Zasady Bezpieczeństwa Informacji Uniwersytetu Ekonomicznego we Wrocławiu

Wrocław, czerwiec 2022

§1 Słownik pojęć

Administrator biznesowy SI (ABSI)	Wyznaczony Pracownik odpowiedzialny za parametryzację aplikacji Systemu i/lub nadawanie uprawnień Użytkownikom. Szczegółowy zakres obowiązków ABSI zawarty jest w Załączniku nr 1 do ZBI.
Administrator techniczny SI (ATSI)	Wyznaczony Pracownik odpowiedzialny za utrzymanie techniczne Systemu. Szczegółowy zakres obowiązków ATSI zawarty jest w Załączniku nr 1 do ZBI.
Bezpieczeństwo informacji	Ochrona informacji i systemów informatycznych przed nieuprawnionym dostępem, wykorzystaniem, ujawnieniem, uszkodzeniem, modyfikacją i zniszczeniem, w celu zapewnienia poufności, integralności i dostępności.
Chmura obliczeniowa	Pula współdzielonych, dostępnych „na żądanie" przez sieci teleinformatyczne, konfigurowalnych zasobów obliczeniowych (np. sieci, serwerów, pamięci masowych, aplikacji, usług), które mogą być dynamicznie dostarczane lub zwalniane przy minimalnych nakładach pracy zarządczej i minimalnym udziale ich dostawcy.
Chmura obliczeniowa prywatna	Chmura obliczeniowa dostępna do wyłącznego użytku jednego podmiotu, będąca w posiadaniu lub bezpośrednio zarządzana przez ten podmiot.
Dane	Cyfrowa reprezentacja Informacji, w szczególności przetwarzanych w ramach SI lub InT.
Dane chronione	Informacje chronione przetwarzane w sposób elektroniczny, w szczególności te przetwarzane w ramach Systemów Informatycznych.
Dane osobowe	Informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej podlegające ochronie na podstawie RODO.
Elektroniczny nośnik informacji	Nośnik informacji w postaci układu elektronicznego (np. pamięć Flash/USB oraz wbudowana pamięć w Urządzeniu mobilnym), zapisu mechaniczno-optycznego (np. CD/DVD), magnetycznego (taśma magnetyczna) wymagający dostępu do Danych przy udziale Komputera.
Identyfikator użytkownika	Przedmiot, cecha biometryczna, informacja, ciąg znaków, itp, umożliwiające jednoznaczne ustalenie tożsamości danego użytkownika w SI lub InT, celem odróżnienia go od innych użytkowników.
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 ZBI.
Informacje	Wszelkie zasoby informacyjne stanowiące wartość dla Uczelni.
Informacje chronione	Informacje podlegające 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).
Infrastruktura teleinformatyczna (InT)	Zespół urządzeń i łączy transmisyjnych (elementy InT) obejmujący w szczególności platformy sprzętowe (np.: serwery, macierze, stacje robocze), sieć teleinformatyczną (w tym: routery, przełączniki, punkty dostępowe WiFi, zapory sieciowe oraz inne urządzenia sieciowe), oprogramowanie systemowe, narzędziowe (w tym systemy operacyjne, serwery aplikacji, silniki baz danych) oraz inne elementy umożliwiające bezawaryjną i bezpieczną pracę ww. zasobów (w tym zasilacze UPS, generatory prądotwórcze, urządzenia klimatyzacyjne dedykowane dla punktów dystrybucji oraz PSIT), realizujących usługi utrzymania zasobów dla SI. W skład InT wchodzi też Sprzęt komputerowy, Urządzenia drukujące i Urządzenia skanujące.
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.
Kierownik Pionu	Rektor, Prorektor, Kanclerz, Dziekan lub Kwestor.
Kierujący Jednostką organizacyjną	Kierownik jednostki organizacyjnej zgodnie z Regulaminem Organizacyjnym Uczelni.
Konto użytkownika	Logiczna przestrzeń utrzymywana w ramach SI lub InT i/lub zbiór zasobów przypisany lub udostępniony Użytkownikowi.
KSC	Ustawa z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (t.j. Dz.U. z 2020 r., poz. 1369 z późn. zm.)
MDM	(ang. mobile device management) – oprogramowanie do zarządzania UM oraz sprzętem komputerowym z systemem MacOS, obsługiwane przez CI.
Mechanizm uwierzytelnienia użytkownika (Uwierzytelnianie)	Proces weryfikacji tożsamości lub innych atrybutów zgłaszanych przez podmiot lub przejętych od podmiotu (Użytkownika, procesu lub urządzenia) pozwalający na jego jednoznaczną identyfikację.
Menedżer Bezpieczeństwa Teleinformatycznego (MBT)	Wyznaczony pracownik Centrum Informatyki odpowiedzialny za monitorowanie i utrzymywanie wysokiego poziomu bezpieczeństwa teleinformatycznego Uczelni.
Nośnik informacji	Medium fizyczne, które w sposób ulotny (fale elektromagnetyczne, fale dźwiękowe) lub trwały (dokumenty papierowe lub wykonane z innego materiału, Elektroniczne nośniki informacji) zawiera lub przenosi Informacje.
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.

PBI	Polityka Bezpieczeństwa Informacji Uniwersytetu Ekonomicznego we Wrocławiu wprowadzona Zarządzeniem nr 54/2021 Rektora Uniwersytetu Ekonomicznego we Wrocławiu z dnia 7 maja 2021r. z późniejszymi zmianami.
Pomieszczenie specjalne IT (PSIT)	Wydzielone, zamykane pomieszczenie, chronione KD o dostępie fizycznym ograniczonym do wyznaczonych osób (serwerownia, punkt dystrybucji sieci).
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).
Sprzęt komputerowy (Urządzenie komputerowe, Komputer)	Urządzenie, które przetwarza Informacje w postaci Danych na podstawie programu lub sekwencji instrukcji dotyczących sposobu przetwarzania tych danych.
Stanowisko pracy	Miejsce przebywania / pomieszczenie z umeblowaniem / niezbędne elementy infrastruktury fizycznej, które stanowią bezpośrednie otoczenie oraz umożliwiają realizację czynności służbowych przez Pracownika.
System informatyczny (SI)	Zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania danych i narzędzi programowych zastosowanych w celu przetwarzania danych.
System kontroli dostępu (KD)	Zespół rozwiązań organizacyjno-technicznych umożliwiający nadawanie uprawnień dostępu fizycznego do budynków oraz pomieszczeń.
Student	Osoba fizyczna korzystająca z realizowanego przez Uczelnię procesu dydaktycznego (w tym także doktorant).
Środki bezpieczeństwa	Zastosowane środki ochrony w celu spełnienia wymogów bezpieczeństwa (tj. poufności, integralności i dostępności) informacji dla danego SI. Środki bezpieczeństwa mogą obejmować funkcje zabezpieczeń, ograniczenia zarządzania, bezpieczeństwo personelu i bezpieczeństwo struktur fizycznych, obszarów i urządzeń.
Terminal	Komputer umożliwiający dostęp do SI lub InT poprzez środowisko terminalowe pozwalające na zdalne uruchomienie instancji systemu operacyjnego na serwerze terminalowym i udostępnienie obrazu jego pulpitu oraz zwrotne przekazywanie

	poleceń / informacji sterujących (np. klawiatura, myszka).
Uczelnia	Uniwersytet Ekonomiczny we Wrocławiu.
Urządzenie drukujące	Urządzenie pozwalające na zmianę Danych na Informacje zawarte na Nośniku informacji w postaci fizycznej np. w formie dokumentu papierowego lub wykonanego z innego materiału.
Urządzenie mobilne (UM)	UP w postaci np. tabletu, telefonu komórkowego, smartfona.
Urządzenie przenośne (UP)	Urządzenie komputerowe mogące Przetwarzać Dane niezależnie od miejsca jego użycia, w szczególności poza Uczelnią (np. drukarka przenośna, Komputer przenośny w tym UM).
Urządzenia skanujące	Urządzenie pozwalające na zmianę Informacji zawartych na Nośniku informacji w formie np. papierowej na postać Danych.
Urządzenie wielofunkcyjne	Urządzenie łączące cechy Urządzenia drukującego i Urządzenia skanującego.
Użytkownik	Pracownik, Współpracownik, Student lub Osoba zewnętrzna upoważniona do dostępu do SI Uczelni. W szczególnych przypadkach proces lub mechanizm, który jest upoważniony do uzyskana dostępu do określonych zasobów.
Użytkownik uprzywilejowany	Pracownik, który w danym SI lub w ramach elementu InT, posiada uprawnienia wyższego rzędu pozwalające np. na: konfigurowanie parametrów SI lub umożliwiające zakładanie innych Użytkowników, modyfikowanie ich uprawnień lub posiadający uprawnienia techniczne niskiego poziomu pozwalające realizować czynności związane z administracją techniczną elementem InT na poziomie uprawnień typu: root, administrator, sysadm, admin itp.,
Właściciel biznesowy SI (WBSI)	Wyznaczony Kierownik Jednostki organizacyjnej odpowiedzialny za realizację procesów Uczelni wspieranych przez dany SI lub moduł SI.
Właściciel InT (WInT)	Dyrektor CI, odpowiedzialny za utrzymanie i rozwój usług informatycznych zapewniających prawidłowe funkcjonowanie SI. Szczegółowy zakres obowiązków WInT zawarty jest w Załączniku nr 1 do ZBI.
Współpracownik	Osoba świadcząca usługi na rzecz Uczelni na podstawie umowy cywilnoprawnej z wyłączeniem umowy o pracę.
Zadania Uczelni	Podstawowe zadania Uczelni określone w Statucie Uniwersytetu Ekonomicznego we Wrocławiu oraz zadania określone w Regulaminie organizacyjnym Uniwersytetu Ekonomicznego we Wrocławiu.
ZBI	Niniejsze Zasady Bezpieczeństwa Informacji w Uniwersytecie Ekonomicznym we Wrocławiu.
Zdarzenie	Wystąpienie specyficznych cech lub okoliczności, które mogą wskazywać na naruszenie Bezpieczeństwa Informacji.
Zewnętrzny System Informatyczny (ZSI)	SI którego właścicielem i stroną odpowiedzialną za jego utrzymanie oraz zapewnienie odpowiedniego poziomu Bezpieczeństwa Informacji jest podmiot zewnętrzny.

W dokumencie zastosowano skróty nazw komórek organizacyjnych zgodne ze skrótami przyjętymi w Zarządzeniu Rektora w sprawie symboli komórek organizacyjnych i organów Uniwersytetu Ekonomicznego we Wrocławiu.

§2
Wstęp

1. Niniejsze zasady obowiązują w celu zapewnienia niezbędnego poziomu Bezpieczeństwa informacji we wszystkich obszarach działalności Uczelni.
2. Niedopełnienie obowiązków wynikających z ZBI może generować ryzyko wystąpienia błędów, utratę atrybutów Bezpieczeństwa informacji lub skutkować niedostępnością Systemów informatycznych lub elementów InT, na których oparta jest działalność Uczelni. Każdy z tych skutków może generować ryzyko operacyjne, ryzyko prawne oraz ryzyko braku zgodności lub utraty reputacji.
3. Zapewnienie wymaganego poziomu Bezpieczeństwa Informacji i będących ich reprezentacją Danych przetwarzanych w Systemach informatycznych jest realizowane na poziomie organizacyjnym, technicznym i logicznym, przy czym:
   1) poziom organizacyjny stanowią rozwiązania polegające na m.in. przydzielaniu uprawnień dostępu do Informacji zgodnie z zasadą minimalnych niezbędnych uprawnień do wykonywania zadań oraz na oddzieleniu funkcji/ról wykonawczych od funkcji/ról kontrolujących i zatwierdzających;
   2) poziom techniczny stanowią rozwiązania polegające m.in. na zapewnieniu ograniczonego dostępu do budynków, pomieszczeń i lokalizacji, w których są przetwarzane i przechowywane Informacje chronione, wykorzystaniu zamykanych szaf na dokumenty i Nośniki danych oraz na zapewnieniu monitorowania istotnych elementów procesów Uczelni np. przy wykorzystaniu monitoringu wideo;
   3) rozwiązania logiczne polegają m.in. na udostępnianiu funkcjonalności SI oraz InT niezbędnych do realizowania procesów Uczelni w sposób umożliwiający jednoznaczną identyfikację Użytkownika (jednoznaczne identyfikatory – tzw. loginy), wykorzystaniu segmentacji sieci oraz na wykorzystaniu urządzeń chroniących dostęp do sieci lokalnej z sieci zewnętrznych, w tym – z sieci Internet (np. routery, zapory sieciowe typu firewall, urządzenia wykrywające próby penetracji systemów).
4. Szczegółowe zasady zarządzania na poszczególnych poziomach mogą być zawarte w standardach, procedurach i instrukcjach właściwych dla chronionego obszaru.

