Centrum Studiów Zaawansowanych Inżynierii Systemów

WYTYCZNE DO PRACY W SYSTEMIE PLATFORMA ELEARNINGOWA SAP

Wersja 01

Metryka dokumentu			
Nazwa dokumentu	Wytyczne do pracy w systemie Platforma eLearningowa SAP.		
Opis dokumentu	Dokument zawiera wytyczne do pracy w systemie Platforma eLearningowa SAP dla jego użytkowników (wykładowców i studentów), uwzględniające fakt, że w systemie tym przetwarzane są dane osobowe. Dokument został opracowany na podstawie wytycznych określonych w aktualnie obowiązującej w WAT dokumentacji bezpieczeństwa przetwarzania danych osobowych (wydanie 2 z roku 2017).		
Autorzy	dr inż. Stefan Rozmus	Liczba stron	9

Wersja	Data wydania	Opis	Akcja (*)	Rozdziały (**)	Autorzy (***)
01	2018-03-16	Utworzenie dokumentu	N	W	SR

(*) Akcje: W = Wstaw, Z = Zamień, We = Weryfikuj, N = Nowy

(**) Rozdziały: W = Wszystkie

(***) Inicjały autorów: patrz metryka dokumentu

Spis treści

1. POSTANOWIENIA OGÓLNE

§ 1

1. System ***Platforma eLearningowa SAP***, zwany dalej systemem PeLSAP jest systemem informatycznym, przeznaczonym do wsparcia kształcenia na odległość.
2. ***Wytyczne do pracy w systemie Platforma eLearningowa SAP*** określają warunki i sposób postępowania z tym systemem mając na uwadze fakt, że przetwarzane są w nim dane osobowe.
3. Ze względu na połączenie systemu PeLSAP z siecią publiczną, w systemie stosuje się zabezpieczenia na poziomie wysokim.
4. Za realizację i przestrzeganie zasad zawartych w niniejszym dokumencie odpowiada użytkownik systemu PeLSAP.

§ 2

Przez użyte w niniejszej instrukcji określenia rozumie się:

1) System informatyczny - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
2) Administrator Systemu Informatycznego PeLSAP (ASI) – osoba odpowiedzialna za zapewnienie właściwego funkcjonowania systemu informatycznego, przestrzegania zasad i wymagań bezpieczeństwa przewidzianych dla systemu, przeciwdziałanie dostępowi osób trzecich do systemu oraz podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w tym systemie.
3) Lokalny Administrator Danych Osobowych (LADO) – dziekan Wydziału Cybernetyki.
4) Lokalny Administrator Bezpieczeństwa Informacji (LABI) – kierownik Centrum Studiów Zaawansowanych Inżynierii Systemów.
5) Dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
6) Zabezpieczenie danych osobowych – wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.
7) Rola – rola osoby (wykładowca lub student), określająca zakres jego uprawnień do przetwarzania danych osobowych w systemie PeLSAP.
8) Potencjalny użytkownik – osoba (pracownik lub student) posiadająca uprawnienia do przetwarzania danych w systemie PeLSAP na zasadach określonych w dokumencie ***Regulamin Korzystania z Platformy eLearningowej SAP*** nadane przez ASI.
9) Użytkownik – potencjalny użytkownik, któremu ASI przekazał informacje o danych dostępowych (login i hasło) do systemu PeLSAP.
10) Osoba upoważniona – osoba legitymująca się prawem do przetwarzania danych osobowych w systemie PeLSAP.

11) Identyfikator użytkownika (login) – ciąg znaków jednoznacznie identyfikujący użytkownika w systemie PeLSAP.

12) Hasło – ciąg znaków wykorzystywany podczas uwierzytelniania użytkownika w systemie PeLSAP.

§ 3

1. Student może przetwarzać w systemie PeLSAP tylko i wyłącznie swoje dane osobowe.
2. Wykładowca może przetwarzać w systemie PeLSAP swoje dane osobowe oraz dane osobowe studentów.
3. Kontakt do LABI i ASI podany jest na stronie Wydziału Cybernetyki (ścieżka dostępu: ***Usługi i serwisy*** -> ***Platforma eLearningowa SAP***).

