Załącznik do zarządzenia Rektora nr 3/2020 z dn. 2.01.2020 r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

I. POSTANOWIENIA OGÓLNE

1. Niniejsza Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwana dalej Instrukcją, przyjęta została w celu wykazania, że dane osobowe w systemach informatycznych Państwowej Wyższej Szkoły Zawodowej w Głogowie przetwarzane są w sposób zgodny z przepisami prawa mającymi zastosowanie do takiej czynności, zgodnie z zasadą art. 5 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (dalej RODO).
2. Instrukcja określa zasady i tryb wykonywania czynności w Systemie Informatycznym Państwowej Wyższej Szkoły Zawodowej w Głogowie związanych z ochroną danych osobowych.
3. Jeśli w niniejszej Instrukcji Zarządzania Systemem Informatycznym mowa o:
   1) **Administratorze Danych Osobowych (ADO)** – rozumie się przez to Państwową Wyższą Szkolę Zawodową w Głogowie, reprezentowaną przez Rektora (podmiot decydujący o celach i środkach przetwarzania danych osobowych);
   2) **Administratorze Systemów Informatycznych (ASI)** – rozumie się przez to osobę fizyczną nadzorującą bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych, pracownika Sekcji IT;
   3) **Haśle** - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
   4) **Identyfikatorze użytkownika** - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
   5) **Instrukcji** – rozumie się przez niniejszą instrukcję zarządzania systemem informatycznym;
   6) **Odbiorcy danych** - rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią, z wyłączeniem organów administracji publicznej, które mogą otrzymywać dane osobowe w ramach konkretnego prowadzonego przez nie postępowania;
   7) **Przetwarzaniu danych** - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie, a zwłaszcza te, które wykonuje się w systemach informatycznych;
   8) **Systemie informatycznym** - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
   9) **Usuwaniu danych** - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;

10) **Uwierzytelnianiu** - rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;

11) **Użytkowniku** – rozumie się przez to osobę, która posiada upoważnienie do przetwarzania danych osobowych i posiada uprawnienia do uwierzytelnionego dostępu do systemu informatycznego;

12) **Zbiorze danych** - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

4. Za przestrzeganie w podmiocie zapisów Instrukcji odpowiedzialny jest Administrator Danych Osobowych lub zgodnie z zapisem „Polityki Bezpieczeństwa Informacji" wyznaczony Inspektor Ochrony Danych Osobowych (IOD) wraz z Administratorem Systemów Informatycznych (ASI).
5. W związku z tym, że w Państwowej Wyższej Szkole Zawodowej w Głogowie przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest z siecią publiczną, oraz uwzględniając kategorie przetwarzanych danych i zagrożenia wprowadza się poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym na poziomie wysokim.
6. Niezależnie od niniejszej Instrukcji Administrator Danych wdrożył Politykę Bezpieczeństwa Informacji.

II. PROCEDURY NADAWANIA, MODYFIKOWANIA I USUWANIA UPRAWNIEŃ ORAZ UWIERZYTELNIENIA DOSTĘPU DO SYSTEMU INFORMATYCZNEGO

1. Na podstawie wprowadzonej Polityki Bezpieczeństwa Informacji funkcję Administratora Systemów Informatycznych w Państwowej Wyższej Szkole Zawodowej w Głogowie przekazuje się pracownikowi Sekcji IT.
2. Za nadawanie, modyfikowanie i usuwanie uprawnień Użytkownika do przetwarzania danych osobowych w systemach informatycznych, a także za rejestrowanie takich uprawnień w tymże systemie, odpowiedzialny jest ASI.
3. Uprawnienia dla nowego Użytkownika mogą być nadane wyłącznie osobie upoważnionej do przetwarzana danych osobowych zgodnie z Polityką Bezpieczeństwa Informacji.
4. Każdemu Użytkownikowi ASI przyznaje unikalny identyfikator oraz hasło.
5. Identyfikator Użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.
6. Użytkownik uwierzytelnia dostęp do systemu informatycznego poprzez wpisanie swojego unikalnego identyfikatora oraz hasła.
7. Użytkownik jest obowiązany dokonywać zmiany hasła nie rzadziej niż co 30 dni.
8. Hasło składa się ono co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.
9. Użytkownik ma obowiązek zachować hasło w tajemnicy w czasie jego obowiązywania oraz po ustaniu jego ważności.
10. Użytkownik systemu informatycznego zobowiązany jest niezwłocznie poinformować IOD o stwierdzeniu naruszenia zabezpieczeń danych osobowych w systemie informatycznym.

