Załącznik nr 1
Polityki Bezpieczeństwa Informacji
Świętokrzyskiego Urzędu
Wojewódzkiego

PROCEDURA KONTROLI DOSTĘPU DO INFORMACJI

WYDANIE - 1

Wersja – 1

Spis treści

1. Cel procedury. 3
2. Zakres stosowania. 3
3. Odpowiedzialność. 3
4. Udzielanie dostępu do zasobów informatycznych. 3
   4.1. Procedura przydzielania stanowisk roboczych 3
   4.2. Procedura uzyskiwania kont 4
5. Określenie sposobu przydziału haseł dla użytkowników i częstotliwość ich zmiany oraz wskazanie osoby/osób odpowiedzialnej/odpowiedzialnych za te czynności. 5
6. Zasady postępowania dotyczące dostępu pracowników Urzędu do systemów informatycznych udostępnianych do celów służbowych przez zewnętrzne instytucje poprzez sieć Internet lub inną sieć rozległą. 6
7. Kontrola dostępu do sieci komputerowej. 6
8. Zasady postępowania dotyczące pracy na odległość oraz urządzeń przenośnych i nośników danych wynoszonych poza siedzibę Urzędu. 6
9. Kontrola dostępu do pomieszczeń technicznych oraz serwerowni. 7
10. Przegląd uprawnień do systemów. 8

1. Cel procedury.

Celem procedury 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 procedura 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 do Wydziału Organizacji i Kadr w przypadku zmiany danych podanych we wniosku w terminie 7 dni od wystąpienia zdarzenia powodującego zmianę.

4.2.1.2 Złożyć wniosek do Wydziału Organizacji i Kadr 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.
3. Oddział Zarządzania Zasobami jest zobowiązany informować administratora systemu o zmianach kadrowych w Urzędzie.

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 procedurze 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 Kierownika Oddziału ds. Informatyki. 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 technicznych oraz 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. Zasada ta dotyczy także osób sprzątających. 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 309, 310, 311,312,313,314. W strefie wydzielonej stosuje się następujące mechanizmy bezpieczeństwa:

a) gwarantowane zasilanie z centralnym UPS-em i agregatem prądotwórczym,
b) odrębna klimatyzacja oraz kontrola temperatury,
c) system automatycznego gaszenia gazem dla pomieszczeń serwerowni,
d) drzwi zewnętrzne przeciwwłamaniowe posiadające zabezpieczenie wejścia na kartę,
e) drzwi wewnętrzne otwierane na PIN.

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 technicznych oraz serwerowni ŚUW pod warunkiem, że zasady ich

umieszczania i użytkowania będą szczegółowo określone w porozumieniach i umowach zawieranych z tymi podmiotami.

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

Klucze do serwerowni i pomieszczeń technicznych oraz klucze do szaf w pomieszczeniach technicznych są w dyspozycji uprawnionych pracowników Oddziału ds. Informatyki.

Uprawnieni pracownicy Oddziału ds. Informatyki prowadzą rejestr dostępu do serwerowni oraz pomieszczeń technicznych.

10. Przegląd 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 SZBI 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 1
Procedury Kontroli Dostępu

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. Adres IP stanowiska *(wypełnia WOiK):*

---

5. 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
Procedury Kontroli Dostępu

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