Załącznik
do Zarządzenia
Rektora

Polityka Bezpieczeństwa Teleinformatycznego Uniwersytetu Przyrodniczego w Lublinie

SPIS TREŚCI

ROZDZIAŁ I – Zagadnienia wstępne i cele Polityki Bezpieczeństwa Informacji

§ 1 Zagadnienia wstępne

1. Niniejsza Polityka Bezpieczeństwa Informacji określa ogólne ramy oraz normuje zagadnienia związane z bezpieczeństwem danych i informacji przetwarzanych, transmitowanych lub przechowywanych w jednostkach organizacyjnych Uniwersytetu.
2. Ochrona aktywów informacyjnych Uniwersytetu jest podstawowym obowiązkiem każdego pracownika, wszystkich studentów oraz obliguje do jej stosowania współpracujące z Uniwersytetem podmioty.
3. Władze Uniwersytetu w pełni popierają i wyrażają potrzebę funkcjonowania Uniwersytetu zgodnie z przepisami prawa oraz dobrymi praktykami rynkowymi związanymi z zapewnieniem bezpieczeństwa Informacji.
4. Władze Uniwersytetu deklarują zapewnienie odpowiednich środków technicznych i organizacyjnych niezbędnych do ochrony przetwarzanych informacji w zakresie zidentyfikowanych potrzeb.
5. Polityka Bezpieczeństwa Informacji Uniwersytetu Przyrodniczego w Lublinie została opracowana w oparciu o obowiązujące przepisy prawa oraz z wykorzystaniem zaleceń i najlepszych praktyk rynkowych.
6.

§ 2 Cele Polityki Bezpieczeństwa Informacji

Cele Polityki Bezpieczeństwa Informacji Uniwersytetu:

1) zapewnienie zgodności działalności Uniwersytetu z przepisami powszechnie obowiązującego prawa, dla obszaru bezpiecznego przetwarzania informacji;
2) zabezpieczenie interesów Uniwersytetu w odniesieniu do przetwarzanych informacji poprzez ograniczenie lub eliminację ryzyka wystąpienia incydentów naruszenia bezpieczeństwa informacji na skutek wdrożenia wymaganych mechanizmów bezpieczeństwa;
3) zapewnienie potencjalnych partnerów lub organizacji współpracujących, o wdrożeniu odpowiednich działań w zakresie bezpieczeństwa informacji przed podjęciem współpracy;
4) kształtowanie świadomości pracowników w podejściu do bezpieczeństwa informacji poprzez udokumentowanie tego, czego się oczekuje, co jest zabronione, kto jest odpowiedzialny oraz za jakie elementy struktury bezpieczeństwa informacji.

ROZDZIAŁ II –Postanowienia ogólne

§ 3 Słownik definicji i pojęć

Przez użyte w Polityce określenia należy rozumieć:

1) administrator systemu informatycznego lub administrator serwera: pracownik nadzorująca pracę systemu informatycznego oraz wykonująca czynności administracyjne wymagające specjalnych uprawnień;
2) inspektor ochrony informacji: wyznaczona przez Uniwersytet osoba odpowiedzialna za monitorowanie i utrzymywanie wymaganego poziomu bezpieczeństwa teleinformatycznego Uniwersytetu;
3) autentyfikacja użytkownika: proces weryfikacji dostępu użytkownika do systemu informatycznego opierający się na identyfikatorach, hasłach lub uwierzytelnieniu wieloskładnikowym;
4) autoryzacja: nadanie uprawnienia na dostęp do konkretnych informacji lub zasobów;
5) Centrum Informatyki (CI): jednostka organizacyjna odpowiedzialna za administrowanie i utrzymywanie systemów informatycznych oraz świadczenie usług IT w Uniwersytecie;
6) dane chronione: informacje chronione przetwarzane w sposób elektroniczny w szczególności te przetwarzane w ramach systemów informatycznych;

