Zarządzenia nr 211/2021
Rektora Politechniki Częstochowskiej
z dnia 7.12.2021 roku

w sprawie: zmian w Zarządzeniu nr 356/2020 Rektora PCz z dnia 3.08.2020 roku w sprawie wprowadzenia Polityki bezpieczeństwa informacji w systemach teleinformatycznych Politechniki Częstochowskiej

§ 1

Wprowadza się następujące zmiany w Zarządzeniu nr 356/2020 Rektora PCz z dnia 3.08.2020 roku w sprawie wprowadzenia Polityki bezpieczeństwa informacji w systemach teleinformatycznych Politechniki Częstochowskiej:

Dotychczasowe brzmienie:

„§ 3

1. Nadzór nad wdrożeniem i utrzymaniem właściwego poziomu bezpieczeństwa informacji w uczelni sprawuje Kanclerz.
2. Zarządzanie systemami informatycznymi wdrożonymi przez UCI i nadzór nad pozostałymi systemami informatycznymi należy do UCI.
3. Za stan bezpieczeństwa danych komputerowych, zainstalowanego oprogramowania oraz sprzętu komputerowego odpowiedzialni są:
   a) Kierownicy jednostek organizacyjnych - poprzez wyznaczenie administratorów systemów informatycznych użytkowanych w jednostce organizacyjnej, zgodnie z procedurą opisaną w § 36.
   b) Administrator systemu;
   c) Użytkownik – odpowiedzialny za przetwarzane dane i wszelkie czynności wykonywane z poziomu swojego konta w systemie informatycznym."

Nowe brzmienie:

§ 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.
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:

PC

a) Kierownicy jednostek organizacyjnych - poprzez wyznaczenie administratorów systemów informatycznych użytkowanych w jednostce organizacyjnej, zgodnie z procedurą opisaną w § 36,
b) Administrator systemu teleinformatycznego,
c) Użytkownik – odpowiedzialny za przetwarzane dane i wszelkie czynności wykonywane z poziomu swojego konta w systemie informatycznym.

Dotychczasowe brzmienie:

„§ 4

1. Do czynników zagrażających bezpieczeństwu danych należą:
   a) próby naruszenia spójności i poufności danych, a w szczególności: włamania do systemu, podsłuch, kradzież danych, nieumyślna lub celowa modyfikacja danych, zniszczenie danych,
   b) szkodliwe oprogramowanie tj. wirusy, konie trojańskie, itp.
   c) awarie sprzętu lub oprogramowania,
   d) utrata sprzętu lub nośników z ważnymi danymi,
   e) próby wyłudzenia danych np. phising,
   f) inne, skutkujące utratą lub uszkodzeniem danych."

Nowe brzmienie:

§ 4

1. Do czynników zagrażających bezpieczeństwu danych należą:
   a) próby naruszenia spójności i poufności danych, a w szczególności: włamania do systemu, podsłuch, kradzież danych, nieumyślna lub celowa modyfikacja danych, zniszczenie danych,
   b) szkodliwe oprogramowanie,
   c) awarie sprzętu lub oprogramowania,
   d) utrata sprzętu lub nośników z ważnymi danymi,
   e) próby wyłudzenia danych np. phising,
   f) inne, skutkujące utratą lub uszkodzeniem danych.

Dotychczasowe brzmienie:

„§ 5

1. Pomieszczenia, w których eksploatowane są systemy informatyczne oraz pomieszczenia, w których przechowywane są nośniki danych, powinny być:
   a) wolne od zagrożeń związanych ze zjawiskami fizycznymi typu:
      i. wyładowania elektrostatyczne i atmosferyczne (np. elektryzujące się

wykładziny, sąsiedztwo urządzeń odgromowych),

ii. silne działanie pól elektromagnetycznych (np. 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.),

b) zabezpieczone systemem ochrony przeciw pożarowej,

c) zabezpieczone przed zalaniem."

Nowe brzmienie:

§ 5

1. Pomieszczenia serwerowni, w których eksploatowane są systemy informatyczne oraz pomieszczenia, w których przechowywane są nośniki danych, powinny być:
   a) wolne od zagrożeń związanych ze zjawiskami fizycznymi typu:
      - wyładowania elektrostatyczne i atmosferyczne (np. elektryzujące się wykładziny, sąsiedztwo urządzeń odgromowych),
      - silne działanie pól elektromagnetycznych (np. 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.),
   b) zabezpieczone systemem ochrony przeciwpożarowej,
   c) zabezpieczone przed zalaniem.

