załącznik nr 1 do Zarządzenia 99/2022
z dnia 3 listopada 2022 r.

Dokumentacja ochrony danych osobowych

tekst jednolity

Instrukcja Zarządzania Systemem Informatycznym

w

Akademii Nauk Stosowanych Angelusa Silesiusa

Spis treści

PODSTAWY PRAWNE

Instrukcja zarządzania systemem informatycznym, zwana dalej Instrukcją, została opracowana w szczególności z uwzględnieniem:

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 (ogólne rozporządzenie o ochronie danych) – zwane dalej RODO.
2) Wyników analizy ryzyka dla zasobów przetwarzających dane osobowe.
3) Wyników oceny skutków przetwarzania (DPIA).
4) Planu postepowania z ryzykiem.

CEL I ZAKRES REGULACJI

1. Celem Instrukcji jest określenie jednolitych zasad zabezpieczeń technicznych i organizacyjnych danych osobowych w ANS AS (zgodnie z wymaganiami art. 32 RODO).
2. Odbiorcami dokumentu są pracownicy odpowiedzialni za nadzór, utrzymanie oraz rozwój środowiska teleinformatycznego funkcjonującego u Administratora, a także pracownicy mający upoważnienie do przetwarzania danych osobowych we właściwym zakresie.
3. Instrukcja dotyczy wszystkich użytkowanych komponentów informatycznych Administratora wykorzystywanych do przetwarzania danych osobowych:
    1) sprzęt (sprzęt transmisji danych WAN/LAN, infrastruktura serwerowni, sprzęt biurowy, sprzęt ogólnodostępny),
    2) systemy operacyjne i aplikacje,
    3) strony internetowe przetwarzające dane osobowe,
    4) formaty plików w postaci elektronicznej (dane nieustrukturyzowane),
    5) osoby przetwarzające dane osobowe,
    6) główne lokalizacje i obszary krytyczne,
    7) krytyczne umowy,
    8) dokumenty w formie papierowej.

PROCEDURA WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI

1. Konserwacja sprzętu komputerowego, systemów informatycznych oraz nośników informacji Administratora ma na celu zapewnienie nieprzerwanej i bezpiecznej pracy tych systemów, zapobieganiu utraty danych, uszkodzeniu danych lub naruszenia bezpieczeństwa danych.
2. Sprzęt podlega konserwacji według ustalonego planu, wynikającego z zaleceń producentów.
3. Wszelkie naprawy oraz konserwacje urządzeń komputerowych oraz zmiany w systemie informatycznym Administratora przeprowadzane są – o ile to możliwe – przez upoważnionych pracowników Administratora.

4. Naprawy, konserwacje i zmiany w systemie informatycznym Administratora przeprowadzane przez serwisanta zewnętrznego prowadzone są pod nadzorem służb informatycznych w siedzibie Administratora (jeśli to możliwe) lub poza siedzibą Administratora, po uprzednim usunięciu elementów zawierających dane osobowe, o ile nie wiąże się to z nadmiernymi utrudnieniami.
5. Wszelkie prace, o których mowa powyżej, wykonywane przez podmiot zewnętrzny, powinny odbywać się na zasadach określonych w szczegółowej umowie pomiędzy Administratorem a tymże podmiotem, z uwzględnieniem klauzuli powierzenia przetwarzania danych oraz klauzuli dotyczącej zachowania w poufności przez wykonawcę wszelkich informacji, do których ma dostęp w czasie wykonywania usługi.
6. Służby informatyczne lub osoba upoważniona zobligowana jest do skontrolowania urządzenia przed jego ponownym uruchomieniem, po przeprowadzeniu jego konserwacji lub naprawy przez podmiot zewnętrzny, w celu zapewnienia, że sprzęt nie został zmanipulowany i nie realizuje szkodliwych funkcji
7. W przypadku odsprzedaży sprzętu komputerowego lub przekazania go podmiotowi nieuprawnionemu do przetwarzania danych osobowych Administratora uprzednio nośnik takiego urządzenia należy zdemontować lub poddać procesowi kilkukrotnego nadpisywania jego zawartości
8. Jeśli nośnik danych (dysk, płyta lub inne) zostanie uszkodzony i nie można go odczytać ani usunąć z niego danych, należy go zniszczyć mechanicznie np. przy użyciu niszczarki spełniającej wymagania normy DIN 66399 na poziomie bezpieczeństwa nie niższym niż 3.

MONITOROWANIE RYZYKA WYSTĄPIENIA AWARII SYSTEMÓW INFORMATYCZNYCH

1. Systemy informatyczne monitorowane są pod kątem ryzyka wystąpienia awarii systemów i zawodności procesów, w sposób umożliwiający identyfikację i usuwanie błędów:
    1) za monitorowanie pracy systemów informatycznych odpowiadają administratorzy tych systemów w zakresie parametrów technicznych określonych przez producenta systemu,
    2) monitorowaniu podlegają także parametry wydajności i pojemności.
2. Za nadzór nad monitoringiem systemów informatycznych, o którym mowa w ust.1, odpowiedzialny jest IODO i służby informatyczne ANS AS.
3. Zarządzanie pojemnością i wydajnością jest procesem zarządzania komponentami infrastruktury informatycznej, służącym dostarczaniu zasobów i usług na ustalonym poziomie, uwzględniającym parametry pojemności i wydajności systemu informatycznego.

MECHANIZMY ZAPEWNIAJĄCE CIĄGŁOŚĆ DZIAŁANIA ZASOBÓW

1. Służby informatyczne odpowiadają za rozwiązania techniczne i proceduralne zapewniające ciągłość działania zasobów informatycznych adekwatne do potrzeb zgłoszonych przez właściciela procesu i Administratora.

