Załącznik nr 5 do Polityki Ochrony Danych Osobowych
w PWSTE w Jarosławiu

Regulamin Ochrony Danych Osobowych w PWSTE w Jarosławiu

Regulamin określa podstawowe obowiązki z zakresu przestrzegania zasad ochrony danych osobowych zgodnie z przepisami dla: pracowników, współpracowników, pracowników podmiotów trzecich, posiadających dostęp do danych osobowych przetwarzanych przez Administratora/Podmiot przetwarzający, użytkowników systemów informatycznych z dostępem do danych osobowych przetwarzanych przez Administratora/Podmiot przetwarzający.

Każda z w/w osób powinna zapoznać się z poniższym regulaminem oraz zobowiązać się do stosowania zasad w nim zawartych

SPIS TREŚCI

1 ZASADY BEZPIECZNEGO UŻYTKOWANIA SPRZĘTU IT, DYSKÓW, PROGRAMÓW

1. W przypadku, gdy użytkownik przetwarzający dane osobowe korzysta ze sprzętu IT, zobowiązany jest do jego ochrony przed jakimkolwiek zniszczeniem lub uszkodzeniem. Za sprzęt IT rozumie się: komputery stacjonarne, monitory, drukarki, skanery, ksera, laptopy, służbowe tablety i smartfony.
2. Użytkownik ma obowiązek natychmiast zgłosić zagubienie, utratę lub zniszczenie powierzonego mu Sprzętu IT.
3. Samowolne otwieranie (demontaż) sprzętu IT, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) lub podłączanie jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego jest zabronione.
4. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. pracownikom innych działów) wglądu do danych wyświetlanych na monitorach komputerowych – **tzw. „polityka czystego ekranu".**
5. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu (WINDOS + L) lub wylogować się z systemu bądź z programu.
6. Po zakończeniu pracy, użytkownik zobowiązany jest:

a. wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy,

b. zabezpieczyć stanowisko pracy, w szczególności wszelkie nośniki magnetyczne i optyczne, na których znajdują się dane osobowe.

7. Użytkownik jest zobowiązany do usuwania plików z nośników/dysków, do których mają dostęp inni użytkownicy nieupoważnieni do dostępu do takich plików (np. podczas współużytkowania komputerów).

8. Jeśli użytkownik jest uprawniony do niszczenia nośników, powinien trwale zniszczyć sam nośnik lub trwale usunąć z niego dane (np. zniszczenie płyt DVD w niszczarce, zniszczenie twardego dysku, pendrive np. przy użycia młotka).

9. W przypadku przechowywania na komputerze przenośnym danych osobowych lub stanowiących tajemnicę pracodawcy, użytkownik zobowiązany jest do ich przechowywania na dysku szyfrowanym, zabezpieczonym, co najmniej 8 znakowym hasłem (duże, małe litery, znaki specjalne lub cyfry).

10. W przypadku kradzieży lub zgubienia komputera przenośnego, Użytkownik powinien natychmiast powiadomić o tym osobę odpowiedzialną za ochronę danych (IOD), zaznaczając jednocześnie, jakiego rodzaju dane były na tym urządzeniu przechowywane.

2 ZASADY UŻYWANIA KOMPUTERÓW PRZENOŚNYCH

1. W przypadku przechowywania na komputerze przenośnym danych osobowych lub stanowiących tajemnicę pracodawcy, użytkownik zobowiązany jest do przechowywania na dysku szyfrowanym, zabezpieczonym, co najmniej 8 znakowym hasłem.

2. Na komputerach przenośnych przeznaczonych do prezentacji multimedialnych nie powinny, o ile jest to możliwe, znajdować się dane osobowe lub stanowiące tajemnicę pracodawcy.

3. W przypadku kradzieży lub zgubienia komputera przenośnego, użytkownik powinien natychmiast powiadomić o tym osobę odpowiedzialną za ochronę danych (IOD), zaznaczając jednocześnie, jakiego rodzaju dane były na komputerze przechowywane.

