ZARZĄDZENIE Nr 392/2023
Rektora Politechniki Częstochowskiej
z dnia 19 czerwca 2023 roku

w sprawie: wprowadzenia znowelizowanej Polityki bezpieczeństwa informacji w systemach teleinformatycznych Politechniki Częstochowskiej

§ 1

W związku z Obwieszczeniem Prezesa Rady Ministrów z dnia 9 listopada 2017 r. w sprawie ogłoszenia jednolitego tekstu rozporządzenia Rady Ministrów 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 roku poz. 2247) oraz Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku 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 119.1, z późn. zm.), wprowadza się znowelizowaną Politykę bezpieczeństwa informacji w systemach teleinformatycznych Politechniki Częstochowskiej, stanowiącą integralną część niniejszego zarządzenia.

§ 2

Traci moc:

- Zarządzenie nr 356/2020 Rektora Politechniki Częstochowskiej z dnia 3.08.2020 roku w sprawie wprowadzenia Polityki bezpieczeństwa informacji w systemach teleinformatycznych Politechniki Częstochowskiej,
- Zarządzenie nr 211/2021 Rektora Politechniki Częstochowskiej z dnia 7.12.2021 roku w sprawie zmian w Zarządzeniu nr 356/2020 Rektora PCz z dnia 03.08.2020 w sprawie wprowadzenia Polityki bezpieczeństwa informacji w systemach teleinformatycznych Politechniki Częstochowskiej.

§ 3

Zarządzenie wchodzi w życie z dniem podpisania.

Rektor
Politechniki Częstochowskiej

RADCA PRAWNY
Aneta Kępa

Prof. dr hab. inż. Norbert Sczygiol

Polityka bezpieczeństwa informacji w systemach teleinformatycznych Politechniki Częstochowskiej

Rozdział I
Postanowienia ogólne
§ 1

Niniejsza Polityka bezpieczeństwa informacji w Politechnice Częstochowskiej (zwana dalej „PBI PCz" lub „polityką bezpieczeństwa") reguluje zagadnienia związane z bezpieczeństwem danych przetwarzanych, przechowywanych, transmitowanych oraz udostępnianych w systemach teleinformatycznych wykorzystywanych w jednostkach organizacyjnych Politechniki Częstochowskiej, w których przetwarzane są ważne dane w kontekście funkcjonowania Uczelni. PBI PCz określa również metody zabezpieczenia systemów teleinformatycznych oraz przetwarzanych informacji przed nieupoważnionym dostępem, awarią oraz utratą danych.

§ 2
Słownik pojęć

1) **administrator systemu teleinformatycznego** (administrator systemu) – osoba nadzorująca pracę systemu teleinformatycznego oraz wykonująca w nim czynności wymagające specjalnych uprawnień;
2) **baza danych** – zbiór uporządkowanych powiązanych ze sobą tematycznie danych zapisanych, np. w pamięci zewnętrznej komputera; baza danych jest złożona z elementów o określonej strukturze rekordów lub obiektów, w których są zapisane dane jednostkowych obiektów;
3) **firewall** (ściana ognia) – urządzenie (lub grupa urządzeń), którego głównym zadaniem jest zabezpieczenie sieci wewnętrznej przed nieuprawnionym dostępem z zewnątrz, jak również zapewnienie kontrolowanego dostępu użytkowników wewnętrznych do sieci publicznej;
4) **hasło** – fraza złożona z liter, cyfr lub innych znaków, które musi podać użytkownik, aby mógł korzystać z dostępu do zastrzeżonych zasobów np. sieci komputerowej, bazy danych, komputera; hasło jest jednym ze sposobów ochrony danych przed osobami nieupoważnionymi;
5) **IOD** – Inspektor Ochrony Danych w rozumieniu art. 37 ogólnego rozporządzenia o ochronie danych osobowych (tzw. RODO);

6) **jednostki organizacyjne** – poszczególne jednostki określone w strukturze organizacyjnej Uczelni, zgodnie z Regulaminem organizacyjnym Politechniki Częstochowskiej;
7) **kierownik** – osoba pełniąca funkcję kierowniczą w jednostce organizacyjnej Uczelni;
8) **klucz kryptograficzny** – parametr przekształcenia matematycznego, który służy do złożenia podpisu cyfrowego;
9) **koń trojański** – program, który podszywając się pod przydatne lub ciekawe dla użytkownika aplikacje, dodatkowo implementuje niepożądane, ukryte przed użytkownikiem szkodliwe funkcje, np. wykrada hasła;
10) **kopie archiwalne** – kopie plików z danymi lub plików oprogramowania, tworzone na nośniku wymiennym lub dysku twardym komputera, przeznaczone do trwałego przechowywania, jak również do odtworzenia danych w przypadku ich utraty lub uszkodzenia;
11) **kopie bezpieczeństwa** – kopie plików danych lub plików programowania tworzone na nośniku wymiennym lub dysku twardym komputera w celu ich odtworzenia w przypadku utraty lub uszkodzenia danych;
12) **MSK CzestMAN** – Miejska Sieć Komputerowa CzestMAN (CzestMAN), jednostka organizacyjna zarządzająca siecią komputerową Politechniki Częstochowskiej, w szczególności infrastrukturą światłowodową, sieciami bezprzewodowymi oraz niektórymi usługami dostępnymi dla pracowników i studentów Uczelni;
13) **ogólnouczelniany system informatyczny** – system informatyczny, który zainstalowany jest na serwerach CzestMAN lub UCI, jest kluczowy dla poprawnego i stabilnego funkcjonowania Uczelni oraz udostępniania usługi dla Uczelni; np.: (Simple.ERP, USOS, Eduroam, e-Learning);
14) **nadzór nad systemami informatycznymi** – sprawowanie kontroli w zakresie przestrzegania zapisów PBI PCz dla systemów teleinformatycznych w Uczelni;
15) **nośnik danych** – wszelkie urządzenia i materiały służące do przechowywania danych w postaci cyfrowej (np. dyski twarde, taśmy magnetyczne, pamięci flash, płyty, itp.);
16) **plik** – ciąg bajtów posiadający swoją nazwę odróżniającą ją od innych plików i parametry, tj.: rozmiar, data powstania lub data ostatniej modyfikacji itp.;
17) **pracownik** – osoba zatrudniona w Politechnice Częstochowskiej w oparciu o umowę o pracę, akt mianowania lub realizująca zlecone czynności na podstawie umowy cywilnoprawnej;

18) **program komputerowy** – zbiór instrukcji, które po umieszczeniu na rozpoznawalnym przez urządzenie nośniku i automatycznym przetłumaczeniu na język zrozumiały dla tego urządzenia powoduje, że osiąga on zdolność do wykonywania danej czynności lub też wykonuje daną czynność;
19) **rejestr administratorów** – lista osób pełniących obowiązki administratorów systemów teleinformatycznych;
20) **serwer** – wyróżniony, specjalistyczny komputer świadczący usługi na rzecz mających z nim łączność innych komputerów np. przechowujący pliki, pośredniczący w przekazywaniu poczty itp.;
21) **serwerownia** – wydzielone pomieszczenie będące środowiskiem pracy komputerów pełniących rolę serwerów, a także aktywnych i pasywnych elementów sieci komputerowych;
22) **sieć komputerowa** – połączenie komputerów umożliwiające im dzielenie się swoimi zasobami, np.: pamięć dyskowa, programy, urządzenia peryferyjne;
23) **sieć publiczna** – sieć telekomunikacyjna wykorzystywana głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych;
24) **system teleinformatyczny** (system IT) – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych; w skład systemu IT wchodzi z reguły komputer (jeden lub wiele połączonych w sieć lub nie) wraz z oprogramowaniem, a także różne urządzenia (urządzenia peryferyjne, np. drukarki, skanery, a także nośniki danych itp.), system IT może być uniwersalny lub przeznaczony do specjalnych zadań (np. system IT finansowo-księgowy itp.);
25) **szkodliwe oprogramowanie** – ogół programów mających szkodliwe działanie w stosunku do systemu komputerowego lub jego użytkownika; do szkodliwego oprogramowania zalicza się wirusy, konie trojańskie, itp.;
26) **transmisja danych, teletransmisja** – przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;
27) **Uczelniane Centrum Informatyczne (UCI)** – jednostka organizacyjna obsługująca administrację centralną w zakresie informatycznym, zarządzająca systemami informatycznymi wdrożonymi przez UCI i nadzorująca pozostałe systemy informatyczne; UCI monitoruje bezpieczeństwo i prawidłowość pracy urządzeń, systemów oraz oprogramowania użytkowego;
28) **Uczelnia** – Politechnika Częstochowska;

29) **uczelniana sieć komputerowa** – własna lub dzierżawiona sieć komputerowa wraz z wszelkimi zasobami teleinformatycznymi będącymi własnością Uczelni;
30) **uwierzytelnianie** – proces poprawnej identyfikacji użytkownika systemu teleinformatycznego w stopniu umożliwiającym przyznanie odpowiednich uprawnień lub przywilejów w systemie informatycznym Uczelni;
31) **użytkownik** – pracownik posiadający uprawnienia do pracy w systemie teleinformatycznym, zgodnie z zakresem obowiązków służbowych; użytkownik z uprawnieniami na poziomie administratora staje się administratorem systemu;
32) **ważne dane** – dane wymagające szczególnej ochrony ze względu na interes Uczelni lub objęte tajemnicą na podstawie odrębnych przepisów;
33) **wirus** – program, który uaktywniony w pamięci operacyjnej, powoduje wadliwe działanie, zniszczenie lub modyfikację systemu operacyjnego, programu komputerowego lub danych;
34) **VPN** – skrót określający wirtualną sieć prywatną (Virtual Private Network); połączenie to zapewnia wyższy poziom ochrony i prywatności podczas połączenia z siecią wewnętrzną PCz; VPN tworzy bezpieczne połączenie za pośrednictwem sieci publicznych (np. Wi-Fi w hotelach), a także w sieciach domowych.

