INSTRUKCJA
bezpieczeństwa systemów informatycznych UKSW

Spis treści

POSTANOWIENIA OGÓLNE

§ 1

1. Instrukcja, obejmuje swoim zakresem wszystkie osoby biorące udział w procesie przetwarzania informacji w UKSW, a w szczególności:
   1) ABI;
   2) LA;
   3) ASI;
   4) bezpośrednich przełożonych osób przetwarzających dane osobowe;
   5) inne osoby wskazane przez ADO.
2. Instrukcja ma zastosowanie także, do podmiotów zewnętrznych i osób fizycznych, które współpracują z UKSW i na podstawie przepisów współuczestniczą w procesie przetwarzania informacji, a w szczególności:
   1) podmiotów, którym na podstawie przepisów prawa udostępniono dane osobowe;
   2) podmiotów, którym na podstawie umowy powierzono lub udostępniono dane osobowe do przetwarzania;
   3) przedsiębiorców świadczący usługi związane z konserwacją systemu informatycznego;
   4) innych osób, niebędących pracownikami Uczelni, wykonujących czynności na podstawie umów cywilnoprawnych.

PROCEDURA NADAWANIA UPRAWNIEŃ DO SYSTEMU

§ 2

1. Dostęp i uprawnienia do Systemu są przydzielane i odwoływane na podstawie wniosku, generowanego za pomocą generatora wniosków i kierowany do właściwego LA, który z kolei:
   1) po wydaniu pozytywnej opinii przekazuje wniosek do ABI, w przypadku wniosku o nadanie, cofnięcie lub modyfikację uprawnień do przetwarzania informacji szczególnie chronionych, zgodnie z § 15 pkt 4 pkt e Polityki bezpieczeństwa informacji;
   2) po dokonaniu akceptacji wniosku o nadanie, cofnięcie lub modyfikację uprawnień do przetwarzania informacji szczególnie chronionych, zgodnie z § 15 pkt 4 pkt a, b, c, d i w przypadku wniosku o nadanie, cofnięcie lub modyfikację uprawnień do danych nie stanowiących danych poufnych, przekazuje go do realizacji CASI.

§ 3

1. Uprawnienia **użytkownika** do pracy w systemach informatycznych, w których przetwarzane są dane osobowe, obejmują w swym zakresie dostęp do baz danych w jednostce organizacyjnej, w której użytkownik jest zatrudniony, w tym:
   1) odczyt danych;
   2) wprowadzanie i edycja danych;
   3) modyfikację istniejących danych;
   4) wydruk danych;
   5) usuwanie danych ze zbiorów swojej jednostki organizacyjnej;
   6) przekazywanie danych wewnątrz jednostki organizacyjnej.
2. Uprawnienia **użytkownika uprzywilejowanego** do pracy w systemach informatycznych, zastosowanym do przetwarzania danych osobowych, w jednostce w której użytkownik nie jest zatrudniony, mogą obejmować uprawnienia, o których mowa w ust. 2 oraz:
   1) dostęp do baz danych innych jednostek organizacyjnych;

2) udostępnianie danych podmiotom i osobom, o których mowa w § 1 ust. 2;

3) użytkowanie komputera przenośnego.

§ 4

1. CASI odbiera lub ogranicza uprawnienia użytkownika na wniosek przełożonego użytkownika, zgodnie z zapisem w § 2 niniejszej instrukcji, po zmianie lub utracie upoważnienia dostępu do danych, które może nastąpić w przypadku:

   1) ustania zatrudnienia użytkownika w UKSW;

   2) zmiany zakresu obowiązków służbowych użytkownika;

   3) oddelegowania lub przeniesienia pracownika do innej jednostki organizacyjnej.

2. W przypadku rozwiązania stosunku pracy lub zmiany zakresu obowiązków służbowych użytkownika, która spowoduje brak konieczności posiadania przez użytkownika dostępu do Systemu, dotychczasowy bezpośredni przełożony użytkownika zobowiązany jest powiadomić niezwłocznie o tym fakcie ASI, który zobowiązany jest niezwłocznie wyłączyć aktywność konta użytkownika w Systemie. Konta użytkowników w Systemie przechowywane są bezterminowo.

2. W przypadku zmiany zakresu obowiązków służbowych użytkownika, powodującej konieczność zmiany zakresu uprawnień lub roli użytkownika w Systemie, przełożony użytkownika zobowiązany jest złożyć nowy wniosek o dostęp użytkownika do Systemu, zawierający nowy zakres wnioskowanych uprawnień lub wskazanie nowej roli w Systemie. Po akceptacji ww wniosku zgodnie z ust. 2, CASI modyfikuje odpowiednio uprawnienia użytkownika w Systemie.