4. W przypadku pozostawiania komputerów przenośnych w biurze zaleca się umieszczenie ich po zakończeniu pracy w zamykanych szafkach.

5. Pracując na komputerze przenośnym w miejscach publicznych użytkownik zobowiązany jest chronić wyświetlane na monitorze informacje przed wglądem osób nieupoważnionych.

3 ZASADY PRACY NA PRYWATNYCH URZĄDZENIACH IT

1. Pracownik może pracować na prywatnym sprzęcie tylko w wyjątkowych sytuacjach.
2. Każdorazowe używanie prywatnych urządzeń wymaga zgody przełożonego a ponadto powinno być poprzedzone sprawdzeniem przez informatyka i zeskanowaniem w celu wykrycia ewentualnych zagrożeń.

3. Jeżeli pracownik wykorzystuje własne urządzenia do pracy z danymi osobowymi, powinno być one odpowiednio zabezpieczone poprzez wprowadzenie haseł zgodnie z polityką haseł.

4 ZARZĄDZANIE UPRAWNIENIAMI

1. Każdy użytkownik z dostępem do danych osobowych (np. na swoim komputerze, na dysku sieciowym, w programie lub aplikacji, w poczcie elektronicznej) musi posiadać swój własny indywidualny identyfikator (login) do logowania.
2. Użytkownik otrzymuje dostęp i odpowiednie uprawnienia do zasobów i aplikacji na polecenie przełożonych i przy realizacji informatyków. Procedura nadawania uprawnień została określona w Polityce Ochrony Danych w Państwowej Wyższej Szkole Techniczno-Ekonomicznej im. ks. Bronisława Markiewicza w Jarosławiu.
3. Użytkownicy nie mają prawa do samodzielnej zmiany uprawnień, np. przydzielenia sobie uprawnień administratora.
4. Użytkowników obowiązuje zasada pracy na własnym koncie. Zabronione jest, zatem umożliwianie innym osobom pracy na koncie innego użytkownika.

5 POLITYKA HASEŁ

1. Pierwsze (pierwotne) hasło użytkownika nadawane jest przez Administratora i przekazywane mu w poufny sposób.
2. Użytkownik systemu zobowiązany jest do niezwłocznej zmiany tego hasła.
3. Hasła powinny składać się, z co najmniej 8 znaków.
4. Hasła powinny zawierać duże litery + małe litery + cyfry (lub znaki specjalne).
5. Hasła nie mogą być łatwe do odgadnięcia. Nie powinny być powszechnie używanymi słowami. W szczególności nie należy, jako haseł wykorzystywać: dat, imion i nazwisk osób bliskich, imion zwierząt, popularnych dat, popularnych słów, typowych zestawów: 123456, qwerty.
6. Hasła nie powinny być ujawnianie innym osobom. Nie należy zapisywać haseł na kartkach i w notesach, nie naklejać na monitorze komputera, nie trzymać pod klawiaturą lub w szufladzie.
7. W przypadku ujawnienia hasła – należy natychmiast go zmienić.
8. Hasła muszą być zmieniane, co 32 dni.
9. Jeżeli system nie wymusza zmiany haseł, użytkownik zobowiązany jest do samodzielnej zmiany hasła.
10. W przypadku utraty uprawnień przez osobę administrującą systemem należy niezwłocznie zmienić hasła, do których miała dostęp.

6 ZABEZPIECZENIE DOKUMENTACJI PAPIEROWEJ Z DANYMI OSOBOWYMI

1. Pracownicy są zobowiązani do stosowania tzw. „**polityki czystego biurka**". Polega ona na zabezpieczaniu (zamykaniu) dokumentów np. w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych po godzinach pracy lub podczas ich nieobecności w trakcie godzin pracy.

