Załącznik nr 2 do zarządzenia Rektora WSM 2/05/2018 r. z dnia 22 maja 2018 r

INSTRUKCJA zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Wyższej Szkole Menedżerskiej w Warszawie

Spis treści:

Rozdział 1

Postanowienia ogólne

§ 1

Niniejsza „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Wyższej Szkole Menedżerskiej w Warszawie" zwana dalej **Instrukcją,** ma zastosowanie do ochrony zbiorów danych osobowych przetwarzanych w Wyższej Szkole Menedżerskiej w Warszawie, w celu ich bezpiecznego wykorzystywania oraz zabezpieczenia danych osobowych przed zagrożeniami, w tym zwłaszcza przed ich udostępnieniem osobom nieupoważnionym, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem. .

§ 2

Instrukcja została opracowana na podstawie art. 66 ust.2 ustawy z dnia 27 lipca 2005 roku Prawo o szkolnictwie wyższym. (tj. Dz. U. z 2012 r., poz. 572, z późń. zm.), art. 3 ust 1 Rozporządzenia 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

§ 3

Określenia i skróty użyte w Instrukcji oznaczają:

1. **Administrator Danych Osobowych –** Rektor Wyższej Szkoły Menedżerskiej w Warszawie, zwany

dalej **ADO .**

2. **Inspektor Ochrony Danych Osobowych** - osoba wyznaczona przez **Administratora Danych Osobowych**, odpowiedzialna za bezpieczeństwo danych osobowych przetwarzanych w systemach informatycznych, zwana dalej **IODO.**
3. **Administrator Systemów Informatycznych** - osoba wyznaczona przez **ADO**, odpowiedzialna za sprawność i konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych w przetwarzanych zbiorach danych osobowych, zwany dalej **ASI.**
4. **Bezpieczeństwo systemu informatycznego** - wdrożenie przez Administratora lub osobę przez niego uprawnioną środków organizacyjnych i technicznych w celu zabezpieczenia oraz ochrony danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz nieuprawnioną zmianą, utratą, uszkodzeniem lub zniszczeniem.
5. **Przetwarzanie danych osobowych** - wykonywanie jakichkolwiek operacji na danych osobowych, takich jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i ich usuwanie.
6. **Osoba upoważniona lub użytkownik systemu** - osoba posiadająca upoważnienie wydane przez **ADO** lub uprawnioną przez niego osobę i dopuszczona jako użytkownik do przetwarzania danych osobowych w systemie informatycznym danej komórki organizacyjnej w zakresie wskazanym w upoważnieniu, zwana dalej **użytkownikiem.**
7. **Przełożony użytkownika** - kierownik komórki organizacyjnej **WSM** , zwany dalej **przełożonym**.
8. **Osoba uprawniona – osoba posiadająca upoważnienie wydane przez Administratora do wykonywania w jego imieniu określonych czynności.**
9. **Użytkownik uprzywilejowany** – osoba posiadająca najwyższy stopień uprawnień do zarządzania systemem informatycznym.

§ 4

1. **ADO** może upoważnić inną osobę, zatrudnioną w **WSM** do wykonywania określonych czynności, leżących w zakresie realizacji zadań Administratora.
2. Kontrola prawidłowości wykonywania czynności, o których mowa w ust. 1, należy do **ADO** lub osoby uprawnionej.
3. Osoba, o której mowa w ust. 1, informuje **IODO** lub osoby uprawnione o podjętych przez siebie czynnościach.

Rozdział 2

Procedury związane z zarządzaniem systemem informatycznym służącym do przetwarzania danych osobowych w WSM

§ 1

Nadawanie uprawnień i wyrejestrowywanie użytkowników.

1 Nadawanie i rejestrowanie uprawnień

1) Dostęp do systemu informatycznego służącego do przetwarzania danych osobowych może uzyskać wyłącznie upoważniony do przetwarzania danych osobowych, zarejestrowany jako użytkownik w tym systemie przez administratora systemu na wniosek kierownika działu kadr lub kierownika działu.

Administrator systemu jest obowiązany upoważnić co najmniej jednego pracownika działu informatyki do rejestracji użytkowników w systemie informatycznym w czasie swojej nieobecności dłuższej niż 14 dni.

Rejestracja użytkownika, o której mowa w ppkt 1), polega na nadaniu identyfikatora i przydzieleniu hasła oraz wprowadzeniu tych danych do ewidencji użytkowników systemu.