§3
Kontrola dostępu do SI

1. Prawa dostępu do SI muszą być przydzielone na podstawie uzasadnionych potrzeb związanych z realizacją powierzonych zadań służbowych (zasada uprawnień / wiedzy koniecznej).
2. Kierownicy jednostek są zobowiązani do zapewnienia przestrzegania w podległych Jednostkach następujących zasad:
   1) dostęp do SI możliwy jest tylko dla Pracowników, Współpracowników i Studentów z zastrzeżeniem ust. 3,
   2) SI służą wyłącznie do realizacji procesów i zadań wynikających z realizacji Zadań Uczelni,
   3) poziomy uprawnień w ramach SI należy przyznawać adekwatnie do potrzeb wynikających z wykonywanych obowiązków służbowych.

4) należy przestrzegać obowiązujących procedur w zakresie organizacji pracy jak i nadawania i odbierania uprawnień.

3. Dopuszcza się dostęp do SI oraz elementów InT Osób zewnętrznych jednak pod warunkiem, że osoba ta jest pracownikiem lub zleceniobiorcą wykonawcy, z którym Uczelnia posiada zawartą umowę w zakresie wsparcia / serwisu SI lub elementów InT, pod warunkiem zapewnienia bezpośredniego nadzoru realizowanych działań Osoby zewnętrznej przez Pracownika CI.
4. Dopuszczalne jest wykorzystywanie zewnętrznego mechanizmu Uwierzytelniającego do danego SI, ang. Single Sign-On (SSO) np. Kerberos, ADFS itp., z zastrzeżeniem możliwości zablokowania użytkowania (odebrania wszelkich uprawnień do danego systemu) w sposób niezależny od zewnętrznego systemu Uwierzytelniającego.
5. Bezpośredni przełożony lub osoba nadzorująca realizację prac przez Pracownika lub Współpracownika występuje o zablokowanie/zmodyfikowanie praw dostępu danego Użytkownika do właściwego ABSI, lub w inny sposób, zgodnie z przyjętymi szczegółowymi zasadami, w terminie maksymalnie 3 dni roboczych lub jeśli jest to wymagane niezwłocznie, po zaistnieniu zmian dotyczących danej osoby, mających jakikolwiek wpływ na posiadane uprawnienia dostępu do SI, a w szczególności po:
   1) zaprzestaniu realizacji obowiązków wymagających uprawnień w danym SI;
   2) przeniesieniu do innej Jednostki;
   3) zmianie stanowiska lub zmianie danych teleadresowych mających wpływ na poziom dostępu do SI;
   4) utracie statusu Pracownika lub Współpracownika przez daną osobę;
   5) ujawnieniu w wyniku przeglądu uprawnień nieaktualności praw dostępu Pracownika lub Współpracownika.
6. ABSI zobowiązany jest do przechowywania wniosków potwierdzających podstawę wykonania zmian lub blokady uprawnień Użytkowników SI co najmniej 12 miesięcy po zablokowaniu lub zmianie uprawnień danego Użytkownika.
7. Studenci tracą dostęp do SI oraz InT w sposób automatyczny po okresie roku od skreślenia z listy studentów. Ponowne uzyskanie uprawnień przez byłego studenta możliwe jest wyłącznie w drodze ponownej immatrykulacji.
8. Dla kont Studentów przegląd uprawnień realizowany jest w sposób automatyczny na bieżąco poprzez synchronizację kont Studentów w systemie USOS z systemem AD.
9. Dla kont Pracowników i Współpracowników przegląd uprawnień realizowany jest na trzech poziomach:
   1) automatyczny bieżący poprzez synchronizację danych o stanie zatrudnienia Pracowników i Współpracowników w systemie ERP z systemem AD przez CI,
   2) ręczny okresowy przez WBSI przy współpracy z ABSI,
   3) weryfikacja jakości przeglądu uprawnień przez MBT.
10. Ręczny okresowy przegląd uprawnień Użytkowników w zakresie Pracowników i Współpracowników wykonywany jest nie rzadziej niż raz na rok, nie później niż do dnia 31 marca.
11. Przegląd uprawnień opisany w ust. 10 pkt. 2) polega na porównaniu listy osób zatrudnionych z listą osób uprawnionych w SI. Różnice podlegają wyjaśnieniu i raportowaniu zgodnie z ust. 13 oraz w uzgodnieniu z ABSI odpowiedniej korekcie. Celem realizacji przeglądu uprawnień ABSI dostarcza do WBSI do dnia 28 lutego zestawienie wszystkich użytkowników SI wraz z ich poziomem uprawnień.
12. Przegląd uprawnień w zakresie Użytkowników uprzywilejowanych danego SI należy wykonać ze szczególną uwagą w zakresie niezbędnego poziomu uprawnień tego Użytkownika.

13. Raport, który jednocześnie jest potwierdzeniem przeglądu uprawnień przez WBSI przesyłany jest w formie skanu z podpisanej notatki, której wzór stanowi Załącznik nr 3 do ZBI, pocztą elektroniczną na skrzynkę MBT. Oryginał notatki przechowywany jest przez WBSI właściwego dla danego SI.
14. MBT dokonuje kontroli kompletności i jakości wykonanych raportów określonych w ust. 14. Brak otrzymania raportu z przeglądu uprawnień w wymaganym terminie skutkuje poinformowaniem o tym RKBI. Opóźnienie kontroli o ponad 2 tygodnie skutkuje koniecznością dostarczenia przez danego WBSI wyjaśnień odnośnie przyczyn braku realizacji kontroli w terminie do RKBI oraz skutkuje identyfikacją podwyższonego ryzyka w zakresie kontroli uprawnień w ramach jednostki przynależnej do WBSI.
15. Weryfikacja jakości przeglądu uprawnień polega na porównaniu listy osób zatrudnionych uzyskanych od COSP, CKU, Dziekanatu, z wykazem Użytkowników wygenerowanym przez ABSI wprost z SI oraz z wynikami przeglądu uprawnień Użytkowników danego SI. Wykazy Użytkowników SI mogą mieć postać elektroniczną, np. pliku arkusza kalkulacyjnego, o ile zostały przysłane pocztą elektroniczną z konta osoby odpowiedzialnej za przygotowanie tego wykazu. Weryfikacja jakości przeglądu uprawnień dotyczy dwóch SI wybranych przez MBT na podstawie jego oceny poziomu ryzyka związanego z procesem nadawania uprawnień w ramach wszystkich SI.
16. MBT dokonuje oceny skuteczności procesu kontroli uprawnień w SI i prezentuje podsumowanie oraz wnioski na posiedzeniu RKBI w ciągu miesiąca po terminie okresowej kontroli. Na podstawie podsumowanie przeglądu uprawnień, w przypadku gdy RKBI uzna potrzebę podjęcia określonych działań są one ujmowane w ramach ogólnej oceny ryzyka związanego z bezpieczeństwem Informacji.
17. W przypadku zidentyfikowanego zagrożenia utraty poufności lub integralności Informacji chronionych, bądź w wyniku rażącego naruszenia regulacji wewnętrznych, Kierownik właściwego Pionu, Przewodniczący RKBI, IOD, Dyrektor CI, MBT może zlecić właściwemu ABSI odebranie prawa dostępu do SI dla danego Użytkownika. Realizacja następuje bez zbędnej zwłoki. ABSI potwierdza wówczas realizację takiego zlecenia w postaci zgłoszenia zgodnie z §12 ZBI.

§4
Kontrola dostępu do InT

1. Właściciel InT odpowiada za proces nadawania uprawnień dla Użytkowników uprzywilejowanych w obrębie InT, celem administracji technicznej InT.
2. Uprawnienia dla Użytkowników uprzywilejowanych w zakresie InT nadawane są zgodnie z potrzebami wynikającymi z kompetencji oraz ilości Pracowników wyznaczonych do administrowania InT z uwzględnieniem posiadanych kompetencji przez Pracowników.
3. Nadrzędną zasadą przyznawania uprawnień w ramach InT jest zasada ograniczonych uprawnień wyłącznie do niezbędnych z uwzględnieniem odpowiedniego poziomu zastępowalności.
4. Właściciel InT nadzoruje w tych samych terminach, które określono w §3, przegląd uprawnień Użytkowników uprzywilejowanych w zakresie InT, który polega na weryfikacji zasadności utrzymywania kont administracyjnych w stosunku do obecnego zatrudnienia lub wskazania Pracowników do realizacji zadań związanych z administracją InT.
5. Przegląd uprawnień realizowany jest przez Kierowników Działów CI realizujących czynności administracyjne w ramach InT przy wsparciu MBT oraz Biura CI.

6. Przegląd uprawnień w zakresie InT wykonywany jest w stosunku do elementów InT utrzymujących zasoby lub procesy biznesowe, w których przetwarzane są Informacje chronione. W procesie kontroli powinny być uwzględnione wszystkie elementy InT utrzymujące dany SI lub wszystkie elementy InT danego typu np. wszystkie bazy danych Oracle lub wszystkie serwery Linux.
7. Przegląd uprawnień Użytkowników uprzywilejowanych w zakresie InT raportowany jest zbiorczo zgodnie z procedurą opisaną w §3.

