Monitor Prawny Politechniki Śląskiej

poz. 413

ZARZĄDZENIE NR 89/2021
REKTORA POLITECHNIKI ŚLĄSKIEJ
z dnia 27 maja 2021 r.

w sprawie wprowadzenia Regulaminu przestrzegania zasad ochrony informacji na Politechnice Śląskiej

Działając na podstawie art. 23 ust. 1 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce (j.t. Dz. U. z 2021 r. poz. 478, z późn. zm.), w związku z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. 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.U.UE.L.2016.119.1) oraz ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (j.t. Dz.U. z 2019 r. poz. 1781), zarządza się, co następuje:

§ 1

Wprowadza się Regulamin przestrzegania zasad ochrony informacji na Politechnice Śląskiej stanowiący załącznik do niniejszego zarządzenia.

§ 2

Zarządzenie wchodzi w życie z dniem podpisania.

Rektor PŚ: *A. Mężyk*

Regulamin przestrzegania zasad ochrony informacji na Politechnice Śląskiej

Rozdział I
Przepisy ogólne

§ 1

Niniejszy Regulamin przestrzegania zasad ochrony informacji na Politechnice Śląskiej, zwany dalej Regulaminem, stanowi wykaz podstawowych obowiązków dotyczących przestrzegania zasad ochrony informacji w zakresie m.in. danych osobowych podczas ich przetwarzania, w tym wykonywania pracy stacjonarnie lub wykonywania na polecenie pracodawcy pracy zdalnie przez osoby nazwane w dalszej części użytkownikami, tj.:

1) osoby zatrudnione na Politechnice Śląskiej w jakiejkolwiek formie, np. na podstawie umowy o pracę, umowy cywilnoprawnej, umowy o współpracy,
2) inne osoby, które, współpracując z Politechniką Śląską, wykorzystują jej zasoby informacyjne,
3) osoby fizyczne prowadzące własną działalność gospodarczą z dostępem do zasobów sprzętowych i informacyjnych Politechniki Śląskiej,
4) pracowników podmiotów trzecich posiadających dostęp do informacji Politechniki Śląskiej (w tym danych osobowych),
5) osoby będące związane z Politechniką Śląską każdą dowolną formą kształcenia, mające dostęp do systemów lub informacji będących własnością Politechniki Śląskiej.

§ 2

1. Każdy użytkownik jest odpowiedzialny za prawidłowe użytkowanie sprzętu i oprogramowania będących własnością Politechniki Śląskiej, z poszanowaniem praw licencyjnych, zasad własności intelektualnej oraz uwzględnieniem zasad opisanych w rozdziale II Najlepsze praktyki zachowania bezpieczeństwa informacji – Zasady bezpiecznego użytkowania sprzętu IT przeznaczonego do pracy zdalnej.
2. Dla zapewnienia bezpieczeństwa podczas przetwarzania informacji każdy użytkownik powinien mieć nadane takie uprawnienia, aby, gwarantując najwyższy stopień bezpieczeństwa, móc wykorzystać wszystkie funkcje użytkowanego oprogramowania z uwzględnieniem zasad opisanych w rozdziale II Najlepsze praktyki zachowania bezpieczeństwa informacji – Zarządzanie uprawnieniami.
3. Każdy użytkownik jest zobowiązany do ochrony wszelkich dokumentów papierowych zawierających informacje będące własnością Politechniki Śląskiej, w szczególności z uwzględnieniem zasad opisanych w rozdziale II Najlepsze praktyki zachowania bezpieczeństwa informacji – Zabezpieczenie dokumentacji papierowej zawierającej informacje niemające statusu jawne, w tym dane osobowe.
4. Podczas korzystania z zasobów sieci Internet każdy użytkownik powinien zachować szczególną ostrożność przy czynnościach, które mogą narazić Politechnikę Śląska na utratę wiarygodnej i pewnej informacji, w szczególności powinien stosować się do wytycznych opisanych w rozdziale II Najlepsze praktyki zachowania bezpieczeństwa informacji – Zasady korzystania z Internetu.
5. Podczas korzystania z poczty elektronicznej każdy użytkownik powinien zapewnić bezpieczeństwo pracy, w tym poufność przesyłanych danych, z zastosowaniem zasad opisanych w rozdziale II Najlepsze praktyki zachowania bezpieczeństwa informacji – Zasady korzystania z poczty elektronicznej.
6. W przypadku stwierdzenia naruszenia zasad ochrony informacji (w tym danych osobowych) należy podjąć czynności zaradcze minimalizujące negatywne skutki tych naruszeń, z uwzględnieniem działań opisanych w rozdziale II Najlepsze praktyki zachowania bezpieczeństwa informacji – Skrócona instrukcja postępowania w przypadku naruszenia ochrony informacji.
7. Każdy użytkownik podczas przetwarzania informacji będących własnością Politechniki Śląskiej jest zobowiązany do zachowania szczególnej staranności oraz przestrzegania zasad poufności zgodnych z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. 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), zwanym dalej RODO, ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych, oraz odpowiednio ustawą z dnia 26 czerwca 1974 r. Kodeks pracy, Regulaminem pracy Politechniki Śląskiej (Monitor Prawny PŚ z 2019 r. poz. 224) oraz innymi obowiązującymi przepisami. Zadania powinny być realizowane z zastosowaniem zasad opisanych w rozdziale II Najlepsze praktyki zachowania bezpieczeństwa informacji – Obowiązek zachowania poufności i ochrony informacji, w tym danych osobowych.

