Załącznik do Zarządzenia Nr 33
Rektora Politechniki Poznańskiej
z dnia 18 października 2024 r. (RO/X/33/2024)

POLITYKA BEZPIECZEŃSTWA INFORMACJI POLITECHNIKI POZNAŃSKIEJ

Spis treści:

1. CEL I ZAKRES STOSOWANIA POLITYKI BEZPIECZEŃSTWA INFORMACJI

Politechnika Poznańska rozumiejąc znaczenie bezpieczeństwa informacji ustanawia Politykę Bezpieczeństwa Informacji mającą na celu:

a) wsparcie w realizacji i osiągnięciu celów mających fundamentalne znaczenie dla funkcjonowania Uczelni,
b) ochronę poufności, integralności oraz dostępności informacji, zgodnie z wymaganiami przepisów prawa, przepisami wewnętrznymi Uczelni, wytycznymi oraz normami, w szczególności dążąc do zapewnienia zgodności z normą ISO/IEC 27001,
c) ciągłe doskonalenie poprzez kształtowanie świadomości w zakresie istotności i konieczności przestrzegania zasad bezpieczeństwa informacji,
d) przeciwdziałanie incydentom bezpieczeństwa informacji, poprzez identyfikację i klasyfikację informacji, analizę ryzyk i podejmowanie działań zapobiegawczych, których celem jest minimalizacja prawdopodobieństwa wystąpienia zdarzeń bądź incydentów bezpieczeństwa informacji,
e) zapewnienie optymalnych pod względem kosztowym warunków eksploatacji i rozwoju zasobów IT,
f) zakomunikowanie, że przestrzeganie zasad dotyczących bezpieczeństwa informacji i podejmowanie działań na rzecz jego zapewnienia, w celu zachowania ciągłości pracy Uczelni, dotyczy każdego pracownika, studenta, a także osoby zewnętrzne współpracujące z Uczelnią.

Szczegółowe zasady bezpieczeństwa informacji przetwarzanych w Uczelni określa niniejsza Polityka Bezpieczeństwa Informacji oraz związane procedury i akty wewnętrzne, w tym dotyczące procesów i projektów, w których są przetwarzane dane i informacje, istniejących i wdrażanych obecnie lub w przyszłości systemów, wszystkich lokalizacji, budynków, pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie.

2. TERMINY I DEFINICJE

Definicje stosowane w niniejszej polityce mają następujące znaczenie:

a) System Zarządzania Bezpieczeństwem Informacji (SZBI) – zbiór polityk, procedur, wytycznych, zarządzanych wspólnie przez organizację w celu ochrony zasobów informacyjnych,
b) Uczelnia – Politechnika Poznańska,
c) Rektor – rektor Politechniki Poznańskiej,
d) Inspektor ochrony danych (IOD) – osoba, którą wyznaczono do realizacji zadań zgodnie z Rozporządzeniem o ochronie danych osobowych (RODO),
e) Inspektor bezpieczeństwa informacji (IBI) – osoba odpowiedzialna za utrzymanie, monitorowanie i doskonalenie SZBI,
f) Użytkownik – osoba przetwarzająca informacje, w tym dane osobowe, posiadająca dostęp do systemów informatycznych Uczelni,
g) Pracownik – osoba świadcząca prace na rzecz Uczelni na podstawie umowy o pracę,
h) Student – student I, bądź II stopnia, doktorant, bądź uczestnik studiów, korzystający