METODY UWIERZYTELNIANIA

§ 5

1. System, w szczególności w którym przetwarza się dane osobowe, wyposażony jest w mechanizmy uwierzytelnienia użytkownika oraz kontroli dostępu osób. Jednym z elementów umożliwiających dostęp do systemu jest weryfikacja loginu i hasła użytkowników, które pełni rolę weryfikatora tożsamości użytkownika.
2. Hasło dostępu składa się z ciągu znaków literowych, cyfrowych lub innych i nie może kojarzyć się bezpośrednio z użytkownikiem. Hasła dostępu nie powinny powtarzać się w danym roku.
3. Hasło dostępu wyświetlane jest na ekranie monitora w formie niejawnej i znane jest tylko użytkownikowi.
4. Hasło dostępu do systemu, o którym mowa w ust. 1, powinno być tworzone zgodnie z zasadami:
   1) powinno składać się z co najmniej 8 znaków oraz znaków specjalnych;
   2) nie może posiadać prostej formy, np.: 1234556789, itp.
5. W systemie informatycznym, w którym hasło użytkownika nie jest zmieniane cyklicznie przez CASI, użytkownik powinień zmieniać swoje hasło, co najmniej raz w miesiącu.
6. W wypadku podejrzenia lub stwierdzenia ujawnienia hasła użytkownik ma obowiązek niezwłocznie je zmienić.
7. Hasła dostępu do baz danych są różne od haseł uwierzytelniających użytkowników w systemie z wyjątkiem systemów informatycznych, gdzie stosowana jest tzw. autoryzacja domenowa użytkownika. W tym przypadku uwierzytelnienie użytkowników w systemie jest równoznaczne z dostępem do baz danych.

§ 6

1. Identyfikator przyznaje się użytkownikom w przypadku dostępu do systemu informatycznego upoważnionej osoby, która nie jest pracownikiem UKSW.

2. Identyfikator użytkownika składa się z ciągu znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujących w systemie osobę upoważnioną do przetwarzania danych osobowych.
3. Identyfikator użytkownikowi przyznaje CASI, za zgodą ABI.
4. Podczas przetwarzania danych osobowych w systemie posługiwanie się identyfikatorem innej osoby jest zabronione.
5. Użytkownik, o którym mowa w ust. 1 ponosi odpowiedzialność za czynności wykonywane w systemie przy użyciu jego identyfikatora i hasła.
6. Hasło nie może być przechowywane w taki sposób, aby mogły się z nim zapoznać osoby nieuprawnione w szczególności nie może ono zostać nigdzie zapisane w postaci jawnej.
7. ADO dopuszcza możliwość stosowania do weryfikacji tożsamości użytkowników w systemie innych sposobów np.: karty mikroprocesorowe lub metody biometryczne.
8. CASI odpowiada za prawidłowe funkcjonowanie mechanizmów uwierzytelniających w systemie.

ZASADY PRACY W SYSTEMIE

§ 7

1. Użytkownicy rozpoczynający pracę zobowiązani są do przestrzegania procedur mających na celu sprawdzenie działania systemu, a w szczególności:
   1) sprawdzenie ogólnego stanu urządzeń i miejsca przechowywania nośników zawierających dane osobowe;
   2) po włączeniu urządzeń sprawdzenie i dokonanie oceny jakości ich pracy.
2. Użytkownik przystępując do przetwarzania danych powinien zalogować się w systemie zgodnie z poleceniami wyświetlanymi na ekranie monitora, posługując się swoim loginem lub identyfikatorem i hasłem wiedząc, że dostęp do przyznanych zasobów i systemu jest możliwy z wydzielonego obszaru sieciowego właściwego dla jednostki organizacyjnej.
3. Przetwarzając dane osobowe w systemie użytkownik zobowiązany jest do wykonywania czynności mających na celu zapewnienie im bezpieczeństwa poprzez:
   1) ustawienie monitorów w sposób uniemożliwiający osobom nieupoważnionym podgląd ekranów;
   2) zablokowanie komputera w przypadku, kiedy przerwa w pracy użytkownika w systemie trwa dłużej niż 15 minut, ponowne logowanie jest zabezpieczone hasłem, znanym tylko użytkownikowi;
   3) wylogowanie się z systemu, kiedy przerwa w pracy użytkownika w systemie trwa dłużej niż 30 minut.
4. Po zakończeniu pracy w systemie użytkownik zobowiązany jest:
   1) zapisać wszelkie zmiany w opracowywanych dokumentach;
   2) zamknąć wszystkie używane programy;
   3) zamknąć system przez polecenie „Zamknij system" i zaczekać na jego wyłączenie;
   4) sprawdzić, czy elektroniczne nośniki informacji zawierające dane osobowe nie zostały pozostawione bez nadzoru.

