Załącznik Nr 1 do Zarządzenia Rektora Nr 95/2022

Polityka bezpieczeństwa informacji Uniwersytetu Ekonomicznego we Wrocławiu

Wrocław, czerwiec 2022

§1 Postanowienia ogólne

1. Zasoby informacyjne będące w posiadaniu Uniwersytetu Ekonomicznego we Wrocławiu to wysokiej wagi aktywa mające zasadnicze znaczenie zarówno dla interesów Uczelni jak i dla pracowników oraz studentów. Ochrona tych aktywów jest podstawowym obowiązkiem każdego pracownika oraz studenta Uczelni.
2. Niniejsza Polityka Bezpieczeństwa Informacji Uniwersytetu Ekonomicznego we Wrocławiu określa ogólne ramy bezpieczeństwa wszystkich informacji przetwarzanych w ramach Uniwersytetu Ekonomicznego we Wrocławiu. Polityka Bezpieczeństwa Informacji odnosi się do wszystkich procesów i czynności realizowanych w ramach Uczelni oraz dotyczy wszystkich osób w nich uczestniczących.
3. Szczegółowe zasady i procedury bezpieczeństwa poszczególnych informacji przetwarzanych przez Uniwersytet Ekonomiczny we Wrocławiu określają akty wewnętrzne, w szczególności takie jak:
    a. Zasady Bezpieczeństwa Informacji
    b. Polityka Bezpieczeństwa Danych Osobowych,
    c. Regulamin zarządzania i użytkowania sieci komputerowej Uniwersytetu Ekonomicznego we Wrocławiu.
4. Niniejszy dokument został opracowany w oparciu o obowiązujące przepisy prawa oraz na podstawie obowiązujących wytycznych, zaleceń oraz najlepszych praktyk.

§2 Słownik pojęć

Administrator biznesowy SI (AB SI)	Wyznaczony Pracownik odpowiedziany za parametryzację aplikacji Systemu i/lub nadawanie uprawnień Użytkownikom.
Administrator techniczny SI (AT SI)	Wyznaczony Pracownik odpowiedzialny za utrzymanie techniczne Systemu.
Bezpieczeństwo informacji	Ochrona informacji i systemów informatycznych przed nieuprawnionym dostępem, wykorzystaniem, ujawnieniem, uszkodzeniem, modyfikacją i zniszczeniem, w celu zapewnienia poufności, integralności i dostępności.
CI	Centrum Informatyki
Dane	Informacje przetwarzane w sposób elektroniczny w szczególności te przetwarzane w ramach Systemów Informatycznych.
Dane chronione	Informacje chronione przetwarzane w sposób elektroniczny w szczególności te przetwarzane w ramach Systemów Informatycznych.
Właściciel biznesowy SI (WB SI)	Wyznaczony Kierownik Jednostki organizacyjnej odpowiedzialny za realizację procesów Uczelni wspieranych przez dany SI lub moduł SI.
Incydent	Niespodziewane lub niepożądane Zdarzenie lub seria takich Zdarzeń świadczących o naruszeniu lub wysokim ryzyku naruszenia bezpieczeństwa Informacji. Identyfikacja Incydentu skutkuje koniecznością podjęcia stosownej reakcji opisanej w ramach regulacji wewnętrznych Uczelni.
Informacje	Wszelkie zasoby informacyjne stanowiące wartość dla Uczelni.