z realizowanego przez Uczelnię procesu dydaktycznego,

i) Osoba zewnętrzna – osoba fizyczna, osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, niebędąca pracownikiem lub studentem, mająca dostęp do informacji, realizująca współpracę z Uczelnią (np. prace zlecone przez Uczelnię),
j) System informatyczny Uczelni – sprzęt komputerowy, oprogramowanie, serwery eksploatowane centralnie w Uczelni, w zespole współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych; w systemie tym pracuje co najmniej jeden komputer centralny i system ten tworzy sieć teleinformatyczną administratora danych,
k) Dane osobowe – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"),
l) Informacje – aktywa niezbędne do zapewnienia prawidłowego funkcjonowania organizacji, realizacji zadań jej powierzonych, wymagające ochrony. Informacje mogą być przechowywane w wielu formach: w postaci elektronicznej, na papierze, bądź niematerialnie w postaci wiedzy posiadanej przez pracowników,
m) Przetwarzanie – rozumie się przez to operację lub zestaw operacji wykonywanych na informacjach, w tym danych osobowych lub zestawach danych osobowych, w sposób zautomatyzowany lub niezautomatyzowany (zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie),
n) Hasło – ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi,
o) Identyfikator (login) – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę w systemie informatycznym,
p) Integralność – właściwość zapewniająca, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
q) Poufność – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom,
r) Dostępność – właściwość określająca możliwość wykorzystania informacji przez użytkownika na żądanie, w określonym czasie,
s) Uwierzytelnianie – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu,
t) Ryzyko – prawdopodobieństwo wystąpienia zagrożenia, które może spowodować powstanie szkód w zasobach Uczelni, przerw bądź zakłóceń w jej funkcjonowaniu i realizacji zaplanowanych celów i zadań,
u) Zagrożenie – rozumie się przez to sytuację / zdarzenie wywołane celowo lub losowo, które stwarza potencjalną możliwość wystąpienia szkody, przerw bądź zakłóceń w funkcjonowaniu Uczelni,
v) Incydent bezpieczeństwa informacji – zdarzenie zakwalifikowane jako istotne lub krytyczne, świadczące o naruszeniu bezpieczeństwa informacji, którego wystąpienie skutkuje utratą poufności, dostępności lub integralności danych.

3. ODPOWIEDZIALNOŚĆ ZA BEZPIECZEŃSTWO INFORMACJI

Odpowiedzialność za bezpieczeństwo informacji ponoszą wszyscy pracownicy, zgodnie z posiadanymi zakresami obowiązków, studenci oraz osoby zewnętrzne, przetwarzające informacje Uczelni.

Rektor odpowiedzialny jest za podejmowanie niezbędnych i odpowiednich kroków mających na celu zapewnienie bezpieczeństwa informacji, w szczególności poprzez:

a) zapewnienie wytycznych i wsparcia dla działań na rzecz bezpieczeństwa informacji zgodnie z przepisami prawa, normami i innymi regulacjami,
b) ustanowienie celów dla bezpieczeństwa informacji,
c) powołanie Inspektora bezpieczeństwa informacji i zapewnienie środków pozwalających wypełniać zlecone zadania,
d) ustanawianie i zatwierdzanie dokumentacji SZBI.

Inspektor bezpieczeństwa informacji odpowiedzialny jest za monitorowanie i doskonalenie SZBI oraz dostosowanie go do zmieniającego się otoczenia organizacyjno-prawnego, w szczególności poprzez:

a) nadzorowanie przestrzegania postanowień SZBI oraz aktualizowania jego zapisów,
b) podejmowanie działań zmierzających do wzrostu świadomości pracowników, studentów i osób zewnętrznych, w zakresie bezpieczeństwa informacji,
c) udzielanie informacji i wytycznych dotyczących SZBI,
d) przeprowadzanie we współpracy z jednostkami organizacyjnymi szacowania i analizy ryzyka elementów SZBI oraz planu postępowania ze zidentyfikowanymi ryzykami,
e) przekazywanie do rektora informacji o działaniach podejmowanych w ramach wdrożenia i utrzymania SZBI ,
f) koordynowanie audytów wewnętrznych i zewnętrznych dot. obszaru bezpieczeństwa informacji,
g) koordynowanie obsługi incydentów bezpieczeństwa informacji.

Kierownicy jednostek organizacyjnych są odpowiedzialni za:

a) nadzorowanie realizacji zapisów wynikających z SZBI w ramach podległych jednostek,
b) określanie dostępu dla podległych pracowników do danych i informacji w systemach informatycznych, w formie tradycyjnej oraz monitorowanie dostępu i wprowadzanie ewentualnych modyfikacji,
c) podejmowanie działań w sytuacjach materializacji ryzyk lub wystąpień incydentów dotyczących bezpieczeństwa informacji,
d) współpracę z Inspektorem bezpieczeństwa informacji w zakresie utrzymywania i doskonalenia systemu, w tym identyfikacji, klasyfikacji informacji i analizy ryzyk w tym zakresie.

Kierownicy:

a) Działu Obsługi i Eksploatacji,
b) Działu Zintegrowanego Systemu Informatycznego,

c) Działu Rozwoju Oprogramowania,
d) Centrum Spraw Studenckich,
e) Działu Bezpieczeństwa,

oraz

f) Inspektor ochrony danych,

z uwagi na podstawowy zakres zadań, ustanowiony regulacjami wewnętrznymi, w sposób szczególny odpowiedzialni są za zapewnienie bezpieczeństwa informacji i podejmowanie działań na rzecz utrzymania i rozwoju SZBI.