8. Przed przystąpieniem do wykonywania pracy zdalnej użytkownik zapoznaje się z treścią niniejszego Regulaminu, co potwierdza oświadczeniem złożonym w formie pisemnej lub elektronicznej – skan podpisanego dokumentu należy przesłać e-mailem. Wzór oświadczenia stanowi załącznik do Regulaminu.
9. Postępowanie sprzeczne z zasadami ujętymi w niniejszym Regulaminie może zostać uznane przez Politechnikę Śląską za naruszenie zasad wynikających z obowiązujących przepisów dotyczących bezpieczeństwa informacji, w tym Regulaminu pracy Politechniki Śląskiej, RODO oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.

Rozdział II
Najlepsze praktyki zachowania bezpieczeństwa informacji

§ 3

Zasady bezpiecznego użytkowania sprzętu IT przeznaczonego do pracy zdalnej

1. Użytkownik odpowiada za zabezpieczenie należącego do Uczelni sprzętu IT (w szczególności laptopa, tabletu, smartfona) przed zniszczeniem, uszkodzeniem, utratą oraz kradzieżą.
2. Użytkownik jest zobowiązany do przechowywania wszelkich informacji, które nie mają statusu jawne, w tym danych osobowych związanych z wykonywaniem zadań służbowych, na odpowiednio zabezpieczonych dyskach, partycjach i kartach pamięci zamontowanych w sprzęcie IT zgodnie z zasadami wprowadzonymi przez Administratora Systemów Informatycznych (ASI) lub Lokalnego Administratora Systemów Informatycznych (LASI).
3. Dane niemające statusu informacji jawnej, przechowywane na nośnikach (dysk przenośny, pendrive, CD, DVD, karta pamięci) poza siedzibą pracodawcy, muszą być zaszyfrowane.
4. Pliki z danymi osobowymi przechowywane na niezabezpieczonych nośnikach na sprzęcie IT firmowym lub prywatnym powinny być zabezpieczone hasłem spełniającym wymagania bezpieczeństwa jak dla hasła do domeny Politechniki Śląskiej.
5. Użytkownik jest zobowiązany do zabezpieczenia sprzętu IT i nośników danych, na których znajdują się informacje niemające statusu jawne, w tym dane osobowe, przed osobami postronnymi oraz domownikami.
6. Użytkownik jest zobowiązany do bezpiecznego przewożenia sprzętu IT.
7. Zakazane jest wynoszenie niezaszyfrowanych nośników z zapisanymi jakimikolwiek informacjami, które nie mają statusu jawne, w tym danych osobowych, poza siedzibę Uczelni.
8. Zakazane jest kopiowanie/zapisywanie danych osobowych związanych z wykonywaniem zadań służbowych lub wynikających z umownych zobowiązań/umów cywilnoprawnych/zadań projektowych na niezabezpieczone, prywatne nośniki zewnętrzne.
9. W przypadku podłączania się do sieci Internet przy wykorzystaniu sieci publicznej oraz pracy na danych stanowiących własność Politechniki Śląskiej użytkownik zobowiązuje się do stosowania zabezpieczonego przed podsłuchem połączenia zdalnego do systemów Politechniki Śląskiej (eduVPN, SSL).
10. Dostęp do domowej sieci Wi-Fi, jeżeli sprzęt i oprogramowanie to umożliwiają, powinien być zabezpieczony hasłem o odpowiednim poziomie.
11. Nie należy używać domyślnego hasła – rekomendowana jest zmiana hasła i loginu dostępowego do routera, z wyłączeniem systemów dostępowych, do których użytkownik nie posiada takich uprawnień.
12. Sprzęt IT używany do pracy zdalnej musi być zabezpieczony aktywnym firewallem pochodzącym z systemu operacyjnego lub, w przypadku starszych systemów operacyjnych niemających wbudowanego systemu firewall, dodatkowego oprogramowania.
13. Sprzęt komputerowy używany do pracy zdalnej musi być zabezpieczony (odpowiednio przez system operacyjny lub, w przypadku sprzętu starszego, przez instalację dodatkowego programu) przed wirusami.
14. Do transferu danych należy używać tylko kanałów transmisyjnych dopuszczonych i skonfigurowanych przez centralne służby informatyczne Politechniki Śląskiej.