§5
Obowiązki i odpowiedzialność Pracownika i Współpracownika

1. Każdy Pracownik i Współpracownik jest odpowiedzialny za realizowane czynności w ramach SI lub InT.
2. Pracownicy posiadający uprawnienia Użytkownika uprzywilejowanego są dodatkowo odpowiedzialni za realizację czynności związanych z nadawaniem uprawnień innym Użytkownikom w sposób zgodny z obowiązującymi regulacjami z zachowaniem zasady niezbędnego minimum uprawnień.
3. Pracownik posiadający uprawnienia administracyjne na Komputerach odpowiada za zgodność licencyjną w przypadku samodzielnej instalacji oprogramowania strony trzeciej.
4. Każdy Pracownik i Współpracownik odpowiada za nieuprawnione przetwarzanie Danych, co do których Uczelnia nie ma uprawnień (np. danych prywatnych lub należących do stron trzecich).
5. Pracownik, Współpracownik oraz Student nie ma prawa uzyskiwać lub próbować uzyskiwać dostępu do Informacji, które nie są wymagane do wykonywanych przez niego czynności służbowych, a w przypadku Studenta realizacji praw wynikających z Regulaminu studiów.
6. Pracownik, Współpracownik oraz Student nie ma prawa korzystać z Identyfikatora użytkownika i hasła innej osoby lub przekazywać swój Identyfikator użytkownika i hasło innej osobie.
7. Do obowiązków Pracownika i Współpracownika należy:
   1) używanie SI oraz InT tylko do celów przewidzianych jego zakresem obowiązków;
   2) niezwłoczne zgłaszanie zgodnie z §12 ZBI wszelkich prób włamania lub kradzieży majątku lub Informacji chronionych bezpośredniemu przełożonemu (w przypadku Studentów prowadzącemu zajęcia);
   3) znajomość zasad postępowania na wypadek identyfikacji Incydentu związanego z naruszeniem Bezpieczeństwa informacji zgodnie z §12 ZBI;
   4) odpowiednia, wynikająca z przepisów wewnętrznych ochrona wszelkich Informacji chronionych;
   5) przestrzeganie regulacji wewnętrznych i instrukcji dotyczących używanych SI, InT oraz realizacji zadań w zgodzie z przepisami prawa.
8. Pracownikowi i Współpracownikowi nie wolno:
   1) modyfikować lub podejmować prób modyfikacji jakiegokolwiek elementu InT za wyjątkiem Pracowników do tego upoważnionych;
   2) korzystać z oprogramowania nie dopuszczonego do użytku w ramach Uczelni lub z naruszeniem wymogów licencyjnych;
   3) instalować lub podłączać do InT urządzeń nie będących własnością Uczelni za wyjątkiem dedykowanych sieci WiFi dla gości lub infrastruktury przeznaczonej do realizacji procesów edukacyjnych i naukowych np. sieć WiFi eduroam;

4) instalować oprogramowania licencjonowanego Uczelni na urządzeniach nie będących własnością Uczelni niezgodnie z zasadami licencjonowania;
5) nawiązywać połączeń sieciowych z użyciem służbowego Sprzętu komputerowego z niezaufanymi sieciami (poprzez Ethernet, WiFi, LTE itp.), co do których nie ma pewności, że są udostępnione przez zaufaną i znaną stronę trzecią;
6) dokonywać przetwarzania Informacji chronionych podmiotów trzecich z wykorzystaniem służbowego Sprzętu komputerowego bez niezbędnych upoważnień oraz umów regulujących takie przetwarzanie;
7) doprowadzać do sytuacji, w której możliwe jest zapoznanie się z Informacjami chronionymi Uczelni przez osoby nieuprawnione;
8) bez posiadanych uprawnień sondować, podejmować próby obejścia lub łamania któregokolwiek ze stosowanych na Uczelni Środków bezpieczeństwa SI lub InT;
9) wykorzystywać odkrytych luk w zabezpieczeniach SI lub InT. Takie postępowanie, będzie traktowane jako ciężkie naruszenie obowiązków pracowniczych lub złamanie regulaminu studiów i/lub działanie na szkodę Uczelni w przypadku Osób zewnętrznych.

9. ZBI wraz z innymi aktami prawa wewnętrznego realizuje cele PBI w zakresie ochrony Informacji. W stosunku do Użytkownika, który dopuścił się naruszenia obowiązujących zasad Bezpieczeństwa informacji Uczelnia ma prawo skorzystać ze wszelkich dostępnych środków organizacyjnych oraz prawnych wynikających z obowiązujących regulacji, wytycznych oraz przepisów prawa, w tym do złożenia zawiadomienia o popełnieniu przestępstwa oraz dochodzenia roszczeń przewidzianych w Kodeksie Cywilnym.

§6
Hasła

Na Uczelni obowiązują następujące zasady dotyczące użytkowania haseł:

1) hasła należy utrzymywać w ścisłej tajemnicy;
2) nie wolno udostępniać haseł innym Użytkownikom ani ujawniać ich w żadnych okolicznościach;
3) haseł nie wolno zapisywać na papierze, innych nośnikach fizycznych;
4) dopuszcza się zapisywanie haseł w wersji elektronicznej z zastosowaniem mechanizmów ograniczających do nich dostęp wyłącznie dla uprawnionej osoby np. w formie zapamiętywanych haseł we wspieranych przez producenta przeglądarkach internetowych;
5) hasła do kont technicznych i systemowych o najwyższych uprawnieniach typu root, administrator, sys itp., muszą być zapisywane i przechowywane w sposób bezpieczny oraz uniemożliwiający do nich dostęp osobom nieuprawnionym w sposób określony przez Dyrektora CI;
6) przy wprowadzaniu hasła należy upewnić się, że czynność ta nie jest rejestrowana lub obserwowana przez inne osoby;
7) celem zapewnienia dodatkowej ochrony zaleca się stosowanie przez Pracowników i Współpracowników dodatkowego mechanizmu uwierzytelniającego w postaci uruchomienia mechanizmu MFA (ang. Multi Factor Autentication) w ramach dostępnych usług w ramach produktów Microsoft 365 A3 oraz konfiguracji mechanizmu samodzielnego odzyskiwania hasła SSPR (ang. Self Support Password Recovery) umożliwiającego bezpieczny reset hasła przez użytkownika.
8) hasła podlegają zmianie przynajmniej raz na 90 dni;

9) hasło musi zawierać minimum 10 znaków (hasła dla kont uprzywilejowanych np. osób pełniących funkcje administracyjne w ramach InT lub Użytkowników uprzywilejowanych powinny zawierać minimum 16 znaków). Dla Urządzeń mobilnych należy stosować minimum 6 znakowy PIN lub inną adekwatną formę odblokowywania takiego urządzenia oraz uruchomić dostępne metody szyfrowania pamięci wbudowanej;
10) w haśle muszą występować znaki co najmniej z trzech spośród czterech grup znaków: małe litery, duże litery, znaki specjalne (np. !@#$%^&*()_+=-„:;’/.,<|\>?~`), cyfry;
11) po 5-krotnym użyciu niewłaściwego hasła w czasie nie dłuższym niż 5 minut SI lub element InT powinien zablokować dostęp dla danego użytkownika na co najmniej 5 minut,
12) SI oraz elementy InT powinny wymuszać, a Użytkownik ma obowiązek niezwłocznie zmieniać wszelkie hasła tymczasowe;
13) jeżeli zaistnieje podejrzenie, że hasło zostało ujawnione, należy je natychmiast zmienić;
14) nie wolno stosować mechanizmów logowania automatycznego skutkującego brakiem potrzeby zastosowania środka uwierzytelniającego Użytkowników do Sprzętu komputerowego, lub stosować skryptów posługujących się parametrami logowania Użytkowników. Zastosowanie tego typu mechanizmów możliwe jest wyłącznie w uzasadnionych przypadkach po udokumentowaniu i akceptacji Dyrektora CI.
15) stosowanie skryptów automatyzujących prace Użytkowników możliwe jest w przypadku dedykowanych kont technicznych służących do automatyzacji pracy elementów InT lub w ramach realizowanych czynności przez ATSI. Istnienie takich mechanizmów i kont technicznych powinno być określone w dokumentacji technicznej elementu InT. Hasła kont technicznych powinny być przynajmniej 16 znakowe, znane wyłącznie Pracownikom upoważnionym oraz osobom zastępującym. Stosowanie wbudowanych kont technicznych o najwyższych uprawnieniach powinno być ograniczone do niezbędnego minimum;
16) hasła należy tak dobierać, aby były łatwe do zapamiętania, ale trudne do odgadnięcia dla innych osób;
17) nie wolno używać słów i wyrażeń łatwo kojarzonych z Użytkownikiem np. imię, nazwisko, data urodzenia, imię partnera, imię dziecka, numer pesel lub dowodu tożsamości, numerów kart płatniczych lub kodów PIN używanych do obsługi płatności, prostych sekwencji znaków lub cyfr, nie wolno używać haseł stworzonych poprzez dodanie cyfry na początku lub na końcu hasła utworzonego metodą opisaną w punktach 14-15;
18) nie należy używać nazw własnych ani słów podawanych przez słowniki;
19) Identyfikator użytkownika w SI nie może być zmieniany i musi umożliwić jednoznaczną identyfikację osoby, a po odebraniu uprawnień Użytkownikowi w SI powinien być zablokowany; nie powinien być usuwany z SI (kasowany) ani przydzielany innemu Użytkownikowi. W przypadku ponownego zatrudnienia tej samej osoby przydzielone wcześniej konto powinno by ponownie odblokowywane i przydzielone tej osobie;
20) jeżeli w SI funkcjonuje wbudowany przez producenta Identyfikator użytkownika z prawami administratora (wbudowane konto administracyjne), wówczas nie wolno go wykorzystywać do jego obsługi. Konto takie musi być zabezpieczone przy użyciu przynajmniej 16 znakowego hasła spełniającego wymogi ZBI i przechowywane w sposób zapewniający jego poufność. Okres zmian takiego hasła może być dłuższy niż

rok lecz hasło powinno być zmienione w przypadku utraty poufności. Osobą odpowiedzialną za stosowanie się do powyższych zasad jest Pracownik wskazany do administrowania danym elementem InT. Obowiązkiem osoby nadzorującej pracę w/w Pracownika jest inwentaryzacja i zdeponowanie w sposób bezpieczny Identyfikatorów wbudowanych kont technicznych oraz administracyjnych wraz z hasłami. Każdorazowe użycie wbudowanego konta administracyjnego wymaga stosownego zapisu w dzienniku eksploatacji danego SI lub elementu InT wraz z podaniem celu użycia i osoby używającej. Każde użycia wbudowanego konta administracyjnego wymaga zmiany jego hasła i ponownego zdeponowania. Sposób zdeponowania wbudowanych kont administracyjnych musi umożliwiać identyfikację braku jego kompromitacji (np. w ramach zatwierdzonych przez Dyrektora CI systemów dedykowanych do przechowywania haseł lub bezpiecznej koperty). Dopuszcza się przechowywanie wielu Identyfikatorów i haseł do wbudowanych kont administracyjnych w sposób zbiorczy jednak pod warunkiem możliwości zachowania w poufności Identyfikatorów, które nie są potrzebne. Należy tak zorganizować sposób przechowywania Identyfikatorów haseł administracyjnych by dostęp do depozytu wymagał wiedzy i zgody przynajmniej dwóch osób w tym Dyrektora CI;

21) hasła do kont Użytkowników posiadających uprawnienia do zarządzania urządzeniami sieciowymi nie są objęte mechanizmami wymuszania zmiany zgodnymi z ZBI, jednak muszą być zmieniane w przypadku podejrzenia utraty jego poufności lub nie rzadziej niż raz na dwa lata oraz przechowywane w sposób zapewniający ich poufność i dostępność w sytuacjach awaryjnych. Fakt zmiany hasła urządzenia sieciowego musi być odnotowany w dzienniku eksploatacji danego elementu InT;
22) wszelkie urządzenia pracujące w sieci LAN/WAN wyposażone w konsolę zarządzającą (np. Urządzenia drukujące, sieciowe, printservery, karty zarządzające w serwerach, UPS-y), w których nie ma możliwości użycia innego konta niż wbudowane, powinny mieć zmienione hasła zgodnie z ZBI. Nazwa konta wraz z hasłem powinna być przechowywana w bezpiecznej lokalizacji o dostępie ograniczonym do uprawnionych Pracowników. Hasła muszą być zmieniane w przypadku podejrzenia utraty ich poufności lub nie rzadziej niż raz na dwa lata. Fakt zmiany hasła musi być odnotowany w dzienniku eksploatacji danego elementu InT;
23) hasła wymienione w pkt. 20-21 muszą być przechowywane w budynku i pomieszczeniu właściwym do miejsca pracy administratora oraz ich kopia w lokalizacji zapasowej na terenie Uczelni;
24) w przypadku braku możliwości technicznych stosowania w danym SI lub elemencie InT polityki haseł opisanej w niniejszym paragrafie oraz gdy nie ma innych wytycznych dedykowanych dla danego SI lub elementu InT, Dyrektor CI określa na podstawie analizy ryzyka, inną politykę haseł pod warunkiem zastosowania adekwatnych Środków bezpieczeństwa. W każdym przypadku analiza ryzyka oraz zastosowanie odstępstwa podlegają udokumentowaniu oraz przeglądowi w okresach nie dłuższych niż co dwa lata.