Informacje chronione	Informacje polegające właściwej ochronie ze względu na obowiązujące przepisy prawa (tj. RODO, KSC, 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 (t.j. Dz. U. z 2017 r., poz. 2247 z późn. zm.), ustawę z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (t.j. Dz.U. z 2020 r. poz. 1913 z późn. zm.), wytyczne Narodowego Centrum Nauki oraz akty prawa wewnętrznego Uczelni).
Inspektor Ochrony Danych (IOD)	Osoba wyznaczona przez Uczelnię, wykonująca zadania, o których mowa w art. 39 RODO.
Jednostka organizacyjna	Jednostka organizacyjna Uczelni w rozumieniu Regulaminu Organizacyjnego Uczelni.
Kierujący Jednostką organizacyjną	Kierownik jednostki organizacyjnej zgodnie z Regulaminem Organizacyjnym Uczelni.
KSC	Ustawa z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (t.j. Dz.U. z 2020 r., poz. 1369 z późn. zm.)
Menedżer Bezpieczeństwa Teleinformatycznego (MBT)	Wyznaczony pracownik Centrum Informatyki odpowiedzialny za monitorowanie i utrzymywanie wysokiego poziomu bezpieczeństwa teleinformatycznego Uczelni.
Osoba zewnętrzna	Osoba fizyczna, osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, której ustawa przyznaje zdolność prawną, niebędąca Pracownikiem lub Studentem realizująca na rzecz Uczelni prace zlecone przez Uczelnię, mająca dostęp do Informacji.
Polityka (PBI)	Niniejsza Polityka Bezpieczeństwa Informacji Uniwersytetu Ekonomicznego we Wrocławiu.
Pracownik	Osoba świadcząca pracę na rzecz Uczelni na podstawie umowy o pracę.
Przetwarzanie Informacji	Oznacza operację lub zestaw operacji wykonywanych na Informacjach lub zestawach Informacji w sposób zautomatyzowany lub niezautomatyzowany, taką jak 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.
RKBI	Rektorska Komisja Bezpieczeństwa Informacji.
RODO	Rozporządzenie Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE. L Nr 119, str. 1).
System informatyczny (SI)	Zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania danych i narzędzi programowych

	zastosowanych w celu przetwarzania danych.
Student	Osoba fizyczna korzystająca z realizowanego przez Uczelnię procesu dydaktycznego (w tym także doktorant).
Uczelnia	Uniwersytet Ekonomiczny we Wrocławiu.
Użytkownik	Pracownik, Współpracownik, Student lub Osoba zewnętrzna upoważniona do dostępu do SI Uczelni. W szczególnych przypadkach proces lub mechanizm, który jest upoważniony do uzyskania dostępu do określonych zasobów.
Zdarzenie	Wystąpienie specyficznych cech lub objawów, które mogą wskazywać na naruszenie bezpieczeństwa Informacji.
Wykonawca umowy UE	Kierownik Jednostki organizacyjnej, który jest odpowiedzialny za wykonywanie ze strony Uczelni danej umowy zawartej z Osobą zewnętrzną i kontroluje jej wykonanie przez Osobę zewnętrzną.
Współpracownik	Osoba świadcząca usługi na rzecz Uczelni na podstawie umowy cywilnoprawnej z wyłączeniem umowy o pracę.

§3 Deklaracja Władz Uczelni

1. Władze Uczelni wyrażają potrzebę szczególnego dbania o bezpieczeństwo Informacji, jak też funkcjonowania Uczelni zgodnie z przepisami prawa oraz dobrymi praktykami związanymi z zapewnieniem bezpieczeństwa Informacji.
2. Władze Uczelni zapewniają dostępność środków technicznych i organizacyjnych niezbędnych do ochrony przetwarzanych Informacji odpowiednich do zagrożeń wynikających z prowadzeniem działalności statutowej Uczelni.
3. Władze Uczelni zapewniają wspieranie i podejmowanie stosownych działań mających na celu promowanie postaw Pracowników i Studentów Uczelni dbających o wysoki poziom bezpieczeństwa Informacji.

§4 Cele Polityki

Celami Polityki Bezpieczeństwa Informacji są:

1. zapewnienie zgodności działalności Uczelni z przepisami powszechnie obowiązującego prawa, w zakresie bezpiecznego przetwarzania Informacji i ich reprezentacji w postaci Danych przetwarzanych w SI będących własnością lub utrzymywanych przez Uczelnię.
2. zapewnienie wytycznych w celu właściwego bezpieczeństwa Informacji w ramach realizowanych procesów administracyjnych, dydaktycznych oraz naukowych oraz bezpieczeństwa Danych w ramach utrzymywanych SI.
3. przeciwdziałanie Incydentom bezpieczeństwa Informacji.
4. kształtowanie świadomości Pracowników w zakresie konieczności przestrzegania zasad bezpieczeństwa Informacji.
5. wspieranie podstaw będących elementem budowy i stosowania w Uczelni dobrych praktyk w zakresie bezpieczeństwa Informacji.
6. dbanie o interes Uczelni w odniesieniu do przetwarzanych Informacji.
7. zapewnienie w odniesieniu do przetwarzanych Informacji chronionych odpowiedniego poziomu atrybutów bezpieczeństwa zgodnie z poniższymi wymaganiami:

a) **Poufność**

Nie wolno ujawniać Informacji chronionych Uczelni osobom nieuprawnionym.