Pracownicy, studenci, osoby zewnętrzne odpowiedzialni są za:

a) przestrzeganie zapisów dokumentacji składającej się na SZBI, w tym procedur, instrukcji i zarządzeń,
b) zachowanie w tajemnicy podlegającej ochronie informacji, do których uzyskają dostęp w związku z wykonywanymi obowiązkami, zarówno w trakcie trwania stosunku pracy, lub innego stosunku prawnego, jak i po ich ustaniu,
c) dołożenie starań, aby chronić powierzone im informacje i używane zasoby, w tym w zakresie zapewnienia ochrony przed ich udostępnieniem osobom nieuprawnionym,
d) przeciwdziałanie próbom naruszenia zasad bezpieczeństwa i zgłaszanie wszystkich zdarzeń i incydentów dotyczących naruszenia SZBI zgodnie z obowiązującymi procedurami,
e) zgłaszanie uwag i propozycji zmian SZBI,
f) zaangażowanie w ponoszenie świadomości w zakresie SZBI.

4. BEZPIECZEŃSTWO ZASOBÓW LUDZKICH

W ramach zatrudnienia zobowiązuje się pracowników do zapoznania się z obowiązującymi regulacjami, w tym do realizacji szkoleń wstępnych i stanowiskowych, m.in. z zakresu bezpieczeństwa i ochrony zasobów oraz danych osobowych, zasad bezpieczeństwa fizycznego i kontroli dostępu. W chwili rozpoczęcia wykonywania pracy pracownik otrzymuje uprawnienia dostępu niezbędne do realizowania powierzonych zadań, w przypadku zmiany warunków zatrudnienia uprawienia dostępu podlegają stosownej modyfikacji, w oparciu o wniosek przełożonego.

W przypadku zmiany bądź ustania zatrudnienia uprawnienia dostępu są odbierane lub zmieniane. Odebranie lub zmiana uprawnień dotyczy dostępu fizycznego, a także w ramach systemów informatycznych.

5. ZASADY WSPÓŁPRACY Z OSOBAMI ZEWNĘTRZNYMI

Osoba zewnętrzna uzyskująca dostęp do wybranych informacji i danych Uczelni, zobowiązana jest do przestrzegania wymagań przepisów prawa, a także regulacji wewnętrznych związanych z zapewnieniem bezpieczeństwa informacji.

W Uczelni obowiązują zasady dostępu do sieci i poszczególnych zasobów w tych sieciach, zgodnie z którymi nadawane są na wniosek pracownika koordynującego współpracę, uprawnienia dostępu dla osób zewnętrznych współpracujących z Uczelnią.

6. WSPÓŁPRACA Z ORGANAMI WŁADZY I SPECJALISTAMI ZEWNĘTRZNYMI

Uczelnia utrzymuje kontakty z organami władzy i podmiotami nadzorującymi w przypadkach wskazanych w przepisach prawa i zgodnie z przepisami wewnętrznymi Uczelni, zarówno w zakresie bezpieczeństwa fizycznego (Dział Bezpieczeństwa koordynujący kontakt m.in. z służbami państwowymi odpowiedzialnymi za utrzymanie porządku publicznego i bezpieczeństwa), jak i w zakresie cyberbezpieczeństwa (Inspektor bezpieczeństwa informacji koordynujący kontakt z CSIRT NASK).

Uczelnia umożliwia również utrzymywanie kontaktów ze specjalistami zewnętrznymi, stowarzyszeniami, partnerami, co pozwala na:

a) pogłębianie wiedzy w zakresie bezpieczeństwa informacji, pod kątem prawnym i technicznym,
b) otrzymywanie niezwłocznych informacji o niebezpieczeństwach mogących mieć wpływ na działalność Uczelni,
c) wymianę doświadczeń z podmiotami sektora szkolnictwa wyższego.

7. BEZPIECZEŃSTWO PRZESYŁANYCH I UDOSTĘPNIANYCH INFORMACJI

Udostępniając dane i informacje podlegające szczególnej ochronie zwraca się szczególną uwagę na poprawność danych odbiorcy, któremu przekazywane są informacje.

