Załącznik Nr 1 do Zarządzenia Nr 34/2017 Rektora UKSW z dnia 02 czerwca 2017 r.
w sprawie wprowadzenia Polityki bezpieczeństwa informacji w UKSW

POLITYKA
BEZPIECZEŃSTWA INFORMACJI UNIWERSYTETU KARDYNAŁA STEFANA WYSZYŃSKIEGO W WARSZAWIE

SPIS TREŚCI

DEFINICJA I STRATEGIA POLITYKI BEZPIECZEŃSTWA

§ 1

1. Polityka bezpieczeństwa określa podstawowe zasady zarządzania bezpieczeństwem zbiorów danych, informacji i bezpieczeństwem systemów, w których zbiory danych i informacje są lub mogą być przetwarzane.
2. Polityka bezpieczeństwa ma na celu osiągnięcie takiego poziomu organizacyjnego i technicznego systemu zarządzania bezpieczeństwem informacji, który:
   1) będzie gwarantem pełnej ochrony informacji oraz ciągłości procesu ich przetwarzania;
   2) zapewni zachowanie poufności informacji chronionych, integralności i dostępności informacji chronionych oraz jawnych;
   3) zagwarantuje odpowiedni poziom bezpieczeństwa informacji, bez względu na jej postać, we wszystkich systemach, w których jest jej przetwarzana;
   4) maksymalnie ograniczy występowanie zagrożeń dla bezpieczeństwa informacji, które wynikają z celowej bądź przypadkowej działalności człowieka oraz ich ewentualnego wykorzystania na szkodę UKSW;
   5) zapewni poprawne i bezpieczne funkcjonowanie wszystkich systemów przetwarzania informacji;
   6) zapewni gotowość do podjęcia działań w sytuacjach kryzysowych dla bezpieczeństwa UKSW, jego interesów oraz posiadanych i powierzonych mu informacji.
3. Polityka bezpieczeństwa ma zastosowanie do wszystkich jednostek organizacyjnych uczelni i obowiązkiem jej pracowników jest przestrzeganie postanowień niniejszego dokumentu.

§ 2

Polityka bezpieczeństwem informacji ma zapewnić w Uczelni następujące reguły:

1) poufności - zapewnienie dostępu do informacji wyłącznie podmiotom upoważnionym;
2) integralności - zapewnienia dokładności i kompletności danych i informacji oraz określenie metod ich przetwarzania;
3) dostępności informacji - zapewnienia, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów tylko wtedy, gdy zachodzi taka potrzeba;
4) rozliczalności - zapewnienia przechowywania pełnej historii dostępu do danych wraz z informacją kto taki dostęp posiada lub posiadał i w jakim zakresie.

§ 3

Cele, o których mowa w § 1 ust. 2 realizowane są w oparciu o zasady:

1) minimalizacji uprawnień, tzn. każdy pracownik powinien posiadać tylko takie uprawnienia jakie są wymagane do realizacji jego obowiązków;
2) wielowarstwowych zabezpieczeń, tzn. system informatyczny podlega ochronie równolegle na wielu poziomach;
3) ograniczania dostępu, tzw. domyślnym uprawnieniem w systemach informatycznych jest „zabroniony dostęp”. Dopiero w przypadku zaistnienia odpowiedniej potrzeby, przyznawane są stosowne uprawnienia.

DEKLARACJA INTENCJI

§ 4

Niniejsza polityka wyraża stanowisko władz Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie, realizującego zadania publiczne w zakresie zarządzania bezpieczeństwem informacji. W celu zapewnienia właściwej ochrony informacji własnych i powierzonych UKSW, władze UKSW deklarują zapewnienie im cech: poufności, integralności, dostępności i rozliczalności poprzez podejmowanie działań:

1) niezbędnych do adekwatnego zabezpieczenia informacji gromadzonych i przetwarzanych w Uniwersytecie;
2) w zakresie stałego podnoszenia świadomości pracowników przetwarzających informacje;
3) w zakresie egzekwowania właściwego wykonywania obowiązków pracowniczych od osób zatrudnionych przy przetwarzaniu informacji.

ZAKRES POLITYKI BEZPIECZENSTWA

§ 5

1. Polityka bezpieczeństwa informacji ma zastosowanie do całego mechanizmu informacyjnego uczelni i obejmuje:
   1) wszystkie istniejące, wdrażane obecnie lub w przyszłości systemy informatyczne oraz tradycyjne (papierowe), w których przetwarzane są lub będą informacje;
   2) informacje będące własnością uczelni;
   3) informacje będące własnością kontrahentów, które zostały przekazane uczelni na podstawie zawartych umów;
   4) wszystkie typy nośników, na których są lub będą znajdować się informacje;
   5) wszystkie lokalizacje uczelni, budynki i pomieszczenia, w których są lub będą przetwarzane informacje;
   6) wszystkich pracowników uczelni w rozumieniu Kodeksu Pracy, kontrahentów, stażystów, praktykantów i innych osób mających dostęp do informacji, na zasadach określonych w niniejszej polityce bezpieczeństwa.
2. Dane i informacje mogą być przetwarzane wyłącznie w miejscu i systemach, które spełniają warunki opisane w niniejszej polityce bezpieczeństwa.