PROCEDURA TWORZENIA I PRZECHOWYWANIA KOPII ZAPASOWYCH

§ 8

1. W celu zapewnienia bezpieczeństwa przetwarzania danych osobowych istnieje obowiązek tworzenia kopii zapasowych.
2. Kopie zapasowe tworzy się według potrzeb, na odpowiedniej jakości nośnikach informacji metodą przyrostową i całościową.
3. Kopie zapasowe tworzy się wykorzystując narzędzia programowe i urządzenia systemu do tego przystosowane. Kopie zapasowe wykonuje CASI, zgodnie z zasadami zawartymi w Polityce bezpieczeństwa.

§ 9

1. Elektroniczne nośniki informacji zawierające dane oraz wydruki przechowuje się wewnątrz obszaru przetwarzania danych, w szafach i pomieszczeniach posiadających zamknięcia. Nośniki i wydruki nie powinny być wynoszone poza obszar przetwarzania danych bez zgody przełożonego.
2. Kopie zapasowe przechowuje się w szafach metalowych w pomieszczeniach, które zapewniają właściwą ochronę przed nieuprawnionym dostępem, modyfikacją uszkodzeniem lub zniszczeniem.
3. Czas przechowywania kopii zapasowych zależy od aktualności zapisanych danych oraz potrzeby tworzenia kolejnych kopii.

§ 10

1. Kopie zapasowe i elektroniczne nośniki informacji, które zostały uszkodzone lub przeznaczone do likwidacji należy niszczyć mechanicznie pod nadzorem CASI, w sposób uniemożliwiający ich ponowne użycie.
2. Niepotrzebne wydruki z systemu, które zawierają dane osobowe należy niszczyć w niszczarkach w sposób uniemożliwiający ich odtworzenie.

§ 11

1. Przekazanie i niszczenie elektronicznych nośników informacji zawierających dane osobowe, odbywa się na podstawie protokołu sporządzanego i podpisanego przez ASI oraz wskazanych użytkowników.
2. Kopię protokołu zatwierdzonego przez przełożonego użytkownika należy przesłać do ABI.

§ 12

1. Na czas trwania transportu nośniki, kopie i wydruki, o których mowa w § 9 ust. 1 i 2, umieszcza się w trwałych opakowaniach i chroni przed utratą zniszczeniem lub uszkodzeniem. Przenosić lub przewozić mogą tylko osoby do tego upoważnione.
2. Urządzenia, elektroniczne nośniki informacji i wydruki z systemu zawierające dane wrażliwe, przekazywane poza obszar ich przetwarzania zabezpiecza się w sposób zapewniający poufność, integralność i rozliczalność tych danych.
3. Osoby użytkujące komputery przenośne, które są wykorzystywane do przetwarzania danych osobowych, zobowiązane są do stosowania właściwych zabezpieczeń technicznych oraz zachowania szczególnej ostrożności podczas ich transportu i przechowywania.

SPOSÓB ZABEZPIECZENIA DANYCH OSOBOWYCH W SYSTEMIE INFORMATYCZNYM

§ 13

1. System, w którym przetwarzane są dane osobowe jest wyposażony w mechanizmy ochrony antywirusowej.
2. Obszarami systemu narażonymi na ingerencję wirusów oraz innego szkodliwego oprogramowania są dyski twarde urządzeń i pamięć RAM oraz elektroniczne nośniki informacji.
3. Drogą przedostania się wirusów lub szkodliwego oprogramowania może być sieć publiczna, wewnętrzna sieć teleinformatyczna lub elektroniczne nośniki informacji.
4. Kontrola antywirusowa obejmuje urządzenia oraz wszelkiego rodzaju nośniki służące do przetwarzania danych.
5. Obowiązkiem CASI jest zarządzanie bazą antywirusową, w tym określanie warunków działania oprogramowania przy zachowaniu maksymalnej efektywności i minimalizacji jej negatywnego wpływu na korzystanie przez użytkowników z systemu, a w szczególności:
   1) instalowanie i konfigurowanie modułów bazy antywirusowej;
   2) uaktualnianie sygnatur w bazie antywirusowej;
   3) dostosowywanie czasu pracy urządzeń systemu do określonego w UKSW czasu pracy użytkowników.

§ 14

1. System posiada zabezpieczenia przed działaniem oprogramowania mającego na celu uzyskanie nieuprawnionego dostępu do danych.
2. CASI ma obowiązek realizacji przedsięwzięć mających na celu wdrażanie technicznych i logicznych zabezpieczeń chroniących system przed nieuprawnionym dostępem do danych.
3. Nadzór nad czynnościami, o których mowa w ust. 2, sprawuje Kierownik Centrum Systemów Informatycznych.