§7
Zasada czystego biurka oraz ekranu

1. Pracownicy i Współpracownicy muszą stosować się do poniższych zaleceń:
   1) przed każdorazowym opuszczeniem Stanowiska pracy uniemożliwiającym bezpośredni nadzór Pracownika lub Współpracownika należy zablokować dostęp do

konsoli Komputera tak by do ponownej pracy konieczne było ponowne, poprawne uwierzytelnienie Użytkownika;

2) nośniki Informacji chronionych, gdy nie są używane, należy przechowywać w sposób zabezpieczający je przed niepowołanym dostępem;
3) nie wolno pozostawiać w ramach Stanowiska pracy przychodzących / wychodzących dokumentów / wydruków na okres dłuższy niż jest to konieczne, nie dłużej niż do końca czasu pracy osoby zajmującej to stanowisko;
4) przekazywanie nośników informacji jest dopuszczalne tylko „do ręki" lub do wskazanych miejsc dystrybucyjnych korespondencji wewnętrznej np. w ramach kancelarii ogólnej, nigdy „na biurko";
5) monitory Komputerów należy ustawiać w sposób uniemożliwiający wgląd w wyświetlaną treść osobom nieupoważnionym;
6) komputery po zakończeniu pracy należy wyłączyć, zasada ta nie dotyczy wyznaczonych stanowisk do obsługi ciągłej np. portiernie, administracja InT;
7) w przypadku Terminali obowiązuje użytkowników zasada wylogowanie ze zdalnej sesji terminalowej po zakończeniu pracy / zajęć;
8) ze względu na specyfikę obsługi procesu biznesowego lub technicznego (np. administracja techniczna, aktualizacja oprogramowania) dopuszcza się pozostawienie włączonego Komputera po zakończonym dniu pracy przy zablokowanej konsoli oraz wylogowaniu z nieużywanych SI. Dopuszcza się również by wyznaczone osoby w ramach realizowanych czynności przez CI dokonywały włączenia Komputerów innych jednostek w sposób fizyczny lub zdalny celem zarządzania nimi lub zlecania Pracownikom lub Współpracownikom pozostawiania włączonego Komputera celem np. ich aktualizacji;
9) korespondencja pisemna, listy / zestawienia osób, książki wejścia lub wyjścia, a także pieczątki firmowe, adresowe, imienne, datowniki i pieczątki specjalne powinny być przechowywane przez ich użytkowników w miejscu zabezpieczonym przed nieuprawnionym dostępem, w celu uniemożliwienia ich wykorzystania lub manipulacji przez osoby nieupoważnione.

2. Prezentacje/szkolenia przy użyciu Sprzętu komputerowego dla Osób zewnętrznych powinny być realizowane w sposób minimalizujący możliwość wycieku Informacji chronionych;
3. W celu dodatkowego zabezpieczenia konsoli Komputerów stosuje się automatyczny mechanizm blokady po określonym czasie bezczynności. Mechanizm ten nie jest stosowany w przypadku konsoli do urządzeń znajdujących się w ramach Technicznych pomieszczeniach specjalnych oraz na konsolach służących do monitorowania pracy SI w ramach obowiązków realizowanych przez CI lub w przypadku wyboru trybu prezentacji przez Użytkownika celem realizacji czynności dydaktycznych.

§8
Zabezpieczenia Sprzętu komputerowego i ochrona antywirusowa

1. Zabrania się wynoszenia poza lokalizację Uczelni Sprzętu komputerowego za wyjątkiem UP przypisanych do Pracownika / Współpracowników lub innych urządzeń dedykowanych do zajęć dydaktycznych organizowanymi poza lokalizacjami Uczelni, na których pobranie i użytkowanie przez Pracownika poza Uczelnią zgodnie z Instrukcją Inwentaryzacyjną została wyrażona zgoda przez Kierownika jednostki organizacyjnej i został podpisany rewers na wypożyczenie środka trwałego stanowiącego własność Uczelni.

2. Każdy przypadek potrzeby wyniesienia Sprzętu komputerowego nie będącego UP należy zgłosić do biura Centrum Informatyki (biuro.ci@ue.wroc.pl) podając typ, model i numer inwentarzowy, data wyniesienia oraz planowany okres wyniesienia celem ewidencji, wskazania Pracownika / Współpracownika odpowiedzialnego za dany sprzęt oraz przedłożenia zgody osoby odpowiedzialnej materialnie. W przypadku, gdy nie jest możliwe zastosowanie środków ochrony adekwatnych dla UP oraz gdy przetwarzane dane na wnioskowanym sprzęcie podlegają ochronie, wówczas na podstawie opinii Dyrektora CI zgoda na wyniesienie danego Sprzętu komputerowego może być cofnięta w uzgodnieniu z Kierownikiem danej jednostki.
3. Zabrania się dokonywania samodzielnego modyfikowania i napraw Sprzętu komputerowego poza wskazanymi Pracownikami Centrum Informatyki.
4. Zabrania się pozostawiania Sprzętu komputerowego bez bezpośredniej opieki Pracownika / Współpracownika w samochodzie, przechowalni bagażu, środkach transportu publicznego lub w innych miejscach o zwiększonym ryzyku kradzieży.
5. Każdy Sprzęt komputerowy podlega zasadom związanym z Bezpieczeństwem informacji zgodnie z poniższym:
    1) Każdy Komputer osobisty podlega nadzorowi w zakresie:
        a. weryfikacji zainstalowanego oprogramowania,
        b. weryfikacji zainstalowania, poprawności funkcjonowania i aktualizacji oprogramowania antywirusowego,
        c. weryfikacji poprawności funkcjonowania oprogramowania systemowego i sprzętu,
        d. weryfikacji miejsca podłączenia do sieci komputerowej Uczelni.
    2) Każdy Komputer osobisty podlega konfiguracji w zakresie:
        a. podłączenia do domeny Active Directory i zastosowania obowiązujących polityk bezpieczeństwa (w przypadku MacOS przyłączenia i konfiguracji obowiązującego profilu MDM oraz uwierzytelnienia Użytkowników w ramach AD/AAD),
        b. przypisania do ujednoliconego systemu nazw Sprzętu komputerowego,
        c. ujednoliconego pakietu konfiguracji startowej i oprogramowania określonego przez Dyrektora CI,
        d. konfiguracji ujednoliconego systemu nadawania adresacji IP i rozwiązywania nazw DNS,
        e. identyfikacji i przypisywania do odpowiednich, wydzielonych sieci,
        f. ograniczenia uprawnień administracyjnych Pracowników i Współpracowników NNA za wyjątkiem osób dla których uprawnienia te są niezbędne celem realizacji obowiązków służbowych pod warunkiem uzyskania zgody Dyrektora CI na wniosek Kierownika danej Jednostki organizacyjnej,
        g. ograniczenia uprawnień administracyjnych Pracowników NA pod warunkiem uzgodnienia przez Dyrektora CI takiego ograniczenia z Kierownikiem danej Katedry,
        h. zarządzania aktualizacjami oprogramowania w tym oprogramowania systemowego.
    3) Każdy Komputer przenośny podlega konfiguracji zgodnej z pkt. 2) oraz w zakresie szyfrowania dysków lokalnych poprzez wbudowane mechanizmy w system operacyjny lub inne specjalistyczne oprogramowanie zarządzane przez CI.
    4) Każdy Pracownik i Współpracownik użytkujący Komputer przenośny ma obowiązek podłączenia go do sieci Uczelni poprzez jego podłączenie do infrastruktury kablowej Uczelni (lub sieci WiFi dla Pracowników / Współpracowników) lub zestawienie połączenia VPN przynajmniej raz w miesiącu przez przynajmniej 4 godziny.

5) Każdy Pracownik / Współpracownik użytkujący Komputer przenośny powinien przechowywać w miarę możliwości Dane chronione na dedykowanych zasobach sieciowych Uczelni lub dedykowanym dysku wirtualnym OneDrive, celem ograniczenia ich wycieku lub niedostępności w przypadku kradzieży sprzętu.

6. Każde oprogramowanie lub aplikacja, zanim zostanie dopuszczona do użytkowania na Komputerach służbowych i/lub Urządzeniach mobilnych należących do Uczelni, wymaga pozytywnej opinii w zakresie: zgodności licencyjnej, zgodności z obecnie eksploatowanym oprogramowaniem oraz brakiem zastrzeżeń w zakresie bezpieczeństwa teleinformatycznego. Opinia w zakresie zgodności z pozostałym oprogramowaniem oraz w zakresie bezpieczeństwa teleinformatycznego wydawana jest przez Dyrektora CI z chwilą pozytywnej opinii w zakresie zakupu danego oprogramowania.
7. Dopuszcza się instalowanie oprogramowania bez zgody CI pod warunkiem pobierania go z zaufanego i sprawdzonego źródła, weryfikacji zgodności licencji dopuszczającej użycie danego oprogramowania przez Uczelnie w sposób nieodpłatny i nie łamiący zasad określonych w warunkach licencjonowania tego oprogramowania lub w ramach obowiązujących umów z zastrzeżeniem zapisów określonych w ust. 6. Dopuszczenie to dotyczy wyłącznie obowiązków wykonywanych przez nauczycieli akademickich w celach naukowych lub dydaktycznych. Oprogramowanie zainstalowane bez zgody CI nie podlega wsparciu przez HelpDesk IT. CI jest uprawnione do weryfikacji legalności oraz bezpieczeństwa każdego oprogramowania zainstalowanego na komputerach osobistych.
8. Zabronione jest pobieranie, instalowanie, uruchamianie aplikacji niezgodnych z ZBI oraz nie związanych z realizacją Zadań Uczelni. Ograniczenie to nie dotyczy Pracowników realizujących czynności w ramach CI administrujących oprogramowaniem oraz testujących oprogramowanie, które potencjalnie będzie dopuszczane do użytkowania.
9. Wszystkie Komputery pracujące w ramach Uczelni powinny być chronione przed oprogramowaniem szkodliwym. Rodzaj stosowanej ochrony powinien wynikać z analizy ryzyka związanego z ich eksploatowaniem.
10. Stosowanym środkiem ochrony przed oprogramowaniem szkodliwym jest obowiązek posiadania na każdym Komputerze osobistym oprogramowania antywirusowego Uczelni.
11. Zmian w konfiguracji zabezpieczeń antywirusowych mogą dokonywać jedynie uprawnieni Pracownicy administrujący systemem ochrony antywirusowej i/lub Pracownicy administrujący InT w ramach CI.
12. Komputery nienależące do Uczelni (będące na przykład własnością Osób zewnętrznych realizujących zlecenia dla Uczelni) nie mogą być podłączone do sieci telekomunikacyjnej Uczelni za wyjątkiem dedykowanych rozwiązań np. w postaci sieci WiFi dla gości lub sieci eduroam.
13. Zabrania się umieszczania w napędach i podłączania do Komputerów służbowych jakiegokolwiek typu Elektronicznych nośników nieznanego pochodzenia. W celu realizacji zadań służbowych należy używać wyłącznie Elektronicznych nośników należących do Uczelni. Zabrania się również używania Elektronicznych nośników informacji należących do Uczelni do celów niezwiązanych z realizacją obowiązków służbowych, w szczególności do celów prywatnych. Przed podłączeniem Elektronicznego nośnika informacji należy bezwzględnie sprawdzać aktualność oprogramowania antywirusowego na Komputerze służbowym. Brak aktualizacji należy niezwłocznie zgłaszać zgodnie z obowiązującą procedurą rejestracji i obsługi problemów technicznych w zakresie wsparcia IT. Dodatkowo, jeżeli istnieje podejrzenie lub ryzyko infekcji takiego nośnika, przed jego użyciem należy bezwzględnie wykonać skanowanie dostępnym oprogramowaniem antywirusowym.