7) hasło: ciąg znaków złożony z liter, cyfr lub innych znaków, które musi podać użytkownik, aby mógł korzystać z dostępu do zastrzeżonych zasobów np. sieci komputerowej, bazy danych, komputera. Hasło jest jednym ze sposobów ochrony danych przed osobami nieupoważnionymi;
8) incydent bezpieczeństwa: niespodziewane i niepożądane zdarzenie lub seria takich zdarzeń świadczących o naruszeniu lub wysokim ryzyku naruszenia bezpieczeństwa informacji. Identyfikacja Incydentu skutkuje koniecznością podjęcia stosownej reakcji opisanych w innych szczegółowych regulacjach wewnętrznych Uniwersytetu;
9) informacje chronione: zasoby informacyjne stanowiące wartość dla Uniwersytetu. Informacje polegające właściwej ochronie ze względu na obowiązujące przepisy prawa (tj. w szczególności: RODO, KRI - Rozporządzenie 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, Ustawę z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji, Ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych oraz inne regulacje wewnętrzne Uniwersytetu);
10) inspektor ochrony danych (IOD): osoba wyznaczona przez Uniwersytet, wykonująca zadania, z zakresu nadzoru nad ochroną przetwarzanych danych osobowych (w oparciu o Rozporządzenie RODO);
11) kierownik jednostki organizacyjnej: kierownik, dyrektor albo inna osoba pełniąca funkcje kierownicze jednostki organizacyjnej Uniwersytetu. Osoba odpowiedzialna merytorycznie za wykorzystywane w jednostce organizacyjnej aplikacje użytkowe (merytoryczny właściciel aplikacji Uniwersytetu);
12) Polityka: Polityka Bezpieczeństwa Informacji Uniwersytetu Przyrodniczego w Lublinie;
13) serwer: wyróżniony specjalistyczny komputer świadczący usługi na rzecz mających z nim łączność innych komputerów np. przechowujący pliki, pośredniczący w przekazywaniu poczty itp.;
14) sieć publiczna: sieć komputerowa inna niż uczelniana sieć komputerowa np. Internet;
15) służby informatyczne: pracownicy Centrum Informatyki Uniwersytetu odpowiedzialni za należyte funkcjonowanie systemów informatycznych;
16) system informatyczny (system): zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych; (np.: systemy operacyjne, aplikacje użytkowe);
17) Uniwersytet: Uniwersytet Przyrodniczy w Lublinie;
18) uczelniana sieć komputerowa: własna lub dzierżawiona sieć komputerowa wraz z wszelkimi zasobami teleinformatycznymi będącymi własnością Uniwersytetu;
19) użytkownik: pracownik posiadający uprawnienia do pracy w systemie informatycznym zgodnie z zakresem obowiązków służbowych. Użytkownik z uprawnieniami na poziomie administratora staje się administratorem systemu;

§ 4 Zakres stosowania Polityki

1. Polityka obowiązuje wszystkich pracowników i studentów Uniwersytetu oraz wszystkich pracowników podmiotów współpracujących z Uniwersytetem.
2. Użytkownicy systemów informatycznych zobowiązani są do zapoznania się z przepisami normującymi kwestie związane z bezpieczeństwem systemów teleinformatycznych w Uniwersytecie.

§ 5 Zakresy odpowiedzialności za bezpieczeństwo informacji

1. Za ogólny stan bezpieczeństwa informacji chronionych oraz danych chronionych w systemach informatycznych będących własnością Uniwersytetu odpowiedzialne są Władze Uniwersytetu oraz kierownicy jednostek organizacyjnych.

2. Za zabezpieczenie informacji i danych przetwarzanych i gromadzonych w poszczególnych urządzeniach komputerowych odpowiedzialni są ich użytkownicy.
3. Nadzór nad bezpieczeństwem danych osobowych sprawuje IOD.
4. Nadzór nad bezpieczeństwem informacji chronionych:
   1) w obszarze ochrony fizycznej oraz systemów monitorowania wizyjnego sprawuje kierownik Działu Administracyjno-Gospodarczego;
   2) w obszarze ochrony informacji z kategorii informacji niejawnych sprawuje pełnomocnik ds. ochrony informacji niejawnych.
5. Nadzór nad bezpieczeństwem danych chronionych przetwarzanych w systemach informatycznych:
   1) administrowanych i utrzymywanych administrowanych przez CI sprawuje kierownik CI;
   2) administrowanych i utrzymywanych przez poszczególne jednostki organizacyjne sprawuje kierownik jednostki organizacyjnej.