§ 4

Zarządzanie uprawnieniami

1. Każdy użytkownik programów i systemu operacyjnego jest zobowiązany do pracy na własnym koncie. Niedozwolona jest praca innych osób (np. innych domowników) na koncie użytkownika.
2. Zabronione jest udostępnianie konta innemu użytkownikowi.
3. W przypadku posiadania możliwości zmiany uprawnień użytkownik powinien to uczynić za zgodą przełożonego.
4. Użytkownik komputera oraz programów rozpoczyna pracę logowaniem i kończy wylogowaniem się.
5. Użytkownik przed tymczasowym odejściem od komputera jest zobowiązany włączyć wygaszacz ekranu zabezpieczony hasłem lub wylogować się z systemu bądź z programu.
6. Zabrania się uruchamiania jakiejkolwiek aplikacji lub programu na prośbę innej osoby, o ile nie jest to znana aplikacja wykorzystywana do wykonywania obowiązków służbowych, w szczególności do prowadzenia badań naukowych lub dydaktyki, bądź osoba, o której mowa wyżej, nie została zweryfikowana jako pracownik Uczelni (w szczególności pracownik odpowiedniego działu IT lub przełożony). Dotyczy to zwłaszcza programów przesłanych za pomocą poczty elektronicznej lub wskazanych w formie hiperlinku (http/https).
7. Po zakończeniu pracy użytkownik jest zobowiązany wylogować się z systemu informatycznego oraz zabezpieczyć nośniki elektroniczne, magnetyczne i optyczne, na których znajdują się informacje niemające statusy jawne, w tym dane osobowe.

§ 5

Zabezpieczenie dokumentacji papierowej zawierającej informacje niemające statusu jawne, w tym dane osobowe

1. Pracownik jest zobowiązany do przechowywania dokumentacji papierowej zawierającej informacje niemające statusu jawne, w tym dane osobowe, w sposób uniemożliwiający dostęp osobom postronnym, nieupoważnionym czy domownikom, np. przechowując je w zamykanych na klucz szafach, biurkach, sejfach, z wyjątkiem pomieszczeń odpowiednio nadzorowanych w Uczelni.
2. Zabrania się pozostawiania dokumentów w miejscach dostępnych dla osób postronnych.
3. Zabrania się wyrzucania niezniszczonych skutecznie dokumentów.
4. Należy zapewnić bezpieczne przewożenie dokumentacji uniemożliwiające jej zniszczenie, ujawnienie jej treści osobom postronnym, zagubienie lub kradzież.