§ 3

1. Nadzór nad wdrożeniem i utrzymaniem właściwego poziomu bezpieczeństwa informacji w Uczelni sprawuje kanclerz.
2. Za realizację oraz przestrzeganie postanowień polityki bezpieczeństwa odpowiadają kierownicy jednostek organizacyjnych.
3. Zarządzanie systemami informatycznymi wdrożonymi przez UCI i nadzór nad pozostałymi systemami informatycznymi należy do UCI.
4. Za stan bezpieczeństwa danych komputerowych, zainstalowanego oprogramowania oraz sprzętu komputerowego odpowiedzialni są:
   1) kierownicy jednostek organizacyjnych – poprzez wyznaczenie administratorów systemów informatycznych użytkowanych w jednostce organizacyjnej, zgodnie z procedurą określoną w § 36;
   2) administrator systemu teleinformatycznego;
   3) użytkownik – odpowiedzialny za przetwarzane dane i wszelkie czynności wykonywane z poziomu swojego konta w systemie informatycznym.
5. Wszyscy użytkownicy systemu teleinformatycznego są zobowiązani do zapoznania się z przepisami normującymi kwestie związane z bezpieczeństwem informacji w Uczelni. Zapoznanie się z PBI PCz musi zostać potwierdzone

stosownym oświadczeniem (Załącznik nr 1) poprzez wygenerowanie dokumentu elektronicznego na stronie internetowej UCI. Dokument potwierdzający, opatrzony sumą kontrolną przechowuje kierownik jednostki organizacyjnej. UCI prowadzi elektroniczny rejestr złożonych oświadczeń.

Rozdział II
Możliwe zagrożenia bezpieczeństwa informacji
§ 4

1. Do czynników zagrażających bezpieczeństwu danych należą:
   1) próby naruszenia spójności i poufności danych, a w szczególności: włamania do systemu, podsłuch, kradzież danych, nieumyślna lub celowa modyfikacja danych, zniszczenie danych;
   2) szkodliwe oprogramowanie;
   3) awarie sprzętu lub oprogramowania;
   4) utrata sprzętu lub nośników z ważnymi danymi;
   5) próby wyłudzenia danych (np. phishing);
   6) inne, skutkujące utratą lub uszkodzeniem danych.
2. W przypadku wystąpienia podejrzenia naruszenia bezpieczeństwa informacji, a w szczególności zaistnienia zdarzenia, o którym mowa w ust. 1, pracownik Uczelni jest zobowiązany postępować zgodnie z procedurą określoną w Załączniku nr 2.

Rozdział III
Zabezpieczenie systemów informatycznych przed zjawiskami fizycznymi
§ 5

1. Pomieszczenia serwerowni, w których eksploatowane są systemy informatyczne oraz pomieszczenia, w których przechowywane są nośniki danych, powinny być:
   1) wolne od zagrożeń związanych ze zjawiskami fizycznymi typu:
      a) wyładowania elektrostatyczne i atmosferyczne (itp. elektryzujące się wykładziny, sąsiedztwo urządzeń odgromowych),
      b) silne działanie pól elektromagnetycznych (itp. bliskie sąsiedztwo stacji transformatorowych i urządzeń rozdzielczych wysokiego napięcia, pól magnetycznych, pochodzących od urządzeń z silnikami elektrycznymi wysokiej mocy lub od transformatorów zasilania budynków itp.);
   2) zabezpieczone systemem ochrony przeciwpożarowej;
   3) zabezpieczone przed zalaniem.

2. Serwerownie powinny mieć zapewnione gwarantowane zasilanie w postaci niezależnego przyłącza zasilania rezerwowego lub agregatu prądotwórczego oraz zastosowane bezprzerwowe zasilacze awaryjne UPS. W pomieszczeniu serwerowni, dla poprawnej pracy urządzeń, powinna być stale monitorowana i utrzymywana odpowiednia wilgotność i temperatura powietrza. Pomieszczenie serwerowni powinno być wyposażone w zabezpieczenia fizyczne i kontrolę dostępu.
3. Szafy, w których przechowywane są nośniki magnetyczne, powinny zapewniać ochronę przed czynnikami zewnętrznymi, mogącymi doprowadzić do utraty danych oraz zabezpieczać przed dostępem osób nieupoważnionych.

Rozdział IV
Zabezpieczenie systemu teleinformatycznego przed nieuprawnionym dostępem

§ 6

1. Serwery, profesjonalne stacje robocze (posiadające dostęp na poziomie administratora do kluczowych systemów teleinformatycznych), urządzenia teletransmisyjne, szafy teletechniczne, wyłączniki zasilania elektrycznego, szafy z nośnikami magnetycznymi zawierające kopie danych, powinny być usytuowane w pomieszczeniu uniemożliwiającym dostęp osobom nieupoważnionym.
2. Dostęp do pomieszczeń, o których mowa w ust. 1, winien być ściśle kontrolowany poprzez zainstalowane systemy alarmowe oraz systemy kontroli dostępu do pomieszczeń.
3. Zaleca się dodatkowe zabezpieczenie serwerów oraz komputerów, w których są zapisane ważne dane poprzez zastosowanie urządzeń mechanicznych, uniemożliwiających swobodne przemieszczanie oraz utrudniających ich ewentualny zabór.

§ 7

1. Lokalizacja urządzeń komputerowych powinna uniemożliwiać osobom postronnym dostęp do nich, a także wgląd do danych wyświetlanych na monitorach komputerowych.
2. Ograniczenie dostępu nie dotyczy urządzeń przeznaczonych do samoobsługi użytkowników, np. infokiosków, terminali informacyjnych, stanowisk do rejestracji kandydatów.
3. Zasady rozpoczynania, zawieszenia i zakańczania pracy w systemie

informatycznym określa Załącznik nr 3.

§ 8

1. Wszelkie prace konserwacyjne i naprawcze urządzeń komputerowych oraz uaktualnienia systemu teleinformatycznego, wykonywane przez firmę zewnętrzną, powinny odbywać się na zasadach określonych w szczegółowej umowie pomiędzy Uczelnią a tymże podmiotem, z uwzględnieniem klauzuli dotyczącej ochrony przez Zleceniobiorcę wszelkich informacji, do których ma dostęp w czasie wykonywania usługi.
2. Prace, o których mowa w ust. 1, winny zostać odnotowane w rejestrze wykonanych usług/napraw, prowadzonym przez administratora systemu.
3. W przypadku naprawy sprzętu komputerowego w serwisie zewnętrznym ważne dane należy zabezpieczyć (zarchiwizować) oraz, o ile to możliwe, usunąć z nośników informacji.
4. Zlecone UCI naprawy lub modernizacje sprzętu komputerowego upoważniają pracowników centrum do zdjęcia zabezpieczeń i ustawienia haseł tymczasowych po wykonaniu usługi.

§ 9

1. Wszyscy użytkownicy są zobowiązani do przekazywania uszkodzonych nośników danych, zawierających ważne dane do UCI w celu ich zniszczenia, aby uniemożliwić ich odczyt.
2. Przekazanie nośnika winno zostać potwierdzone protokołem zdawczo-odbiorczym, przedstawionym przez pracownika UCI.
3. Uszkodzone nośniki danych, zawierające ważne dane, powinny być fizycznie zniszczone. Z wykonanych czynności sporządza się protokół.

§ 10

1. Za bezpieczeństwo komputerów przenośnych odpowiedzialni są ich użytkownicy.
2. Komputery, o których mowa w ust. 1, po zakończonej pracy winny być przechowywane w warunkach zapewniających ich bezpieczeństwo. Dopuszcza się zabezpieczenie poprzez użycie urządzeń mechanicznych, uniemożliwiających swobodne przemieszczanie sprzętu oraz utrudniających ewentualny zabór.
3. Użytkowanie komputera przenośnego poza terenem Politechniki Częstochowskiej jest dozwolone na zasadach określonych w odrębnym zarządzeniu rektora na podstawie protokołu powierzenia sprzętu według Załącznika nr 13 do Zasad dokumentowania gospodarki środkami trwałymi oraz wartościami niematerialnymi i prawnymi w Politechnice Częstochowskiej.

Rozdział V

Kontrola dostępu do systemów informatycznych

§ 11

1. Dostęp do systemu teleinformatycznego mogą posiadać upoważnieni:
   1) pracownicy – w zależności od wykonywanych czynności służbowych;
   2) wykonawcy usług oraz dostawcy sprzętu lub oprogramowania – w zakresie koniecznym do realizowania danej usługi lub wykonania określonych czynności w systemie za zgodą administratora systemu;
   3) inni użytkownicy – w zakresie ustalonym w stosownej umowie.
2. Osoby, o których mowa w ust. 1, muszą posiadać w systemie własne konto, do którego dostęp powinien być możliwy jedynie poprzez podanie właściwego identyfikatora i hasła.
3. Właściciel konta jest odpowiedzialny za wszelkie działania wykonane z wykorzystaniem jego identyfikatora.
4. Pracownicy dostawców sprzętu i oprogramowania wykonują usługę tylko za zgodą administratorów systemu. Jeśli rodzaj wykonywanych czynności (np. uaktualnienie, poprawienie błędnej lub wadliwie działającej konfiguracji oprogramowania bądź sprzętu) wymusza pracę na kontach administracyjnych – usługa winna być nadzorowana przez administratora systemu. Z przeprowadzonych zmian powstaje protokół.