OBOWIĄZKI I ODPOWIEDZIALNOŚĆ

§6

1. Rektor odpowiada za wykonanie obowiązków Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie, jako Administrator Danych Osobowych (ADO).
2. Odpowiedzialność za bezpieczeństwo informacji w UKSW ponoszą wszyscy pracownicy zgodnie z posiadanym zakresem obowiązków. Rektor UKSW jest odpowiedzialny za zapewnienie zasobów niezbędnych do funkcjonowania, utrzymania i doskonalenia procedur zarządzania bezpieczeństwem informacji.
3. Rektor, przewidziane w Ustawie o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922), zwanej w dalszej treści dokumentu „ustawą”, zadania dla podmiotu publicznego, o którym mowa w ust. 1, powierza na mocy upoważnienia:
   1) dyrektorowi Biblioteki Głównej;
   2) dyrektorowi Wydawnictwa Naukowego Uniwersytetu;

3) kanclerzowi;
4) kierownikowi Działu Kadr;
5) kierownikowi Działu Kształcenia;
6) kierownikowi Działu Pomocy Materialnej dla Studentów;
7) kwestorowi.

4. Osoby, wymienione w ust. 3 pełnią funkcję Lokalnych Administratorów (LA).
5. Zadania Centralnego Administratora Systemu Informatycznego (CASI), zgodnie z regulaminem działania jednostki, realizuje Centrum Systemów Informatycznych UKSW.
6. Zadania zarządzania systemem informatycznym lub wydzielonym jego modułem realizuje Administrator Systemu Informatycznego (ASI) - osoba lub zespół osób - wyznaczony zgodnie z Instrukcją bezpieczeństwa systemów informatycznych, stanowiąca **załącznik nr 1** do niniejszej polityki.
7. Proces zarządzania bezpieczeństwem jest działaniem ciągłym i realizowanym przy współpracy użytkowników systemów informatycznych z Administratorem Bezpieczeństwa Informacji (ABI) oraz CASI.

§ 7

Do zadań LA przy zachowaniu ścisłej współpracy z ABI i CASI należy:

1) określanie indywidualnych obowiązków i odpowiedzialności osób zatrudnionych przy przetwarzaniu danych osobowych, wynikających z ustawy o ochronie danych osobowych;
2) zapewnienie dostępu osobom zatrudnionym przy przetwarzaniu danych osobowych do obowiązujących w tym zakresie przepisów;
3) wykonywanie zaleceń ABI w zakresie ochrony danych osobowych i baz danych w systemach informatycznych funkcjonujących w podległych im jednostkach;
4) prowadzenie dokumentacji odzwierciedlającej wykonywanie zadań z zakresu ochrony danych osobowych i baz danych, która obejmuje:
   a) prowadzenie ewidencji baz danych, w których przetwarzane są dane osobowe;
   b) prowadzenie ewidencji osób zatrudnionych przy przetwarzaniu danych osobowych w systemach informatycznych i ich identyfikatorów;
   c) prowadzenia ewidencji ASI odpowiedzialnych za zarządzanie systemem informatycznym lub jego wydzielonym modułem;
   d) prowadzenie ewidencji miejsc (budynków i pomieszczeń) przetwarzania danych osobowych oraz informacji o sposobie ich zabezpieczania;
5) zapewnienie warunków organizacyjnych i technicznych umożliwiających spełnienie wymogów wynikających z ustawy, o której mowa w § 6 ust. 3, w podległych jednostkach oraz zatwierdzanie ról i zakresu uprawnień definiowanych w nadzorowanym systemie informatycznym, w porozumieniu z ABI i CASI.

§ 8

LA są zobowiązani do przekazywania do ABI bieżącej informacji dotyczącej:

1) wykazu baz danych, w których przetwarzane są dane osobowe;
2) wykazu osób zatrudnionych przy przetwarzaniu danych osobowych w systemach informatycznych i ich identyfikatorów;
3) wykazu miejsc (budynków i pomieszczeń) przetwarzania danych osobowych i sposobu ich zabezpieczania;

4) ocen i wniosków wynikających z zagrożeń bezpieczeństwa i analizy stanu ochrony obszarów przetwarzania danych osobowych.

§ 9

Do obowiązków CASI należy:

1) nadawanie, ograniczanie lub cofanie kont, uprawnień i ról użytkownikom systemów, w tym wyznaczanie ASI;
2) zakładanie, modyfikacja, usuwanie baz danych;
3) migracja danych pomiędzy bazami;
4) zabezpieczanie danych w sposób uniemożliwiający nieautoryzowany do nich dostęp, w bazach danych;
5) wykonywanie kopii zapasowych i archiwizowanie baz danych;
6) zarządzanie bazą antywirusową;
7) realizację zadań mających na celu wdrażanie technicznych i logicznych zabezpieczeń chroniących system przed nieuprawnionym dostępem do danych oraz reagowanie w sytuacji naruszenia lub zagrożenia bezpieczeństwa danych przetwarzanych w systemie;
8) instalowanie, aktualizowanie i konfigurowanie oprogramowania systemowego i aplikacyjnego oraz urządzeń, o ile czynności te nie są wykonywane przez dostawcę systemu na podstawie zawartej umowy;
9) przygotowywanie urządzeń i elektronicznych nośników informacji zawierających dane osobowe, do likwidacji, przekazania innemu podmiotowi w celu konserwacji lub naprawy;
10) przekazywania do ABI opisów struktur zbiorów danych, schematów przepływu danych pomiędzy systemami, zawartości poszczególnych pól informacyjnych w aplikacjach oraz wszelkich zmian zachodzących w tym zakresie;
11) natychmiastowe reagowanie i informowanie ABI o zdarzeniach, o których mowa w pkt. 7;
12) wykonywanie bieżącej konserwacji i przeglądu systemu.