11. ASI może zablokować Użytkownikowi dostęp do systemu informatycznego w każdym czasie, jeśli uzna to za konieczne dla zapewnienia bezpieczeństwa danych osobowych.
12. Po zakończeniu pracy w systemie informatycznym, Użytkownik zobowiązany jest wylogować się z systemu.
13. Identyfikatory i hasła Użytkowników przechowuje się w systemie informatycznym w postaci zaszyfrowanej.
14. Użytkownik, który utracił hasło, zobowiązany jest zgłosić to niezwłocznie ASI, który ustali nowe hasło.
15. Użytkownik zobowiązany jest zapamiętać hasło, o którym mowa wyżej (nie zapisywać go).

III. PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY

1. W celu uruchomienia podsystemu informatycznego Użytkownik powinien:
   a) uruchomić komputer;
   b) wybrać odpowiednią opcję umożliwiającą logowanie do systemu;
   c) zalogować się do systemu poprzez wskazanie loginu oraz poufnego i aktualnego hasła.
2. Za każdym razem, kiedy Użytkownik opuszcza stanowisko pracy, zobowiązany jest do wylogowania się z systemu.
3. Użytkownik jest zobowiązany do zapisywania i zamykania wszystkich dokumentów zawierających dane osobowe przed odejściem od komputera.
4. Wylogowanie następuje poprzez wybranie w systemie opcji „wyloguj" lub zablokowanie ekranu w sposób, który uniemożliwia odblokowanie bez znajomości hasła, dzięki zastosowaniu funkcji wygaszacza ekranu.

IV. PROCEDURY TWORZENIA KOPII ZAPASOWYCH

1. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych. Kopie wszystkich danych osobowych muszą być tworzone nie rzadziej niż raz w tygodniu.
2. Kopie zapasowe:
   a) przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem w pomieszczeniu zamkniętym dział IT/serwerownia zaopatrzonym w drzwi zamykane na klucz, szafy niemetalowe zamykane na klucz, monitoring wewnętrzny i zewnętrzny, alarm w budynku od godziny 22.00 + portiernia 24 h,
   b) usuwa się niezwłocznie po ustaniu ich użyteczności.
3. Za tworzenie kopii zapasowych odpowiedzialny jest ASI lub wyznaczona przez niego osoba posiadająca upoważnienie do przetwarzania danych osobowych.
4. Kopie zapasowe systemów informatycznych zawierające dane osobowe przechowywane są na własnym serwerze podmiotu.
5. Kopie zapasowe systemów informatycznych, po ustaniu ich przydatności, są usuwane w sposób wykluczający ich odtworzenie.

V. ZABEZPIECZENIE SYSTEMÓW INFORMATYCZNYCH

1. Administrator stosuje w systemie informatycznym jak najbezpieczniejsze dostępne systemy operacyjne.
2. Systemy informatyczne są zabezpieczone przed atakami z zewnątrz za pomocą oprogramowania typu firewall.
3. Systemy informatyczne są zabezpieczone przed szkodliwym oprogramowaniem za pomocą aktualnego oprogramowania antywirusowego.
4. Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania danych osobowych w tym stosuje hasła dostępu do komputera przenośnego oraz do plików, w których przetwarzane są dane osobowe.
5. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
   a) likwidacji - pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
   b) przekazania podmiotowi nieuprawnionemu do przetwarzania danych - pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
   c) naprawy - pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.
6. W przypadku wykrycia jakiegokolwiek zagrożenia Użytkownik niezwłocznie zawiadamia ASI.
7. W przypadku stwierdzenia braku zasilania należy zapisać dane osobowe oraz wylogować się.
8. Ekrany komputerów, na których przetwarzane są dane osobowe, należy chronić wygaszaczami zabezpieczonymi hasłem.
9. Monitory komputerów należy ustawić tak, aby ograniczyć dostęp do danych osobom nieupoważnionym do przetwarzania danych, w szczególności nie mogą one być zwrócone w stronę drzwi.
10. Użytkownik systemu zobowiązany jest do prawidłowej eksploatacji powierzonego sprzętu i oprogramowania oraz ochrony zasobów informatycznych przed dostępem osób nieupoważnionych, w tym zabezpieczenia komputerowych stanowisk dostępu do danych osobowych przed wglądem osób nieupoważnionych, zabezpieczenia danych przed ich zmianą.

VI. INFORMACJE ODNOTOWYWANE PRZEZ SYSTEM INFORMATYCZNY

1. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym – z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie - system ten zapewnia odnotowanie:
   a) daty pierwszego wprowadzenia danych do systemu;
   b) identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba;

c) źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą;

d) informacji o odbiorcach danych, którym dane osobowe zostały udostępnione, oraz dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych;

e) wniesienia przez osobę, której dane są przetwarzane, sprzeciwu w przypadkach przewidzianych w stosownych przepisach.