§ 6

Zasady korzystania z Internetu

1. W przypadku posiadania praw administratora wszystkie programy pobierane z Internetu można instalować na sprzęcie należącym do Politechniki Śląskiej, jednak dopiero po konsultacji z LASI i uzyskaniu jego akceptacji (w celach dowodowych pisemnej - w tym e-mailowej), która jest warunkiem koniecznym do instalacji, z wyjątkiem znanych programów do wykonywania obowiązków służbowych, w szczególności prowadzenia badań naukowych lub dydaktyki.
2. W przypadku braku odpowiedzi LASI na zapytanie w sprawie konsultacji w ciągu 2 dni roboczych, użytkownik powinien o tym fakcie niezwłocznie powiadomić ASI, który wyznaczy innego pracownika do przeprowadzenia konsultacji i wydania lub odmowy wydania akceptacji.
3. W przypadku zainstalowania na sprzęcie IT należącym do Politechniki Śląskiej programów lub aplikacji bez konsultacji z LASI, użytkownik odpowiada za szkody wyrządzone wskutek działania tych programów lub aplikacji.
4. Zabrania się wchodzenia na strony z nielegalnym oprogramowaniem, a także pobierania i instalacji takiego oprogramowania.
5. W przypadku korzystania w pracy zdalnej z komputera prywatnego, użytkownik odpowiada za szkody wyrządzone na skutek działania oprogramowania na nim zainstalowanego.
6. Zabrania się uruchamiania na urządzeniach będących własnością Politechniki Śląskiej oraz korzystania z dostępu do Internetu w sieci Uczelni w celu instalacji jakichkolwiek aplikacji związanych z udostępnianiem zasobów Politechniki Śląskiej bez zgody bezpośredniego przełożonego, w szczególności wydobywania kryptowalut.

7. Zabrania się uruchamiania lub udostępniania zasobów informatycznych Uczelni bez zgody bezpośredniego przełożonego, gdy nie jest to związane z wykonywaniem obowiązków służbowych wynikających z zajmowanego stanowiska.
8. Uruchamianie aplikacji angażujących znaczne zasoby jednostki, w tym przetwarzających duże zbiory danych lub wymagających wielogodzinnych obliczeń, wymaga zgody bezpośredniego przełożonego.

§ 7

Zasady korzystania z poczty elektronicznej

1. Pliki zawierające dane osobowe (np. w formacie Word, Excel, PDF lub spakowane, np. w formacie ZIP) przed wysłaniem ich do osób trzecich powinny być zabezpieczone hasłem, które powinno być przekazane do odbiorcy innym kanałem łączności, np. telefonicznie lub SMS-em.
2. W przypadku zabezpieczenia plików hasłem obowiązuje minimum 8 znaków: duże i małe litery oraz cyfry lub znaki specjalne, tak jak w przypadku logowania do domeny Politechniki Śląskiej.
3. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy poczty.
4. Nie należy otwierać bez uprzedniej weryfikacji w odpowiednim dziale IT załączników poczty pochodzącej z nietypowych zdaniem użytkownika domen.
5. Nie należy otwierać linków w podejrzanej poczcie nieznanego pochodzenia bez uprzedniej weryfikacji w odpowiednim dziale IT, gdyż grozi to zainfekowaniem komputera, a nawet całej sieci, w której komputer pracuje.
6. Nie należy wprowadzać loginów i haseł służbowych do formularzy zawartych w poczcie bez uprzedniej weryfikacji w odpowiednim dziale IT, gdyż mogą to być próby wyłudzenia danych dostępowych, tzw. phishing (np. e-mail przesłany rzekomo z banku z opcją zalogowania się bądź e-mail przesłany rzekomo przez producenta wyszukiwarki internetowej z komunikatem o próbie włamania do poczty i sugestią zalogowania się do panelu umieszczonego w treści wiadomości).
7. Należy bezzwłocznie zgłaszać administratorom poczty elektronicznej Politechniki Śląskiej przypadki niezidentyfikowanych e-maili, plików w e-mailach, prób wyłudzeń, kontaktów oczekujących dostępu do danych.
8. Podczas wysyłania e-maili do wielu adresatów jednocześnie należy użyć metody „Ukryte do wiadomości" (UDW). Nie wolno rozsyłać e-maili do wielu adresatów z użyciem opcji „Do wiadomości"(DW). Otrzymanie takiej poczty należy bezzwłocznie zgłaszać administratorom poczty elektronicznej Politechniki Śląskiej oraz LASI. Nie dotyczy to sytuacji, w której adresaci stanowią grupę współpracującą nad sprawą i celowe jest, aby komunikowali się ze sobą w tej sprawie i monitorowali obieg informacji.
9. W celu zapewnienia sprawnego działania systemu poczty zaleca się okresowe usuwanie niepotrzebnych e-maili lub przenoszenie ich do archiwizacji.
10. Nie należy wysyłać korespondencji służbowej na prywatne skrzynki pocztowe osób posiadających konto w domenie polsl.pl.