§ 10

Do obowiązków ASI należy:

1. wykonywanie poleceń ABI i LA w zakresie zarządzania podległymi systemami informatycznymi lub ich wydzielonymi modułami;
2. prowadzenia, w nadzorowanych przez nich systemach bieżącej ewidencji:
   1) osób oraz ich identyfikatorów uczestniczących w przetwarzaniu danych osobowych;
   2) ról i uprawnień osób posiadających dostęp podglądu i edycji danych nie związanych przetwarzaniem danych osobowych;
   3) zdarzeń wpływających na bezpieczeństwo systemów informatycznych, w tym stwierdzenia faktu korzystania z systemu informatycznego przez osobę niepowołaną lub awarii;
3. kontrolowania prawidłowego przebiegu czynności serwisowych w nadzorowanych systemach informatycznych zawierających dane osobowe;
4. reagowanie na zdarzenia związane z naruszeniem zasad i bezpieczeństwa ochrony danych osobowych, o których mowa w ust. 2 pkt 2 i postępowanie zgodnie z obowiązującą w tym zakresie procedurą.

§ 11

1. Rektor wyznacza Administratora Bezpieczeństwa Informacji (ABI), do którego głównych zadań należy:
   1) koordynowanie działań w zakresie określonym w § 5;
   2) wydawanie w imieniu ADO zgody na przyznanie uprawnień do przetwarzania danych osobowych lub dokonuje jej cofnięcia, ograniczenia lub odmowy;
   3) przygotowywanie projektów wytycznych ADO w zakresie ochrony danych osobowych;
   4) nadzorowanie opracowania i aktualizowania dokumentacji odzwierciedlającej wykonywanie zadań z zakresu ochrony danych osobowych i baz danych, prowadzonej przez LA i kierowników jednostek organizacyjnych;
   5) zgłaszanie i aktualizowanie zbiorów wrażliwych danych osobowych do rejestracji w GIODO;
   6) prowadzenie rejestru zbioru danych przetwarzanych przez ADO, zgodnie z art. 36a ust. 2 pkt 2 ustawy, o której mowa w § 6 ust. 4, zawierającego nazwę zbioru oraz informacje, o których mowa w art. 41 ust. 1 pkt 2 – 4 a i 7 ustawy;
   7) prowadzenie planowych rocznych sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych i przedstawianie ADO sprawozdania z ich wykonania;
   8) prowadzenie na podstawie upoważnienia ADO korespondencji z GIODO;
   9) przekazywanie ADO informacji dotyczących naruszeń bezpieczeństwa ochrony danych.
2. ABI w celu zapewnienia właściwej ochrony danych współpracuje z LA i CASI.

§ 12

1. Do przetwarzania danych osobowych dopuszczone są wyłącznie osoby posiadające stosowne upoważnienie ADO.
2. Upoważnienia, o których mowa w ust. 1 podlegają rejestracji w Centralnym Rejestrze Pełnomocnictw i Upoważnień.
3. Dział Kadr zobowiązany jest do bieżącego uzupełniania akt osobowych pracowników UKSW zatrudnionych przy przetwarzaniu danych osobowych o:
   1) imienne upoważnienia do dostępu i przeważania danych zgromadzonych w systemie tradycyjnym lub bazie danych w systemie informatycznym;
   2) „deklarację zachowania tajemnicy służbowej”.

§ 13

1. Kierownicy jednostek organizacyjnych UKSW występują do właściwych LA, o których mowa w § 6 ust. 4 z wnioskiem o nadanie, cofnięcie lub zmianę upoważnienia do przetwarzania danych osobowych oraz ról w systemach informatycznych.
2. Kierownicy jednostek organizacyjnych UKSW zobowiązani są do bieżącego przekazywania do LA informacji o zmianach w lokalizacji miejsc przetwarzania danych osobowych, wydanych lub unieważnionych upoważnieniach i rolach w systemach informatycznych oraz o wykazach przetwarzanych zbiorów w terminie do 14 dni od dokonania zmian.

OZNACZANIE I KLASYFIKACJA ZASOBÓW INFORMACYJNYCH

§14

1. UKSW jest podmiotem zarządzającym zasobami informacji i infrastrukturą niezbędną do przetwarzania informacji w jednostkach organizacyjnych uczelni.

2. Informacje przetwarzane i przechowywane w systemie teleinformatycznym uczelni, nie są objęte prawem do prywatności, jakie przewiduje Konstytucja Rzeczpospolitej Polskiej, ze szczególnym uwzględnieniem zasobów gromadzonych na komputerach użytkowników oraz poczty elektronicznej.
3. Korzystanie z zasobów informacji innych niż wytworzone w uczelni, wymaga posiadania odpowiednich praw autorskich, dowodów zakupu, aktów darowizny itp. do tych zasobów. W szczególny sposób dotyczy to oprogramowania, baz danych, patentów.
4. Klasyfikacji informacji, oceny ich istotności dla Uniwersytetu oraz wskazania mechanizmów ich ochrony dokonuje ABI, zgodnie z zasadami zawartymi w niniejszej Polityce bezpieczeństwa informacji.
5. Za każdy zasób informacji uczelni odpowiada kierownik jednostki organizacyjnej, odpowiednio do swoich kompetencji wynikających z Regulaminu Organizacyjnego UKSW i posiadanego zakresu obowiązków.