Dotychczasowe brzmienie:

„§ 9

1. Wszyscy użytkownicy zobowiązani są do przekazywania uszkodzonych nośników danych, zawierających ważne dane, do służb informatycznych.
2. Przekazanie winno zostać potwierdzone protokołem zdawczo-odbiorczym.
3. Uszkodzone nośniki danych, zawierające ważne dane, powinny być komisyjnie fizycznie niszczone lub przekazane do zniszczenia specjalistycznej firmie. Z wykonanych czynności sporządza się protokół."

Nowe brzmienie:

§ 9

1. Wszyscy użytkownicy zobowiązani są do przekazywania uszkodzonych nośników danych, zawierających ważne dane, do UCI w celu ich zniszczenia uniemożliwiającego odczyt danych.
2. Przekazanie nośnika winno zostać potwierdzone protokołem zdawczo-odbiorczym.

3. Uszkodzone nośniki danych, zawierające ważne dane, powinny być fizycznie zniszczone. Z wykonanych czynności sporządza się protokół.

Dotychczasowe brzmienie:

„§ 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 ich poprzez użycie urządzeń mechanicznych uniemożliwiających swobodne przemieszczanie sprzętu oraz utrudniających ewentualny zabór.
3. Wynoszenie komputera przenośnego poza teren Politechniki Częstochowskiej, dozwolone jest po uzyskaniu pisemnej zgody zgodnie z *Regulaminem użytkowania komputerów przenośnych* (Załącznik nr 4).
4. Wzór wniosku o zgodę na użytkowanie sprzętu komputerowego poza uczelnią, stanowi Załącznik nr 5."

Nowe brzmienie:

§ 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 ich poprzez użycie urządzeń mechanicznych uniemożliwiających swobodne przemieszczanie sprzętu oraz utrudniających ewentualny zabór.
3. Użytkowanie komputera przenośnego poza terenem Politechniki Częstochowskiej dozwolone jest na zasadach określonych w Zarządzeniu nr 181/2021 Rektora PCz z dnia 30.09.2021 roku, na podstawie protokołu powierzenia sprzętu według Załącznika nr 13 do Zasad dokumentowania gospodarki środkami trwałymi oraz wartościami niematerialnymi i prawnymi w Politechnice Częstochowskiej.
4. (skreślony)

Dotychczasowe brzmienie:

„§ 11

1. Dostęp do systemu teleinformatycznego mogą posiadać upoważnieni:
   a) pracownicy – w zależności od wykonywanych czynności służbowych,
   b) wykonawcy usług oraz dostawcy sprzętu lub oprogramowania – w zakresie koniecznym do realizowania danej usługi lub wykonania określonych

czynności w systemie za zgodą administratora systemu,

c) inni użytkownicy – w zakresie ustalonym w stosownej umowie.

2. Osoby, o których mowa w ust. 1, mogą posiadać w systemie własne konto, dostęp do którego winien być możliwy jedynie po podaniu właściwego identyfikatora i hasła."

Nowe brzmienie:

§ 11

1. Dostęp do systemu teleinformatycznego mogą posiadać upoważnieni:
   a) pracownicy – w zależności od wykonywanych czynności służbowych,
   b) wykonawcy usług oraz dostawcy sprzętu lub oprogramowania – w zakresie koniecznym do realizowania danej usługi lub wykonania określonych czynności w systemie za zgodą administratora systemu,
   c) inni użytkownicy – w zakresie ustalonym w stosownej umowie.
2. Osoby, o których mowa w ust. 1, muszą posiadać w systemie własne konto, dostęp do którego winien być możliwy jedynie po podaniu właściwego identyfikatora i hasła.

Dotychczasowe brzmienie:

„§ 13

1. Rejestracja użytkowników w systemie informatycznym, nadawanie lub modyfikacja uprawnień oraz wyrejestrowywanie użytkowników z systemu odbywa się zgodnie z poniższymi procedurami:
   a) Bezpośredni przełożony składa u administratora danego systemu zlecenie zarejestrowania użytkownika w systemie,
   b) Wzór „Zlecenia zarejestrowania użytkownika, modyfikacji uprawnień, wyrejestrowania użytkownika" określa Załącznik nr 6,
   c) Administrator systemu po otrzymaniu zlecenia, o którym mowa powyżej, rejestruje użytkownika w systemie nadając mu identyfikator oraz wnioskowane uprawnienia,
   d) W przypadku zmiany przez użytkownika uprawnień do obsługi danego systemu, administrator systemu niezwłocznie modyfikuje uprawnienia na podstawie zlecenia, o którym mowa w pkt. 1, otrzymanego od bezpośredniego przełożonego użytkownika,
   e) W przypadku utraty przez użytkownika uprawnień do obsługi danego systemu teleinformatycznego (np. rozwiązanie stosunku pracy, nie obsługiwanie systemu z powodu zmiany stanowiska pracy) bezpośredni

przełożony niezwłocznie występuje do administratora systemu z wnioskiem o wyrejestrowanie użytkownika z systemu, usunięcie użytkownika (zablokowanie dostępu do systemu), przekazując mu stosowne zlecenie,

f) Administrator systemu, po otrzymaniu zlecenia, niezwłocznie blokuje dostęp użytkownika do systemu,

g) Ze względów na odrębne przepisy w niektórych systemach, konta użytkownika nie są kasowane, a jedynie blokowane."