Administrator systemu albo upoważniony pracownik, o którym mowa w ppkt. 2), przekazuje do działu kadr informację o identyfikatorze, który został nadany użytkownikowi.

2 Wyrejestrowywanie uprawnień

1) Wyrejestrowania użytkownika z systemu informatycznego dokonuje administrator systemu na wniosek kierownika działu kadr.
2) Wyrejestrowanie, o którym mowa w ppkt. 1), może mieć charakter czasowy lub trwały.
3) Wyrejestrowanie następuje poprzez:
   a) zablokowanie konta użytkownika do czasu ustania przyczyny uzasadniającej blokadę (wyrejestrowanie czasowe),
   b) usunięcie danych użytkownika z bazy użytkowników systemu (wyrejestrowanie trwałe).
4) Wyrejestrowanie czasowe musi nastąpić w przypadku:
   a) nieobecności użytkownika w pracy trwającej dłużej niż 21 dni kalendarzowych,
   b) zawieszenia w pełnieniu obowiązków służbowych.

Wyrejestrowanie czasowe może nastąpić w przypadku:

a) wypowiedzenia umowy o pracy,
b) wszczęcie postępowania dyscyplinarnego względem osoby upoważnionej do przetwarzania danych osobowych.

Wyrejestrowanie trwałe następuje w przypadku rozwiązania lub wygaśnięcia stosunku pracy lub innego stosunku prawnego, w ramach którego zatrudniony był użytkownik.

Ustanie stosunku pracy jest równoważne z cofnięciem uprawnień do przetwarzania danych osobowych.

Osoby dopuszczone do przetwarzania danych osobowych zobowiązane są do zachowania tajemnicy w zakresie tych danych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje również po ustaniu zatrudnienia.

2. W celu zarządzania metodami oraz środkami uwierzytelniania mają zastosowanie *(załącznik nr **1**):*
   a) „Procedura uwierzytelniania użytkownika w systemie informatycznym"
   b) „Procedura rejestrowania /wyrejestrowania użytkownika z systemu informatycznego".

3. W celu rozpoczęcia, zawieszenia i zakończenia pracy w systemie informatycznym mają zastosowanie następujące procedury (załącznik nr 2):

   1. Procedura rozpoczęcia pracy w systemie informatycznym
   2. Procedura zawieszenia/odwieszenia pracy w systemie informatycznym
   3. Procedura zakończenia pracy w systemie informatycznym

4. W przypadku podejrzenia lub stwierdzenia naruszenia ochrony danych osobowych ma zastosowanie

procedura postępowania w sytuacjach naruszenia ochrony danych osobowych.

1. **Procedura postępowania w sytuacjach naruszenia ochrony danych osobowych**
    1. Na fakt naruszenia zabezpieczeń systemu informatycznego mogą wskazywać:
        1. Stan stacji roboczej (np. brak zasilania, problemy z uruchomieniem).
        2. Wszelkiego rodzaju różnice w funkcjonowaniu systemu (np. komunikaty informujące o błędach, brak dostępu do funkcji systemu, nieprawidłowości w wykonywanych operacjach).
        3. Różnice w zawartości zbioru danych osobowych (np. brak lub nadmiar danych).
        4. Jakości komunikacji w sieci telekomunikacyjnej (gwałtowne opóźnienia lub przyśpieszenia wykonywanych czynności).
        5. Stwierdzenie obecności w systemie nowego oprogramowania bądź oprogramowania niewiadomego pochodzenia
        6. Pojawienie się w systemie nowych procesów.
        7. Inne sytuacje nadzwyczajne.
    2. W przypadku podejrzenia naruszenia zabezpieczenia systemu informatycznego użytkownik niezwłocznie powiadamia bezpośredniego przełożonego oraz **IODO**.
    3. **IODO** niezwłocznie wszczyna postępowanie wyjaśniające.
    4. Wyniki postępowania wyjaśniającego są zapisywane w formie notatki służbowej, jeżeli **IODO** stwierdzi faktyczne naruszenie zabezpieczenia systemu informatycznego.
    5. Treść notatki **IODO** przekazuje do wiadomości Administratorowi.