2. PROCEDURY NADAWANIA I COFANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH W SYSTEMIE PeLSAP

§ 4

1. Student jest osobą upoważnioną do przetwarzania swoich danych osobowych w systemie PeLSAP jeżeli posiada status ***aktywny*** w systemie USOS.
2. Wykładowca jest osobą upoważnioną do przetwarzania danych osobowych w systemie PeLSAP jeżeli posiada status ***aktywny*** w systemie USOS, a ponadto posiada upoważnienie do przetwarzania danych osobowych w systemie PeLSAP, nadane mu przez LADO.
3. Upoważnienia do przetwarzania danych w systemie PeLSAP sporządzane są w dwóch egzemplarzach, jeden przeznaczony jest dla LABI, drugi dla osoby upoważnionej do przetwarzania danych osobowych. Osoba upoważniona jest zobowiązana do dostarczenia jednego egzemplarza rzeczonego upoważnienia do LABI.

§ 5

1. Przed rozpoczęciem każdego semestru ASI aktualizuje wykaz osób upoważnionych do przetwarzania danych osobowych w systemie PeLSAP na podstawie danych, zaimportowanych z systemu USOS.
2. Dla każdej nowej osoby z rolą *student* uprawnienia do korzystania z systemu PeLSAP nadawane są automatycznie na podstawie wykazu otrzymanego z systemu USOS.
3. Uprawnienia do korzystania z systemu PeLSAP dla danego wykładowcy, widniejącego w wykazie danych, uzyskanych z USOS, tworzy ASI po otrzymaniu od LABI kopii upoważnienia tego wykładowcy do przetwarzania danych osobowych w systemie PeLSAP.

§ 6

1. Informacje o danych dostępowych oraz opis sposobu pierwszego logowania do systemu PeLSAP dla potencjalnych użytkowników mających rolę *student* zostały zawarte w dokumencie *CIS-Platforma eLearning SAP-Podręcznik studenta* dostępny na na stronie Wydziału Cybernetyki (ścieżka dostępu: ***Usługi i serwisy*** -> ***Platforma eLearningowa SAP***).
2. Informacje o danych dostępowych oraz opis sposobu pierwszego logowania do systemu PeLSAP dla potencjalnego użytkownika mającego rolę *wykładowca* przesyła ASI po

nadaniu mu uprawnień do przetwarzania danych osobowych w systemie PeLSAP. Dane dostępowe są przesyłane na adres email, podany w zaimportowanym wykazie.

3. Wraz z danymi dostępowymi przesyłana jest informacja o umiejscowieniu dokumentów, z którymi powinien zapoznać się potencjalny użytkownik, przed pierwszym logowaniem do systemu PeLSAP oraz inne, wymagane informacje.

§ 7

1. Przy pierwszym logowaniu należy zmienić hasło tymczasowe, klikając w wyświetlonym formularzu na link ***Nie pamiętasz hasła?***. Obowiązują następujące zasady tworzenia hasła:
   1) Musi składać się z co najmniej 8 znaków, zawierać małe i wielkie litery oraz cyfry i znaki specjalne.
   2) Nie może składać się z identycznych znaków lub ciągów znaków z klawiatury.
   3) Nie może być jednakowe z identyfikatorem użytkownika.
   4) Musi być unikalne, tj. takie, które nie było poprzednio stosowane przez użytkownika.
2. Hasło w trakcie wpisywania nie może być wyświetlane na ekranie. Użytkownik jest zobowiązany do utrzymania hasła w tajemnicy, również po utracie jego ważności.
3. Hasło musi być zmieniane nie rzadziej niż co 30 dni. Jeżeli hasło nie zostanie zmienione przez użytkownika po upływie 30 dni, zmiana hasła zostanie wymuszana przez system PeLSAP przy kolejnym logowaniu.
4. W przypadku podejrzenia utraty poufności hasła, użytkownik zobowiązany jest natychmiast poinformować o tym fakcie ASI i niezwłocznie zmienić hasło.
5. Przyjmuje się, że reguła „Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego służącego do przetwarzania danych osobowych nie powinien być przydzielany innej osobie" jest zachowana w systemie USOS.
6. Użytkownika, który utracił uprawnienia do przetwarzania danych osobowych w systemie PeLSAP, jest dezaktywowany po unieważnieniu przez ASI przypisanego mu hasła.
7. Za utworzenie bezpiecznego hasła zgodnie z zasadami określonymi w pkt.1 niniejszego paragrafu odpowiada użytkownik.