Dostęp do Informacji chronionych ograniczony jest do osób posiadających ściśle określone prawa dostępu.

Prawa dostępu osób uprawnionych są udzielane ściśle według potrzeb związanych z zakresem wykonywanych obowiązków służbowych lub ich praw wynikających z obowiązujących przepisów.

SI posiadają odpowiednie zabezpieczenia zapewniające poufność Danych chronionych zarówno trakcie ich przetwarzania, przesyłania i magazynowania.

b) **Integralność**

Informacja chroniona przetwarzana w Uczelni musi być kompletna, aktualna oraz zabezpieczona przed modyfikacją przez osoby nieuprawnione, tak, aby mogła być ona użyta do podejmowania prawidłowych decyzji oraz działań.

SI dysponują odpowiednimi rozwiązaniami zapewniającymi integralność Danych chronionych w sposób adekwatny do potrzeb wynikających ze wspieranego procesu.

c) **Dostępność**

Informacja chroniona przetwarzana w Uczelni musi być dostępna do użytku w każdym momencie, kiedy zachodzi taka potrzeba.

SI zapewniają dostępność Danych chronionych adekwatnie do potrzeb wynikających ze wspieranego procesu stosownie do oczekiwanego czasu ich dostępności.

SI zapewniają dostępność Danych chronionych w przypadkach awarii lub katastrofy zapewniając mechanizmy odtworzenia Danych chronionych zgodnie z ustalonymi czasami wynikającymi z wymagań obsługi wspieranych procesów.

8. Poufność, dostępność i integralność Informacji chronionych zapewniana jest z uwzględnieniem takich atrybutów jak:

a) **Autentyczność**

Pochodzenie lub zawartość (treść) Informacji chronionej przetwarzanej w Uczelni musi być zgodna z rzeczywistą.

b) **Rozliczalność**

Działania na Informacjach chronionych przetwarzanych przez SI muszą być wiarygodnie dokumentowane w postaci elektronicznych zapisów w dziennikach systemów (logach).

W dziennikach systemów odnotowuje się co najmniej działania Użytkowników polegających na dostępie do: SI z uprawnieniami administracyjnymi, konfiguracji SI (w tym konfiguracji zabezpieczeń) oraz przetwarzanych w SI danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa.

c) **Niezaprzeczalność**

Przetwarzanie Informacji chronionych w Uczelni przez SI musi odbywać się w taki sposób, by nie było możliwości zanegowania uczestnictwa w całości lub części wymiany Informacji chronionych przez podmioty uczestniczące w tej wymianie.

Realizacja powyższych wymagań uwzględnia adekwatność stosowanych środków organizacyjno-technicznych celem ich zapewnienia.

§5 Zakres stosowania i zakres odpowiedzialności

1. Polityka obowiązuje:
   a) wszystkich Pracowników oraz Studentów;
   b) wszystkie Osoby zewnętrzne.
2. Nadzór nad bezpieczeństwem danych osobowych (w rozumieniu RODO) sprawuje IOD.
3. Nadzór nad bezpieczeństwem Informacji chronionych w tym Danych chronionych sprawują:
   a) w obszarze ochrony fizycznej - Zastępca Kanclerza ds. Technicznych;
   b) w ramach SI administrowanych i utrzymywanych przez CI oraz systemów monitorowania i rejestracji audiowizualnych - Dyrektor CI.
4. Nadzór nad bezpieczeństwem Danych chronionych w zakresie SI administrowanych i utrzymywanych przez poszczególne Jednostki organizacyjne sprawuje Kierujący Jednostką organizacyjną.
5. Do obowiązków Kierującego Jednostką organizacyjną należy rozwój oraz wspieranie świadomości bezpieczeństwa Informacji w podległym sobie obszarze zarządzania.
6. Wszyscy Pracownicy, Studenci oraz Osoby zewnętrzne zobowiązani są do przestrzegania Polityki.