§ 15

Informacje gromadzone i przetwarzane w UKSW podlegają inwentaryzacji i klasyfikacji w „aktywa informacyjne", według następujących kategorii:

1) informacje jawne – informacje publicznie dostępne;
2) informacje wewnętrzne – informacje, których przetwarzanie i udostępnianie podlega restrykcjom ze względu na szczególne znaczenie dla UKSW, jako właściciela informacji:
   a) informacje wewnętrzne – dostępne dla wszystkich pracowników uczelni;
   b) informacje wewnętrzne wrażliwe – dostępne dla grupy pracowników upoważnionych ze względu na stanowisko, funkcję lub na wykonywany zakres obowiązków służbowych;
   c) informację stanowiące tajemnicę UKSW – informacje, których przetwarzanie i ujawnianie może narazić UKSW na szkodę:
3) informacje niejawne – informacje, do których stosuje się przepisy o ochronie informacji niejawnych lub o ochronie danych osobowych lub innych tajemnic prawnie chronionych.
4) informacje podlegające szczególnej ochronie oznaczają:
   a) informacje o realizowanych kontraktach (zarówno planowane, bieżące jak i historyczne);
   b) informacje finansowe uczelni;
   c) informacje organizacyjne;
   d) dane dostępowe do systemów IT;
   e) dane osobowe;
   f) informacje stanowiące o przewadze konkurencyjnej;
   g) inne informacje oznaczone jako „informacje wrażliwe" lub „dane wrażliwe";
   h) oznaczone jako „zastrzeżone".

§ 16

1. Informacje gromadzone i przetwarzane w sposób o, o którym mowa w § 15 posiadają trzystopniową skalę bezpieczeństwa:
   1) Wrażliwość „W" - ze względu na rozmiar szkód, które mogłoby wywołać ich ujawnienie nieuprawnionym osobom lub instytucjom:
      a) W1 (poziom niski) – dotyczy informacji, które mogą być publicznie znane lub, których ujawnienie nie powoduje lub powoduje niewielkie konsekwencje natury prawnej lub finansowej;

b) W2 (poziom średni) – dotyczy informacji, których ujawnienie może wiązać się z poważnymi konsekwencjami natury prawnej lub finansowej. Do tej grupy zaliczymy również dane osobowe;

c) W3 (poziom wysoki) – informacje krytyczne których ujawnienie mogłoby zagrozić funkcjonowaniu Uniwersytetu lub spowodować bardzo poważne szkody natury prawnej lub finansowej. Do tej grupy zaliczamy również dane sensytywne.

2) Integralność „I" - ze względu na rozmiar szkód, które mogłoby wywołać ich nieautoryzowana zmiana:

a) I1 (poziom niski) – informacje, których nieautoryzowana zmiana nie powoduje lub powoduje niewielkie konsekwencje natury prawnej lub finansowej;

b) I2 (poziom średni) – informacje, których nieautoryzowana zmiana może wiązać się z poważnymi konsekwencjami natury finansowej lub prawnej. Do tej grupy zaliczamy dane osobowe;

c) I3 (poziom wysoki) – informacje, których nieautoryzowana zmiana mogłaby zagrozić funkcjonowaniu Uniwersytetu lub spowodować bardzo poważne szkody natury prawnej lub finansowej.

3) Dostępność „D" - ze względu na maksymalny akceptowalny okres niedostępności do informacji lub konsekwencje ich utraty:

a) D1 (poziom niski) – długotrwały brak dostępu do tych informacji nie odbija się (negatywnie) w istotny sposób na funkcjonowaniu uczelni oraz nie pociąga za sobą konsekwencji prawnych lub finansowych;

b) D2 (poziom średni) – informacje dla których brak dostępu krótszy niż jeden dzień nie odbija się (negatywnie) w istotny sposób na funkcjonowaniu uczelni oraz nie pociąga za sobą konsekwencji prawnych lub finansowych;

c) D3 (poziom wysoki) – informacje dla których brak dostępu dłuższy niż cztery godziny w istotny sposób odbije się na funkcjonowaniu uczelni lub może pociągać za sobą poważne konsekwencje natury prawnej lub finansowej.

DOSTĘP I ZABEZPIECZENIE

§ 17

Polityka bezpieczeństwa informacji oraz danych przechowywanych i przetwarzanych w UKSW polega na:

1) wydzieleniu obszarów przeznaczonych do przetwarzania i przechowywania zbiorów danych, od obszarów ogólnie dostępnych i zapewnieniu odpowiednich barier fizycznych przeciwdziałających nieuprawnionemu dostępowi;
2) zarządzaniu uprawnieniami poszczególnych użytkowników, z zastosowaniem zasady „minimalnych uprawnień", to znaczy przydzielania dostępu wyłącznie do danych związanych z realizacją obowiązków służbowych;
3) stosowaniu zasady ograniczonego dostępu, gdzie domyślnymi uprawnieniami jest zabronienie dostępu. Stosowne uprawnienia są nadawane przez CASI w przypadku zaistnienia uzasadnionej potrzeby;
4) stosowaniu wielowarstwowych zabezpieczeń systemów przetwarzania informacji;
5) monitorowania adekwatności i skuteczności stosowanych w uczelni środków kontroli dostępu do informacji w ramach audytów wewnętrznych.

§ 18

1. UKSW współpracuje z kontrahentami na podstawie zawartych umów, które zawierają deklarację o zachowaniu poufności oraz zobowiązanie do przestrzegania zasad bhp i ppoż, w przypadku umów, na mocy których kontrahent wykonuje zlecenie na terenie UKSW.
2. Dostęp do pomieszczeń zewnętrznego serwisu technicznego zajmującego się konserwacją sprzętu jest nadzorowany przez pracowników UKSW.
3. Pomieszczenia jednostek zajmujących się przetwarzaniem danych chronionych wyposażone są w bariery fizyczne (lady) umożliwiające obsługę klientów przy jednoczesnym odseparowaniu od zasobów informacyjnych.
4. Pomieszczenia, w których znajdują się urządzenia przetwarzające zasoby informacyjne i ciągi komunikacyjne pozostają pod nadzorem systemu monitoringu wizyjnego i alarmowego oraz są zabezpieczone fizycznie.
5. Każde nowe lub zamienione urządzenie służące do przetwarzania informacji, bądź mogące mieć w jakikolwiek sposób wpływać na bezpieczeństwo informacji musi zostać zweryfikowane w zakresie zgodności z wymaganiami sytemu bezpieczeństwa informacji i zaakceptowane przez CASI.