§ 12

1. Zabronione jest podejmowanie działań mogących stwarzać zagrożenie dla systemu teleinformatycznego oraz przetwarzanych w nim informacji. W szczególności niedopuszczalne jest:
   1) udostępnianie identyfikatorów i haseł osobom postronnym;
   2) łamanie haseł;
   3) dokonywanie włamań na konta innych użytkowników;
   4) nieprawne uzyskiwanie dostępu do kont administracyjnych;
   5) zakłócanie działania usług;
   6) omijanie i badanie zabezpieczeń (nie dotyczy audytu lub testowania);
   7) umyślne rozpowszechnianie wirusów, robaków i koni trojańskich oraz niechcianej poczty (spam);
   8) praca na koncie innego użytkownika, za wyjątkiem sytuacji określonej w § 8 ust. 4;
   9) podłączanie prywatnych urządzeń sieciowych typu routery, switche,

accesspointy itp.;

10) podłączanie prywatnych komputerów, laptopów, drukarek itp.;

11) podejmowanie innych działań mogących być zagrożeniem dla systemu.

2. Wykonywanie zabronionych czynności, o których mowa w ust. 1, stanowi naruszenie obowiązków pracowniczych.
3. Zabronione jest użytkowanie sprzętu komputerowego przez osoby nie posiadające uprawnień do pracy w systemie informatycznym.
4. Zabronione jest podłączanie prywatnego sprzętu do fizycznej infrastruktury sieciowej Uczelni.
5. Zasady korzystania z elektronicznej poczty e-mail, określa Regulamin pracy Politechniki Częstochowskiej.

§ 13

1. Rejestracja użytkowników w systemie informatycznym, nadawanie lub modyfikacja uprawnień oraz wyrejestrowywanie użytkowników z systemu odbywa się zgodnie z poniższymi zasadami:
   1) bezpośredni przełożony składa u administratora danego systemu wniosek o zarejestrowanie użytkownika w systemie; wzór Wniosku o zarejestrowanie użytkownika, modyfikację uprawnień, wyrejestrowanie użytkownika określa Załącznik nr 5;
   2) administrator systemu po otrzymaniu wniosku, o którym mowa powyżej, rejestruje użytkownika w systemie nadając mu identyfikator oraz stosowne uprawnienia;
   3) w przypadku zmiany przez użytkownika uprawnień do obsługi danego systemu, administrator po dokonaniu weryfikacji zakresu uprawnień modyfikuje uprawnienia na podstawie wniosku, o którym mowa w pkt. 1, otrzymanego od bezpośredniego przełożonego tego użytkownika;
   4) w przypadku utraty przez użytkownika uprawnień do obsługi danego systemu teleinformatycznego (np. rozwiązanie stosunku pracy, nieobsługiwanie systemu z powodu zmiany stanowiska pracy), bezpośredni przełożony niezwłocznie występuje do administratora systemu z wnioskiem o wyrejestrowanie użytkownika z systemu;
   5) administrator systemu, po otrzymaniu wniosku, weryfikuje wskazany zakres uprawnień i nadaje/modyfikuje dostęp użytkownika do systemu, a w razie wątpliwości – konsultuje go z wnioskodawcą;
   6) ze względów na odrębne przepisy w niektórych systemach konta użytkownika

nie są kasowane, a jedynie blokowane.

2. Procedury związane z nadawaniem upoważnień do przetwarzania danych osobowych określa rektor w drodze odrębnego zarządzenia.

Rozdział VI

Polityka haseł

§ 14

1. Wszystkie systemy informatyczne muszą mieć aktywne mechanizmy kontroli dostępu.
2. Każdy użytkownik systemu teleinformatycznego musi posiadać unikatowy, jawny identyfikator i wprowadzone przez siebie poufne hasło (hasła) autoryzujące jego osobę.
3. Hasłami powinny być zabezpieczone również udostępniane w wewnętrznej sieci uczelnianej zasoby zawierające ważne dane.
4. W celach bezpieczeństwa zaleca się:
   1) zabezpieczenie hasłem plików zawierających ważne dane;
   2) uaktywnienie wygaszaczy ekranów zabezpieczonych hasłem.

§ 15

1. Zalecane jest, aby hasła, o których mowa w § 14 ust. 2 i 3 oraz hasła służące do administrowania systemami i programami nie były krótsze niż 12 znaków. W systemach, które na to zezwalają, w uzupełnieniu do podstawowej formy hasła, zaleca się stosowanie dodatkowo dużych i małych liter, cyfr oraz znaków specjalnych.
2. O długości haseł, o których mowa w § 14 ust. 4, decyduje użytkownik – z uwzględnieniem zaleceń wymienionych w ust. 1.
3. Hasła powinny być wprowadzane w sposób maskowany.
4. Hasła wykorzystywane w systemach informatycznych Uczelni nie powinny być używane w innych miejscach, np. do zabezpieczania zasobów prywatnych użytkownika.
5. Hasła powinny być trudne do odgadnięcia. Nie zaleca się stosowania nazw potocznych, imion i nazwisk, dat urodzenia, numerów dokumentów, innych danych osobistych oraz standardowych kombinacji znaków (np. 12345678).
6. Zabronione jest przekazywanie haseł innym osobom (np. poprzez umieszczanie w miejscach łatwo dostępnych lub widocznych).
7. Następne hasła nie powinny być tworzone według stałego schematu

(np.: Kowal_01, Kowal_02 itp.).

8. Hasła nie mogą być zapisywane i przechowywane w jawnej postaci zarówno jako tekst w pliku, jak i zapisane na papierze. Wyjątkiem jest zdeponowanie zapisanych haseł zgodnie z § 16 ust. 1.
9. W przypadku prac serwisowych, serwisant z ramienia UCI jest upoważniony do zresetowania hasła i wykonania prac na koncie użytkownika.

§ 16

1. Hasła służące do administrowania systemami i programami przetwarzającymi ważne dane powinny być spisane oraz umieszczone w zamkniętych kopertach, opisanych imieniem i nazwiskiem osoby upoważnionej do ich otwarcia. Koperty należy przechowywać w miejscu uniemożliwiającym dostęp do nich osobom nieupoważnionym, chroniącym przed utratą lub zniszczeniem oraz gwarantującym w przypadkach nadzwyczajnych ich odczytanie upoważnionemu użytkownikowi, a także kierownikowi właściwej jednostki organizacyjnej Uczelni.
2. Odpowiedzialnym za egzekwowanie wymagań wskazanych w ust. 1 jest właściwy kierownik jednostki organizacyjnej.
3. Zarejestrowane hasła, o których mowa w ust. 1, powinny posiadać adnotację o dacie ich wprowadzenia oraz być przechowywane przez okres ich ważności z uwzględnieniem 30-dniowej karencji.

§ 17

1. Hasła, o których mowa w § 16, należy zmieniać zgodnie z instrukcją dedykowaną konkretnemu systemowi oraz niezwłocznie w przypadku stwierdzenia ich ujawnienia lub podejrzenia ujawnienia osobie nieuprawnionej.
2. W przypadku utraty uprawnień przez osobę administrującą systemem, należy niezwłocznie zmienić hasła, o których mowa w ust. 1.
3. Wszystkie używane w systemach hasła, powinny być niezwłocznie zmieniane w przypadku stwierdzenia ich ujawnienia lub podejrzenia ich ujawnienia osobie nieuprawnionej.
4. Hasła bezterminowo zachowują swoją poufność również po ustaniu ich czasu ważności.

§ 18

1. W systemach obsługujących transmisję ważnych danych wykorzystywane są klucze kryptograficzne, służące do ich zabezpieczenia.
2. Za generowanie, przechowywanie i bezpieczną dystrybucję kluczy kryptograficznych, służących do uzyskiwania połączeń VPN, odpowiada kierownik

UCI, który może również przekazać to zadanie pracownikowi UCI.

3. Obowiązkiem użytkownika jest zabezpieczenie kluczy przed dostępem osobom nieupoważnionym.
4. W przypadku stwierdzenia ujawnienia klucza osobie nieupoważnionej lub podejrzenia o jego ujawnieniu należy powiadomić bezpośredniego przełożonego, który ma obowiązek powiadomić osobę, o której mowa w ust. 2.
5. Ważne informacje, do których nie stosuje się kluczy kryptograficznych, należy przekazywać w postaci zaszyfrowanej.

Rozdział VII
Sieć komputerowa Politechniki Częstochowskiej

§ 19

1. Wewnętrzna, uczelniana sieć komputerowa powinna być odseparowana od sieci publicznej za pomocą systemów typu firewall.
2. Ważne dane lub systemy nie mają bezpośredniego dostępu do sieci Internet, a ich dołączenie do sieci może być realizowane jedynie w sposób zabezpieczony poprzez firewall.
3. Korzystanie z wewnętrznych, niepublicznych usług uczelnianych poprzez sieć publiczną powinno odbywać się po zastosowaniu przez właściwą jednostkę organizacyjną systemów zabezpieczeń – w szczególności firewalli oraz systemu uwierzytelniania użytkownika i szyfrowania danych – VPN.
4. Usługa VPN jest dostępna dla każdego pracownika pod warunkiem posiadania aktywnego konta w zarządzanym przez UCI Uczelnianym Systemie Autoryzacji, założonego na podstawie karty obiegowej.