§ 15

1. System, w którym przetwarzane są dane osobowe posiada mechanizmy pozwalające zabezpieczyć je przed utratą lub nieautoryzowaną zmianą spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.
2. Dane osobowe przetwarzane w systemie chroni się stosując filtry zabezpieczające przed skutkami spadku napięcia oraz urządzenia podtrzymujące zasilanie do momentu poprawnego zapisania danych i wylogowania się użytkownika z systemu.
3. Dane osobowe przetwarzane w bazach umieszczonych na serwerach zabezpiecza się przed zanikiem napięcia wykorzystując centralne UPS.

§ 16

1. ADO lub z upoważnienia ADO – ABI, na wniosek CASI może wprowadzić alternatywne metody ochrony przed szkodliwym działaniem programów mających na celu uzyskanie nieuprawnionego dostępu do danych.
2. Do alternatywnych metod ochrony zalicza się:
   1) odłączenie systemu od sieci publicznej oraz urządzeń umożliwiających odczyt danych z elektronicznych nośników informacji na określonych stanowiskach komputerowych;
   2) tworzenie indywidualnych stanowisk komputerowych, które spełniają wymogi bezpieczeństwa przetwarzania danych osobowych na poziomie wysokim;
   3) zastosowanie w urządzeniach kart PCI (Recovery Card), itp.

WYMOGI DOTYCZĄCE PRZETWARZANIA DANYCH W SYSTEMIE

§ 17

1. ADO zapewnia ochronę obszarów, w których są przetwarzane dane osobowe w UKSW, zgodnie z zasadami określonymi w Polityce bezpieczeństwa.
2. Do obszarów podlegających szczególnej ochronie zalicza się serwerownie i pomieszczenia, w których przetwarzane są dane wrażliwe.
3. Osobom, których dane są przetwarzane w systemie, ASI może udostępnić informacje dotyczące:
   1) daty pierwszego wprowadzenia danych do systemów;
   2) identyfikatora użytkownika wprowadzającego dane osobowe do systemu chyba, że dostęp do systemu posiada tylko jedna osoba;
   3) źródła danych, w przypadku zbierania danych nie od osoby, której one dotyczą;
   4) informacji o odbiorcach, którym dane osobowe zostały udostępnione (data i zakres udostępnienia) chyba, że system używany jest do przetwarzania danych w zbiorach jawnych.
4. Odnotowywanie w systemie informacji, o których mowa w ust. 3 pkt. 1-2 następuje automatycznie, po zatwierdzeniu przez użytkownika operacji wprowadzania danych.
5. System zapewnia każdej osobie, której dane są przetwarzane, wydrukowanie raportu zawierającego w zrozumiałej formie informacje, o których mowa w ust. 3.
6. Dane osobowe przetwarzane w systemie przechowywane są nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania tych danych. W każdym przypadku, gdy cel przetwarzania danych osobowych został osiągnięty dane te podlegają niezwłocznemu usunięciu.

ZABEZPIECZENIE JEDNOSTEK KOŃCOWYCH PRZED DZIAŁANIEM ZŁOŚLIWEGO KODU

§18

1. Za zabezpieczenie Systemu przed złośliwym kodem (np.: wirusami komputerowymi, końmi trojańskimi, oprogramowaniem szpiegującym, kradnącym dane lub hasła dostępu) na komputerach użytkowników odpowiada CASI.
2. Niedozwolone jest samodzielne instalowanie przez użytkownika na jego komputerze oprogramowania zabezpieczającego bez zgody CASI.
3. Niedozwolone jest wyłączanie, blokowanie i odinstalowywanie programów zabezpieczających komputer przed złośliwym kodem oraz nieautoryzowanym dostępem z zewnątrz (np.: skanerów, programów antywirusowych, zapór firewall).

PRZEGLĄD, KONSERWACJA I ZGŁASZANIE AWARII SYSTEMU

§ 19

Wykonywanie przeglądów i konserwacji systemu i nośników danych ma na celu:

1) sprawdzenie działania technicznych zabezpieczeń;
2) sprawdzenie funkcjonalności i jakości pracy;
3) sprawdzenie i określenie przydatności elektronicznych nośników informacji;
4) zakwalifikowanie urządzeń do naprawy.

§ 20

Zgłoszenia błędów i awarii w systemie informatycznym dokonywane są zgodnie z § 8 Regulaminu korzystania z zasobów informatycznych UKSW stanowiącym załącznik do Zarządzenia Nr 17/2010 Rektora UKSW z dnia 8 kwietnia 2010 r. w sprawie zawierania umów o odpowiedzialności materialnej z pracownikami korzystającymi z komputerów z uprawnieniami administratora oraz regulaminu korzystania z zasobów informatycznych.