Nowe brzmienie:

§ 13

1. Rejestracja użytkowników w systemie informatycznym, nadawanie lub modyfikacja uprawnień oraz wyrejestrowywanie użytkowników z systemu odbywa się zgodnie z poniższymi procedurami:
   a) bezpośredni przełożony składa u administratora danego systemu zlecenie zarejestrowania użytkownika w systemie,
   b) wzór „Zlecenia zarejestrowania użytkownika, modyfikacji uprawnień, wyrejestrowania użytkownika" określa Załącznik nr 6,
   c) administrator systemu po otrzymaniu zlecenia, o którym mowa powyżej, rejestruje użytkownika w systemie nadając mu identyfikator oraz wnioskowane uprawnienia,
   d) w przypadku zmiany przez użytkownika uprawnień do obsługi danego systemu, administrator systemu niezwłocznie modyfikuje uprawnienia na podstawie zlecenia, o którym mowa w pkt. 1, otrzymanego od bezpośredniego przełożonego użytkownika,
   e) w przypadku utraty przez użytkownika uprawnień do obsługi danego systemu teleinformatycznego (np. rozwiązanie stosunku pracy, nie obsługiwanie systemu z powodu zmiany stanowiska pracy) bezpośredni przełożony niezwłocznie występuje do administratora systemu z wnioskiem o wyrejestrowanie użytkownika z systemu, usunięcie użytkownika (zablokowanie dostępu do systemu), przekazując mu stosowne zlecenie,
   f) administrator systemu, po otrzymaniu zlecenia, niezwłocznie modyfikuje uprawnienia dostępu użytkownika do systemu,
   g) ze względów na odrębne przepisy w niektórych systemach, konta użytkownika nie są kasowane, a jedynie blokowane.

§ 2

W Polityce bezpieczeństwa informacji w systemach teleinformatycznych Politechniki Częstochowskiej:

1) zmianie ulegają załączniki nr 1 i 4, które stanowią integralną część niniejszego zarządzenia;
2) w związku ze skreśleniem § 10 ust. 4 zostaje usunięty Załącznik nr 5 - Wzór wniosku o zgodę na użytkowanie sprzętu komputerowego poza uczelnią (skreślenie dotyczy również spisu załączników wyszczególnionych w Rozdziale XIII);
3) zostaje dodany Załącznik nr 14 – Główni właściciele biznesowi systemów (dotyczy również spisu załączników wyszczególnionych w Rozdziale XIII).

§ 3

Zarządzenie wchodzi w życie z dniem wydania.

Rektor
Politechniki Częstochowskiej

Prof. dr hab. inż. Norbert Sczygiol

Załącznik nr 1 *- Oświadczenie o zapoznaniu się z Polityką Bezpieczeństwa Informacji Politechniki Częstochowskiej*
(Zarządzenie nr 211/2021 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:
   a) przestrzegać obowiązujących przepisów prawa;
   b) chronić przetwarzane w systemach informatycznych PCz dane, w szczególności dane osobowe i tajemnicę przedsiębiorstwa przed ich uszkodzeniem, udostępnieniem osobom nieupoważnionym, niepożądaną modyfikacją lub usunięciem;
   c) nie udostępniać nikomu haseł, kart dostępowych, podpisów kwalifikowanych ani innego typu poświadczenia do przydzielonych mi zasobów – pomieszczeń, sieci, aplikacji, poczty elektronicznej;
   d) informować przełożonego lub administratora systemu o wszelkich podejrzanych zmianach w działaniu oprogramowania, mogących być skutkiem ataku;
   e) informować osobę odpowiedzialną materialnie o wszelkich zmianach dotyczących lokalizacji lub konfiguracji sprzętu komputerowego;
   f) chronić przed zniszczeniem lub uszkodzeniem sprzęt komputerowy stanowiący majątek PCz; zauważone uszkodzenia i usterki zgłaszać do odpowiedniego działu;
   g) nie wykorzystywać do celów prywatnych powierzonego sprzętu, służbowej skrzynki e-mail oraz nie udostępniać kluczy licencyjnych oprogramowania;
   h) używać do celów służbowych wyłącznie służbowych urządzeń, oprogramowania i adresów e-mail,
   i) informować przełożonego lub administratora systemu, o próbach wyłudzania haseł lub innych informacji związanych z zabezpieczeniami systemów informatycznych PCz dokonywanych drogą telefoniczną, pocztą elektroniczną lub w bezpośrednim kontakcie oraz o wszelkich innych podejrzanych działaniach mogących mieć negatywny wpływ na bezpieczeństwo danych,
   j) blokować dostęp do komputera w sytuacji, kiedy konieczne jest opuszczenie stanowiska pracy;
   k) w systemach przetwarzających ważne dane, z punktu widzenia funkcjonowania