§ 8

Skrócona instrukcja postępowania w przypadku naruszenia ochrony informacji, w tym danych osobowych

1. Każdy użytkownik jest zobowiązany do powiadomienia Lokalnego Pełnomocnika Ochrony Danych Osobowych (LPODO)(w przypadku wystąpienia zdarzenia niedotyczącego systemu informatycznego) lub Lokalnego Administratora Systemów Informatycznych (LASI) (w przypadku wystąpienia zdarzenia dotyczącego systemu informatycznego), gdy zidentyfikuje lub podejrzewa naruszenie ochrony informacji, w tym danych osobowych. Jeżeli występuje podejrzenie wystąpienia poważnego zdarzenia naruszenia ochrony informacji, dotyczącego wielu osób lub danych wrażliwych oraz wysokości wynagrodzenia, należy powiadomić bezpośrednio Inspektora Ochrony Danych (IOD).
2. Do incydentów wymagających powiadomienia LPODO lub LASI należą:
   1) zdarzenia losowe zewnętrzne (zniszczenie, zalanie dokumentów),
   2) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki użytkowników, utrata/zagubienie danych),
   3) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, nieświadome zniszczenie dokumentów/

danych, działanie wirusów i innego szkodliwego oprogramowania, kradzież dokumentów, nieuprawniona zmiana treści dokumentu, nieuprawnione wybrakowanie dokumentu),

4) telefoniczne próby wyłudzenia danych osobowych,
5) kradzież, zagubienie komputerów lub nośników optycznych, dysków przenośnych, pendrive'ów z danymi osobowymi, dokumentów papierowych,
6) e-maile zachęcające do ujawnienia identyfikatora i/lub hasła,
7) pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów.

§ 9

Obowiązek zachowania poufności i ochrony informacji, w tym danych osobowych

1. Zobowiązuje się wszystkich użytkowników do niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań.
2. Zobowiązuje się wszystkich użytkowników do zachowania w tajemnicy sposobów zabezpieczenia danych osobowych.
3. Zakazane jest przekazywanie bezpośrednio bądź przez telefon danych osobowych osobom nieupoważnionym lub osobom, których tożsamości nie można zweryfikować, lub osobom podejrzanym o fałszowanie tożsamości.
4. Zakazane jest przekazywanie lub ujawnianie danych osobom bądź instytucjom, które nie wykazały podstawy prawnej umożliwiającej dostęp do tych danych.
5. Każda z osób dopuszczonych do przetwarzania danych osobowych jest zobowiązana do zabezpieczenia ich przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem, nieuprawnionym dostępem oraz przetwarzaniem.
6. Zabrania się wykonywania pracy zdalnej w miejscach publicznych stwarzających ryzyko wglądu do informacji, w tym w danych osobowych, osób postronnych.
7. Pracując w domu, należy zadbać o to, aby domownicy nie mieli wglądu w wykonywaną pracę – w szczególności należy właściwie ustawić ekran urządzenia, a także zapewnić pracę z dokumentami w sposób uniemożliwiający wgląd.

....
(imię i nazwisko) (miejscowość i data)

OŚWIADCZENIE
o poufności przy wykonywaniu pracy zdalnej

Oświadczam, że zapoznałem(-łam) się z zasadami wykonywania zleconej mi przez pracodawcę pracy zdalnej opisanymi w Regulaminie przestrzegania zasad ochrony informacji na Politechnice Śląskiej.

W szczególności zobowiązuję się do:

1) przetwarzania informacji wyłącznie w zakresie i celu przewidzianych w zadaniach powierzonych mi przez pracodawcę,
2) zachowania w tajemnicy informacji, do których mam lub będę mieć dostęp w związku z wykonywaniem zadań podczas pracy zdalnej,
3) niewykorzystywania informacji w celach niezgodnych z zakresem i celem zadań powierzonych mi przez pracodawcę,
4) zachowania w tajemnicy sposobów zabezpieczenia sprzętu IT i systemów informatycznych wykorzystywanych do pracy zdalnej,
5) ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem, nieuprawnionym dostępem oraz przetwarzaniem,
6) niedopuszczania domowników oraz innych osób trzecich do urządzeń i nośników przekazanych mi przez pracodawcę oraz powierzonych mi informacji, w tym danych osobowych,
7) zwrotu powierzonych mi nośników wraz z kompletnymi danymi na każde żądanie pracodawcy.

Przyjmuję do wiadomości, że postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane przez Politechnikę Śląską za naruszenie zasad wynikających z obowiązujących przepisów dotyczących bezpieczeństwa informacji, w tym Regulaminu pracy Politechniki Śląskiej, RODO oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.

.....
(podpis oświadczającego)