2. Upoważnieni pracownicy zobowiązani są do niszczenia dokumentów i wydruków w niszczarkach lub utylizacji ich w specjalnych bezpiecznych pojemnikach z przeznaczeniem do bezpiecznej utylizacji.
3. Zabrania się pozostawiania dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami, np. w korytarzach, na kserokopiarkach, drukarkach, w pomieszczeniach konferencyjnych.
4. Zabrania się wyrzucania niezniszczonych dokumentów na śmietnik lub porzucania ich na zewnątrz.
5. Ważna dokumentacja jednostki, zwłaszcza zawierająca dane osobowe powinna być niszczona komisyjnie oraz zakończona protokołem niszczenia.

7 ZASADY WYNOSZENIA NOŚNIKÓW Z DANYMI POZA UCZELNIĘ

1. Użytkownicy nie mogą wynosić na zewnątrz organizacji wymiennych elektronicznych nośników informacji z zapisanymi danymi osobowymi bez zgody pracodawcy / zleceniodawcy. Do takich nośników należą m.in.: wymienne twarde dyski, pendrive, płyty CD, DVD, pamięci typu Flash.
2. Dane osobowe wynoszone poza uczelnię muszą być opatrzone hasłem (hasłowane dyski, hasłowane pliki).
3. Należy zapewnić bezpieczne przewożenie dokumentacji papierowej w plecakach, teczkach.
4. Należy korzystać ze sprawdzonych firm kurierskich.
5. W przypadku, gdy dokumenty przewozi pracownik, zobowiązany jest do zabezpieczenia przewożonych dokumentów przed zagubieniem i kradzieżą.
6. Pracownik zajmujący się przenoszeniem/przewożeniem nośników danych na zewnątrz jednostki powinien posiadać co do tego stosowne upoważnienie Administratora.

8 ZASADY PRZEBYWANIA W POMIESZCZENIACH SŁUŻBOWYCH POZA GODZINAMI PRACY

1. Przebywanie przez pracowników w pomieszczeniach służbowych poza obowiązującym ich rozkładem czasu pracy, w tym także w dni wolne od pracy jest dozwolone wyłącznie po uzyskaniu zgody przełożonego.
2. Zgoda powinna być wyrażona najpóźniej przed rozpoczęciem pracy poza ustalonymi godzinami pracy.
3. Przebywanie pracowników gospodarczych w pomieszczeniach szczególnie chronionych (pomieszczenia takie zostały określone w Załączniku do Polityki Ochrony Danych Osobowych w PWSTE w Jarosławiu- Załącznik nr 11) może odbywać się wyłącznie w obecności osób upoważnionych.

9 Zasady korzystania z Internetu

1. Użytkownik zobowiązany jest do korzystania z Internetu wyłącznie w celach służbowych.
2. Zabrania się zgrywania na dysk twardy komputera oraz uruchamia jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą osoby upoważnionej do administrowania infrastrukturą IT i tylko w uzasadnionych przypadkach.
3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu.
4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez prawo (na większości stron tego typu jest zainstalowane szkodliwe oprogramowanie infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem).
5. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.
6. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą "https:". Dla pewności należy „kliknąć" na ikonkę kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel.
7. Należy zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę lub podania naszych loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet. Szczególnie tyczy się to żądania podania takich informacji przez rzekomy bank.

10 Zasady korzystania z poczty elektronicznej

1. Przesyłanie danych osobowych z użyciem maila poza uczelnię może odbywać się tylko przez osoby do tego upoważnione.
2. W przypadku przesyłania danych osobowych poza organizację należy wykorzystywać mechanizmy kryptograficzne (hasłowanie wysyłanych dokumentów lub plików zzipowanych).
3. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 8 znaków: duże i małe litery i cyfry lub znaki specjalne a hasło należy przesłać odrębnym mailem lub inną metodą, np. telefonicznie lub SMS-em. Szczegółowa procedura przesyłania plików poza uczelnie określa instrukcja przesyłania plików, która stanowi załącznik do niniejszego Regulaminu.
4. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
5. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.
6. **WAŻNE:** Nie należy otwierać załączników (plików) w mailach nawet od rzekomo znanych nam nadawców bez weryfikacji tegoż nadawcy. Tego typu maile większości przypadków

zawierają załączniki ze szkodliwymi programami, które po „kliknięciu" infekują komputer użytkownika oraz często pozostałe komputery w sieci. W wyniku działania takiego szkodliwego oprogramowania może dojść do poważnych incydentów, łącznie z pełną utratą danych osobowych lub zaszyfrowanie m przez kryptowirusy.