§ 19

1. Dostęp do danych, o których mowa w § 15 pkt 3, na stacjach komputerowych:
   1) dostęp w LAN realizowany jest na przeznaczonych do tego serwerach;
   2) dostęp (udany lub nieudany) na serwerach jest odnotowywany;
   3) jeśli stacja PC jest komputerem przenośnym (laptopem) to musi ona być dodatkowo zabezpieczona (np. z wykorzystaniem szyfrowania dysku twardego);
   4) dostęp z zewnątrz firmy powinien odbywać się z wykorzystaniem kanału szyfrowanego (np. dostęp do e-mail poprzez protokół SSL);
   5) dostęp poprzez uczelnianą sieć WiFi powinien odbywać się z wykorzystaniem kanału szyfrowanego;
2. Komputerowe stacje robocze powinny być zabezpieczone przed nieautoryzowanym dostępem osób trzecich. Minimalne środki ochrony to:
   1) zainstalowane na stacjach systemy typu: firewall oraz antywirus;
   2) wdrożony system aktualizacji systemu operacyjnego oraz jego składników;
   3) wymaganie podania hasła przed uzyskaniem dostępu do stacji;
   4) niepozostawianie niezablokowanych stacji komputerowych bez nadzoru;
   5) bieżąca praca z wykorzystaniem konta nieposiadającego uprawnień administracyjnych.
3. Sieć lokalna uczelni jest chroniona przed nieuprawnionym dostępem, co oznacza, że:
   1) istotne serwery muszą być odseparowane od sieci klienckich;
   2) gniazdka sieciowe dostępne publiczne muszą być nieaktywne;
   3) nieuprawnieni użytkownicy spoza UKSW nie mogą uzyskiwać dostępu do sieci LAN.
4. Infrastruktura IT uczelni udostępniana publicznie musi być szczególnie zabezpieczona, z wykorzystaniem:
   1) separacji od sieci LAN;
   2) wykonaniem hardeningu systemu;
   3) weryfikację bezpieczeństwa systemu.

5. Zasady tworzenia i wykorzystania haseł:
   1) hasła powinny być okresowo zmieniane;
   2) hasła nie mogą być przechowywane w formie otwartej (nie zaszyfrowanej);
   3) hasła nie powinny być łatwe do odgadnięcia.

§ 20

W celu zapewnienia ochrony zasobów informacji, UKSW może stosować z zachowaniem obowiązującego prawa, monitoring wykorzystania infrastruktury informatycznej, w szczególności obejmujący następujące elementy:

1) analizę oprogramowania wykorzystanego na stacjach roboczych;
2) analizę stacji roboczych pod względem wykorzystania nielegalnego oprogramowania i plików multimedialnych oraz innych elementów naruszających Prawo Autorskie;
3) analizę odwiedzanych stron WWW;
4) analizę godzin pracy na stanowiskach komputerowych;
5) analizę wszelkich dostępów (autoryzowanych oraz nieautoryzowanych) do systemów IT ;
6) analizę ruchu sieciowego pod względem komunikacji, szkodliwej dla bezpieczeństwa danych uczelni.

§ 21

1. UKSW, w procesie zarządzania ciągłością działania systemu dba o zapewnienie usług związanych z przetwarzaniem danych, po przez przewidywanie możliwości wystąpienia krytycznych zdarzeń i przeciwdziałanie awariom i przerwom w działaniu systemów i urządzeń.
2. UKSW zapewnia cykliczną edukację pracowników w zakresie bezpieczeństwa informacji. Pracownicy w zależności od zajmowanego stanowiska mogą uczestniczyć w szkoleniach z zakresu ochrony danych osobowych i szczegółowych aspektów bezpieczeństwa.

§ 22

1. Pracownik UKSW zobowiązany jest do ochrony swoich danych dostępowych do systemów informatycznych, które obejmują między innymi takie elementy jak:
   1) loginy i hasła dostępowe;
   2) klucze softwareowe (pliki umożliwiające dostęp, np. certyfikaty do VPN) oraz sprzętowe oraz inne mechanizmy umożliwiające dostęp do systemów IT, których nie należy przechowywać w miejscach łatwo dostępnych i należy zabezpieczać przed dostępem osób nieupoważnionych.
2. Pracownikom uczelni zabrania się:
   1) przenoszenia niezabezpieczonych danych poufnych poza teren uczelni, w szczególności zabrania się przenoszenia danych poufnych na nośnikach elektronicznych;
   2) zabrania się korzystania z firmowej infrastruktury IT w celach prywatnych.

§ 23

1. W przypadku rozwiązania umowy o pracę z pracownikiem, dezaktywowane są wszystkie jego dostępy w systemach IT, chyba, że przepisy prawa wewnętrznego UKSW stanowią inaczej.
2. Wszelkie podejrzenia naruszenia Polityki bezpieczeństwa należy zgłaszać do ABI.
3. Każdy incydent jest odnotowywany w stosownej bazie danych. ABI w porozumieniu z ADO podejmuje właściwe kroki zaradcze.

STRUKTURY ZBIORÓW I PRZEPŁYW DANYCH MIĘDZY SYSTEMAMI

§ 24

1. Dane osobowe przetwarzane są w UKSW przy zastosowaniu systemów informatycznych.
2. Zbiory danych zlokalizowane są w bazach danych umieszczonych na serwerach bazodanowych i przetwarzane w programach dostosowanych do merytorycznych potrzeb jednostek organizacyjnych UKSW.
3. Zawartość pól informacyjnych w programach, o których mowa w ust. 2 musi być zgodna z przepisami prawa w zakresie przetwarzania danych osobowych.