§ 20

1. Zabrania się wykonywania połączeń modemowych z systemów (serwerów, stacji zarządzających, konsol, komputerów) funkcjonujących w wewnętrznej sieci administracyjnej do publicznej sieci Internet, z wyjątkiem połączeń rezerwowych (awaryjnych) na wydzielonych i zabezpieczonych stanowiskach.
2. Zdalny dostęp do serwerów w celach administracyjnych powinien być realizowany z użyciem narzędzi zapewniających bezpieczną komunikację – szyfrowania danych i certyfikatów.

§ 21

1. Dopuszcza się obieg dokumentów elektronicznych pomiędzy jednostkami organizacyjnymi Uczelni.

2. Do przesyłania dokumentów elektronicznych pomiędzy jednostkami organizacyjnymi Uczelni należy stosować uczelnianą pocztę elektroniczną lub inne uczelniane rozwiązania technologiczne.

§ 22

Za techniczne umożliwienie użytkownikom korzystania z zasobów sieciowych odpowiada CzestMAN oraz UCI.

Rozdział VIII
Przesyłanie danych do podmiotów zewnętrznych

§ 23

1. W celu przesyłania ważnych danych do podmiotów zewnętrznych mogą być wykorzystywane systemy informatyczne, które uzyskały pozytywną opinię administratora systemu i oraz zostały zatwierdzone przez UCI.
2. Ważne dane należy przesyłać w formie niejawnej (zaszyfrowane).
3. Zasady przesyłania ważnych danych, w tym danych osobowych, określa Załącznik nr 6.
4. Za przesyłanie danych, o których mowa w ust. 2, jest odpowiedzialny pracownik wyznaczony przez kierownika danej jednostki organizacyjnej.

§ 24

Kwestie związane z wykorzystywaniem uczelnianych systemów informatycznych w celu do przekazywania danych do podmiotów zewnętrznych mogą podlegać szczegółowym uregulowaniom w zawieranych obustronnie umowach, których procedury i klauzule dotyczące bezpieczeństwa systemów informatycznych muszą być zgodne z uregulowaniami niniejszej polityki.

Rozdział IX
Zabezpieczenie oprogramowania i archiwizacja danych

§ 25

1. Oprogramowanie stosowane w Uczelni musi pochodzić wyłącznie ze źródeł legalnych i posiadać łatwo dostępną informację o identyfikatorze wersji i licencji.
2. Wykorzystywane w Uczelni oprogramowanie powinno być ewidencjonowane w formie rejestru oprogramowania. Zasady ewidencjonowania zakupionych licencji regulują odrębne przepisy wewnętrzne.
3. Należy używać wyłącznie oprogramowania zainstalowanego przez administratora systemu.
4. Zabronione jest instalowanie oprogramowania nielegalnego oraz niezwiązanego

merytorycznie z wykonywaną pracą, a w szczególności oprogramowania, którego eksploatacja jest sprzeczna z ustawą o prawie autorskim i prawach pokrewnych.

5. Instalacja oprogramowania, o którym mowa w ust. 4, stanowi naruszenie Regulaminu pracy Politechniki Częstochowskiej.
6. Dopuszcza się, po pozytywnym zaopiniowaniu przez administratora systemu, instalowanie w celach służbowych oprogramowania darmowego (freewarowego) lub testowych wersji oprogramowania, tzw. sharewarowego, na wydzielonym stanowisku komputerowym ze wszystkimi obostrzeniami umowy licencyjnej oprogramowania (EULA).
7. W przypadku wystąpienia konieczności zainstalowania na komputerze nowego oprogramowania należy zgłosić ten fakt administratorowi systemu.

§ 26

1. Umowy dotyczące świadczenia usług teleinformatycznych, zakupu lub modernizacji urządzeń komputerowych, systemów informatycznych i oprogramowania powinny zawierać niezbędne wymagania dotyczące bezpieczeństwa informacji lub odniesienie do odpowiednich dokumentów regulujących te kwestie w Uczelni, w tym zakres odpowiedzialności stron umowy.
2. W celu ograniczenia ryzyka niewydolności funkcjonalnej systemów informatycznych należy prognozować przyszłe wymagania dotyczące pojemności zasobów dyskowych, mocy obliczeniowej procesorów, przepustowości sieci itd. Wymagania te powinny być określone i udokumentowane przed zaakceptowaniem i wdrożeniem nowych lub modernizowanych systemów.
3. Przed dokonaniem odbioru nowych lub modernizowanych systemów informatycznych, istotnych z punktu widzenia działalności Uczelni, należy ustalić kryteria ich odbioru oraz przeprowadzić testy sprawdzające.
4. Kryteria odbioru systemu teleinformatycznego powinny uwzględniać następujące elementy:
   1) wymagania dotyczące wydajności i pojemności;
   2) wymagania dotyczące wdrożonych zabezpieczeń;
   3) przygotowania procedur zarządzania incydentami zagrażającymi bezpieczeństwu informacji przetwarzanej i gromadzonej w systemie;
   4) szkolenie w obsłudze i użytkowaniu;
   5) optymalne warunki gwarancji i serwisu;
   6) potwierdzenie, że instalacja nowego systemu nie będzie wpływała niekorzystnie na istniejące systemy.

5. Testowanie istotnego oprogramowania z punktu widzenia działalności Uczelni należy przeprowadzać w wydzielonym środowisku testowym.
6. Testowanie przeprowadzają osoby upoważnione do podpisania protokołu odbioru.
7. Jeżeli osoby, o których mowa w ust. 6, uznają to za konieczne, testowanie może odbywać się przy współudziale pracowników CzestMAN i/lub UCI.
8. Zmiany w istotnych, z punktu widzenia funkcjonowania Uczelni, eksploatowanych programach podlegają takim samym rygorom, jak włączenie do eksploatacji nowego oprogramowania.

§ 27

1. Bazy danych, oprogramowanie oraz konfiguracja systemów operacyjnych w jednostkach organizacyjnych powinny być zabezpieczone w postaci kopii bezpieczeństwa lub archiwalnych.
2. Jeżeli inne obowiązujące przepisy nie stanowią inaczej, ~~to~~ zaleca się wykonywanie następujących kopii bezpieczeństwa:
   1) przed dokonaniem zmian w konfiguracji systemów operacyjnych lub oprogramowania;
   2) przed dokonaniem zmian w programach (np. zmiana wersji);
   3) po każdej istotnej zmianie danych w bazie danych.
3. Oprócz kopii, o których mowa w ust. 2, należy wykonywać kopie archiwalne, zgodnie z przyjętą przez administratora systemu procedurą wykonywania i kontroli kopii zapasowych.
4. Administrator jest zobowiązany do opracowania i przestrzegania procedury wykonywania i kontroli kopii zapasowych, zgodnie z Załącznikiem nr 7.

§ 28

Kopie bezpieczeństwa i archiwalne należy:

1) wykonać w co najmniej dwóch egzemplarzach każda, przy czym przynajmniej jedną na nośniku wymiennym;
2) przechowywać w dwóch różnych urządzeniach i miejscach innych niż te, w którym eksploatowane zbiory przechowywane są na bieżąco.

§ 29

1. Kopie bezpieczeństwa należy przechowywać do momentu wykonania następnej kopii bezpieczeństwa.
2. Kopie archiwalne miesięczne należy przechowywać przez okres 1 roku, a kopie roczne przez okres 5 lat, chyba że inne terminy wynikają z powszechnie obowiązujących przepisów prawa.

§ 30

Nośniki danych, na których znajdują się kopie bezpieczeństwa i kopie archiwalne, powinny być oznaczone w sposób trwały, jednoznaczny i czytelny.

§ 31

Kopie archiwalne należy:

1) okresowo sprawdzać pod kątem ich dalszej przydatności do odtwarzania;
2) bezzwłocznie usuwać po ustaniu ich użyteczności.

§ 32

1. W jednostkach organizacyjnych ważne dane przychodzące pocztą elektroniczną powinny być zabezpieczone na dysku sieciowym, nośniku wymiennym lub lokalnym dysku twardym komputera.
2. O trybie archiwizowania danych decyduje administrator systemu odpowiedzialny za obsługę poczty elektronicznej.
3. Okres przechowywania kopii, określonych w ust. 1, powinien wynikać z rodzaju zarchiwizowanych danych oraz być zgodny z przepisami dotyczącymi archiwizowania.

§ 33

1. W celu bezpieczeństwa należy archiwizować istotne dane zapisane na dyskach twardych komputerów poszczególnych użytkowników, w szczególności dane z komputerów przenośnych.
2. O trybie archiwizowania danych, o których mowa w ust. 1, decyduje użytkownik. Przekazanie do pracy komputera używanego powinno nastąpić po usunięciu zbędnych danych i oprogramowania przez UCI w porozumieniu z poprzednim użytkownikiem.
3. Oprogramowanie oraz bazy danych, które przestały być wykorzystywane w Uczelni należy usunąć z urządzeń komputerowych po uprzednim dokonaniu archiwizacji.

Rozdział X

Ochrona przed szkodliwym oprogramowaniem

§ 34

1. Potencjalnymi źródłami przedostawania się szkodliwego oprogramowania na stacje robocze są:
   1) załączniki do poczty elektronicznej;
   2) przeglądane strony internetowe;

3) pliki i aplikacje pochodzące z nośników wymiennych uruchamiane i odczytywane na stacji roboczej.

2. W celu zapewnienia ochrony antywirusowej administrator systemu lub użytkownik jest odpowiedzialny za zarządzanie systemem wykrywającym i usuwającym wirusy. System antywirusowy posiadać skonfigurowany:
   1) rezydentny monitor antywirusowy (uruchomiony w pamięci operacyjnej stacji roboczej);
   2) antywirusowy skaner ruchu internetowego;
   3) monitor zapewniający ochronę przed wirusami w dokumentach MS Office;
   4) skaner poczty elektronicznej.