Uczelni, nie instalować samowolnie i używać wyłącznie oprogramowania zainstalowanego przez Administratora systemu;

l) w przypadku wystąpienia konieczności zainstalowania na komputerze nowego oprogramowania, zgłosić ten fakt Administratorowi systemu;

m) dbać o bezpieczeństwo danych zapisanych w plikach mających znaczenie dla skutecznego wykonywania obowiązków służbowych, poprzez ich składowanie na archiwizowanych zasobach sieciowych;

n) 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);

o) informować Administratora systemu o wykrytym przez program antywirusowy złośliwym oprogramowaniu, które nie zostało automatycznie naprawione;

p) 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;

q) nie podłączać samodzielnie do wewnętrznej sieci teleinformatycznej PCz prywatnych urządzeń, np.: laptop, tablet, smartphone, router WiFi lub innych.

2. Przyjmuję do wiadomości, że:

a) 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.) - w szczególności za samodzielnie wgrane pliki;

b) historia operacji wykonywanych przeze mnie w systemach informatycznych jest zapisywana oraz archiwizowana i może podlegać kontroli i analizie;

c) zawartość służbowej skrzynki e-mail podlega archiwizacji i kontroli;

d) 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;

e) jestem zobowiązana/-y do zachowania w tajemnicy wszystkich danych, z którymi mam kontakt w związku z wykonywaną przeze mnie pracą oraz sposobu ich zabezpieczenia;

f) tajemnica, o której mowa w pkt. 2e obowiązuje mnie bezterminowo, również po zakończeniu pracy w PCz;

g) tajemnica, o której mowa w pkt. 2e nie dotyczy sytuacji, gdy ujawnienia informacji, o których mowa, żądają uprawnione organy lub urzędy państwowe na podstawie bezwzględnie obowiązujących przepisów prawa oraz gdy mamy do czynienia z informacją jawną, publiczną lub opublikowaną przez PCz;

h) dostęp do internetu jest w PCz monitorowany, a historia zapisywana i może być udostępniona przełożonym;

i) dostęp do internetu może być ograniczany zarówno pod względem zakresu dostępnych stron, jak i pod względem czasu, w którym internet będzie udostępniany pracownikom;

j) zdalna praca w wewnętrznej sieci PCz możliwa jest wyłącznie z użyciem silnie szyfrowanego kanału VPN po wcześniejszym, pozytywnym zaopiniowaniu przez przełożonego, Inspektora Ochrony Danych i Administratora systemu.

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 ustawie z dnia z dnia 26 czerwca 1974 r. - Kodeks pracy (Dz. U. z 2020 r. poz. 1320, z późn. zm.).
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

Załącznik nr 4 *- Regulamin użytkowania komputerów przenośnych*

(Zarządzenie nr 211/2021 Rektora PCz)

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, zobowiązana jest 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:
   a) niepozostawiania komputera w samochodzie, przechowalni bagażu itp.;
   b) przenoszenia komputera w specjalnej torbie/plecaku;
   c) transportowania komputera w bagażu podręcznym;
   d) niepozostawiania komputera bez nadzoru;
   e) niekorzystania z publicznych sieci komputerowych.
3. Zabrania się użytkowania komputera w miejscach publicznych i w środkach transportu publicznego, jeśli istnieje niebezpieczeństwo, że dane wyświetlane mogą zostać podejrzane lub przejęte przez osoby postronne.
4. Administrator systemu zobowiązany jest do podejmowania działań mających na celu zabezpieczenie komputerów przenośnych. W szczególności powinien on:
   a) 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;
   b) zabezpieczyć dane na dyskach komputerów przenośnych poprzez zastosowanie oprogramowania szyfrującego;
   c) dokonać na komputerze przenośnym instalacji i konfiguracji uczelnianego oprogramowania antywirusowego;
   d) 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 zobowiązany jest do natychmiastowego powiadomienia o tym fakcie bezpośredniego przełożonego, administratora oraz Inspektora Ochrony Danych (jeżeli na komputerze przetwarzane były dane osobowe).

Załącznik nr 14 *– Główni właściciele biznesowi systemów*

(Zarządzenie nr 211/2021 Rektora PCz)

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 ds. planowania i analiz
4.	Report Portal - Personel	Kierownik Działu Kadr, Płac i Spraw Socjalnych
5.	Report Portal - Finanse i księgowość	Zastępca kanclerza ds. planowania i analiz