§ 25

1. Opisy struktur zbiorów danych wskazujące zawartość i wzajemne powiązania poszczególnych pól informacyjnych wykonuje CASI w oparciu o aplikacje zastosowane do przetwarzania danych osobowych.
2. Opisy, o których mowa w ust. 1 wykonywane są w postaci wydruków, zrzutów ekranowych lub struktur tablic bazy. W przypadku braku możliwości uzyskania wydruku zrzutu ekranowego, CASI sporządza inne dostępne opisy.
3. Schematy przepływu danych pomiędzy systemami informatycznymi zastosowanymi do przetwarzania danych osobowych wykonuje CASI, zgodnie z relacjami występującymi w programach służących do przetwarzania danych osobowych.

§ 26

1. Przepływ danych pomiędzy systemami może dokonywać się w sposób jednokierunkowy lub dwukierunkowy.
2. Przesyłanie danych może odbywać się w sposób:
   1) manualny, przy wykorzystaniu nośników zewnętrznych;
   2) półautomatyczny przy wykorzystaniu funkcji eksportu/importu danych za pomocą teletransmisji poprzez wewnętrzną sieć teleinformatyczną;
   3) zautomatyzowany – np. ERP-> USOS, USOS->LDAP,
3. Przesyłanie danych za pomocą poczty elektronicznej dopuszczalne jest tylko po spełnieniu następujących wymagań:
   1) w obrębie komputerowej sieci UKSW, gdy nadawca i adresat maja ważne upoważnienia do przetwarzania danych osobowych, oraz gdy do przesyłania danych wykorzystywane są ich służbowe konta pocztowe w domenie *uksw.edu.pl*, bez konieczności stosowania dodatkowych zabezpieczeń kryptograficznych, zastrzeżeniem, że przesyłane w plikach załączniki powinny być zahasłowane ;
   2) poza komputerową siecią wewnętrzną UKSW, gdy nadawca ma ważne upoważnienie do przetwarzania danych osobowych oraz do wysyłki wykorzystuje się służbowe konta pocztowe w domenie *uksw.edu.pl*, a adresatem jest podmiot, z którym UKSW ma zawartą ważną umowę o przetwarzaniu danych osobowych, w tym przypadku nadawca ma obowiązek zastosować techniki kryptograficzne do zabezpieczania danych osobowych.

POLITYKA ZARZĄDZANIA KOPIAMI ZAPASOWYMI

§ 27

1. Każde istotne dane są archiwizowane na wypadek awarii w infrastrukturze IT.
2. Nośniki z kopiami zapasowymi są przechowywane w miejscu uniemożliwiającym dostęp osobom nieupoważnionym.

3. Kopie zapasowe są testowane okresowo pod względem rzeczywistej możliwości odtworzenia danych.
4. Za wykonanie i nadzorowanie wykonywania kopii zapasowej odpowiada CASI.
5. Kopia może być wykonana przez innego pracownika (operator) niż administrator odpowiedzialny za system (serwer), w przypadku jego nieobecności w pracy, z zachowaniem zasady rozliczalności. Operatora wyznacza bezpośredni przełożony administratora i zleca założenie konta z uprawnieniami do wykonania kopii i kontrolowania ich poprawności.
6. Dostęp fizyczny do sprzętu umieszczonego w serwerowni oraz nośników, w tym kopii zapasowych, możliwy jest jedynie dla osób upoważnionych.
7. Wykorzystane nośniki kopii zapasowych niszczone są w sposób uniemożliwiający odtworzenie z nich danych.

ŚRODKI OCHRONY

§ 28

1. Kierownicy jednostek organizacyjnych dokonują okresowej oceny ryzyka dla poszczególnych systemów i przedstawiają ABI, za pośrednictwem właściwego LA propozycje dotyczące zastosowania środków technicznych i organizacyjnych w celu zapewnienia właściwej ochrony przetwarzania danych.
2. Analiza ryzyka dotyczy:
   1) identyfikacji występujących zagrożeń dla systemów, zbiorów i baz danych;
   2) oceny dotychczas stosowanej ochrony przetwarzania danych osobowych;
   3) określenia skali ryzyka, tj. prawdopodobieństwa wystąpienia określonego zagrożenia;
   4) identyfikacji obszarów wymagających szczególnych zabezpieczeń.

§29

1. ADO jest zobowiązany do zastosowania środków ochrony, tj. środki fizyczne, osobowe i techniczne, które zapewnią poufność, integralność i rozliczalność przetwarzanych w UKSW informacji.
2. Środki ochrony fizycznej obejmują:
   1) lokalizację miejsc przetwarzania danych osobowych w pomieszczeniach o ograniczonym i kontrolowanym dostępie;
   2) ustalenie zasad kontroli dostępu do obiektów, pomieszczeń i szaf;
   3) wyposażenia pomieszczeń, w których przetwarzane są dane osobowe we właściwe, w tym antywłamaniowe zabezpieczenia tj. wzmocnione drzwi, odpowiednio zabezpieczone okna i meble oraz niezbędne zabezpieczenia alarmowe;
   4) przechowywanie danych wrażliwych oraz nośników wymiennych i nośników kopii zapasowych w odpowiednio zabezpieczonych miejscach;
   5) odpowiednie wyposażenie i zabezpieczenie pomieszczeń serwerowni.
3. Środki ochrony osobowej obejmują:
   1) dopuszczenie do przetwarzania danych osobowych i informacji wrażliwych wyłącznie osób posiadających upoważnienie;
   2) zapewnienie osobom, o których mowa w ust. 1 odpowiedniego przygotowania zgodnie z zasadami i obsługą systemu przetwarzania danych osobowych;

3) prowadzenie dokumentacji zawierającej stosowne zobowiązania i oświadczenia tj. do zachowania w tajemnicy danych i sposobów ich zabezpieczania czy oświadczenia o zapoznaniu się z treścią przepisów określających zasady postępowania przy przetwarzaniu danych osobowych.