   Wszystkie elementy składowe systemu antywirusowego powinny być stale włączone.

Rozdział XI
Administracja systemem informatycznym
§ 35

1. Administratorem systemu teleinformatycznego może zostać osoba posiadająca odpowiednie kwalifikacje, potwierdzone ukończonymi szkoleniami lub doświadczeniem zawodowym.
2. Podstawowym obowiązkiem administratora systemu teleinformatycznego jest:
   1) administrowanie systemami informatycznymi;
   2) zachowanie ciągłości funkcjonowania systemów informatycznych poprzez utrzymywanie, konfigurowanie i monitorowanie ich wydajności;
   3) wykrywanie nieautoryzowanego dostępu do systemu teleinformatycznego,
   4) konfigurowanie kont użytkowników;
   5) nadzór nad stosowaniem mechanizmów kontroli dostępu do systemu, a w szczególności do danych osobowych;
   6) systematyczne kontrolowanie zastosowanych środków technicznych i organizacyjnych, zapewniających ochronę systemu i przetwarzanych danych osobowych, odpowiednią do zagrożeń oraz kategorii danych objętych ochroną;
   7) zabezpieczenie systemów służących do przetwarzania danych osobowych przed działaniem złośliwego oprogramowania;
   8) zabezpieczenie systemów, zbiorów danych oraz programów służących do przetwarzania ważnych danych poprzez systematyczne wykonywanie kopii

zapasowych;

9) nadzór nad naprawą oraz likwidacją urządzeń komputerowych;
10) kontrola przeglądu i konserwacji systemów informatycznych zgodnie z procedurą określoną w Załączniku nr 8;
11) współpraca z IOD przy przygotowaniu i wdrażaniu dokumentacji dotyczącej ochrony danych osobowych, jeżeli w systemie takie dane są przetwarzane;
12) konsultacje i zgłaszanie uwag o zauważonych anomaliach do UCI lub CzestMAN.

3. W przypadkach wyjątkowych nieszablonowych, wynikających m.in. z zagrożenia działaniem złośliwego oprogramowania, wykrytych luk bezpieczeństwa, w przypadku ryzyka utracenia integralności systemów, administrator systemu teleinformatycznego ma prawo, po uzyskaniu zgody kierownika UCI, reglamentować dostęp użytkownikom do czasu rozwiązania problemu i zaimplementowania odpowiednich łat bezpieczeństwa. W takim przypadku niezbędne jest poinformowanie użytkowników o zaistniałej sytuacji poprzez komunikat na stronie internetowej lub wysłanie informacji pocztą elektroniczną.
4. W Uczelni prowadzone są rejestry administratorów systemów informatycznych:
   1) lokalne rejestry administratorów – prowadzone na każdym wydziale/ w jednostkach organizacyjnych, za które odpowiadają odpowiednio: dziekan/kierownik oraz UCI – w przypadku pionu kanclerza i prorektorów;
   2) centralny rejestr administratorów – rejestr składający się z danych pochodzących z rejestrów lokalnych;
5. Utworzony rejestr jak i każdorazowa jego zmiana musi zostać niezwłocznie zgłoszona do rejestru centralnego, a odpowiedzialnym za to jest dziekan/ kierownik.
6. Rejestr, o którym mowa w ust. 4 powinien minimum zawierać:
   1) imię i nazwisko administratora;
   2) nazwę systemu teleinformatycznego, którym administruje;
   3) adres e-mail oraz nr telefonu administratora;
   4) daty wpisania i wykreślenia z rejestru.
7. Wzór rejestru administratorów stanowi Załącznik nr 9.

§ 36

1. Administratora systemu teleinformatycznego wyznacza:
   1) w przypadku systemów wydziałowych – dziekan na wniosek bezpośredniego przełożonego administratora systemu teleinformatycznego lub samego

kandydata na administratora poprzez akceptację wniosku – Załącznik nr 10;

2) w przypadku systemów w pozostałych jednostkach organizacyjnych – kanclerz na wniosek kierownika jednostki organizacyjnej, w której ten system jest eksploatowany lub samego kandydata na administratora systemu teleinformatycznego, poprzez akceptację wniosku – Załącznik nr 10;
3) w przypadku ogólnouczelnianego systemu teleinformatycznego – kanclerz na wniosek bezpośredniego przełożonego administratora systemu lub samego kandydata na administratora poprzez akceptację wniosku – Załącznik nr 10.

2. Wniosek na administratora ogólnouczelnianego systemu teleinformatycznego musi być dodatkowo zaopiniowany przez kierownika UCI lub CzestMAN, w zależności od przynależności danego systemu.
3. Administratorem systemu w przypadku komputerów stacjonarnych i komputerów przenośnych staje się każda osoba, której powierzono sprzęt komputerowy i posiada do niego prawa administracyjne.
4. Osoba, której powierzono sprzęt komputerowy może zrzec się uprawnień administratora, wypełniając odpowiedni wniosek (Załącznik nr 11) i przekazując go do bezpośredniego przełożonego, który koryguje rejestr administratorów i dokonuje zgłoszenia do rejestru centralnego. W takim przypadku administratora systemu wskazuje kierownik UCI, a zatwierdza kanclerz.

Rozdział XII
Postanowienia końcowe
§ 37

1. Zobowiązuje się wszystkich pracowników Uczelni do zapoznania się z treścią niniejszej polityki oraz jej bezwzględnego przestrzegania.
2. Każdy nowo zatrudniony pracownik, którego praca wiąże się z obsługą komputera, zobowiązany jest do złożenia oświadczenia (ZAŁĄCZNIK nr 1) w postaci elektronicznej za pośrednictwem strony internetowej UCI.

Rozdział XIV

Załączniki

Załącznikami do niniejszej polityki są:

Załącznik nr 1. Oświadczenie o zapoznaniu się z Polityką bezpieczeństwa informacji w systemach teleinformatycznych Politechniki Częstochowskiej;

Załącznik nr 2. Procedura zgłaszania incydentów;

Załącznik nr 3. Procedura rozpoczynania, zawieszenia i zakańczania pracy w systemie informatycznym;

Załącznik nr 4. Regulamin użytkowania komputerów przenośnych;

Załącznik nr 5. Wniosek o zarejestrowanie użytkownika, modyfikację uprawnień, wyrejestrowanie użytkownika;

Załącznik nr 6. Procedura wysyłania ważnych danych, w tym danych osobowych, za pomocą e-maila;

Załącznik nr 7. Procedura wykonywania i kontroli kopii zapasowych;

Załącznik nr 8. Procedura wykonywania przeglądów i konserwacji systemów teleinformatycznych;

Załącznik nr 9. Wzór rejestru administratorów systemu;

Załącznik nr 10. Wniosek o wyznaczenie administratora systemu;

Załącznik nr 11. Wzór wniosku o rezygnacji z uprawnień administratora systemu;

Załącznik nr 12. Główni właściciele biznesowi systemów.

Załączniki niniejszej polityki mogą być składane do UCI drogą elektroniczną za pośrednictwem strony internetowej (uci.pcz.pl) lub w formie tradycyjnej – na papierze.

Zał. nr 1 do Polityki bezpieczeństwa informacji w Politechnice Częstochowskiej
(ZARZĄDZENIE Nr 392/2023 Rektora PCz)

Oświadczenie o zapoznaniu się z Polityką bezpieczeństwa informacji w systemach teleinformatycznych Politechniki Częstochowskiej

1. Ja, niżej podpisana/-y, pracując na sprzęcie komputerowym Politechniki Częstochowskiej (zwanej dalej „PCz") zobowiązuję się stosować procedury określone w Polityce bezpieczeństwa informacji w systemach teleinformatycznych Politechniki Częstochowskiej, a w szczególności:
   1) przestrzegać obowiązujących przepisów prawa;
   2) chronić dane przetwarzane w systemach teleinformatycznych PCz, w szczególności dane osobowe i tajemnicę przedsiębiorstwa przed ich uszkodzeniem, udostępnieniem osobom nieupoważnionym, niepożądaną modyfikacją lub usunięciem;
   3) nie udostępniać nikomu haseł, kart dostępowych, podpisów kwalifikowanych ani innego typu poświadczenia do przydzielonych mi zasobów – pomieszczeń, sieci, aplikacji, poczty elektronicznej;
   4) informować przełożonego lub administratora systemu o wszelkich podejrzanych zmianach w działaniu oprogramowania, mogących być skutkiem ataku;
   5) informować osobę odpowiedzialną materialnie o wszelkich zmianach dotyczących lokalizacji lub konfiguracji sprzętu komputerowego;
   6) chronić przed zniszczeniem lub uszkodzeniem sprzęt komputerowy stanowiący majątek PCz; zauważone uszkodzenia i usterki zgłaszać do odpowiedniego działu;
   7) nie wykorzystywać do celów prywatnych powierzonego sprzętu, służbowej skrzynki e-mail oraz nie udostępniać kluczy licencyjnych oprogramowania;
   8) używać do celów służbowych wyłącznie służbowych urządzeń, oprogramowania i adresów e-mail;
   9) informować przełożonego lub administratora systemu o próbach wyłudzania haseł lub innych informacji związanych z zabezpieczeniami systemów teleinformatycznych PCz dokonywanych drogą telefoniczną, pocztą elektroniczną lub w bezpośrednim kontakcie oraz o wszelkich innych podejrzanych działaniach mogących mieć negatywny wpływ na bezpieczeństwo danych;
   10) blokować dostęp do komputera w sytuacji, kiedy konieczne jest opuszczenie

stanowiska pracy;