W przypadku wysyłania danych szczególnej kategorii (wskazane w art. 9 rozporządzenia o ochronie danych osobowych) lub informacji podlegających szczególnej ochronie (np. dane objęte tajemnicą przedsiębiorstwa, dane finansowe, a także nieopublikowane, dotyczące know-how, w szczególności dot. rozwiązań technologicznych oraz dane dostępowe do zasobów) z wykorzystaniem narzędzi elektronicznych, powinny być zaszyfrowane poprzez zabezpieczenie plików hasłem, które przekazane winno zostać odbiorcy za pomocą innego kanału komunikacji, niż zastosowany w celu przekazania informacji.

W przypadku konieczności regularnego przesyłania danych pomiędzy Uczelnią, a innymi podmiotami zaleca się uzgodnienie między stronami sposobu wymiany informacji.

Procedury dotyczące danych i informacji niejawnych oraz sposobu ich przetwarzania i udostępniania regulują odrębne przepisy zewnętrzne i wewnętrzne dotyczące przetwarzania informacji niejawnych.

8. BEZPIECZEŃSTWO ZASOBÓW I SYSTEMÓW

W Uczelni wdrażane, rozwijane i utrzymywane są mechanizmy wielopoziomowych zabezpieczeń ruchu sieciowego, systemów i serwerów Uczelni, chroniące przed nieuprawnionym dostępem, mechanizmy filtrowania poczty elektronicznej, a także zabezpieczenia urządzeń końcowych (komputerów, serwerów, drukarek, dysków), które obejmują konfigurację zapewniającą bieżącą aktualizację oprogramowania, instalację narzędzi sprawdzających, chroniących przed złośliwym oprogramowaniem.

W Uczelni zastosowanie ma zasada ograniczonego dostępu, zgodnie z którą dostęp do zasobów fizycznych, danych i informacji w systemach informatycznych jest ograniczany w szczególności do elementów niezbędnych do prawidłowej realizacji zadań przez pracownika, studenta, bądź osobę zewnętrzną, zgodnie z możliwościami funkcjonalnymi systemu informatycznego. Dostęp do systemów informatycznych realizowany jest w oparciu o procedury uwierzytelniania użytkownika, zapewniające również możliwość uwierzytelniania dwuskładnikowego.

W Uczelni wprowadza się zasady pracy z wykorzystaniem urządzeń przenośnych, nośników danych, korzystania z zasobów IT, w ramach realizacji pracy spoza lokalizacji Uczelni. W ramach zarządzania systemami informatycznymi Uczelni wdrażane i utrzymywane są również zasady dotyczące:

a) projektowania architektury i funkcjonalności z uwzględnieniem aspektów bezpieczeństwa,
b) przeprowadzania testów przedwdrożeniowych, w celu weryfikacji mechanizmów zapewniających bezpieczeństwo danych i informacji,
c) tworzenia i testowania kopii zapasowych oprogramowania,
d) nadzoru nad usługami dostarczanymi przez podmioty zewnętrzne i osoby trzecie,
e) zarządzania hasłami i uwierzytelnianiem użytkowników.

Celem wdrażanych w Uczelni środków bezpieczeństwa jest utrzymanie i bezpieczna eksploatacja zasobów IT i systemów Uczelni, bezpieczeństwo i ciągłość usług, minimalizacja ryzyk, skutków zdarzeń i incydentów bezpieczeństwa.

9. BEZPIECZEŃSTWO FIZYCZNE I ŚRODOWISKOWE

W celu redukcji ryzyka wynikającego z zagrożeń fizycznych i środowiskowych w Uczelni zastosowanie mają procedury kontroli dostępu oraz zasady bezpieczeństwa fizycznego, obejmujące:

a) zarządzanie dostępem fizycznym do obiektów, pomieszczeń i innych miejsc przechowywania informacji, w tym wdrożenie barier fizycznych chroniących przed nieautoryzowanym dostępem,
b) monitoring ruchu osobowego w budynkach i pomieszczeniach Uczelni,
c) stosowanie zabezpieczeń środowiskowych, chroniących informacje i inne aktywa przed zniszczeniem albo uszkodzeniem wywołanym zjawiskami naturalnymi.

Celem wdrażanych w Uczelni środków bezpieczeństwa fizycznego jest ograniczenie możliwości nieuprawnionego dostępu, utraty, uszkodzenia, kradzieży, bądź naruszenia aktywów Uczelni.