4. Środki ochrony technicznej obejmują:
   1) mechanizmy kontroli dostępu do systemów i zasobów;
   2) zastosowanie i aktualizowanie narzędzi ochrony (programy antywirusowe) systemów i baz danych;
   3) regularne tworzenie kopii zapasowych zbiorów danych przetwarzanych w systemach informatycznych;
   4) zastosowanie ochrony zasilania.

§ 30

1. Uwzględniając kategorie, o których mowa w § 14 oraz zagrożenia przeprowadzone w wyniku oceny ryzyka stosuje się następujące poziomy bezpieczeństwa dla systemów:
   1) podstawowy;
   2) podwyższony
   3) wysoki.
2. Nadanie właściwego poziomu bezpieczeństwa sytemu informatycznego dokonuje ABI w porozumieniu z LA, na wniosek kierowników jednostek administracyjnych.
3. Systemy informatyczne którym przypisano poziomy bezpieczeństwa, o których mowa w ust. 1 muszą spełniać wymagania określone w rozporządzeniu 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. z 2004 r. Nr 100, poz. 1024 z póź. zm.).

POSTĘPOWANIE W SYTACJACH NARUSZENIA ZASAD BEZPIECZEŃSTWA

§ 31

1. Za naruszenie zabezpieczenia systemu bądź urządzenia, w którym są przetwarzane dane wrażliwe, przyjmuje się każdy stwierdzony fakt nieuprawnionego ujawnienia danych, udostępnienia lub umożliwienia dostępu osobom nie upoważnionym, zabrania danych przez osobę nieupoważnioną lub uszkodzenie jakiegokolwiek elementu systemu.
2. Postępowanie w przypadku naruszeń zasad ochrony danych osobowych określa **załącznik nr 2** do niniejszej polityki.

§ 32

1. W przypadku zaistnienia zdarzeń, które mogą wskazywań na naruszenie lub stwierdzenia naruszenia zabezpieczenia systemu oraz wykryte słabości systemów informatycznych należy zgłosić niezwłocznie ABI.
2. Zgłoszenie zdarzenia, o którym mowa w § 31 ust. 1 oraz w ust. 1 niniejszego paragrafu powinno zawierać:
   1) dane osoby zgłaszającej: imię, nazwisko, stanowisko, nazwę komórki organizacyjnej, tel. kontaktowy;
   2) opis oznak naruszenia procedur ochrony danych osobowych;
   3) określenie sytuacji i czasu wystąpienia zdarzenia;

4) identyfikację rodzaju zaistniałego zdarzenia, w tym określenie skali zniszczeń, metody dostępu dokonania nieupoważnionego dostępu;
5) przedstawienie wszystkich istotnych informacji i dokumentów (raportów) wskazujących na przyczynę zdarzenia;
6) wskazanie możliwości zabezpieczenia systemu oraz wszelkich działań podjętych po ujawnieniu zdarzenia w celu uniemożliwienia lub ograniczenia nieuprawnionego dostępu, minimalizacji szkód i sposobów zabezpieczenia śladów naruszenia ochrony danych.

3. Zgłoszenia, o których mowa w ust. 2 podlegają rejestracji w rejestrze incydentów bezpieczeństwa informacji, dostępnym u ABI.

§ 33

1 ABI w porozumieniu z ADO i LA podejmuje wszelkie działania mające na celu:
1) minimalizację negatywnych skutków zdarzenia;
2) wyjaśnienie przyczyn i okoliczności zdarzenia;
3) zabezpieczenie dowodów zdarzenia;
4) zapewnienie możliwości dalszego bezpiecznego przetwarzania danych.

2. W celu realizacji działań, o których mowa w ust. 1 ma prawo do:
1) żądania wyjaśnień od pracowników;
2) korzystania z pomocy konsultantów;
3) wnioskowania do ADO o wydanie zakazu wykonywania prac w zakresie przetwarzania danych osobowych do czasu przywrócenia możliwości przestrzegania procedur bezpieczeństwa.

§ 34

Odmowa udzielania wyjaśnień lub współpracy z ABI w obszarze ochrony danych osobowych traktowana będzie, jako naruszenie obowiązków pracowniczych.

ZARZADZANIE RYZYKIEM

§35

1. Każde zidentyfikowane ryzyko podlega analizie w zakresie jego wpływu na bezpieczeństwo informacji oraz prawdopodobieństwa wystąpienia tego ryzyka.
2. Ustala się trzystopniową skalę oceny wpływu ryzyka na bezpieczeństwo informacji oraz trzystopniową miarę prawdopodobieństwa wystąpienia ryzyka. Miara istotności ryzyka bierze pod uwagę obydwa te czynniki, to jest miarę wpływu ryzyka oraz miarę prawdopodobieństwa wystąpienia ryzyka. Ustala się ją jako iloczyn tych dwu miar.
3. Podczas oceny wpływu ryzyka i prawdopodobieństwa jego wystąpienia należy wziąć pod uwagę klasyfikację informacji na które wpływ może mieć zidentyfikowane ryzyko. Poniżej zdefiniowano miarę wpływu ryzyka, miarę prawdopodobieństwa jego wystąpienia oraz miarę istotności ryzyka:
4. Miara wpływu ryzyka na bezpieczeństwo informacji:
1) W1 (niski, 2 punkty) – zdarzenie objęte ryzykiem powoduje niewielką stratę finansową, zakłócenie lub opóźnienie w wykonywaniu zadań; nie wpływa na reputację; skutki zdarzenia można łatwo usunąć;
2) W2 (średni, 4 punkty) – zdarzenie objęte ryzykiem powoduje znaczną stratę posiadanych zasobów, ma negatywny wpływ na efektywność działania, jakość wykonywanych zadań, reputację; z wystąpieniem zdarzenia może wiązać się trudny proces przywracania stanu poprzedniego;

3) W3 (duży, 6 punktów) – zdarzenie objęte ryzykiem powoduje uszczerbek mający krytyczny lub bardzo duży wpływ na realizację kluczowych zadań albo osiągania założonych celów – poważny uszczerbek w zakresie jakości wykonywanych zadań, poważna strata finansowa lub na reputacji.