14. Celem zapewnienia odpowiedniego poziomu Bezpieczeństwa informacji oprogramowanie antywirusowe lub Pracownik obsługujący to oprogramowanie może:
    1) weryfikować zawartość Elektronicznych nośników przed lub w trakcie ich użytkowania,
    2) wykonywać skan zawartości Komputera, jeśli to możliwe podczas jego nieaktywności, w ramach planowanych sprawdzeń lub w przypadku identyfikacji zagrożenia,
    3) pozyskiwać informacje w zakresie zainstalowanego oprogramowania celem identyfikacji zagrożeń i niezgodności z obowiązującymi zasadami bezpieczeństwa,
    4) ograniczać dostęp do niezgodnych z polityką bezpieczeństwa stron internetowych lub zawartości mogących świadczyć o ich niskiej reputacji,
    5) odłączyć komputer od sieci komputerowej Uczelni i/lub sieci Internet w przypadku wykrycia zagrożenia którego nie można usunąć.

§9
Utrzymanie i rozwój SI

1. Do wszystkich SI Uczelni są przypisane role, które w ramach swoich obowiązków odpowiadają za utrzymanie i rozwój SI w postaci:
    1) Właściciela Biznesowego SI (WBSI),
    2) Administratora Biznesowego SI (ABSI),
    3) Administratora Technicznego (ATSI).
2. Przydzielenie danej osobie odpowiedniej roli oznacza wskazanie Pracownika Uczelni odpowiedzialnego za realizację zadań określonych w Załączniku nr 1 do ZBI. W przypadku wskazania do pełnienia określonej roli Pracownika Uczelni, który pełni funkcję kierowniczą może on wyznaczyć spośród podległych pracowników lub w ramach obowiązujących umów wsparcia zadania, będące elementem realizacji obowiązków wynikających z pełnienia danej roli. Wyznaczenie innego Pracownika do pełnienia określonych zadań lub roli nie zwalnia Pracownika wskazanego pierwotnie z odpowiedzialności za pełnienie obowiązków zgodnie z ZBI. Ponadto wskazanie innego Pracownika wymaga udokumentowania powierzenia danego zakresu obowiązków temu Pracownikowi w zakresie stosownej korekty karty stanowiska pracy lub w zakresie umowy serwisowej oraz pełnienia stosownych funkcji nadzoru nad realizowanymi zadaniami.
3. Lista SI wraz z WBSI stanowi Załącznik nr 2 do ZBI. O umieszczenie SI na liście lub usunięcie go z listy wnioskuje do RKBI Dyrektor Jednostki / kierownik projektu / WBSI po spełnieniu wymagań związanych z SZSI adekwatnie do podstawy zmiany listy SI. Wniosek wymaga wcześniejszego zebrania opinii od dotychczasowych osób pełniących określone role w ramach SI przy zachowaniu obowiązku pozyskania opinii niezależnie od Właściciela InT. Ostateczną decyzję w zakresie potencjalnej zmiany WBSI podejmuje Kanclerz oraz zatwierdza ją Rektor wprowadzając nowelizację Załącznika nr 2 do ZBI.
4. W przypadku budowy interfejsów pomiędzy SI konieczna jest zgoda WBSI, po uprzednim pozyskaniu opinii ABSI i ATSI łączonych SI. W przypadku wdrażanych SI w tym zakresie rolę WBSI pełni osoba powołana do pełnienia roli kierownika projektu, którego celem jest między innymi wdrożenie systemu informatycznego.
5. W przypadku planowanych zmian organizacyjnych na Uczelni, CI przedstawia propozycję ponownego przypisania ról do opinii RKBI oraz Właściciela InT i po pozytywnej decyzji Kanclerza przedstawia nowelizację Załącznika nr 2 do ZBI celem jej wprowadzenia przez Rektora.

6. Kierownicy jednostek organizacyjnych Uczelni zobowiązani są do zgłaszania propozycji zmian lub rozbudowy SI do odpowiedniego WBSI uzyskując wcześniej opinię ABSI, ATSI oraz WInT.

§10
Odpowiedzialność za utrzymanie i rozwój InT

1. InT jest niezależnym od SI obszarem technologicznym, który poprzez poszczególne elementy InT utrzymuje usługi informatyczne dla potrzeb wynikających z utrzymania i rozwoju SI oraz utrzymywania innych usług informatycznych, które mają na celu zapewnienie odpowiednich narzędzi do realizacji obowiązków służbowych przez Pracowników i Współpracowników.
2. Elementy InT utrzymują funkcje oraz zasoby informatyczne, które mogą być współdzielone przez SI, co skutkuje koniecznością ich utrzymania i optymalizacji w sposób niezależny. Niezależność utrzymania i rozwoju elementów InT musi jednak uwzględniać potrzeby wynikające z utrzymania i rozwoju SI oraz zapewnienia odpowiedniego poziomu Bezpieczeństwa informacji.
3. Strategia utrzymania i rozwoju InT powinna bazować na identyfikacji potrzeb związanych z utrzymaniem i rozwojem SI oraz strategią biznesową Uczelni z uwzględnieniem celów oraz priorytetów wynikających z procesu zarządzania ryzykiem w obszarze teleinformatycznym oraz Bezpieczeństwa informacji.
4. Usługi informatyczne świadczone w ramach utrzymania i rozwoju SI powinny podlegać przeglądowi i aktualizacji na podstawie oceny ich adekwatności z uwzględnieniem stosowanych środków ograniczających ryzyko w obszarze teleinformatycznym i Bezpieczeństwa informacji.
5. Identyfikacja nowych ryzyk w otoczeniu oraz w ramach InT powinna odbywać się na bieżąco oraz podlegać adekwatnej reakcji w zależności od stopnia wpływu zgodnie z obowiązującymi regulacjami.

§11
Procedury rozpoczęcia, zawieszania oraz zakończenia pracy w SI.

1. Procedura rozpoczęcia pracy Użytkownika w SI musi być związana z uwierzytelnieniem danej osoby, która ma zamiar realizować czynności w ramach danego SI przed ich rozpoczęciem. Uwierzytelnienie to musi być odnotowywane w logach SI. Zawieszanie pracy w SI wymaga podjęcia działań mających na celu uniemożliwienie dokonywania czynności w danych SI przez inną osobę np. poprzez wylogowanie lub zablokowanie konsoli Komputera.
2. Procedura zakończenia pracy w SI musi obejmować wylogowanie, zamknięcie aplikacji i/lub strony www będących środowiskiem obsługi danego SI.

§12
Postępowanie w razie naruszenia zasad Bezpieczeństwa informacji

1. Każdy Pracownik lub Współpracownik w przypadku podejrzenia naruszenia zasad Bezpieczeństwa informacji zobowiązany jest do niezwłocznego informowania:
   1) bezpośredniego przełożonego w przypadku Pracowników Uczelni,
   2) osoby nadzorującej realizację usług w przypadku Współpracownika,
   3) prowadzącego zajęcia lub innego Pracownika w przypadku Studenta.
2. Pracownik lub Współpracownik z chwilą gdy zidentyfikuje Zdarzenie lub pozyska informacje o nim ma obowiązek niezwłocznego zgłoszenia tego faktu na skrzynkę pocztową incydent@ue.wroc.pl podając podstawowe informacje w zakresie Zdarzenia:
   1) krótki opis Zdarzenia;
   2) datę i godzinę Zdarzenia;
   3) miejsce fizyczne Zdarzenia lub nazwę SI lub aplikacji, nazwę Komputera lub inne informacje umożliwiające identyfikację miejsca Zdarzenia.
3. Za naruszenie zasad Bezpieczeństwa informacji uważa się między innymi:
   1) próbę lub włamanie do pomieszczeń Uczelni;
   2) próbę lub włamanie do SI/InT Uczelni;
   3) dopuszczenie nieupoważnionego Użytkownika do przetwarzania Informacji chronionych;
   4) przetwarzanie danych osobowych niezgodnie z przepisami prawa;
   5) używanie Nośników informacji zawierających Informacje chronione Uczelni w sposób umożliwiający dostęp do nich osób nieupoważnionych;
   6) pozostawienie Nośników informacji, które mogą zawierać lub zawierają Informacje chronione bez nadzoru Pracownika lub Współpracownika;
   7) wystąpienie w SI Uczelni oprogramowania szkodliwego np. wirusów komputerowych, koni trojańskich etc.;
   8) prowadzenie powtarzających się działań zmierzających do wykrycia podatności lub luki w zabezpieczeniach SI i/lub InT, np.: próby penetracji SI / InT z wyłączeniem działań Pracowników realizujących takie czynności zgodnie z zakresem swoich obowiązków w ramach zadań CI;
   9) naruszenie lub próbę naruszenia:
      a. atrybutów Bezpieczeństwa informacji w postaci utraty ich poufności, integralności lub dostępności skutkujących nieuprawnioną modyfikacją, zniszczeniem lub ujawnieniem;
      b. integralności InT lub SI, rozumiane jako wszelkie nieuprawnione modyfikacje konfiguracji, funkcjonalności lub sprzętu;
      c. logiki biznesowej SI skutkującą zmianą zaimplementowanego przepływu informacji lub nieuprawnioną zmianą sposobu przetwarzania;
   10) stan pomieszczeń służbowych lub Stanowisk pracy, który wskazuje na nieuprawnioną ingerencję fizyczną (np. przełamanie zabezpieczeń fizycznych, bałagan, braki wyposażenia);
   11) stan pomieszczeń TPS wskazujący na niewłaściwe funkcjonowanie systemów mających na celu zapewnieni odpowiednich warunków fizycznych pracy InT (np. brak zamknięcia, nieodpowiednia temperatura, brak zasilania, zakurzenie, zalanie, ślady ognia, zadymienie);
   12) przetwarzanie Informacji chronionych z udziałem prywatnej poczty elektronicznej lub przy użyciu prywatnej (nie służbowej) chmury obliczeniowej (tj. usługi OneDrive, Dropbox, Google Drive, inne usługi chmurowe).

4. Powyższy wykaz naruszeń nie stanowi zamkniętego katalogu zdarzeń świadczących o wystąpieniu incydentu w zakresie Bezpieczeństwa informacji, a jest jedynie przykładem identyfikacji tego typu zdarzeń uświadamiający ich istotność w przypadku wystąpienia.
5. W przypadku podejrzenia wystąpienia naruszenia zasad Bezpieczeństwa informacji zakazuje się Użytkownikom, poza obowiązkiem jego zgłoszenia oraz współpracy w ramach jego wyjaśniania, przekazywania jakichkolwiek informacji na temat tego naruszenia innym osobom poza przełożonymi, a w przypadku Studentów poza osobami prowadzącymi zajęcia lub Pracownikiem administracyjnym.
6. Kierujący Jednostkami, w przypadku identyfikacji lub powiadomienia przez Pracownika lub Współpracownika o podejrzeniu naruszenia zasad Bezpieczeństwa informacji, zobowiązani są do:
   1) dopilnowania niezwłocznego i prawidłowego zgłoszenia naruszenia;
   2) określenia kto, kiedy, gdzie i w jaki sposób działał lub zaniechał działania;
   3) określenia rodzaju i wartości wynikłej szkody;
   4) podejmowania niezwłocznego działania celem ograniczenia szkód wynikłych z naruszenia i przywrócenia stanu sprzed naruszenia;
   5) udostępniania informacji służących do wyjaśnienia okoliczności naruszenia szczególnie w przypadku gdy naruszenie zostanie zakwalifikowane jako Incydent;
   6) wnioskowania o ewentualnym wyciągnięciu konsekwencji służbowych wobec osób odpowiedzialnych za naruszenie;
   7) podjęcie działań zaradczych celem uniknięcia podobnego zdarzenia w przyszłości.
7. Naruszenia związane z Bezpieczeństwem informacji w obszarze teleinformatycznym rozwiązywane są zgodnie z obowiązującymi regulacjami przez MBT.
8. Naruszenia związane z Bezpieczeństwem informacji w obszarze fizycznym rozwiązywane są zgodnie z wewnętrznymi regulacjami w zakresie ochrony fizycznej.
9. IOD/MBT/Kanclerz podejmują decyzję o ewentualnym powiadomieniu organów zewnętrznych w swoich obszarach kompetencji. Niezależnie WBSI lub Właściciel InT w porozumieniu z ABSI/ATSI podejmują decyzje o powiadomieniu zewnętrznych dostawców usług lub stron trzecich (klientów, kontrahentów itp.) w zakresie zaistniałego naruszenia w celu podjęcia odpowiednich działań mających na celu ograniczenie potencjalnych strat operacyjnych lub podjęcia współpracy celem rozwiązania Incydentu.
10. Nośniki informacji zawierające potencjalne dowody związane z naruszeniem powinny być zabezpieczone przed modyfikacją lub uszkodzeniem, a w przypadku gdy jest taka możliwość – zdeponowane w bezpiecznym miejscu z ograniczonym dostępem do czasu zakończenia postępowania związanego z naruszeniem.