ROZDZIAŁ III - Ogólne zasady bezpieczeństwa informacji

§ 6 Kluczowe zasady bezpieczeństwa informacji

Kluczową zasadą bezpieczeństwa informacji jest dążenie do zapewnienia najwyższego poziomu poufności, integralności i dostępności przetwarzanych informacji w systemach informatycznych Uniwersytetu. W szczególności:

1) poufność obejmuje zapewnienie, że istotne dane i informacje są utrzymywane w sposób tajny lub prywatny. Aby to osiągnąć, dostęp do tych informacji musi być kontrolowany i zapobiegający nieautoryzowanemu udostępnianiu danych (celowemu lub przypadkowemu). Kluczowym elementem zachowania poufności jest zapewnienie, że osoby nieposiadające odpowiednich uprawnień nie mają dostępu do istotnych informacji i danych. Skuteczny system gwarantuje również, że ci, którzy powinni mieć dostęp, mają niezbędne uprawnienia;
2) integralność oznacza zapewnienie, że dane są godne zaufania i wolne od manipulacji i zmian. Integralność jest zachowana tylko wtedy, gdy są one autentyczne, dokładne i wiarygodne;
3) dostępność oznacza, że systemy, sieci i aplikacje muszą działać tak, jak zostały zaprojektowane (w sposób jak powinny działać i kiedy powinny działać). Ponadto osoby mające dostęp do określonych informacji muszą mieć możliwość korzystania z nich w razie potrzeby, a dotarcie do danych nie powinno zajmować nadmiernej ilości czasu. Nawet jeśli dane są traktowane jako poufne i zachowana jest ich integralność, często są bezużyteczne, gdy brakuje ich dostępności.

§ 7 Zasady bezpieczeństwa informacji wg zagadnień

1. Ogólne zasady udzielania dostępu dla pracowników Uniwersytetu:
   1) dostęp do serwera lub aplikacji dla pracowników Uniwersytetu może być zrealizowany dopiero po ustaleniu ich bieżących potrzeb związanych z wykonywanymi zadaniami;
   2) zalecane jest udostępnianie jedynie minimum informacji, które są zasadnie i niezbędne do osiągnięcia zamierzonego celu służbowego pracownika (adekwatnie do ich zakresów czynności i posiadanych upoważnień dostępu do informacji, w tym upoważnień o przetwarzania danych osobowych);
   3) dostęp jest udzielany po przeprowadzeniu szkolenia w zakresie bezpieczeństwa informacji. Szkolenia powinny być cyklicznie ponawiane.
   4)
2. Administratorzy systemów oraz administratorzy serwerów będących własnością Uniwersytetu oraz serwerów zarządzanych na podstawie umowy z zewnętrznym dostawcą usług na użytek Uniwersytetu są zobowiązani do:
   1) posiadania umiejętności, doświadczenia i/lub szkoleń potrzebnych do wdrożenia wymagań bezpieczeństwa informacji;
   2) wdrożenia obowiązujących wymagań bezpieczeństwa informacji;

3) regularnego podejmowania uzasadnionych działań w celu zapewnienia, że ich systemy nie są podatne na ataki oraz raportowania nieujawnionych wcześniej podatności organizacji współpracujących;
4) nie mogą świadomie zezwalać na wykorzystywanie danych logowania do jednego konta dla wielu użytkowników;
5) rejestrowania incydentów naruszenia bezpieczeństwa informacji i niezwłocznego informowania przełożonego o wszelkich możliwych konsekwencjach naruszeniach bezpieczeństwa;
6) współpracy ze stroną odpowiedzialną za aplikację użytkową (merytorycznego właściciela aplikacji Uniwersytetu) zainstalowaną na serwerze.

3. Wymagania dla haseł dostępowych i danych uwierzytelniających użytkowników:
   1) zabronione jest udostępnianie haseł użytkowników ani innych danych uwierzytelniających;
   2) zabronione jest przechowywanie haseł w postaci zwykłego tekstu lub bezpośrednio w skryptach lub plikach konfiguracyjnych;
   3) hasła używane we wszystkich systemach „produkcyjnych" Uniwersytetu powinny mieć wymaganą długość i złożoność zabezpieczającą je przed „złamaniem";
   4) użytkownicy muszą wykorzystywać uwierzytelnianie wieloskładnikowe (weryfikację dwuetapową) tam, gdzie jest to możliwe;
   5) hasła należy natychmiast zmienić, jeśli istnieje podejrzenie, że zostały naruszone.