5. Miara wpływu ryzyka związanego z aktywami informacyjnymi wyznaczana jest na podstawie klasyfikacji danych aktywów informacyjnych. Należy przyjąć, że dla aktywów informacyjnych, których klasyfikacje są na poziomie niskim (C1, I1, A1) miara wpływu ryzyka wynosi W1. Dla ryzyka związanego z aktywami informacyjnymi dla których, dowolna z klasyfikacji jest na poziomie średnim (C2, I2, A2) miara wpływu ryzyka wynosi W2. Dla ryzyka związanego z aktywami informacyjnymi dla których, dowolna z klasyfikacji jest na poziomie wysokim (C3, I3, A3) miara wpływu ryzyka wynosi W3.
6. Miara prawdopodobieństwa wystąpienia ryzyka:
   1) P1 (niskie, 2 punkty) – istnieją uzasadnione powody by sądzić, że zdarzenie objęte ryzykiem zdarzy się raz w ciąg roku lub nie zdarzy się wcale (w ciągu roku);
   2) P2 (średnie, 4 punkty) – istnieją uzasadnione powody by sądzić, że zdarzenie objęte ryzykiem zdarzy się kilkakrotnie w ciągu roku;
   3) P3 (duże, 6 punktów) – istnieją uzasadnione powody by sądzić, że zdarzenie objęte ryzykiem zdarzy się wielokrotnie w ciągu roku.
7. Miara istotności ryzyka:
   1) IR1 (niska) – iloczyn wpływu ryzyka i prawdopodobieństwa ryzyka znajduje się w przedziale od 4 do 8 punktów;
   2) IR2 (średnia) – iloczyn wpływu ryzyka i prawdopodobieństwa ryzyka znajduje się w przedziale od 12 do 16 punktów;
   3) IR3 (duża) – iloczyn wpływu ryzyka i prawdopodobieństwa ryzyka znajduje się w przedziale od 24 do 36 punktów.
8. W zależności od zidentyfikowanego poziomu ryzyka określa się zasady postępowania z ryzykiem:
   1) ryzyko o niskiej istotności należy traktować jako akceptowalne. Zaakceptowanie ryzyka nie wyklucza możliwości jego monitorowania oraz podejmowania działań zaradczych;
   2) ryzyko oznaczone jako średnie wymaga rozważenia potrzeby wdrożenia działań zaradczych. W sytuacji, gdy zostanie podjęta decyzja o tolerowaniu ryzyka oznaczonego jako średnie, dokonać powtórnej oceny istotności ryzyka nie później niż po 6 miesiącach od daty decyzji o tolerowaniu ryzyka. W sytuacji gdy poziom istotności dla takiego ryzyka nie ulegnie zmianie, postępujemy tak, jak w przypadku ryzyka o wysokim poziomie istotności;
   3) ryzyko oznaczone jako duże wymaga wprowadzenia działań zaradczych (reakcji na ryzyko), w tym modyfikacji lub uzupełnienia mechanizmów kontroli, które ograniczają możliwości wystąpienia ryzyka;
   4) decyzję o akceptacji dużego ryzyka może podjąć Rektor.
9. Ustala się następujące sposoby ograniczania ryzyka:
   1) przeniesienie ryzyka (np. ubezpieczenie);
   2) akceptację ryzyka (trudności w przeciwdziałaniu lub gdy koszty podjętych działań mogą przekroczyć przewidywane korzyści);
   3) przeciwdziałanie (np. wzmocnienie mechanizmów kontrolnych, podjęcie działań zmniejszających prawdopodobieństwo wystąpienia niepożądanych sytuacji);

4) przesunięcie w czasie (np. wycofanie się z realizacji zadania, gdy jego realizacja wiąże się z pojawieniem się dużego ryzyka).

10. Proces zarządzania ryzykiem związanym z bezpieczeństwem informacji musi zostać udokumentowany w postaci dokumentu w postaci tradycyjnej (papierowej) lub elektronicznej, który zawiera:
    1) obszar ryzyka;
    2) jednoznaczne określenie ryzyka;
    3) zidentyfikowane podatności;
    4) działania ograniczające ryzyko z określeniem terminów realizacji tych działań i osób odpowiedzialnych.
11. Akceptacja Ryzyka wymaga sporządzenia Dokumentu Akceptacji Ryzyka zawierającego co najmniej:
    1) opis ryzyka;
    2) klasyfikację istotności ryzyka;
    3) opis stanu dotychczasowego;
    4) zastosowane środki ograniczające ryzyko;
    5) końcową ocenę poziomu ryzyka (niskie, średnie lub duże);
    6) datę ważności akceptacji (dopuszcza się ważność bezterminową dla ryzyka ocenionego jako niskie.
12. Dokument Akceptacji Ryzyka, w przypadku ryzyk o istotności niskiej i średniej akceptacji dokonuje ABI, a w przypadku ryzyk o istotności dużej akceptacji dokonuje Rektor.