7. **WAŻNE:** Bez weryfikacji wiarygodności nadawcy, nie należy „klikać" na hiperlinki w mailach, gdyż mogą to być hiperlinki do stron zainfekowanych lub niebezpiecznych. Użytkownik „klikając" na taki hiperlink bezwiednie infekuje swój komputer oraz często pozostałe komputery w sieci. W wyniku takiej infekcji może dojść do poważnych incydentów, łącznie z pełną utratą danych osobowych lub zaszyfrowanie m przez kryptowirusy.
8. Należy zgłaszać informatykowi przypadki podejrzanych emaili.
9. Użytkownicy nie powinni rozsyłać „niezawodowych" emalii w formie „łańcuszków szczęścia", np. życzenia świąteczne adresowane do 230 osób.
10. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – BCC". Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości" (skrót CC)!
11. Użytkownicy nie powinni rozsyłać, maili zawierających załączniki o dużym rozmiarze.
12. Użytkownicy powinni okresowo kasować niepotrzebne maile.
13. Mail służbowy jest przeznaczony wyłącznie do wykonywania obowiązków służbowych.
14. Zakazuje się wysyłania korespondencji służbowej na prywatne skrzynki pocztowe pracowników lub innych osób.
15. Użytkownicy mają prawo korzystać z poczty mailowej dla celów prywatnych wyłącznie okazjonalnie i powinno być to ograniczone do niezbędnego minimum.
16. Korzystanie z maila dla celów prywatnych nie może wpływać, na jakość i ilość świadczonej przez użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych
17. Użytkownicy nie mają prawa korzystać z maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania.
18. Użytkownik bez zgody Administratora nie ma prawa wysyłać wiadomości zawierających dane osobowe dotyczące Administratora, jego pracowników, klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej.

11 OCHRONA ANTYWIRUSOWA

1. Użytkownicy zobowiązani są do skanowania plików wprowadzanych z zewnętrznych nośników programem antywirusowym, jeśli system antywirusowy taką funkcje posiada.
2. Zakazane jest wyłączanie systemu antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe.

3. W przypadku stwierdzenia zainfekowania systemu lub pojawienia się komunikatów „np.; Twój system jest zainfekowany!, Zainstaluj program antywirusowy", użytkownik obowiązany jest poinformować niezwłocznie o tym fakcie Informatyka lub osobę upoważnioną.

12 Procedura naprawy sprzętu w serwisach zewnętrznych

1. Informatyk odpowiada za sprawdzanie poprawności działania systemu IT, w tym: stacji roboczych, serwerów, drukarek, baz danych, aplikacji, poczty email
2. Informatyk odpowiada za identyfikację i przyjmowanie zgłoszeń o nieprawidłowościach w działaniu systemu informatycznego oraz oprogramowania celem ich niezwłocznego usunięcia
3. W przypadku napraw dokonywanych na zewnątrz (z komputerów należy uprzednio wymontować dyski i wszelkie nośniki, z urządzeń mobilnych karty pamięci, usunąć dane z nośnika z użyciem specjalistycznego oprogramowania).
4. W przypadku naprawy sprzętu z danymi osobowymi na nośniku - rekomendowane jest zawarcie specjalnego zapisu w umowie serwisowej, gwarantującego bezpieczną naprawę (należy na to zwrócić uwagę przy zakupach sprzętu).
5. W przypadku naprawy sprzętu z danymi osobowymi na nośniku - rekomendowane jest przekazywanie do naprawy uszkodzonego sprzętu z danymi zaszyfrowanymi na dysku/karcie pamięci. Sprzęt przekazywany jest do serwisu bez podania hasła.
6. Rekomendowane jest korzystanie z serwisu, który dokonuje napraw u klienta (umowy gwarancyjne on-site).
7. Czynności konserwacyjne i naprawcze wykonywane przez osoby nieposiadające upoważnień do przetwarzania danych (np. specjalistów z firm zewnętrznych) muszą być wykonywane pod nadzorem osób upoważnionych.
8. Wszelkie prace konserwacyjne i naprawcze sprzętu komputerowego oraz uaktualnienia systemu informatycznego wykonywane przez podmiot zewnętrzny, powinny odbywać się na zasadach określonych w szczegółowej umowie z uwzględnieniem klauzuli dotyczącej ochrony danych.