§ 8

1. Cofnięcie uprawnień do przetwarzania w systemie PeLSAP jest obligatoryjne w odniesieniu do osób, które nie figurują w wykazie zaimportowanym z systemu USOS.
2. ASI cofa uprawnienia do przetwarzania w systemie PeLSAP użytkownikowi pełniącemu rolę *wykładowca* jeżeli jego upoważnienie do przetwarzania danych osobowych w systemie PeLSAP straciło ważność lub zostało anulowane. W takim przypadku ASI deaktywuje konto użytkownika. Ponowna aktywacja konta może nastąpić po uzyskaniu przez użytkownika ważnego upoważnienia do przetwarzania danych osobowych w PeLSAP (o ile ma on status ***aktywny*** w systemie USOS).

3. PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY PRZEZ UŻYTKOWNIKÓW SYSTEMU PeLSAP

§ 9

1. Użytkownicy przetwarzają dane w systemie PeLSAP na zasadzie cienkiego klienta, używając przeglądarki internetowej, zainstalowanej na lokalnym komputerze. Powinni oni przestrzegać procedur opisanych w niniejszym rozdziale.
2. Przed rozpoczęciem przetwarzania danych osobowych użytkownik powinien sprawdzić, czy nie ma oznak fizycznego naruszenia zabezpieczeń komputera, na którym przetwarza dane osobowe. W przypadku wystąpienia jakichkolwiek nieprawidłowości, należy powiadomić przełożonych, ASI oraz LABI.
3. Przystępując do pracy w systemie informatycznym służącym do przetwarzania danych osobowych, użytkownik zobowiązany jest w sposób dyskretny, aby nie było możliwości obserwacji klawiatury przez osoby postronne, wprowadzić swój identyfikator oraz hasło dostępu. Zabrania się wykonywania jakichkolwiek operacji w systemie informatycznym służącym do przetwarzania danych osobowych z wykorzystaniem identyfikatora i hasła dostępu innego użytkownika.
4. W przypadku krótkotrwałego opuszczenia stanowiska pracy lub pomieszczenia, w szczególności, gdy w pomieszczeniu pracuje więcej niż jedna osoba, użytkownik systemu informatycznego jest zobowiązany uaktywnić wygaszacz ekranu zabezpieczony hasłem lub w inny sposób zabezpieczyć system przed dostępem innych osób.
5. W przypadku czasowego opuszczenia stanowiska pracy, użytkownik musi wylogować się z systemu informatycznego służącego do przetwarzania danych osobowych.
6. Przed wylogowaniem należy sprawdzić, czy nie ma pozostawionych zadań do wydrukowania zarówno w pamięci komputera, jak i drukarki. Jeżeli są, należy je wykonać lub anulować.
7. Przed opuszczeniem stanowiska pracy należy zabezpieczyć wykonane wydruki przed dostępem osób nieuprawnionych, bądź zniszczyć zbędne dokumenty w niszczarce. Należy skontrolować, czy w komputerze nie pozostały zewnętrzne (przenośne) informatyczne nośniki danych (dyskietki, płyty CD lub DVD, pamięci USB itp.).
8. Kończąc pracę w systemie informatycznym służącym do przetwarzania danych osobowych należy prawidłowo wylogować się z systemu informatycznego, wyłączyć komputer i zabezpieczyć stanowisko przed dostępem osób nieuprawnionych.

§ 10

Zabrania się:

1) Kontynuowania logowania się do systemu informatycznego, w sytuacji kiedy wystąpią jego nietypowe działanie, np. wyświetlanie „dziwnych” komunikatów itp. O takim fakcie należy powiadomić ASI.
2) Kontynuowania pracy w przypadku, kiedy oprogramowanie antywirusowe wykryje obecność wirusa. W takim przypadku należy wylogować się z systemu i wznowić pracę po usunięciu zagrożenia.
3) Zapisywania i pozostawiania w miejscach niezabezpieczonych przed ujawnieniem identyfikatora użytkownika i hasła.
4) Ujawniania innym osobom identyfikatora użytkownika i hasła.

5) Opuszczania pomieszczenia bez zabezpieczenia stanowiska pracy w sposób uniemożliwiający osobom postronnym dostępu do przetwarzanych danych osobowych.
6) Pozostawiania wydruków, wykorzystywanych dokumentów papierowych i informatycznych nośników danych bez nadzoru i zabezpieczenia przed dostępem i wglądem osób nieupoważnionych.
7) Wykonywania czynności wykraczających poza zakres nadanego upoważnienia do przetwarzania danych osobowych, w szczególności dokonywania nieuprawnionych prób dostępu do zasobów i dokonywania na nich wszelkich operacji.
8) Nieuprawnionego kopiowania jakichkolwiek danych znajdujących się w systemie informatycznym.