5. W celu zabezpieczenia danych i programów służących do przetwarzania danych osobowych ma zastosowanie poniższa

Procedura tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania:

1. Kopie zapasowe są tworzone codziennie przez Dział Informatyki WSM po zakończeniu dnia pracy. Kopie pełnie wykonywane są nie rzadziej niż raz na tydzień, kopie zapasowe dzienne mogą być kopiami przyrostowymi.
2. Nośniki z kopiami zapasowymi są przechowywane w pomieszczeniach Działu Informatyki pod nadzorem **IODO**.
3. Kopie zapasowe są tworzone w cyklu miesięcznym nie rzadszym niż tygodniowy. Po tym okresie nośniki są kasowane i ponownie wykorzystywane do tworzenia kopii zapasowych.
4. Kopie zapasowe są okresowo sprawdzane pod kątem ich dalszej przydatności.
5. Na koniec każdego miesiąca Dział Informatyki tworzy kopię miesięczną na nośnikach trwałych
6. Kopie miesięczne są przechowywane przez okres co najmniej 5 lat.
7. Po okresie przechowywania kopie miesięczne podlegają komisyjnej likwidacji poprzez ich fizyczne zniszczenie. W komisji likwidacyjnej biorą udział **IODO** i/lub **ASI**.

Rozdział 3

Inne uregulowania związane z przetwarzaniem danych osobowych w Wyższej Szkole Menedżerskiej

§ 1

1. W celu zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego Wyższa Szkoła Menedżerska wykorzystuje:
    1. Oprogramowanie antywirusowe na serwerze mailowym.
    2. Oprogramowanie na stacjach roboczych.
    3. Oprogramowanie ograniczające niepożądany ruch w sieci.
    4. Fizyczne rozdzielenie sieci zawierającej dane osobowe od sieci ogólnodostępnej.
    5. Logiczny podział sieci uwzględniający komórki organizacyjne.

2. Aktualizacja wyżej wymienionego oprogramowania jest automatyczna. Bazy wirusów są aktualizowane niezwłocznie po opublikowaniu nowej bazy wirusów.

§ 2

1. Systemy informatyczne oraz nośniki informacji służące do przetwarzania danych eksploatowane w WSM podlegają okresowym przeglądom i konserwacjom.
2. Do dokonywania przeglądów i konserwacji uprawniony jest Dział Informatyki pod nadzorem **IODO**.
3. W przypadku stwierdzenia uszkodzenia urządzenia, dyski i inne informatyczne nośniki danych zawierające dane osobowe przed ich przekazaniem w celu naprawy innemu podmiotowi pozbawiane są zawartości.
4. W przypadku likwidacji urządzenia, dyski i inne informatyczne nośniki danych zawierające dane osobowe są uszkadzane w sposób uniemożliwiający odczytanie danych.
5. Naprawa wymienionych urządzeń zawierających dane osobowe, jeżeli nie można danych usunąć, wykonywana jest pod nadzorem **IODO** lub **ASI**.

§ 3

Wszelkie wydruki zawierające dane osobowe przechowywane są w miejscu uniemożliwiającym ich odczyt przez osoby nieuprawnione, w zamkniętych szafach lub pomieszczeniach i po upływie czasu ich przydatności są niszczone przy użyciu niszczarek lub przez wyspecjalizowane firmy posiadające odpowiednie certyfikaty.

§ 4

1. Wykorzystywanie sieci komputerowej w celach innych niż wyznaczone przez **Władze WSM** jest zabronione.

2. Zabroniona jest także samowolna instalacja oprogramowania na stacjach roboczych przez użytkowników

Rozdział 4

Postanowienia końcowe

§ 1

1. Niniejsza Instrukcja przeznaczona jest dla użytkowników i ich przełożonych, którzy nadzorują przetwarzanie danych osobowych.
2. Wykonanie postanowień Instrukcji ma na celu wprowadzenie jednolitego systemu zarządzania systemem informatycznym w WSM.
3. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się i stosować do zasad i procedur określonych niniejszym dokumentem.
4. Naruszenie zasad i procedur określonych w niniejszym dokumencie może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52 Kodeksu pracy.
5. Naruszenie zasad i procedur określonych w niniejszym dokumencie może być potraktowane jako nienależyte wykonanie umowy w rozumieniu Kodeksu cywilnego.
6. Nośniki informacji w rozumieniu § 5 pkt 5 lit. a rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (*Dz.U. Nr 100, poz. 1024*) są przechowywane w pomieszczeniach Działu Informatyki.