10. ZARZĄDZENIE INCYDENTAMI

Pracownicy, studenci oraz osoby zewnętrzne zobowiązani są do poinformowania służb Uczelni o podejrzeniu naruszenia lub naruszeniu bezpieczeństwa informacji, w szczególności w przypadku:

a) stwierdzenia udostępnienia osobom trzecim informacji takich jak: login, hasło, nr PIN itp., bądź stwierdzenie naruszenia dostępu w tym zakresie,
b) wystąpienia nieuprawionego dostępu do urządzenia teleinformatycznego, sieci teleinformatycznej, systemu informatycznego, bądź danych zgromadzonych w systemie informatycznym,
c) celowego zawieszenia działania usługi teleinformatycznej, spowodowanie nieodstępności systemu, usługi,
d) stwierdzenia prób podszywania się pod użytkownika,
e) zidentyfikowania złośliwego oprogramowania, podejrzeń wystąpienia takiego oprogramowania lub prób ataków na infrastrukturę teleinformatyczną Uczelni,
f) zauważeniu elektronicznych lub fizycznych śladów próby włamania do pomieszczeń Uczelni,
g) zidentyfikowaniu zdarzenia bądź incydentu w zakresie bezpieczeństwa fizycznego mienia Uczelni, będącego efektem w szczególności pożaru, zalania itp.

Osoba identyfikująca zdarzenie powinna bezzwłocznie zgłosić ten fakt Uczelni z wykorzystaniem:

a) Systemu Centralnego Punktu Obsługi Zgłoszeń, dostępnego pod adresem pomoc.put.poznan.pl,
b) adresu email pomoc@put.poznan.pl, w przypadku braku dostępu do systemu Centralnego Punktu Obsługi Zgłoszeń,
c) telefonicznie pod numerem 61 663 6111, w przypadku braku możliwości wykonania operacji zgodnych z punktami powyżej.

Do czasu rozwiązania zgłoszenia, zgłaszający zobowiązany jest stosować się do poleceń pierwszej linii wsparcia, Inspektora bezpieczeństwa informacji lub osób przez niego wskazanych, a w szczególności: podjąć działania, mające na celu zapobieganie dalszej eskalacji skutków zdarzenia, w tym:

a) zabezpieczyć urządzenie potencjalnie zainfekowane,
b) odłączyć urządzenie od sieci, odłączając kabel sieciowy lub rozłączając się z siecią bezprzewodową – nie wyłączając maszyny od zasilania,
c) zabezpieczyć miejsce fizyczne, w którym stwierdzono próbę nieuprawnionego dostępu.

W zgłoszeniu przekazać należy wszelkie istotne informacje, w szczególności:

1) dane zgłaszającego:

2) imię, nazwisko, adres email, telefon kontaktowy,
3) miejsce i czas wystąpienia,
4) przebieg zdarzenia bądź incydentu (sposób identyfikacji, wykonane czynności),
5) wskazanie zasobu informatycznego / fizycznego, którego dotyczy zdarzenie bądź incydent,
6) zaobserwowane skutki zdarzenia bądź incydentu,
7) inne istotne informacje.

Inspektor bezpieczeństwa informacji zobowiązany jest do powiadomienia rektora w przypadku stwierdzenia ryzyka mogącego mieć wpływ na podstawową działalność Uczelni, a także koordynuje proces zgłoszenia faktu wystąpienia incydentu do zewnętrznych służb i organów, w tym np. CSIRT NASK, oraz koordynuje komunikację wymaganą w trakcie postępowania ze zdarzeniem bądź incydentem.

11. AUDYTY, PRZEGLĄDY DZIAŁANIA NAPRAWCZE I DOSKONALENIE

W celu zapewnienia wysokiego poziomu bezpieczeństwa informacji, okresowo planowane są audyty wewnętrzne, których celem jest zapewnienie, iż stosowane procedury, zabezpieczenia oraz działania są:

a) zgodne z przepisami prawa powszechnie obowiązującymi, normami, przepisami wewnętrznymi, wytycznymi i procedurami,
b) skuteczne i adekwatne,
c) realizowane zgodnie z założeniami.

Zakres audytu wyznacza Inspektor bezpieczeństwa informacji w uzgodnieniu z rektorem lub wskazanymi osobami i jest on ustalany w oparciu o analizę ryzyka, informacje pozyskiwane od pracowników i współpracowników Uczelni, wyniki kontroli wewnętrznych i zewnętrznych a także wytyczne instytucji zewnętrznych.

W oparciu o działania audytowe, przeglądy zarządzania, zgłoszenia, zdarzenia i incydenty w Uczelni podejmowane są działania naprawcze, mające na celu zapewnienie ciągłego doskonalenia SZBI w Uczelni.