§6 Ogólne zasady bezpieczeństwa informacji

1. Zasady określone w Polityce powinny być uwzględniane we wszystkich dziedzinach działalności Uczelni.
2. Akty prawa wewnętrznego Uczelni, uszczegółowiające zasady i procedury bezpieczeństwa przetwarzania Informacji chronionych, muszą być zgodne z Polityką. Akty prawa wewnętrznego Uczelni muszą być aktualizowane w zakresie wynikającym ze zmieniającego się otoczenia.
3. Umowy zawierane przez Uczelnię z Osobami zewnętrznymi muszą być zgodne z Polityką i zawierać postanowienia gwarantujące odpowiedni poziom bezpieczeństwa Informacji chronionych.
4. Zapewnienie bezpieczeństwa Informacji chronionych oraz będących ich reprezentacją danych przetwarzanych w SI jest realizowane na poziomach organizacyjnym, administracyjnym, technicznym i fizycznym.
5. Wszyscy Pracownicy, Studenci i Osoby zewnętrzne zobowiązane są do ochrony Informacji przed nieuprawnionym Przetwarzaniem, w szczególności nieuprawnionym dostępem, nieuprawnioną modyfikacją, nieuprawnionym zakłóceniem lub nieuprawnionym usunięciem.
6. Podstawową zasadą bezpieczeństwa informacji w obszarze projektowanie i utrzymywania SI, w szczególności systemów bezpieczeństwa teleinformatycznego, jest domyślna odmowa dostępu do informacji chronionych.
7. Każdy Pracownik jest zobowiązany do zapoznania się treścią Polityki i przestrzegania zasad bezpieczeństwa Informacji wynikających z Polityki oraz innych regulacji dotyczących bezpieczeństwa Informacji obowiązujących w Uczelni. Zasada ta ma zastosowanie również do Osób zewnętrznych. Jeżeli w wykonaniu umowy zawartej pomiędzy Uczelnią a Osobą zewnętrzną, Osoba zewnętrzna uzyskuje dostęp do Informacji chronionych, Wykonawca

umowy UE, określa wymagany zakres zapoznania się Osób zewnętrznych z zasadami bezpieczeństwa Informacji obowiązującymi na Uczelni.

8. Wszyscy Pracownicy zobowiązani są do niezwłocznego informowania swojego przełożonego lub IOD / MBT, a Osoby Zewnętrzne osoby nadzorującej ich pracę w Uczelni, o każdym Zdarzeniu (w szczególności mającym charakter Incydentu), które nie jest zgodne z wymogami Polityki lub mogące doprowadzić do naruszenia zasad Polityki.

§7 Nadzór nad realizacją postanowień Polityki

1. Osoby wskazane w § 5 ust. 3 oraz MBT monitorują realizację postanowień Polityki adekwatnie do obszarów odpowiedzialności oraz weryfikują aktualność Polityki we wszystkich obszarach działalności Uczelni.
2. Zastępca Kanclerza ds. Technicznych, IOD oraz MBT przedstawiają RKBI raporty, na podstawie których RKBI raz w roku dokonuje ogólnej oceny ryzyka związanego z bezpieczeństwem Informacji Uczelni, która jest przedstawiana Rektorowi oraz przekazywana Menedżerowi Kontroli Zarządczej.
3. Każdy Kierujący Jednostką organizacyjną zobowiązany jest do stosowania zasad oraz wytycznych w obszarze zarządzania ryzykiem bezpieczeństwa informacji w ramach procesów utrzymywanych w danej jednostce organizacyjnej oraz współpracy w tym zakresie ze służbami nadzorującymi ten obszar w ramach Uczelni.
4. W procesie analizy zagrożeń i szacowania ryzyka w obszarze bezpieczeństwa Informacji, Kierującego Jednostką organizacyjną wspierają:
   a) Dyrektor CI w zakresie stosowania adekwatnych środków technicznych i informatycznych,
   b) AB SI w zakresie dostępnych funkcjonalności SI oraz niezbędnych uprawnień w ramach SI,
   c) AT SI w zakresie stosowanych zabezpieczeń teleinformatycznych oraz ochrony Danych w ramach SI,
   d) Z-ca Kanclerza ds. Technicznych w zakresie stosowanych adekwatnych środków technicznych oraz fizycznych zabezpieczeń informacji.
   e) IOD – w zakresie określonym w art. 39 ust. 1 lit c) RODO, o ile w procesie są przetwarzane dane osobowe w rozumieniu RODO.