13 Skrócona instrukcja postępowania w przypadku naruszenia ochrony danych osobowych

1. Każda pracownik zobowiązany jest niezwłocznie, a najpóźniej do 24 h po zaistnieniu incydentu zgłosić go do bezpośredniego przełożonego lub IOD.
2. Do sytuacji wymagających powiadomienia, należą w szczególności:

a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,

b. niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,

c. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka/ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).

3. Do incydentów wymagających powiadomienia, należą w szczególności:

a. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),

b. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych),

c. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).

4. Typowe przykłady incydentów wymagające reakcji:

a. ślady na drzwiach, oknach i szafach wskazują na próbę włamania,

b. dokumentacja jest niszczona bez użycia niszczarki,

c. fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie,

d. otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe,

e. ustawienie monitorów pozwala na wgląd osób postronnych w dane osobowe,

f. wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz uczelni bez upoważnienia Pracodawcy / Zleceniodawcy,

g. udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej i ustnej,

h. telefoniczne próby wyłudzenia danych osobowych,

i. kradzież, zagubienie komputerów lub CD, twardych dysków, Pendrive z danymi osobowymi,

j. maile zachęcające do ujawnienia identyfikatora i/lub hasła,

k. pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów,

l. hasła do systemów przyklejone są w pobliżu komputera.

14 Obowiązek zachowania poufności i ochrony danych osobowych

1. Każda z osób dopuszczona do przetwarzania danych osobowych jest zobowiązana do:

a. przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez Administratora zadaniach,

b. zachowania w tajemnicy danych osobowych, do których ma lub będzie miał/a dostęp w związku z wykonywaniem zadań powierzonych przez Administratora w trakcie trwania zatrudnienia jak również po ustaniu zatrudnienia,

c. niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań przez Pracodawcę/Zleceniodawcę,

d. zachowania w tajemnicy sposobów zabezpieczenia danych osobowych,

e. ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem.

2. Jeśli jest to przewidziane, osoba dopuszczona do przetwarzania odbywa szkolenie z zasad ochrony danych osobowych.

3. Osoby zapoznane z treścią niniejszego Regulaminu ODO lub przeszkolone zobowiązane są podpisać Oświadczenie o poufności.

4. Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym lub osobom, których tożsamości nie można zweryfikować lub osobom podszywającym się pod kogoś innego.

5. Zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie mogą wykazać się jasną podstawą prawną do dostępu do takich danych.

15 POSTĘPOWANIE DYSCYPLINARNE

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą, jako ciężkie naruszenie obowiązków pracowniczych lub naruszenie zasad współpracy.

2. Postępowanie sprzeczne z powyższymi zobowiązaniami, może też być uznane przez Administratora za naruszenie przepisów o ochronie danych osobowych. Administrator może pociągnąć osobę do postępowania dyscyplinarnego. Obok postępowania dyscyplinarnego pracownik może zostać pociągnięty do odpowiedzialności karną, zgodnie z która na zasadach określonych w ustawie o ochronie danych osobowych i kodeksu karnego odpowiada samodzielnie każdy pracownik.

3. W przypadku ukarania Administratora karą finansową o jakiej mowa w przepisach o ochronie danych osobowych, za czyny zawinione przez pracownika może on dochodzić od pracownika zwrotu kary stosowanie do zawinienia i przepisów kodeksu pracy.