11) w systemach przetwarzających ważne dane, z punktu widzenia funkcjonowania Uczelni, nie instalować samowolnie i używać wyłącznie oprogramowania zainstalowanego przez administratora systemu;
12) w przypadku wystąpienia konieczności zainstalowania na komputerze nowego oprogramowania zgłosić ten fakt administratorowi systemu;
13) dbać o bezpieczeństwo danych zapisanych w plikach mających znaczenie dla skutecznego wykonywania obowiązków służbowych poprzez ich składowanie na archiwizowanych zasobach sieciowych;
14) nie pobierać z internetu, nie przechowywać na nośnikach danych należących do PCz (np. dysk lokalny komputera, dyski przenośne itp.) oraz nie udostępniać materiałów chronionych prawami autorskimi lub innych treści mogących zaszkodzić wizerunkowi PCz (np. materiałów nieobyczajnych);
15) informować administratora systemu o wykrytym przez program antywirusowy złośliwym oprogramowaniu, które nie zostało automatycznie naprawione;
16) nie przekazywać i nie wynosić poza PCz (np. na przenośnych nośnikach danych, za pomocą usług chmury danych, np. Dropbox, OneDrive, GoogleDrive) lub za pośrednictwem poczty elektronicznej) danych, jeśli naruszyłoby to obowiązujące w PCz procedury i/lub obowiązujące przepisy prawa oraz jeśli dane nie są zabezpieczone środkami ochrony kryptograficznej;
17) nie podłączać samodzielnie do wewnętrznej sieci teleinformatycznej PCz prywatnych urządzeń, np.: laptop, tablet, smartphone, router WiFi lub innych.

2. Przyjmuję do wiadomości, że:
   1) ponoszę pełną odpowiedzialność za zawartość użytkowanych przeze mnie służbowych nośników pamięci oraz zasobów pamięci masowej (m.in. dysk twardy, dysk sieciowy, płyty np. CD, pendrive, karty pamięci flash itp.), a w szczególności za samodzielnie wgrane pliki;
   2) historia operacji wykonywanych przeze mnie w systemach teleinformatycznych jest zapisywana oraz archiwizowana i może podlegać kontroli i analizie;
   3) zawartość służbowej skrzynki e-mail podlega archiwizacji i kontroli;
   4) administrator systemu może dokonywać bieżącej kontroli (bez ingerencji w zawartość) zasobów użytkowanych przeze mnie komputerów, ewidencji wykorzystania poszczególnych aplikacji uruchamianych na użytkowanych przeze mnie komputerach (terminalach) oraz, za moją zgodą, łączyć się

zdalnie z komputerem, na którym pracuję w celu świadczenia pomocy technicznej;

5) jestem zobowiązana/-y do zachowania w tajemnicy wszystkich danych, z którymi mam kontakt w związku z wykonywaną przeze mnie pracą oraz sposobu ich zabezpieczenia;
6) tajemnica, o której mowa w pkt. 5 obowiązuje mnie bezterminowo, również po zakończeniu pracy w PCz;
7) tajemnica, o której mowa w pkt. 5 nie dotyczy sytuacji, gdy ujawnienia informacji, o których mowa, żądają uprawnione organy lub urzędy państwowe na podstawie obowiązujących przepisów prawa oraz, gdy mamy do czynienia z informacją jawną, publiczną lub opublikowaną przez PCz;
8) dostęp do internetu jest w PCz monitorowany, a historia zapisywana i może być udostępniona przełożonym;
9) dostęp do internetu może być ograniczany zarówno pod względem zakresu dostępnych stron, jak i pod względem czasu, w którym internet będzie udostępniany pracownikom;
10) zdalna praca w wewnętrznej sieci PCz jest możliwa wyłącznie z użyciem silnie szyfrowanego kanału VPN.

3. Jestem świadoma/-y, iż naruszenie procedur określonych w Polityce bezpieczeństwa informacji w systemach teleinformatycznych Politechniki Częstochowskiej może skutkować odpowiedzialnością karną, dyscyplinarną lub odszkodowawczą na zasadach i w trybie przewidzianym w przepisach prawa, w tym w Kodeksie pracy.
4. Wszystkie powyższe zapisy są dla mnie w pełni zrozumiałe i będę potrafił/-a się do nich zastosować.

Przyjęłam/przyjąłem do wiadomości i stosowania

.....

imię i nazwisko drukowanymi literami

.....

miejsce zatrudnienia

.....

data i podpis

Zał. nr 2 do Polityki bezpieczeństwa informacji w Politechnice Częstochowskiej
(ZARZĄDZENIE Nr 392/2023 Rektora PCz)

Procedura zgłaszania incydentów

1. Wszyscy pracownicy zobowiązani są do pisemnego informowania swojego bezpośredniego przełożonego oraz Administratora systemu teleinformatycznego w przypadku podejrzenia wystąpienia naruszenia bezpieczeństwa. Ponadto w przypadku podejrzenia naruszenia ochrony danych osobowych należy postępować zgodnie z zapisami Polityki Ochrony Danych Osobowych Politechniki Częstochowskiej.
2. Zgłaszający incydent nie powinien podejmować żadnych działań na własną rękę. Jednak w miarę możliwości powinien zabezpieczyć materiał dowodowy, np. robiąc zdjęcie ekranu komputera, co do którego zaistniało podejrzenie, że jego działanie odbiega od normy.
3. Odpowiedzialność za prawidłowe zgłoszenie incydentów dotyczących bezpieczeństwa w systemach teleinformatycznych spoczywa na pracownikach Uczelni dokonujących zgłoszeń. Za rozwiązanie problemu lub zapobieżenie incydentowi dotyczącego Systemu teleinformatycznego odpowiada wyznaczony Administrator systemu teleinformatycznego i działa zgodnie z niniejszą procedurą.
4. Administrator systemu teleinformatycznego odpowiedzialny jest za:
   1) niezwłoczne reagowanie na incydenty naruszeń bezpieczeństwa w systemach teleinformatycznych;
   2) ocenę istniejących i potencjalnych zagrożeń naruszenia bezpieczeństwa w systemach teleinformatycznych;
   3) ocenę przyczyn i skutków incydentów naruszenia bezpieczeństwa w systemach teleinformatycznych (w tym gromadzenie materiału dowodowego);
   4) przygotowywanie propozycji działań korygujących/naprawczych oraz nadzór nad ich wprowadzeniem;
   5) proponowanie zmian do zapisów PBI PCz;
   6) współpracę z Rządowym Zespołem Reagowania na Incydenty Komputerowe CERT.
5. Obsługa incydentu rozpoczyna się od dokonania jego dokładnego rozpoznania, tj. ustalenia oznak naruszenia bezpieczeństwa, identyfikacji rodzaju incydentu (zgodnie z § 4 pkt. 1 PBI PCz), identyfikacji i zabezpieczenia dowodów.

6. Administrator systemu teleinformatycznego, po dokonaniu analizy zdarzenia i okoliczności z nim związanych, w przypadku potwierdzenia faktycznego wystąpienia incydentu, wprowadza dane o incydencie do Rejestru incydentów zdarzeń, zabezpiecza materiał dowodowy oraz informuje Kierownika UCI.
7. Zespół złożony z administratora systemu teleinformatycznego, bezpośredniego przełożonego pracownika dokonującego zgłoszenia oraz osoby wskazanej przez kierownika UCI dokonuje analizy materiału dowodowego oraz przedstawia kanclerzowi raport zawierający rekomendacje dotyczące sposobu dalszego postępowania.

   W przypadku, gdy zgłoszone zdarzenie zostało uznane za incydent naruszenia bezpieczeństwa, dokonuje się oceny jego istotności kierując się następującymi kryteriami:

   1) wpływ incydentu na ciągłość działania Uczelni i wypełnianie jej zadań statutowych;
   2) krytyczność systemów dotkniętych skutkami incydentu bezpieczeństwa;
   3) rozmiar szkód powstałych skutkiem incydentu;
   4) koszt usunięcia i naprawy skutków incydentu bezpieczeństwa;
   5) szacowany czas przywrócenia ciągłości działania systemu;
   6) zasoby konieczne do przywrócenia ciągłości działania systemu (personel, wsparcie firm zewnętrznych, wymagane dodatkowe urządzenia oraz oprogramowanie itp.);
   7) ocenę istniejących i potencjalnych zagrożeń naruszenia bezpieczeństwa w systemach teleinformatycznych,
8. Jeżeli istotność incydentu jest wysoka, należy zawiadomić rządowy Zespół Reagowania na Incydenty Komputerowe CERT. Administrator systemu teleinformatycznego wypełnia formularz zgłoszenia incydentu pobrany ze strony *cert.gov.pl* oraz wysyła go do CERT, zgodnie z informacją zamieszczoną na stronie.
9. W przypadku stwierdzenia działań umyślnych i ustalenia sprawcy incydentu, kanclerz przekazuje wyniki analizy rektorowi celem wyciągnięcia konsekwencji dyscyplinarnych wobec sprawcy, ewentualnego zawiadomienia organów ścigania lub podjęcia kroków prawnych wobec osób trzecich.

Rejestr incydentów i zdarzeń

Lp.	Incydent lub zdarzenie	Źródło zgłoszenia	Data zgłoszenia	Przyczyna niezgodności	Działania korygujące i zapobiegawcze	Odpowiedzialny za realizację czynności naprawczych	Data zakończenia czynności naprawczych	Ocena istotności*	Zgłoszono do CERT**

*Wg pkt. 7 Procedury zgłaszania incydentów.