§13

Zasady poczty elektronicznej oraz dostępu do sieci Internet dla Pracowników i Współpracowników

1. Każdy Pracownik i Współpracownik otrzymuje osobiste konto pocztowe z aliasem przypisanym wyłącznie dla niego. Konto nie jest użytkowane przez inną osobę.
2. Parametry logowania do konta pocztowego są ujednolicone to znaczy, że mogą służyć do uwierzytelnienia w innych SI oraz elementach InT (USOS, WiFi, ePortal, itd.).
3. Wiadomości wysłane z osobistego konta Pracownika lub Współpracownika traktowane są jako wyrażenie jego woli z zastrzeżeniem oświadczeń woli, które wymagają formy pisemnej zgodnie z powszechnie obowiązującymi przepisami prawa .

4. Pracownik oraz Współpracownik ponosi odpowiedzialność ze treść i zasięg wysyłanych wiadomości email, zarówno w zakresie zapewnienia bezpieczeństwa Informacji chronionych jak i zapewnienia prawidłowych relacji pracowniczych.
5. Skrzynka pocztowa udostępniania jest Pracownikowi lub Współpracownikowi wyłącznie w celu realizacji obowiązków służbowych.
6. Zabronione jest konfigurowanie przez Pracownika lub Współpracownika automatycznego przekierowania poczty przychodzącej na zewnętrzny adres mailowy.
7. Zabronione jest wysyłanie pocztą elektroniczną Informacji chronionych do odbiorców z którymi Uczelnia nie ma zawartych stosownych umów współpracy, poufności i/lub powierzenia. Niezależnie od wymagania stosownej relacji prawnej z odbiorcą Informacje chronione należy zabezpieczyć dodatkowo poprzez ich spakowanie do zaszyfrowanego archiwum przy użyciu oprogramowania np. 7-zip z wykorzystaniem algorytmu AES-256 i przynajmniej dwunastoznakowego hasła zgodnego z polityką haseł określoną w par.6 ust.10. Hasło do spakowanego archiwum należy przekazać odbiorcy innym kanałem komunikacji niż poczta elektroniczna np. słownie lub poprzez wiadomość SMS.
8. Wysyłanie wiadomości pocztowych w ramach Uczelni pomiędzy skrzynkami pocztowymi w domenie @ue.wroc.pl zawierających Informacje chronione jest możliwe bez zastosowania dodatkowej ochrony określonej w ust. 7.
9. Poza dostępem do osobistej skrzynki pocztowej dopuszcza się dostęp Pracownika do skrzynki funkcyjnej dedykowanej do obsługi procesów, do której dostęp może mieć więcej Pracowników. Osoby wysyłające wiadomości ze skrzynki funkcyjnej muszą posiadać stosowne upoważnienia do występowania w danej roli lub funkcji. Uruchomienie skrzynki funkcyjnej oraz dostęp Pracownika do skrzynki funkcyjnej realizowany jest na wniosek Kierownika jednostki organizacyjnej. Dopuszcza się wykorzystanie skrzynki funkcyjnej przez danego Pracownika wyłącznie poprzez wcześniejszą identyfikację tego Pracownika osobistym kontem pocztowym.
10. Zabrania się zapisywania / przechowywania informacji chronionych, korespondencji służbowej oraz załączników pochodzących z korespondencji służbowej poza służbowymi Urządzeniami komputerowymi z wyjątkiem opisanym w ust. 11 - 13.
11. Dopuszcza się dostęp przez Pracowników lub Współpracowników do służbowej poczty elektronicznej na urządzeniach prywatnych pod warunkiem stosowania dostępu do zasobów za pomocą wspieranych przez Microsoft i uaktualnionych do najnowszej wersji przeglądarek internetowych wyłącznie poprzez stronę www pod adresem https://office.com lub z wykorzystaniem aplikacji mobilnych Microsoft Outlook, Teams, Yammer, OneDrive na UM pobranych ze sklepów AppStore i/lub Google Play.
12. Dopuszcza się dostęp przez Pracowników lub Współpracowników do SI Uczelni dostępnych w sieci Internet pod warunkiem stosowania i aktualnych przeglądarek internetowych, przy czym Uczelnia wspiera poprawność funkcjonowania SI z wykorzystaniem przeglądarek EDGE, Safari oraz FireFox.
13. W przypadku dostępu do poczty elektronicznej lub do SI Uczelni z urządzenia prywatnego w postaci UM Pracownik lub Współpracownik zobowiązany jest do akceptacji i stosowania się do poniższych zasad:
    1) Pracownik lub Współpracownik jest odpowiedzialny za zabezpieczenie prywatnego UM przed dostępem do Informacji chronionych osób trzecich,
    2) Pracownik lub Współpracownik zobowiązuje się stosować UM z możliwością szyfrowania pamięci wewnętrznej,
    3) Pracownik lub Współpracownik zobowiązuje się stosować blokadę ekranu podczas bezczynności dłuższej niż 3 minuty, stosowania minimum 6 znakowego kodu PIN lub innej adekwatnej formy odblokowywania UM,

4) Pracownik lub Współpracownik zobowiązuje się usunąć wszelkie Informacja pozyskane w trakcie współpracy po jej zakończeniu ze wszystkich urządzeń prywatnych,
5) Nie wolno zapisywać na urządzeniu prywatnym żadnych załączników zawierających Informacje chronione.

14. Każdy Pracownik i Współpracownik pracujący w lokalizacji Uczelni posiada dostęp do sieci Internet, który polega na umożliwieniu korzystania z zasobów sieci Internet w sposób ograniczony do usług związanych z potrzebami wynikającymi z obowiązków służbowych danej Jednostki. Zakres udostępnionych usług dostępnych w sieci Internet dla danej Jednostki określa Dyrektor CI w porozumieniu z Kierownikiem Jednostki lub Kierownikiem Pionu.
15. Dostęp do sieci Internet w lokalizacji Uczelni jest możliwy wyłącznie w celu realizacji czynności służbowych, nie godzących w dobre imię Uczelni oraz związanych z realizacją Zadań Uczelni.
16. Zabrania się wykorzystywania przez Pracownika lub Współpracownika dostępu do sieci Internet w celu prowadzenia czynności nie związanych z czynnościami służbowymi w szczególności takich, które mogłyby narażać Uczelnię na konsekwencje prawne oraz godzić w dobre imię Uczelni.
17. Dostęp do zasobów sieci Internet może być ograniczony ze względu na:
    1) brak dostępności danej usługi w sieci Internet,
    2) brak dostępności części sieci Internet ze względu na ograniczenia wynikające z błędów po stronie operatorów telekomunikacyjnych,
    3) klasyfikację usługi lub treści tej usługi jako jednoznacznie niezwiązanych z potrzebami wynikającymi z realizacji Zadań Uczelni,
    4) klasyfikację usługi lub treści tej usługi jako działającymi na szkodę Uczelni lub na szkodę Bezpieczeństwa Informacji Uczelni.
    5) ograniczoną przepustowość łącza do sieci Internet.
18. Pracownik oraz Współpracownik ponosi odpowiedzialność za swoje działania w sieci Internet.
19. Wszelkie aktywności Pracowników i Współpracowników w sieci Internet mogą być rejestrowane i przechowywane przez CI celem późniejszej weryfikacji i/lub udostępniania w przypadku zidentyfikowanych naruszeń bezpieczeństwa lub sporów.
20. Uczelnia nie świadczy usług w sieci Internet w imieniu i na rzecz podmiotów trzecich nie związanych z realizacją Zadań Uczelni.
21. W uzasadnionych przypadkach Pracownik wyposażony w służbowy Komputer przenośny może uzyskać dostęp do wewnętrznej sieci Uczelni poprzez dostęp zdalny przez sieć Internet realizowany w oparciu o zainstalowane i odpowiednio skonfigurowane oprogramowanie VPN.
22. Dostęp zdalny nadawany jest na wniosek Kierownika Jednostki dla danego Pracownika i umożliwia nie większy zakres dostępu do sieci wewnętrznej Uczelni niż wynikający z dostępu w lokalizacji Uczelni.
23. W szczególnych przypadkach gdy dany Pracownik posiada dostęp do krytycznych zasobów informacyjnych Uczelni, dostęp poprzez VPN do tych zasobów jest możliwy wyłącznie z wykorzystaniem dodatkowych środków ochrony np.. Terminal, stacja przesiadkowa, dodatkowe uwierzytelnienie określone przez Dyrektora CI.
24. Celem zminimalizowania ryzyka infekcji oprogramowaniem szkodliwym przez pocztę elektroniczną, każdy Użytkownik jest zobowiązany do:
    1) nie otwierania wszelkich nieoczekiwanych, nieznanych lub podejrzanych elektronicznych przesyłek pocztowych, szczególnie tych zawierających załączniki;

obowiązuje kategoryczny zakaz zapisywania tego typu przesyłek lub ich załączników na Elektronicznym nośniku informacji, Komputerze lub na udostępnionym zasobie sieciowym;
2) usuwania bez otwierania przesyłek, o których jest mowa powyżej, jeśli jest pewny ich szkodliwości. W przypadku jakichkolwiek podejrzeń kategorycznie nie wolno otwierać takich przesyłek;
3) w przypadku jakichkolwiek wątpliwości w zakresie pochodzenia przesyłek poczty elektronicznej należy natychmiast informować o takich przypadkach wsparcie IT zgodnie z Procedurą rejestracji i obsługi problemów technicznych IT i nie podejmować żadnych czynności związanych z tą przesyłką do czasu obsługi tego zgłoszenia;
4) natychmiastowego poinformowania zgodnie z Procedurą rejestracji i obsługi problemów technicznych IT o wszystkich anomaliach w pracy Komputera lub nieznanych elementach oprogramowania, które nie są rozpoznawane przez Użytkownika;
5) nie przesyłania dalej jakichkolwiek przesyłek nieznanego pochodzenia ostrzegających przed oprogramowaniem szkodliwym, zagrożeniami, lub prośbami o pomoc; w wielu przypadkach są to informacje mające na celu wywołanie fałszywego alarmu lub szerszą dystrybucję złośliwego oprogramowania;
6) nie podejmowania samodzielnych prób usunięcia oprogramowania szkodliwego.

25. Zabrania się używania do celów służbowych poczty elektronicznej innej niż służbowa (np. Gmail, Hotmail, Yahoo, Onet, WP itp.).
26. Używanie przez Pracowników i Współpracowników na Komputerach służbowych prywatnych zasobów chmurowych (OneDrive, Google drive, iCloud itp.) realizowane jest wyłącznie na odpowiedzialność Pracownika. Uczelnia nie ponosi odpowiedzialności za ich usunięcie, zmianę, niedostępność lub ujawnienie.
27. Niezależnie od dostępu do sieci Internet dla Pracowników i Współpracowników, CI utrzymuje dostęp do sieci Internet dla osób uprawnionych do korzystania z dostępu do sieci eduroam, dedykowanych sieci WiFi dla Pracowników / Współpracowników oraz dla gości. Zasady dostępu do sieci Internet dla gości określa Dyrektor CI. Zasady dostępu do sieci komputerowej Uczelni oraz dostępu do sieci WiFi określa „Regulamin Zarządzania Siecią Komputerową Uniwersytetu Ekonomicznego We Wrocławiu”.