4. Ogólne zasady konfigurowania urządzeń komputerowych wykorzystywanych przez pracowników Uniwersytetu :
   1) urządzenia komputerowe łączące się do sieci lub instalowane w sieciach Uniwersytetu (za wyjątkiem wydzielonych podsieci dla gości) muszą być skonfigurowane pod kątem bezpiecznego działania. W szczególności należy zapewnić: zainstalowane oprogramowanie antywirusowe, inne niż domyślne unikalne hasła ograniczające dostęp, prawidłową rejestrację urządzenia w sieci, aktualny system operacyjny, regularne aktualizacje oraz instalowanie poprawek oprogramowania, szyfrowanie pamięci masowej (jeśli jest obsługiwane);
   2) urządzenia mobilne (notebooki, telefony komórkowe itp.) i stacje robocze, które mogą być używane do przechowywania lub uzyskiwania dostępu do informacji Uniwersytetu, muszą być bezpiecznie skonfigurowane (m. in. zapewniać szyfrowanie danych przechowywanych na urządzeniu oraz kryptografię transmitowanych danych, o ile jest to możliwe). Działania powyższe należy podejmować na wypadek zagubienia lub kradzieży urządzenia;
   3) wymagane aktualizacje systemu operacyjnego i aplikacji użytkowych należy instalować niezwłocznie po ich udostępnieniu przez producenta;
   4) w przypadku utylizacji urządzenia komputerowego informacje przechowywane na urządzeniu muszą być usunięte. Informacje chronione Uniwersytetu należy odpowiednio usuwać bezpiecznie nadpisując informacje lub fizycznie niszcząc nośniki, gdy nie są już potrzebne;
   5) informacje na urządzeniu komputerowym należy zabezpieczyć przed przekazaniem urządzenia do naprawy.

5. Wymagania dla serwerów będących własnością Uniwersytetu:
   1) serwery muszą być przechowywane w bezpiecznych lokalizacjach i odpowiednio inwentaryzowane w zakresie ich wyposażenia;
   2) dostęp do pomieszczeń serwerowni powinien być ograniczony do niezbędnego minimum oraz monitorowany;
   3) serwery w tej samej podsieci muszą być chronione przed wzajemnymi atakami;
   4) serwery oraz inne urządzenia teleinformatyczne przetwarzające informacje chronione Uniwersytetu muszą znajdować się w prywatnej przestrzeni adresowej oraz posiadać bezpieczne i redundantne rozwiązania sprzętowe;
   5) ruch wychodzący z serwerów musi być ograniczony do tego, który jest wymagany do prawidłowego działania usługi lub współpracy z innymi usługami;

6) serwery nie mogą być dostępne bezpośrednio z internetu ani z części sieci wewnętrznej, w których znajdują się komputery użytkowników;
7) poprawki systemu operacyjnego serwerów i aplikacji muszą być aktualne i przetestowane przed ich instalacją na serwerze;
8) na wszystkich serwerach musi działać system antywirusowy z aktualnymi plikami sygnatur wirusów;
9) serwery i aplikacje odpowiadające za zarządzanie hasłami muszą: wymuszać ustawienie złożonego hasła, egzekwować uwierzytelnianie wieloskładnikowe (jeżeli jest taka techniczna możliwość), badać złożoność i częstotliwość zmian haseł, posiadać mechanizm wymuszający ponowne uwierzytelnienie kont użytkowników po okresie bezczynności, spełniać inne szczegółowe wymagania bezpieczeństwa Uniwersytetu;
10) domyślne hasła muszą zostać zmienione, a konta ogólne muszą zostać wyłączone lub usunięte przed "produkcyjnym" oddaniem do użytku serwera lub aplikacji;
11) dostępy i działania użytkowników i administratorów na serwerów i zainstalowanych tam aplikacjach musi być rejestrowany. W szczególności muszą być rejestrowane działania i funkcje administracyjne na serwerach i w aplikacjach.

6. Wymagania dla dzienników logów serwerów Uniwersyteckich oraz serwerów zarządzanych na podstawie umowy z zewnętrznym dostawcą usług na użytek Uniwersytetu:
   1) dzienniki logów muszą być okresowo przeglądane pod kątem nietypowych zachowań i działań użytkowników;
   2) rejestracja dostępu użytkowników i administratorów do serwerów i aplikacji w logach musi być bezpiecznie przechowywane na komputerze zdalnym;
   3) dzienniki logów wymagane przez szczegółowe procedury bezpieczeństwa informacji Uniwersytetu muszą być przechowywane przez co najmniej 30 dni.

7. Zasady wykonywania i przechowywania kopii zapasowych:
   1) wszystkie systemy informatyczne oraz bazy danych wykorzystywane w trybie „produkcyjnym” muszą być objęte mechanizmem wykonywania kopii zapasowych;
   2) ustala się, że muszą wystąpić co najmniej trzy egzemplarze danych, w dwóch lokalizacjach z czego jedna poza miejscem fizycznego przechowywania i przetwarzania danych;
   3) za proces wykonania i przechowywania kopii zapasowych odpowiada administrator systemu, któremu został powierzony dany system informatyczny;
   4) szczegóły dotyczące procesu wykonywania kopii zapasowych powinny zostać określone w procedurach eksploatacyjnych Centrum Informatyki.