2. Odnotowanie informacji, o których mowa w ust. 1 pkt a) i b), następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.
3. Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w ust. 1.
4. W przypadku przetwarzania danych osobowych, w co najmniej dwóch systemach informatycznych, wymagania, o których mowa w ust. 1 pkt d), mogą być realizowane w jednym z nich lub w odrębnym systemie informatycznym przeznaczonym do tego celu.

VII. PROCEDURY WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMÓW INFORMATYCZNYCH

1. Przynajmniej raz w roku wykonuje się przegląd systemu informatycznego.
2. Konserwacji poszczególnych elementów systemu informatycznego dokonuje się tak często, jak to wynika z ich specyfiki – nie rzadziej niż raz w roku.
3. W przypadku awarii systemu informatycznego lub nośników informacji naprawia się je lub odzyskuje dane z zachowaniem tajemnicy danych osobowych zgodnie z Polityką Bezpieczeństwa Informacji.
4. Gdy niemożliwa jest naprawa systemu informatycznego, jego elementu lub nośnika danych, w celu przywrócenia sprawności działania systemu należy zastąpić go nowym oraz posłużyć się kopią zapasową.
5. W przypadku przekazania innym podmiotom elementów systemu informatycznego lub nośnika danych w celu naprawy, wszelkie dane osobowe muszą zostać z nich usunięte albo należy zabezpieczyć umieszczone na nim dane osobowe przed dostępem podmiotów trzecich.

VIII. POCZTA ELEKTRONICZNA

1. Pracownicy mogą korzystać z poczty elektronicznej w celach służbowych oraz w celach prywatnych w zakresie ograniczonym swoimi obowiązkami.
2. Dla pracowników dydaktycznych i administracyjnych na czas zatrudnienia w Państwowej Wyższej Szkole Zawodowej w Głogowie tworzone są mailowe skrzynki pocztowe.
3. Informacje o nowozatrudnionych pracownikach przekazuje Administratorowi Sieci pracownik Kadr, po uzyskaniu przez nich stosownych upoważnień.
4. ASI przekazuje pracownikowi szczegóły dotyczące pierwszego logowania oraz hasło do konta pocztowego.
5. Zaleca się stosowanie haseł na poziomie WYSOKIM, składających się z minimum 8 znaków długości, czterech rodzajów znaków (mała litera, duża litera, cyfra, znak specjalny).

6. Adres skrzynki – jest jednoznacznym oznaczeniem Skrzynki Pocztowej i ma postać: imie.nazwisko@pwsz.glogow.pl. Nazwa użytkownika jest unikalna i składa się z pierwszej litery imienia oraz pełnego nazwiska oddzielone kropką, zapisane alfabetem bez polskich znaków diakrytycznych.
7. Informacje o ustaniu zatrudnienia przekazuje Administratorowi Sieci pracownik Kadr.
8. Ze względu na specyfikę działalności Uczelni ustala się następujące terminy przekazywania informacji:
   - nauczyciele akademiccy: - do 31 października (zatrudnienie)
     - do 30 września (ustanie zatrudnienia)
   - pracownicy administracji i obsługi - niezwłocznie po zatrudnieniu lub ustaniu zatrudnienia.
9. Użytkownik poczty zobowiązany jest do okresowej archiwizacji wiadomości (skrzynki pocztowe posiadają ograniczoną wielkość).
10. Użytkownikom poczty zabrania się:
    1) otwierania wiadomości e-mail pochodzących od nieznanego nadawcy bądź z podejrzanym tytułem (tzw. phishing e-mail). W szczególności zabronione jest otwieranie linków bądź pobieranie plików zapisanych w komunikacji zewnętrznej od nieznanego nadawcy.
    2) przesyłania i udostępniania danych naruszających prawo, powszechnie uznanych za obsceniczne lub obraźliwe oraz oszczerstw i treści obrażającej uczucia innych;
    3) rozpowszechniania materiałów o treści pornograficznej, propagujących przemoc, nawołujących do nietolerancji i nienawiści itp., lub naruszających obowiązujące prawo;
    4) uprawiania hazardu;
    5) rozpowszechniania niechcianych wiadomości e-mail (spamu);
    6) prowadzenia działalności komercyjnej nie związanej z działalnością Uczelni;
    7) przesyłania i udostępniania treści niezgodnych z prawem lub będących przedmiotem ochrony własności intelektualnej lub mogących naruszyć czyjekolwiek prawa osobiste;
11. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW”, zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości”.

IX. POSTANOWIENIA KOŃCOWE

1. Przypadki nieuzasadnionego zaniechania obowiązków lub naruszenia innych zasad wynikających z niniejszej Instrukcji mogą stanowić podstawę do pociągnięcia danej osoby do odpowiedzialności, adekwatnie do łączącego ją z podmiotem stosunku prawnego.
2. W sprawach nieuregulowanych niniejszą Instrukcją oraz Polityką Bezpieczeństwa Informacji mają zastosowanie stosowne przepisy.