**TAK/NIE.

Zał. nr 3 do Polityki bezpieczeństwa informacji w Politechnice Częstochowskiej
(ZARZĄDZENIE Nr 392/2023 Rektora PCz)

Procedura rozpoczynania, zawieszenia i zakańczania pracy w systemie informatycznym

1. Stosowane są następujące zasady rozpoczęcia pracy w systemie informatycznym:
   1) przed przystąpieniem do pracy, użytkownik jest zobowiązany do sprawdzenia, czy stacja robocza wykorzystywana do przetwarzania danych w systemie informatycznym nie wskazuje na ingerencję osób trzecich, a także czy stanowisko pracy zastano w takim stanie, jak pozostawiono po zakończeniu pracy;
   2) użytkownik jest zobowiązany do upewnienia się, czy ekran monitora jest ustawiony w sposób uniemożliwiający osobom nieupoważnionym podglądanie lub przeglądanie jego zawartości;
   3) każde rozpoczęcie pracy w danym systemie wymaga logowania;
   4) w przypadku wielokrotnego wprowadzenia błędnych danych (użytkownik lub hasło), dostęp zostanie czasowo zablokowany; po upływie czasu blokady, użytkownik może ponownie podjąć czynności zalogowania się;
   5) w przypadku braku możliwości wprowadzenia indywidualnego identyfikatora i/lub hasła, bądź braku dostępu do określonych zasobów systemu, wymagany jest niezwłoczny kontakt z administratorem systemu;
   6) w przypadku zapomnienia przez użytkownika hasła, winien on niezwłocznie zawiadomić administratora systemu, który nadaje nowe hasło, postępując zgodnie z procedurą obowiązującą przy nadawaniu uprawnień dostępu do systemu teleinformatycznego;
   7) w trakcie pracy, użytkownik powinien mieć:
      a) otwarte tylko te aplikacje, które są niezbędne do wykonywania obowiązków służbowych,
      b) na biurku tylko materiały, które są niezbędne do wykonywania obowiązków służbowych.
2. Stosowane są następujące zasady zawieszenia pracy w systemie informatycznym:
   1) stacje robocze wyposażone są w wygaszacz ekranu lub inny system blokujący stację, włączający się w momencie dłuższej bezczynności użytkownika w systemie; czas trwania nieaktywnej sesji (czas bezczynności) po jakim następuje automatyczne zablokowanie użytkownika wynosi od 5 do 10 min, w zależności od specyfiki środowiska w którym są przetwarzane dane

i przeprowadzonej analizy ryzyka;

2) przy każdorazowym opuszczeniu stanowiska komputerowego lub zawieszenia pracy w systemie, należy dopilnować, aby osoby postronne nie miały dostępu do dokumentów oraz danych przetwarzanych na tym stanowisku.

3. Stosowane są następujące zasady zakończenia pracy w systemie informatycznym:
   1) kończenie pracy polega na wybraniu odpowiedniego polecenia systemowego umożliwiającego zakończenie pracy;
   2) zaleca się zapisanie wyników pracy i zamknięcie wszystkich programów; użytkownik powinien pozostać przy komputerze do chwili ich zamknięcia;
   3) użytkownik kończący pracę powinien sprawdzić, czy wszystkie elektroniczne nośniki informacji i dokumenty zawierające dane zostały zabezpieczone;
   4) osoba opuszczająca pomieszczenie jako ostatnia powinna zamknąć okna oraz drzwi od pomieszczenia na klucz.

Zał. nr 4 do Polityki bezpieczeństwa informacji w Politechnice Częstochowskiej
(ZARZĄDZENIE Nr 392/2023 Rektora PCz)

Regulamin użytkowania komputerów przenośnych

1. Użytkowanie komputerów przenośnych poza siedzibą Politechniki Częstochowskiej powinno być ograniczone do niezbędnych przypadków.
2. Osoba korzystająca z komputera przenośnego w celu przetwarzania danych podlegających ochronie, jest zobowiązana do zwrócenia szczególnej uwagi oraz dołożenia wszelkich starań w celu zabezpieczenia przetwarzanych informacji przed dostępem osób nieupoważnionych oraz naruszeniem ich integralności, a w szczególności do:
   1) niepozostawiania komputera w samochodzie, przechowalni bagażu itp.;
   2) przenoszenia komputera w specjalnej torbie/plecaku;
   3) transportowania komputera w bagażu podręcznym;
   4) niepozostawiania komputera bez nadzoru;
   5) niekorzystania z publicznych sieci komputerowych.
3. Zabrania się użytkowania komputera w miejscach publicznych i w środkach transportu publicznego, jeśli istnieje niebezpieczeństwo, że wyświetlane dane mogą zostać podejrzane lub przejęte przez osoby postronne.
4. Administrator systemu jest zobowiązany do podejmowania działań mających na celu zabezpieczenie komputerów przenośnych. W szczególności powinien on:
   1) dokonać konfiguracji oprogramowania na komputerach przenośnych w sposób wymuszający korzystanie z haseł, wykorzystywanie haseł odpowiedniej jakości oraz okresową zmianę haseł, zgodnie z wymaganiami dla systemu teleinformatycznego;
   2) zabezpieczyć dane na dyskach komputerów przenośnych poprzez zastosowanie oprogramowania szyfrującego;
   3) dokonać na komputerze przenośnym instalacji i konfiguracji uczelnianego oprogramowania antywirusowego;
   4) oznaczyć komputer przenośny programowo lub fizycznie w sposób identyfikujący właściciela tego urządzenia z wskazaniem jednostki organizacyjnej i jej adresu jako właściciela komputera.
5. W razie zgubienia lub kradzieży sprzętu użytkownik jest zobowiązany do natychmiastowego powiadomienia o tym fakcie bezpośredniego przełożonego, administratora oraz Inspektora Ochrony Danych (jeżeli na komputerze przetwarzane były dane osobowe).

Zał. nr 5 do Polityki bezpieczeństwa informacji w Politechnice Częstochowskiej
(ZARZĄDZENIE Nr 392/2023 Rektora PCz)

Wniosek o zarejestrowanie użytkownika, modyfikację uprawnień, wyrejestrowanie użytkownika

NADANIE/MODYFIKACJA/WYCOFANIE* zakresu uprawnień użytkownika do systemu

.....

(wpisać nazwę systemu, np. Simple.ERP)

WNIOSKODAWCA (bezpośredni przełożony):	
Imię i nazwisko:	
Jednostka organizacyjna:	
Stanowisko:	
tel. i e-mail służbowy	
UŻYTKOWNIK:	
Imię i nazwisko:	
Jednostka organizacyjna:	
Stanowisko:	
tel. i e-mail służbowy:	
Login w systemie: (jeśli pracownik jest użytkownikiem systemu)	
Posiadane role w systemie: (jeśli pracownik jest użytkownikiem systemu)	
Wymagany zakres merytoryczny wynikający z niniejszego wniosku: (opis wymaganych funkcjonalności – rola/ funkcja)	
Wskazać rodzaj dostępu: (przegląd/edycja/administracja)	
Data obowiązywania uprawnień. (jeżeli uprawnienie nie ma końcowej daty granicznej, należy wpisać „do odwołania”)	od ..... do ..... (dd-mm-rr) (dd-mm-rr lub „do odwołania”)

Czy dostęp do danych będzie wiązał się z przetwarzaniem danych osobowych?*	TAK	NIE
Podstawa upoważnienia do przetwarzania danych osobowych:*	..... nr upoważnienia do przetwarzania danych osobowych	Przetwarzanie danych osobowych przez nauczycieli akademickich na podstawie aktualnie obowiązującej procedury nadawania upoważnień do przetwarzania danych osobowych w Politechnice Częstochowskiej
Data i podpis wnioskodawcy:		
Data i podpis właściciela biznesowego systemu: (zgodnie z Załącznikiem nr 12)		
Data i podpis administratora systemu:		

Wypełnia administrator systemu:

W dniu ....., zgodnie z powyższym wnioskiem nadano/zmodyfikowano*

uprawnienia nr ..... (kolejny nr wniosku z rejestru)

Utworzono/zmodyfikowano* w systemie .....

(nazwa systemu)

konto użytkownika o nazwie .....

.....

data i podpis administratora

*Niepotrzebne skreślić.

Zał. nr 6 do Polityki bezpieczeństwa informacji w Politechnice Częstochowskiej
(ZARZĄDZENIE Nr 392/2023 Rektora PCz)

Procedura wysyłania ważnych danych, w tym danych osobowych za pomocą e-maila

Użytkownicy wysyłający ważne dane, w tym dane osobowe, przy pomocy e-maila są zobowiązani do postępowania zgodnie z poniższymi zasadami:

1. Przesyłanie danych osobowych e-mailem może odbywać się tylko przez osoby do tego upoważnione.
2. Przesyłane pliki winny być zabezpieczone hasłem, obowiązuje minimum 8 znaków (duże i małe litery oraz cyfry lub znaki specjalne), które należy przekazać odrębnym kanałem komunikacji, np. telefonicznie, SMS-em lub na inny adres e-mail.
3. Zaleca się, aby użytkownik podczas przesyłania danych osobowych e-mailem, zawarł w treści prośbę do adresata o potwierdzenie otrzymania i zapoznania się z informacją lub włączył funkcję żądania potwierdzenia dostarczenia i przeczytania wiadomości.
4. Użytkownicy powinni zwracać szczególną uwagę na poprawność wpisywanego adresu odbiorcy korespondencji.
5. Podczas wysyłania e-maili do wielu adresatów jednocześnie, należy wprowadzić adresy w polu UDW (ang. BCC) – „ukryte do wiadomości".
6. Instrukcja szyfrowania plików dostępna jest na stronie *uci.pcz.pl* w zakładce "Do pobrania", jako „Propozycja użycia oprogramowania do szyfrowania plików."