§14
Zasady poczty elektronicznej oraz dostępu do sieci Internet dla Studentów

1. Każdy Student otrzymuje osobiste konto pocztowe z aliasem przypisanym wyłącznie dla niego. Konto nie jest użytkowane przez inną osobę.
2. Parametry logowania do konta pocztowego są ujednolicone to znaczy, że mogą służyć do uwierzytelnienia w innych SI oraz elementach InT (USOS, WiFi, ePortal, itd.).
3. Wiadomości wysłane z osobistego konta Studenta traktowane są jako wyrażenie jego woli z zastrzeżeniem wymagania przepisami prawa innej formy np. pisemnej.
4. Student ponosi odpowiedzialność za treść i zasięg wysyłanych wiadomości email w tym za bezpieczeństwo Informacji chronionych.
5. Skrzynka pocztowa udostępniania jest Studentowi wyłącznie w celu realizacji toku studiów.
6. Zaleca się dostęp przez Studentów do poczty elektronicznej z wykorzystaniem przeglądarek internetowych wspieranych przez Microsoft uaktualnionych do najnowszych wersji z wykorzystaniem strony www pod adresem https://office.com lub z

wykorzystaniem aplikacji mobilnych Microsoft Outlook, Teams, Yammer, OneDrive na UM pobranych ze sklepów AppStore i/lub Google Play.

7. Zaleca się dostęp przez Studentów do SI Uczelni dostępnych w sieci Internet pod warunkiem stosowania aktualnych przeglądarek internetowych, przy czym Uczelnia wspiera poprawność funkcjonowania SI z wykorzystaniem przeglądarek EDGE, Safari oraz FireFox.
8. Zabrania się wykorzystywania przez Studenta dostępu do sieci Internet w celu prowadzenia czynności nie związanych z realizacją toku studiów oraz niezgodnych z Regulaminem studiów w szczególności takich, które mogłyby narażać Uczelnię na konsekwencje prawne oraz godzić w dobre imię Uczelni.
9. Dostęp do zasobów sieci Internet może być ograniczony ze względu na:
   1) brak dostępności danej usługi w sieci Internet,
   2) brak dostępności części sieci Internet ze względu na ograniczenia wynikające z błędów po stronie operatorów telekomunikacyjnych,
   3) klasyfikację usługi lub treści tej usługi jako jednoznacznie niezwiązanych z potrzebami wynikającymi z realizacji Zadań Uczelni,
   4) klasyfikację usługi lub treści tej usługi jako działającymi na szkodę Uczelni lub na szkodę Bezpieczeństwa Informacji Uczelni.
   5) ograniczoną przepustowość łącza do sieci Internet.
10. Student ponosi odpowiedzialność za swoje działania w sieci Internet.
11. Wszelkie aktywności Studentów w sieci Internet mogą być rejestrowane i przechowywane przez CI celem późniejszej weryfikacji i/lub udostępniania w przypadku zidentyfikowanych naruszeń bezpieczeństwa lub sporów.
12. Niezależnie od dostępu do sieci Internet dla Studentów w ramach pracowni komputerowych lub sali wykładowych, Student ma prawo do korzystania z sieci WiFi o nazwie „eduroam”. Zasady dostępu do sieci „eduroam” określa Dyrektor CI.
13. Dostęp do sieci Internet dla mieszkańców domów studenckich Uczelni uregulowany jest w odrębnych przepisach.

§15
Zasady kontroli wykorzystania infrastruktury Uczelni

1. Jeśli jest to niezbędne do zapewnienia właściwej organizacji pracy lub wykonywania zadań przez Pracowników / Współpracowników / Studentów lub celem weryfikacji przestrzegania obowiązujących przepisów prawa oraz właściwego użytkowania udostępnionych narzędzi, Uczelnia może prowadzić kontrolę służbowej poczty elektronicznej, dostępu do sieci Internet oraz wykorzystania SI przez Pracowników / Współpracowników oraz Studentów. W przypadku dokonania takiej kontroli Uczelnia zapewni, by działania w tym zakresie nie naruszały tajemnicy korespondencji oraz innych dóbr osobistych.
2. Kontrola, o której jest mowa powyżej, może np. polegać na niezwłocznym przeglądzie zawartości skrzynki poczty elektronicznej oraz innej zawartości Nośników informacji lub podjętych czynności w ramach SI oraz Danych przesyłanych lub przechowywanych przez Użytkownika na Sprzęcie komputerowym. Decyzję o dokonaniu przeglądu mogą podjąć: Kierownik właściwego Pionu, IOD, Przewodniczący RKBI działając samodzielnie lub na wniosek Kierownika danej Jednostki.

§16
Zasady eksploatacji Urządzeń przenośnych

1. Używając UP Pracownik lub Współpracownik ponosi pełną odpowiedzialność za sposób ich użytkowania zapewniający właściwą ochronę Informacji zgodną z obowiązującymi regulacjami.
2. Podczas używania UP należy:
   1) zachować szczególną ostrożność w miejscach publicznych celem minimalizacji ryzyka obserwacji przez nieupoważnione osoby, co może skutkować ujawnieniem Informacji chronionych lub kompromitacją Identyfikatora użytkownika i/lub hasła;
   2) starannie zabezpieczyć UP przed kradzieżą, szczególnie podczas podróży;
   3) weryfikować funkcjonowanie i aktualność zainstalowanego na UP oprogramowania służącego do ochrony antywirusowej;
   4) w przypadku używania UP w miejscu zamieszkania, należy stosować nie gorsze Środki bezpieczeństwa w zakresie Stanowiska pracy niż te obowiązujące na Uczelni, uwzględniając zasadę czystego ekranu oraz biurka.
3. Używanie UP poza Uczelnią nie może skutkować obniżeniem poziomu Bezpieczeństwa informacji stosowanego w lokalizacjach Uczelni.
4. W przypadku przetwarzania Danych chronionych na UP muszą być one zabezpieczone przy użyciu nie gorszych metod kryptograficznych niż wykorzystywane na Uczelni. Dodatkowo Pracownik lub Współpracownik zobowiązany jest do szczególnego nadzoru podczas pracy z UP i nieudostępniania Danych chronionych poza InT (np. prywatna chmura, SMS/MMS, iMessage, AirDrop itp.). Dopuszcza się przetwarzanie Danych chronionych wyłącznie w ramach UP oraz ich przesyłanie w ramach udostępnionych kanałów oraz aplikacji (np. kanał Internet z użyciem VPN, SFTP, Microsoft Outlook, OneDrive).
5. W przypadku utraty, zagubienia lub kradzieży UP należy natychmiast poinformować o tym fakcie przełożonych w przypadku Pracowników lub osoby nadzorującej realizację usług w przypadku Współpracowników oraz zgłosić zdarzenie zgodnie z §12 ZBI.
6. W przypadku gdy utrata UP jest wynikiem działania przestępczego należy zgłosić ten fakt na Policji uzyskując potwierdzenie zgłoszenia tego faktu.

§17
Ochrona Nośników informacji

1. Wszystkie Nośniki informacji zawierające Informacje chronione powinny zostać oznaczone w sposób umożliwiający identyfikację źródła ich pochodzenia (jeżeli jest to możliwe do wykonania) i zabezpieczone przed dostępem osób nieuprawnionych.
2. Nośniki informacji chronionych można tworzyć wyłącznie do celów służbowych. Zabronione jest przechowywanie Nośników informacji chronionej bez określonego celu związanego z realizowanym procesem biznesowym.
3. Nośniki informacji w postaci papierowej zawierające Informacje chronione powinny być umieszczone na papierze firmowym lub na zatwierdzonym wzorze pism. Wszelkie wydruki robocze zawierające Informację chronioną służące do użytku tymczasowego generowane poza zatwierdzonymi wzorami pism muszą zawierać informacje o źródle ich pochodzenia (np. wyciąg studentów o nazwisku Nowak z dnia… Dziekanat) wraz z dopiskiem „Informacja chroniona do użytku wewnętrznego Uniwersytetu Ekonomicznego we Wrocławiu”

4. Nośniki informacji w postaci papierowej zawierające Informacje chronione służące do użytku tymczasowego, które nie podlegają archiwizacji lub nie stanowią elementu procesu biznesowego po zakończeniu ich używania należy niezwłocznie, nie później niż w ciągu 3 dni, zniszczyć (minimalna klasa niszczarki dla dokumentów zawierających pojedyncze rekordy Informacji chronionych to P-4, w przypadku zestawień / listingów zajmujących przestrzeń powyżej jednej strony w formacie A4 minimalną klasą niszczarki jest P-5). Dopuszcza się składowanie zużytych Nośników informacji w zabezpieczonych i zaplombowanych pojemnikach przeznaczonych do specjalistycznej utylizacji.
5. Elektroniczne nośniki informacji chronionej należy dodatkowo chronić przed działaniem silnych pól magnetycznych i elektromagnetycznych, wysoką temperaturą, bezpośrednim nasłonecznieniem oraz działaniem sił fizycznych mogących uszkodzić dany nośnik.
6. Miejsce przechowywania Elektronicznych nośników informacji chronionej zawierających kopie zapasowe SI nie powinno znajdować się w budynku oraz w pomieszczeniu, w którym te informacje są przetwarzane produkcyjnie.
7. Prowadzona jest ewidencja Elektronicznych nośników informacji, na których są wykonywane kopie bezpieczeństwa danych z SI oraz dziennik wykonywanych kopii archiwalnych. Ewidencja oraz dziennik mogą być prowadzone w formie elektronicznej lub papierowej. Dopuszczalne jest stosowanie ewidencjonowania w postaci logu operacji z urządzenia realizującego kopię bezpieczeństwa.
8. Każdy Elektroniczny nośnik informacji używany do wykonywania kopii bezpieczeństwa danych z SI musi być jednoznacznie identyfikowalny.
9. Niezależnie od konieczności stosowania odpowiednich umów Elektroniczny nośnik informacji zawierający Informacje chronione, przekazywany poza Uczelnię musi być ewidencjonowany oraz zabezpieczony kryptograficznie przed nieuprawnionym dostępem. Zabrania się przekazywania materiału kryptograficznego umożliwiającego odczyt takiego nośnika tym samym kanałem co sam nośnik. Powyższa zasada rozdzielności kanałów dotyczy również Informacji chronionych przekazywanych przy użyciu zewnętrznej poczty elektronicznej.
10. Elektroniczne nośniki informacji wykorzystywane na Uczelni do przetwarzania Informacji chronionych obsługiwanych przez Komputery osobiste w postaci np. pendrive/dysków zewnętrznych/pamięci flash powinny zapewniać sprzętowe algorytmy szyfrowania wbudowane w nośnik lub dane przechowywane na takich nośnikach powinny być szyfrowane przy użyciu rozwiązań programowych.
11. Dopuszczenie Elektronicznego nośnika informacji (w postaci pendrive/dysków zewnętrznych/pamięci flash) do przetwarzania Informacji chronionych powinno następować wyłącznie w przypadku, gdy nie można zastosować innej, bezpiecznej metody wymiany Danych (dostępnej w trybie ciągłym lub realizowanej ad-hoc np. sftp) lub w przypadku innych, istotnych przesłanek wynikających z przepisów prawa lub obowiązków wobec instytucji zewnętrznych, w przypadkach których nie można użyć innych dostępnych metod.