8. W przypadku podjęcia współpracy z dostawcami i innymi podmiotami zewnętrznymi Uniwersytetu należy stosować poniższe zasady:
   1) dostęp do niepublicznych systemów Uniwersytetu dla pracowników dostawców i organizacji współpracujących może być realizowany dopiero po zawarciu stosownych umów pisemnych zawierających wymagane zapisy dotyczące zapewnienia bezpieczeństwa przetwarzanych informacji;
   2) respektować obowiązek uczestniczenia i obecności wyznaczonych pracowników przy pracach osób trzecich w miejscach szczególnie wrażliwych dla Uniwersytetu;
   3) należy zobowiązać pracowników lub odpowiednio kontrahentów do zgłaszania wszelkich zaobserwowanych lub podejrzewanych słabości związanych z bezpieczeństwem informacji w systemach lub usługach;
   4) w przypadku podmiotów zewnętrznych, które będą gromadzić, przetwarzać lub przechowywać informacje chronione lub zarządzać krytycznymi systemami Uniwersytetu, polityki i procedury bezpieczeństwa informacji tych podmiotów muszą zostać sprawdzone przez specjalistę wyznaczonego przez kierownika CI.

ROZDZIAŁ IV - Identyfikacja zagrożeń i ocena ryzyka

§ 8 Proces oceny ryzyka

1. Proces oceny ryzyka bezpieczeństwa informacji powinien być procesem ciągłym, podejmowanym cyklicznie lub w reakcji na występujące incydenty naruszenia bezpieczeństwa informacji w Uniwersytecie.
2. Kierownik Centrum Informatyki oraz Inspektor Ochrony Informacji zobowiązani są do przeprowadzenia corocznej analizy zagrożeń i szacowania ryzyka w obszarze bezpieczeństwa informacji dla całego Uniwersytetu i opracowania planu postępowania z ryzykiem. Wyniki analizy powinny być każdorazowo osobie, której Rektor powierzył odpowiedzialność za obszar informatyzacji Uczelni.
3. Każdy kierujący jednostką organizacyjną zobowiązany jest do bieżącej analizy zagrożeń i szacowania ryzyka w obszarze bezpieczeństwa informacji w podległej jednostce. Współpracuje w tym zakresie z jednostkami organizacyjnymi i pracownikami nadzorującymi ten obszar w Uniwersytecie. W szczególności:
   1) kierownikiem CI, inspektorem ochrony informacji, administratorami systemów - w zakresie stosowania środków technicznych i organizacyjnych;
   2) IOD – w zakresie określonym w rozporządzeniu ROD.

ROZDZIAŁ V - Kontrola i nadzór nad realizacją Polityki

§ 9 Kontrola i nadzór

1. Do kontroli stanu realizacji Polityki Bezpieczeństw Informacji w jednostkach organizacyjnych Uniwersytetu upoważnieni są:
   1) władze Uniwersytetu;
   2) inspektor ochrony informacji;
   3) upoważnieni przez władze Uniwersytetu pracownicy komórki audytu.
2. Raz w roku inspektor ochrony informacji przedstawia władzom Uniwersytetu sprawozdanie z wyników kontroli stanu zabezpieczenia systemów informatycznych Uniwersytetu.
3. W celu potwierdzenia skuteczności stosowanych środków organizacyjnych i technicznych dla zapewnienia wymaganego poziomu bezpieczeństwa informacji, nie rzadziej niż raz na rok przeprowadzane są wewnętrzne audyty bezpieczeństwa informacji przeprowadzane przez komórkę audytu wewnętrznego.
4. Przeprowadzenie zewnętrznych audytów bezpieczeństwa informacji podlega akceptacji przez kanclerza Uniwersytetu w uzgodnieniu z kierownikiem Centrum Informatyki.

ROZDZIAŁ VI - Przepisy końcowe

§ 10 Przepisy końcowe

1. Zobowiązuje się wszystkich pracowników Uniwersytetu do bezwzględnego przestrzegania ustaleń niniejszej Polityki.
2. Szczegółowe zasady i wytyczne bezpieczeństwa dla poszczególnych kategorii informacji przetwarzanych przez Uniwersytet określają inne regulacje wewnętrzne.
3. Treść Polityki Bezpieczeństwa Informacji podlega corocznemu przeglądowi. Dodatkowo w przypadku wystąpieniu znaczących incydentów naruszenia bezpieczeństwa informacji. Za coroczny przegląd aktualności Polityki odpowiedzialny jest kierownik CI.