§8 Kontrole i audyty bezpieczeństwa

1. W celu weryfikacji przestrzegania Polityki oraz aktów prawa wewnętrznego, o których mowa w § 1 ust. 3, prowadzone są następujące rodzaje kontroli:
   a) samokontrola – polegająca na bieżącym kontrolowaniu prawidłowości i zgodności z Polityką wykonywania własnej pracy przez każdego Pracownika oraz w ramach realizowanego procesu dydaktycznego przez każdego Studenta,
   b) weryfikacja bieżąca – wykonywana przez bezpośrednich przełożonych Pracowników lub osoby nadzorujących pracę Osób zewnętrznych, zgodnie z posiadanymi

upoważnieniami, polegająca na sprawdzeniu prowadzonych działań w zakresie zgodności z regulacjami wewnętrznymi Uczelni.

c) monitorowanie niezależne – czynności sprawdzające realizowane w ramach obowiązków służbowych przez MBT lub osoby zewnętrzne realizujące je na zlecenie Uczelni.

2. W celu potwierdzenia skuteczności stosowanych środków organizacyjnych i technicznych lub celem zapewnienia prawidłowego bezpieczeństwa informacji, osoby wskazane w § 7 ust. 2, nie rzadziej niż raz na rok przeprowadzają wewnętrzne audyty bezpieczeństwa informacji w postaci kontroli wewnętrznych. Wyniki przeprowadzonych kontroli stanowią element raportu, o którym mowa w § 7 ust. 2.
3. W celu potwierdzenia skuteczności stosowanych środków organizacyjnych i technicznych lub celem zapewnienia prawidłowego bezpieczeństwa informacji Kierownicy jednostek organizacyjnych mogą planować w ramach dostępnego budżetu zewnętrzne audyty bezpieczeństwa informacji. Realizacje audytu bezpieczeństwa informacji co do zakresu oraz terminu należy uzgodnić w przypadku audytu obszaru bezpieczeństwa teleinformatycznego z Dyrektorem CI lub w przypadku obszaru bezpieczeństwa fizycznego informacji z Zastępcą Kanclerza ds. Technicznych.
4. Realizacja zewnętrznych audytów bezpieczeństwa Informacji podlega akceptacji przez Kanclerza.
5. Raporty oraz zawarte w nim potencjalne zalecenia w wyniku zleconych audytów bezpieczeństwa Informacji są przedmiotem oceny pod względem zasadności ich wprowadzenia przez Kierownika jednostki organizacyjnej odpowiedzianej z dany obszar. Niezgodności w zakresie zaleceń i opinii Kierownika jednostki co do terminu i zakresu ich wykonania rozstrzygane są przez RKBI.

§9 Przepisy końcowe

1. Szczegółowe zakresy odpowiedzialności poszczególnych Pracowników oraz sposoby postępowania, mające na celu praktyczną realizację zapisów Polityki, zostały opisane w szczegółowych aktach prawa wewnętrznego Uczelni, o których mowa w § 1 ust. 3.
2. Każdy Pracownik zobowiązany jest zapoznać się z treścią aktów prawa wewnętrznego Uczelni, o których jest mowa w § 1 ust. 3 oraz podpisać oświadczenie, którego treść stanowi załącznik do PBI.
3. Polityka podlega obowiązkowemu przeglądowi co rok przez MBT lub po wystąpieniu incydentu bezpieczeństwa skutkującego istotnymi szkodami dla Uczelni. Przeglądu i w razie konieczności rekomendacji w zakresie potrzeby aktualizacji Polityki dokonuje RKBI, akceptuje Kanclerz i zatwierdza Rektor.