##### *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:
2. przestrzegać obowiązujących przepisów prawa;
3. chronić przetwarzane w systemach informatycznych PCz dane, w szczególności dane osobowe i tajemnicę przedsiębiorstwa przed ich uszkodzeniem, udostępnieniem osobom nieupoważnionym, niepożądaną modyfikacją lub usunięciem;
4. nie udostępniać nikomu haseł, kart dostępowych, podpisów kwalifikowanych ani innego typu poświadczenia do przydzielonych mi zasobów – pomieszczeń, sieci, aplikacji, poczty elektronicznej;
5. informować przełożonego lub administratora systemu o wszelkich podejrzanych zmianach w działaniu oprogramowania, mogących być skutkiem ataku;
6. informować osobę odpowiedzialną materialnie o wszelkich zmianach dotyczących lokalizacji lub konfiguracji sprzętu komputerowego;
7. chronić przed zniszczeniem lub uszkodzeniem sprzęt komputerowy stanowiący majątek PCz; zauważone uszkodzenia i usterki zgłaszać do odpowiedniego działu;
8. nie wykorzystywać do celów prywatnych powierzonego sprzętu, służbowej skrzynki e-mail oraz nie udostępniać kluczy licencyjnych oprogramowania;
9. używać do celów służbowych wyłącznie służbowych urządzeń, oprogramowania i adresów e-mail,
10. 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,
11. blokować dostęp do komputera w sytuacji, kiedy konieczne jest opuszczenie stanowiska pracy;
12. w systemach przetwarzających ważne dane, z punktu widzenia funkcjonowania Uczelni, nie instalować samowolnie i używać wyłącznie oprogramowania zainstalowanego przez Administratora systemu;
13. w przypadku wystąpienia konieczności zainstalowania na komputerze nowego oprogramowania, zgłosić ten fakt Administratorowi systemu;
14. dbać o bezpieczeństwo danych zapisanych w plikach mających znaczenie dla skutecznego wykonywania obowiązków służbowych, poprzez ich składowanie na archiwizowanych zasobach sieciowych;
15. 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);
16. informować Administratora systemu o wykrytym przez program antywirusowy złośliwym oprogramowaniu, które nie zostało automatycznie naprawione;
17. 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;
18. nie podłączać samodzielnie do wewnętrznej sieci teleinformatycznej PCz prywatnych urządzeń, np.: laptop, tablet, smartphone, router WiFi lub innych.
19. Przyjmuję do wiadomości, że:
20. 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;
21. historia operacji wykonywanych przeze mnie w systemach informatycznych jest zapisywana oraz archiwizowana i może podlegać kontroli i analizie;
22. zawartość służbowej skrzynki e-mail podlega archiwizacji i kontroli;
23. 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;
24. jestem zobowiązana/-y do zachowania w tajemnicy wszystkich danych, z którymi mam kontakt w związku z wykonywaną przeze mnie pracą oraz sposobu ich zabezpieczenia;
25. tajemnica, o której mowa w pkt. 2e obowiązuje mnie bezterminowo, również po zakończeniu pracy w PCz;
26. 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;
27. dostęp do internetu jest w PCz monitorowany, a historia zapisywana i może być udostępniona przełożonym;
28. dostęp do internetu może być ograniczany zarówno pod względem zakresu dostępnych stron, jak i pod względem czasu, w którym internet będzie udostępniany pracownikom;
29. 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.
30. 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](about:blank) z dnia z dnia 26 czerwca 1974 r. - Kodeks pracy (Dz. U. z 2020 r. poz. 1320, z późn. zm.).
31. 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