4. PROCEDURA POSTĘPOWANIA Z WYDRUKAMI Z SYSTEMU PeLSAP

§ 11

1. Wydruki z systemu PeLSAP zawierające dane osobowe mogą być sporządzane jedynie w związku z realizacją zadań i podlegają ochronie zgodnie z przepisami dotyczącymi ochrony danych osobowych.
2. Wydruki próbne i wadliwie wykonane należy chronić jak dokumenty właściwe.
3. Zniszczenia wydruków dokonuje się w sposób uniemożliwiający ich odtworzenie, przy użyciu niszczarek o poziomie bezpieczeństwa zgodnym z obowiązującymi przepisami (DIN 32757: 3, DIN 66399: P-4/ T-4/ E-3/ F-1).

5. SPOSÓB ZABEZPIECZENIA SYSTEMU PeLSAP PRZED DZIAŁALNOŚCIĄ OPROGRAMOWANIA, KTÓREGO CELEM JEST UZYSKANIE NIEUPRAWNIONEGO DOSTĘPU DO SYSTEMU PeLSAP

§ 12

1. Wykładowcy przed zamieszczeniem materiałów dydaktycznym w systemie PeLSAP zobowiązani są dokonać kontroli plików na obecność wirusów.
2. Na każdym stanowisku wyposażonym w dostęp do sieci Internet, z którego użytkownik loguje się do systemu PeLSAP, musi być zainstalowanie oprogramowanie antywirusowe. Niedopuszczalne jest stosowanie dostępu do sieci Internet bez aktywnej ochrony antywirusowej oraz zabezpieczenia przed dostępem szkodliwego oprogramowania. Zainstalowany program antywirusowy powinien być tak skonfigurowany, by dokonywane było automatycznie sprawdzenie komputera pod kątem obecności wirusów.
3. W przypadku stwierdzenia obecności wirusów, o incydencie należy niezwłocznie powiadomić ASI lub LABI.

6. SPOSÓB ODNOTOWANIA INFORMACJI O ODBIORCACH, KTÓRYM DANE OSOBOWE ZOSTAŁY UDOSTĘPNIONE, DACIE I ZAKRESIE TEGO UDOSTĘPNIENIA

§ 13

W systemie PeLSAP brak jest odbiorców danych w świetle obowiązujących przepisów[1]. Osoby korzystające z systemu albo przetwarzają własne dane, albo przetwarzają je na mocy upoważnienia. Stąd w systemie PeLSAP nie ma podstaw do odnotowywania informacji o odbiorcach, którym udostępniono dane.

7. PROCEDURA POSTĘPOWANIA Z INFORMATYCZNYI NOŚNIKAMI DANYCH

§ 14

1. Procedury postępowania z informatycznymi nośnikami danych, w tym ewidencjonowanie, oznaczanie, przechowywanie, archiwizacja i brakowanie, powinny być zgodne z przepisami dotyczącymi obiegu informacji, dokumentów i archiwizacji w WAT.
2. Zabrania się:
   1) Używania prywatnych informatycznych nośników danych.
   2) Wykorzystywania służbowych informatycznych nośników danych do celów innych niż te, do których są przeznaczone.
3. Nakazuje się:
   1) Przechowywanie informatycznych nośników danych w sposób uniemożliwiający dostęp do nich osób nieuprawnionych.
   2) Usuwanie z informatycznych nośników zbędnych danych osobowych, które nie są wykorzystywane do bieżącej działalności służbowej i nie podlegają archiwizacji.

8. POSTANOWIENIA KOŃCOWE

§ 15

1. Przestrzeganie postanowień niniejszych wytycznych przez użytkowników systemu PeLSAP stanowi podstawę bezpiecznego korzystania z tego systemu.
2. Należy mieć na uwadze, że naruszenie procedur ochrony danych przez użytkowników upoważnionych do przetwarzania danych osobowych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych w rozumieniu art. 52 kodeksu pracy[2], włącznie z rozwiązaniem stosunku pracy (w tym bez wypowiedzenia).

[1] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 2016 poz. 922, Art.7, ust. 6a, 6b).

[2] Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (Dz.U. 1974 Nr 24 poz. 141).