Załącznik nr 1 do Instrukcji zarządzania systemem informatycznym

Procedura uwierzytelniania użytkownika w systemie informatycznym

1. Niepowtarzalny identyfikator oraz pierwsze hasło jest przydzielone użytkownikowi przez **ASI** po nadaniu uprawnień do przetwarzania danych osobowych.
2. Pierwsze hasło jest przekazane przez **ASI** użytkownikowi systemu w formie pisemnej.
3. Użytkownik po otrzymaniu pierwszego hasła jest zobowiązany do niezwłocznej jego zmiany .
4. Bezpośredni dostęp do danych użytkownik uzyskuje po podaniu identyfikatora i właściwego hasła.
5. Hasła w systemie informatycznym musza być przechowywane w postaci zaszyfrowanej .
6. Hasła użytkowników uprzywilejowanych pozostają do wyłącznej wiadomości wybranych pracowników Działu Informatyki WSM. Ich pisemna wersja przechowywana jest zaklejonej kopercie w sejfie Kanclerza WSM.
7. Osobą odpowiedzialną za rejestrowanie oraz wyrejestrowywanie użytkowników jest ASI bądź osoba spośród pracowników Działu Informatyki WSM przez ASI do tego upoważniona.
8. Hasła administratorów systemów informatycznych przechowywane są w szafie pancernej Kasy WSM i ich awaryjne użycie odnotowywane jest każdorazowo przez ABI w specjalnym rejestrze .

Procedura rejestrowania/wyrejestrowania użytkownika z systemu informatycznego

1. Użytkownicy systemu informatycznego są niezwłocznie rejestrowani lub wyrejestrowywani przez **ASI**, gdy uzyskują lub tracą prawo dostępu do systemu, zgodnie z procedurą nadawania/cofania uprawnień do przetwarzania danych osobowych.
2. Identyfikator po wyrejestrowaniu użytkownika zostaje zablokowany przez **ASI**.
3. Ustanie stosunku pracy powoduje wyrejestrowanie użytkownika przez ASI. Odchodzący pracownik wypełnia kartę obiegową w wyznaczonych komórkach organizacyjnych.

   Podstawą wypełnienia karty obiegowej przez ASI jest trwałe usunięcie użytkownika z systemu.
4. Identyfikator po wyrejestrowaniu użytkownika nie jest przydzielany innej osobie .

Załącznik nr 2 do Instrukcji zarządzania systemem informatycznym

Procedura rozpoczęcia pracy w systemie informatycznym

2. W celu rozpoczęcia pracy w systemie informatycznym użytkownik obowiązany jest do podania hasła dostępu do systemu.
3. Podczas pierwszego uwierzytelniania w systemie użytkownik ma obowiązek zmiany hasła.
4. Hasło składa się co najmniej z 6 znaków. Jego długość jest uzależniona od poziomu bezpieczeństwa i zasad stosowanych w odpowiednich systemach informatycznych.
5. Użytkownik ma obowiązek zmieniać hasło nie rzadziej niż co 30 dni kalendarzowych.
6. Zabrania się wpisywania hasła lub jego zmiany w obecności innych osób.
7. Hasło nie może być zapisywane lub przechowywane w miejscu dostępnym dla osób nieuprawnionych.
8. W przypadku zagubienia hasła użytkownik musi skontaktować się z **ASI** w celu uzyskania nowego hasła.
9. Użytkownikowi nie wolno udostępniać swoich haseł innym osobom.

Procedura zawieszenia/odwieszenia pracy w systemie informatycznym

2. W celu zawieszenia pracy w systemie informatycznym służącym do przetwarzania danych osobowych użytkownik zobowiązany jest do wyrejestrowania się z systemu.
3. W przypadku konieczności odejścia od stanowiska pracy, po wyrejestrowaniu się z systemu użytkownik jest zobowiązany zablokować pulpit.
4. W celu ponownego uwierzytelnienia w systemie użytkownik odblokowuje pulpit i rozpoczyna pracę w systemie informatycznym zgodnie z procedurą rozpoczęcia pracy w systemie informatycznym.
5. Zabrania się pozostawiania stanowiska komputerowego z uruchomionym systemem bez kontroli pracującego na nim użytkownika.

Procedura zakończenia pracy w systemie informatycznym

2. W celu zakończenia pracy w systemie informatycznym użytkownik wyrejestrowuje się z programu służącego do obsługi danych osobowych.
3. Użytkownik zamyka sesję użytkownika w systemie operacyjnym (wylogowuje się) i o ile jest to konieczne, wyłącza komputer.