§18
Zasady zdalnego dostępu oraz ochrony sieci i InT

1. W przypadku pracy zdalnej Pracownik lub Współpracownik zobowiązany jest do:
   1) weryfikacji i zapewnienia odpowiednich warunków Stanowiska pracy zgodnie z obowiązującymi regulacjami,
   2) zabezpieczenia środków technicznych wykorzystywanych do pracy zdalnej przed ich użyciem przez osoby nieupoważnione,

3) stosowania tych samych lub nie gorszych środków bezpieczeństwa takich jak np. zasada czystego ekranu oraz czystego biurka, do jakich stosowania jest zobowiązany realizując czynności służbowe w lokalizacjach Uczelni.

2. InT jest podstawowym środkiem wymiany informacji w Uczelni i powinna być wykorzystywana wyłącznie do realizacji Zadań Uczelni.
3. InT powinna zapewnić bezpieczeństwo przesyłanych za jej pośrednictwem informacji, a także utrzymywać zaimplementowaną separację danych w ramach SI, które z niej korzystają.
4. Styk sieci LAN z siecią Internet jest elementem InT zwanym również węzłem dostępowym do sieci Internet (Węzeł dostępowy), który podlega szczególnemu nadzorowi z uwagi na wysoki poziom ryzyka spowodowany możliwym dostępem osób nieuprawnionych do SI. Wszelki ruch sieciowy oraz dostępne w Węźle dostępowym obiekty sieciowe podlegają ścisłej kontroli.
5. W celu zapewnienia mechanizmów zachowania ciągłości działania oraz możliwości odtworzenia konfiguracji stosowane są mechanizmy redundancji elementów InT i/lub, wykonywane są kopie danych i/lub konfiguracji elementów InT celem możliwości odtworzenia ich zgodnie z obowiązującymi planami utrzymania ciągłości biznesowej.
6. Dostęp fizyczny do konsol zarządzających i portów diagnostycznych elementów InT musi być zabezpieczony przed nieautoryzowanym wykorzystaniem poprzez odpowiednie mechanizmy uwierzytelniania i autoryzacji.
7. Ruch sieciowy powinien zostać skonfigurowany tak, by dostęp do konsol administracyjnych elementów InT był ograniczony wyłącznie do wskazanych podsieci administracyjnych lub uzgodnionych wewnętrznych statycznych adresów IP.
8. Pomieszczenia pozostawione bez dozoru, o łatwym dostępie osób postronnych, nie mogą być wyposażone w aktywne gniazda sieciowe, umożliwiające dostęp do sieci teleinformatycznej Uczelni.
9. Dostęp fizyczny do elementów InT znajdujących się w PSIT (serwery, urządzenia sieciowe, UPS, agregaty prądotwórcze itp.) powinien być ograniczony do osób upoważnionych.
10. Dopuszcza się przechowywanie klucza awaryjnego w ramach PSIT w celach p.poż w specjalnie dedykowanych skrytkach, których użycie skutkuje zerwaniem plomby lub zbiciem szybki.
11. InT utrzymująca pracę SI powinna być wyposażona w zasilanie gwarantowane w oparciu o zasilacze awaryjne (UPS) i ewentualnie agregat prądotwórczy o długości podtrzymywania adekwatnym do potrzeb wynikających z planów awaryjnych i znaczenia biznesowego SI.
12. Osoby zewnętrzne mogą przebywać w TPS wyłącznie pod nadzorem uprawnionego Pracownika.
13. W ramach TPS zabrania się rejestracji dźwięku oraz obrazu przez Osoby zewnętrzne.
14. W sytuacji, gdy Jednostka posiada wydzieloną sieć elektryczną służącą do zasilania InT, zabezpieczenia przeciążeniowe i ochronne tej sieci i/lub zabezpieczenia przeciążeniowe, UPS powinny znajdować się w TPS.
15. Wszelkie procedury eksploatacyjne InT powinny być dokumentowane, aktualizowane i dostępne dla odpowiednich Pracowników, którym są niezbędne do wykonywania obowiązków służbowych także w przypadku uruchomienia planów utrzymania ciągłości biznesowej. Dokumentacja techniczna InT oraz SI, zawierająca opis konfiguracji oraz stosowanych zabezpieczeń jest Informacją chronioną.

§19

Zasady używania drukarek i skanerów

1. Dostęp dla Osób zewnętrznych do InT w postaci drukarek i skanerów Uczelni jest zabroniony.
2. Pracownik lub Współpracownik zobowiązany jest odbierać wydruki i skanowane dokumenty niezwłocznie po wydrukowaniu / skanowaniu.
3. Zlecone zadania drukowania i skanowania nie powinny być przechowywane w pamięci urządzenia dłużej niż przez czas potrzebny na realizację tego procesu.
4. Drukarki / skanery do użytku Jednostki mogą być podłączone do sieci teleinformatycznej danej Jednostki.
5. Drukarki lub urządzenia wielofunkcyjne udostępnione w przestrzeni wspólnej dostępnej dla wielu Jednostek (urządzenia współdzielone) muszą być podłączone do dedykowanej sieci z ruchem ograniczonym do niezbędnego celem obsługi wydruku, skanowania, monitorowania stanu urządzenia i rozliczania wydruków.
6. Dostęp do urządzeń współdzielonych powinien być ograniczony wyłącznie dla Pracowników lub Współpracowników oraz pozwalać na rozliczalność realizowanych zadań.
7. Proces wydruku i skanowania na urządzeniach współdzielonych powinien być nadzorowany przez użytkownika od momentu uruchomienia procesu wydruku / skanowania do zakończenia wydruku lub zlecenia przekazania elektronicznego wyników skanowania.
8. Nie wolno konfigurować i realizować na urządzeniach skanujących skanowania z przekazaniem wyników digitalizacji bezpośrednio z urządzenia poza InT Uczelni bez zachowania odpowiednich środków kryptograficznych.

§20
Świadomość Bezpieczeństwa Informacji

1. Budowa i utrzymywanie odpowiedniego poziomu świadomości Pracowników i Współpracowników w zakresie Bezpieczeństwa informacji jest jedną z podstaw Bezpieczeństwa informacji.
2. Pracownicy rozpoczynający pracę na Uczelni powinni odbyć szkolenie wprowadzające w zakresie Bezpieczeństwa informacji. Szkolenie powinno zakończyć się testem z podstawowej wiedzy w tym zakresie. W przypadku nie zaliczenia testu Pracownik powinien go odbyć nie później niż tydzień po podjęciu realizacji zadań. Do tego czasu bezpośredni przełożony nie może dopuścić Pracownika do czynności związanych z przetwarzaniem Informacji chronionych. Pozytywnie zdany test jest podstawą do wydania upoważnienia do przetwarzania danych osobowych. Pracownik po zaliczonym szkoleniu oraz po zapoznaniu się z regulacjami wewnętrznymi w obszarze Bezpieczeństwa informacji ma obowiązek podpisać oświadczenie zawierające zobowiązanie Pracownika do przestrzegania obowiązujących zasad. Oświadczenie, o którym jest mowa powyżej, stanowi Załącznik do Polityki Bezpieczeństwa Informacji na Uniwersytecie Ekonomicznym we Wrocławiu.
3. Wszyscy Pracownicy, przed uzyskaniem dostępu do Informacji chronionych oraz SI, muszą podpisać oświadczenie o zachowaniu w tajemnicy wszelkich Informacji chronionych, które uzyskają w ramach wykonywania czynności służbowych.
4. Podpisane oświadczenia, wymienione w pkt. 2 oraz 3, są przechowywane w aktach osobowych Pracownika. COSP jest odpowiedzialna za akta osobowe Pracowników i sprawuje nadzór nad ich aktualnością oraz kompletnością.

5. W przypadku stwierdzenia przez Jednostkę nadzorującą akta osobowe Pracownika Uczelni braku stosownego oświadczenia COSP występuje do Kierującego Jednostką o uzupełnienie brakującego dokumentu.
6. Umyślne lub nieumyślne naruszenie zasad bezpieczeństwa określonych w ZBI, upoważnia Uczelnię do wszczęcia postępowania wobec Pracownika zmierzającego do wyciągnięcia adekwatnych do popełnionego naruszenia konsekwencji służbowych.
7. Po uzyskaniu informacji o dacie zakończenia umowy z Pracownikiem lub o wcześniejszej dacie zakończenia świadczenia pracy, bezpośredni przełożony lub właściwy Kierownik Jednostki zobowiązany do:
   1) poinformowania zgodnie z obowiązującymi procedurami wewnętrznymi Uczelni o konieczności odebrania uprawnień dla danego Pracownika w udostępnionych SI na koniec ostatniego dnia realizacji czynności służbowych;
   2) upewnienia się, że Pracownik pozostawił w Uczelni wszelkie karty dostępu fizycznego oraz jego identyfikator(y) w SI zostały zablokowane.
8. Pracownicy powinni przechodzić przez cykliczne szkolenia przynajmniej raz w roku w zakresie Bezpieczeństwa informacji uwzględniając aktualizację materiału szkoleniowego w oparciu o najnowsze czynniki ryzyka związane z wykonywanymi czynnościami służbowymi. Realizacja szkoleń powinna służyć ograniczeniu błędów ludzkich, kradzieży, oszustw, nadużyć lub strat, a także budowie kompetencji umiejętności identyfikowania i prawidłowego reagowania na ryzyko związane z Bezpieczeństwem informacji.

§21
Bezpieczeństwo fizyczne

1. Zastępca Kanclerza ds. Technicznych jest odpowiedzialny za przygotowanie ochrony budowlanej i mechanicznej jako ograniczenia dostępu do obiektów i pomieszczeń Uczelni oraz zapewnia odpowiednie środki bezpieczeństwa (w postaci np. zamków) niezbędne w procesie ochrony rozwiązań lub urządzeń służących do przetwarzania Informacji.
2. Centrum Informatyki odpowiada za zgodne z regulacjami wewnętrznymi Uczelni oraz prawem polskim zabezpieczenie odpowiednich pomieszczeń elektronicznymi systemami zabezpieczeń oraz za nadzór nad ich prawidłowym działaniem. W uzasadnionych przypadkach Centrum Informatyki odpowiada również za systemy powiadamiania służb ratunkowych lub Policji.
3. Szczegółowy opis stosowanych zasad bezpieczeństwa fizycznego znajduje się w odrębnych przepisach.

§22
Zgodność z obowiązującymi przepisami prawa

1. Pracownicy / Współpracownicy oraz Osoby Zewnętrzne są zobowiązani do przestrzegania przepisów prawa powszechnie obowiązującego oraz wewnętrznych regulacji. W przypadku wątpliwości, co do zasad postępowania w świetle wymagań wynikających z przepisów prawa, należy zasięgać porad prawnych.
2. Instalowanie i eksploatacja oprogramowania w Systemach informatycznych Uczelni odbywa się z uwzględnieniem przepisów prawa, w tym Ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2017 r. , poz. 880) tj. Dz. U. 2018 poz. 1191.

3. Treść umowy licencyjnej podlega uprzedniej weryfikacjiprzez Biuro Prawne przed jej zawarciem.
4. Za obszar zarządzania licencjami oprogramowania odpowiada Centrum Informatyki.
5. Za obszar zgodności licencyjnej odpowiada Kierownik Jednostki, w ramach której oprogramowanie jest eksploatowane.

§23
Odstępstwa

1. W wyjątkowych przypadkach, kiedy z obiektywnych powodów tymczasowo nie można przestrzegać którejś z zasad zawartych w niniejszym dokumencie, należy uzyskać od RKBI akceptację odstępstwa od tych zasad, chyba że z uregulowań szczegółowych wynika inaczej. Każde odstępstwo podlega regularnemu przeglądowi i ponownemu zatwierdzeniu przez RKBI w czasie nie dłuższym niż 12 miesięcy, w celu weryfikacji zasadności dalszego utrzymywania tego odstępstwa.
2. W przypadkach nieuregulowanych, w których zachodzi niespójność interpretacji zasad określonych w ramach ZBI decyzję rozstrzygającą podejmuje Kanclerz po wcześniejszym uzyskaniu opinii RKBI.