Zał. nr 7 do Polityki bezpieczeństwa informacji w Politechnice Częstochowskiej
(ZARZĄDZENIE Nr 392/2023 Rektora PCz)

Procedura wykonywania i kontroli kopii zapasowych

1. Parametry procesu tworzenia kopii zapasowej oraz odpowiedzialność za wykonywanie kopii zapasowych przedstawiono w poniżej tabeli:

Co podlega kopii	Typ kopii	Częstotliwość	Nośnik	Osoba odpowiedzialna

2. W celu zweryfikowania poprawności danych przechowywanych na kopiach zapasowych oraz możliwości przywrócenia za ich pomocą systemu do stanu sprzed awarii, administrator systemu teleinformatycznego zobowiązany jest do wykonywania okresowych testów odtworzenia kopii zapasowych. Testy powinny być wykonywane nie rzadziej niż raz na kwartał. Wyniki testów powinny zostać udokumentowane.
3. Administrator systemu zobowiązany jest do prowadzenia rejestru harmonogramów wykonywania kopii zapasowych zawierających minimum takie dane:

Harmonogram wykonywania kopii zapasowych danych przetwarzanych w systemach informatycznych Politechniki Częstochowskiej (wzór)

Nazwa systemu	Zasób	Harmonogram wykonywania kopii bazowej	Harmonogram wykonywania kopii przyrostowej

Procedura wykonywania przeglądów i konserwacji systemów teleinformatycznych

1. Administrator systemu wykonuje przeglądy i konserwacje systemów teleinformatycznych zgodnie z terminami określonymi przez producentów sprzętu lub oprogramowania lub zgodnie z harmonogramem określonym przez administratora wynikającym ze specyfiki systemu teleinformatycznego.
2. Administrator systemu jest zobowiązany do prowadzenia dokumentacji dotyczącej przeprowadzanych przeglądów i konserwacji systemu teleinformatycznego. Dokumentacja ta powinna zawierać w szczególności:
   1) czas i datę rozpoczęcia przeglądu lub konserwacji;
   2) zakres wykonanych prac;
   3) wykaz osób przeprowadzających przegląd lub konserwację;
   4) czas i datę zakończenia przeglądu lub konserwacji.
3. Wszelkie prace serwisowe i konserwacyjne systemu teleinformatycznego wykonywane przez podmiot zewnętrzny mogą odbywać się na zasadach określonych w umowie z uwzględnieniem klauzuli dotyczącej ochrony danych osobowych.
4. Wszelkie informacje, dane, oprogramowanie, sprzęt udostępniane firmom lub instytucjom zewnętrznym muszą zostać zabezpieczone przed dostępem osób niepowołanych poprzez: szyfrowanie, zabezpieczenie fizyczne przed uszkodzeniem, zachowanie zasad ochrony informacji, zachowanie zasad ochrony fizycznej i mienia.
5. Wszelkie prace serwisowe i konserwacyjne systemu teleinformatycznego, służącego do przetwarzania danych osobowych, wykonywane doraźnie przez podmiot zewnętrzny mogą być wykonywane wyłącznie w obecności administratora systemu, IOD lub osoby upoważnionej do przetwarzania danych.
6. Rozpoczęcie prac serwisowych lub konserwacyjnych systemu teleinformatycznego, służącego do przetwarzania danych osobowych, przez podmiot zewnętrzny poprzedzone jest wcześniejszą informacją o zakresie planowanych prac. Prace mogą zostać rozpoczęte nie wcześniej niż po akceptacji przedstawionego zakresu prac przez IOD z wyłączeniem przypadków, gdzie podpisano umowę powierzenia danych osobowych. Planowany zakres prac dołączany jest do prowadzonej przez administratora systemu dokumentacji.
7. Przed rozpoczęciem prac serwisowych lub konserwacji systemu teleinformatycznego przez podmiot zewnętrzny, konieczne jest potwierdzenie tożsamości serwisantów przez osobę upoważnioną do przetwarzania danych.

Zał. nr 9 do Polityki bezpieczeństwa informacji w Politechnice Częstochowskiej
(ZARZĄDZENIE Nr 392/2023 Rektora PCz)

Wzór rejestru administratorów systemu

Lp.	Imię i nazwisko	Jednostka organizacyjna	Telefon służbowy	E-mail służbowy	Nazwa administrowanego systemu	Data obowiązywania uprawnień		Przetwarzanie danych osobowych (TAK/NIE)
						od	do	
1.								
2.								
3.								
4.								
5.								

Zał. nr 10 do Polityki bezpieczeństwa informacji w Politechnice Częstochowskiej
(ZARZĄDZENIE Nr 392/2023 Rektora PCz)

Wniosek o wyznaczenie administratora systemu

Do*

.....

.....

Politechniki Częstochowskiej

Zgodnie z § 36 PBI, wnioskuję o NADANIE/MODYFIKACJĘ/WYCOFANIE** uprawnień administratora systemu .....

(wpisać nazwę systemu, np. Simple.ERP, laboratorium)

WNIOSKODAWCA (bezpośredni przełożony lub kandydat na administratora):		
Imię i nazwisko:		
Jednostka organizacyjna:		
Stanowisko:		
tel.oraz e-mail służbowy:		
ADMINISTRATOR (dane powoływanego administratora):		
Imię i nazwisko:		
Jednostka organizacyjna:		
Stanowisko:		
tel. i e-mail służbowy:		
Data obowiązywania uprawnień: (jeżeli uprawnienie nie ma końcowej daty granicznej, należy wpisać „do odwołania")	od ..... (dd-mm-rr) do ..... (dd-mm-rr lub „do odwołania")	
Czy administrowanie systemem będzie wiązało się z przetwarzaniem danych osobowych?**	TAK	NIE
Podstawa upoważnienia do przetwarzania danych osobowych**	..... nr upoważnienia do przetwarzania danych osobowych	Przetwarzanie danych osobowych przez nauczycieli akademickich na podstawie aktualnie obowiązującej procedury nadawania upoważnień do przetwarzania danych osobowych

		w Politechnice Częstochowskiej
Data i podpis wnioskodawcy:		
Wypełnić, jeżeli wniosek dotyczy administratora ogólnouczelnianego systemu teleinformatycznego, np. Eduroam, Simple.	Zatwierdzam/nie zatwierdzam** ..... data i podpis kierownika UCI lub CzestMAN	
Data i podpis dziekana/ kanclerza	Zatwierdzam/nie zatwierdzam**	
Wniosek zarejestrowano w rejestrze administratorów pod numerem:		

Wypełnia administrator systemu teleinformatycznego:

W dniu ....., zgodnie z powyższym wnioskiem nadano/zmodyfikowano** uprawnienia nr .....
(kolejny nr wniosku z rejestru).
Utworzono/zmodyfikowano** w systemie ..... (nazwa systemu)
konto administratora o nazwie: .....

.....
data i podpis administratora

Przyjmuję obowiązki administratora systemu teleinformatycznego oraz potwierdzam odebranie poświadczeń.

.....
data i podpis powołanego administratora

*Dziekan/kanclerz.

**Niepotrzebne skreślić.

Zał. nr 11 do Polityki bezpieczeństwa informacji w Politechnice Częstochowskiej
(ZARZĄDZENIE Nr 392/2023 Rektora PCz)

Wzór wniosku o rezygnację z uprawnień administratora systemu

.....
imię i nazwisko

.....
jednostka organizacyjna

Częstochowa, dn. .....

Do*

.....

.....

Politechniki Częstochowskiej

Niniejszym wnioskuję o wyznaczenie przez UCI administratora dla powierzonego mi sprzętu komputerowego i jednocześnie zrzekam się uprawnień administratora systemu

.....

(podać nazwę systemu lub opis sytemu)

i zobowiązuję się w terminie do 5 dni roboczych, od zatwierdzenia wniosku przez bezpośredniego przełożonego, zgłosić się do Uczelnianego Centrum teleinformatycznego w celu rekonfiguracji Systemu teleinformatycznego.

Jednocześnie oświadczam, że przyjmuję do wiadomości, że tracę prawo do samodzielnego modyfikowania ustawień systemu np. instalacji oprogramowania.

.....

podpis wnioskodawcy

Wyrażam/nie wyrażam** zgodę/zgody.

.....

data i podpis bezpośredniego przełożonego

*Bezpośredni przełożony.

Wypełnia administrator systemu teleinformatycznego

W dniu ....., zgodnie z powyższym wnioskiem nadano/zmodyfikowano**
uprawnienia nr .....

(kolejny nr wniosku z rejestru)

Utworzono/zmodyfikowano** w systemie .....

(nazwa systemu)

konto administratora o nazwie: .....

.....

data i podpis administratora

**Niepotrzebne skreślić.

Zał. nr 12 do Polityki bezpieczeństwa informacji w Politechnice Częstochowskiej
(ZARZĄDZENIE Nr 392/2023 Rektora PCz)

Główni właściciele biznesowi systemów

Lp.	Nazwa systemu	Główny właściciel biznesowy
1.	Simple.ERP – Personel	Kierownik Działu Kadr, Płac i Spraw Socjalnych
2.	Simple.ERP – Finanse i księgowość	Kwestor
3.	Simple.ERP – Budżetowanie	Zastępca Kanclerza
4.	Simple.ERP – Zarządzanie projektami	Kierownik Centrum Zarządzania Projektami
5.	Simple.ERP – Inwentaryzacja	Zastępca Kwestora
6.	Report Portal – Personel	Kierownik Działu Kadr, Płac i Spraw Socjalnych
7.	Report Portal – Finanse i księgowość	Zastępca Kanclerza