadzać okresowe szkolenia pracowników Urzędu w zakresie zarządzania incydentami. Niezależnie od prowadzonych szkoleń wskazane jest przeprowadzanie szkolenia każdego nowozatrudnionego pracownika celem zapewnienia znajomości zasad prawidłowego zgłaszania incydentów.

Załącznik nr 6
Polityki Bezpieczeństwa Informacji
Świętokrzyskiego Urzędu Wojewódzkiego
listopad 2015 r.

Instrukcja w zakresie profilaktyki antywirusowej

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

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

1. Administrator systemu wykorzystuje następujące funkcje systemowe:
   a) rejestracja i śledzenie informacji o dostępach lub próbach dostępu do zasobów i usług danego systemu.
   b) rejestracja i śledzenie komunikatów o błędach w pracy systemu.
   c) szyfrowanie i uwierzytelnianie informacji przesyłanych w sieci.
   d) wykrywanie obecności fałszywego oprogramowania w danych wpływających do systemu z sieci.
   e) kontrola integralności oprogramowania zainstalowanego w systemie.

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

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

3. Aktualizacja baz sygnatur wirusów

   a) Bazy sygnatur wirusów dla serwera są aktualizowane bezpośrednio z serwera producenta systemu antywirusowego.
   b) Bazy sygnatur wirusów dla stanowisk roboczych są aktualizowane bezpośrednio z serwera producenta systemu antywirusowego.
   c) Aktualizacja baz sygnatur wirusów odbywa się nie rzadziej niż jeden raz każdego dnia roboczego.

4. Kontrola antywirusowa.

   a) Zasoby informatyczne są skanowane na bieżąco za pomocą modułu rezydentnego. Kontroli podlegają wszystkie pliki (odczytywane i zapisywane) w tym poczta elektroniczna;
   b) System antywirusowy jest zaprogramowany do wykonywania okresowych kontroli antywirusowych całego systemu plików. Kontrole te są wykonywane przez program automatycznie nie rzadziej niż jeden raz w tygodniu;
   c) Zabrania się korzystania ze stanowiska bez aktywnego programu antywirusowego;

Zalecenia dla użytkowników stacji roboczych.

1. Zabrania się umieszczania w urządzeniach odczytujących dane na stanowisku (czytniki CD-ROM, DVD, porty USB itp.) nośników rozprowadzanych z różnego rodzaju czasopismami, materiałami reklamowymi itp.
2. Zabrania się bez zgody 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 DVD-ROM,USB itp.), wyraźnie oznaczyć i przekazać nośnik administratorowi systemu. Następnie należy sporządzić notatkę służbową ze zdarzenia i przeprowadzić kontrolę antywirusową całego systemu.
3. Po stwierdzeniu obecności wirusa w systemie przez program antywirusowy należy niezwłocznie zgłosić ten fakt do Oddziału ds. Informatyki pod numer telefonu 17-52. Zabrania się samodzielnego usuwania zainfekowanych plików.
4. Użytkownik ma obowiązek zgłaszania do WOiK wszelkich zauważonych niestandardowych zachowań systemu antywirusowego.