2. Za opracowanie procedur zapewniających ciągłość działania procesów przetwarzania danych na wypadek awarii lub zniszczenia systemu oraz nieprawidłowości w jego funkcjonowaniu odpowiedzialny jest IODO i służby informatyczne.

OGÓLNE ZASADY NADAWANIA UPRAWNIEŃ W SYSTEMACH INFORMATYCZNYCH

1. Przydzielanie uprawnień do systemu informatycznego realizowane jest w oparciu o następujące zasady:
    a. „minimalnych przywilejów" – każdy użytkownik posiada prawa dostępu do zasobów ograniczone wyłącznie do tych, które są niezbędne do wykonywania powierzonych mu obowiązków;
    b. „wiedzy koniecznej" – użytkownicy posiadają wiedzę o zasobach ograniczoną wyłącznie do zagadnień, które są niezbędne do realizacji powierzonych im zadań;
    c. „domniemanej odmowy" – wszystkie działania, które nie są jawnie dozwolone są zabronione.
2. Użytkownik systemu informatycznego jest jednoznacznie identyfikowany poprzez nadany mu indywidualny identyfikator użytkownika.
3. Niedopuszczalne jest korzystanie z tego samego identyfikatora przez więcej niż jednego użytkownika.
4. Raz użyty identyfikator nie może być przydzielony innemu użytkownikowi.
5. Uprawnienia dostępu są nadawane wyłącznie w zakresie wynikającym z zajmowanego stanowiska i potrzeby wykonywania obowiązków służbowych na danym stanowisku pracy. Bezzasadne nadawanie uprawnień (przywilejów) może być kwalifikowane jako incydent związany z bezpieczeństwem informacji.

NADAWANIE UPRAWNIEŃ

1. Przed dopuszczeniem do korzystania z systemu informatycznego każdy Użytkownik powinien zapoznać się z Dokumentacją Ochrony Danych Osobowych.
2. Przetwarzać dane osobowe mogą wyłącznie osoby posiadające pisemne upoważnienie do przetwarzania danych osobowych nadane przez ADO lub podmiot przetwarzający, z którym łączy ADO umowa powierzenia.
3. Dostęp do systemów informatycznych mogą posiadać:

a) Rektor, Kanclerz, Z-ca Kanclerza, Prorektor ds. dydaktycznych i studenckich, pracownicy służb informatycznych - w zakresie wglądu do wszystkich systemów informatycznych,
b) Kierownicy komórek organizacyjnych i pracownicy – w zakresie niezbędnym do wykonywania powierzonych im czynności służbowych
c) Podmioty zewnętrzne - wykonawcy usług oraz dostawcy sprzętu lub oprogramowania – w zakresie koniecznym do realizowania danej usługi lub wykonania określonych czynności w systemie.

4. W przypadku wystąpienia naruszenia bezpieczeństwa danych osobowych IODO może wnioskować o czasowe ograniczenie dostępu do systemów

informatycznych, dla osoby bezpośrednio odpowiedzialnej za zaistniałe zdarzenia, na okres prowadzonych wyjaśnień.

5. Za opracowanie szczegółowych zasad nadawania, modyfikacji i anulowania uprawnień do wykorzystywanych systemów informatycznych oraz dostępu do sieci chronionej, jak również wdrożenie i nadzór nad przestrzeganiem przedmiotowych zasad odpowiedzialne są służby informatyczne przy współpracy z IODO.
6. W celu nadania uprawnienia, kierownik komórki organizacyjnej: wnioskuje do służb informatycznych o nadanie lub modyfikację uprawnień do systemu informatycznego dla Pracownika. Służby informatyczne zgodnie z wnioskiem nadają Użytkownikowi uprawnienia w systemie, login i hasło dostępu lub na jego podstawie modyfikują je lub odmawiają nadania uprawnień do systemu informatycznego w przypadku uchybienia wymogom określonym w ogólnych zasadach zarządzania uprawnieniami.
7. Wniosek powinien zawierać poprawną informację o profilu uprawnień (zgodnym z obowiązującym katalogiem profili uprawnień lub przyjętym zakresem obowiązków na danym stanowisku).
8. W przypadku powzięcia podejrzenia co do przekroczenia zakresu uprawnień wymaganych na danym stanowisku, służby informatyczne są zobowiązane skonsultować ten fakt z IODO.
9. W przypadku nadania uprawnień wymagających logowania, służby informatyczne w sposób zapewniający poufność danych przekazują użytkownikowi informację zawierającą wymienione z nazwy systemy informatyczne, do których użytkownik otrzymał dostęp oraz login i hasło na potrzeby pierwszego logowania.
10. Hasło, o którym mowa powyżej powinno zostać wygenerowane w sposób losowy, a jego złożoność i długość powinna uniemożliwiać łatwe przełamanie.
11. Jeśli system nie realizuje funkcjonalności wymuszenia zamiany hasła tymczasowego przy pierwszym logowaniu użytkownik przy pomocy służb informatycznych jest zobowiązany do manualnej zmiany wygenerowanych tymczasowych haseł dostępowych.
12. Wniosek o nadanie uprawnień może zostać sporządzony i przekazany służbom informatycznym w formie papierowej lub elektronicznej.
13. Procedura zarządzania tożsamością dla usługi logowania federacyjnego, stanowi załącznik nr 1 do Instrukcja Zarządzania Systemem Informatycznym.[1]

ODBIERANIE UPRAWNIEŃ

1. Kierownik komórki organizacyjnej jest zobowiązany do złożenia wniosku o odebranie uprawnień do systemów informatycznych wykorzystywanych przez Administratora.
2. Terminami obowiązującymi przy składaniu wniosku są w szczególności:

[1] w rozdziale pn. „NADAWANIE UPRAWNIEŃ" po pkt. 12 dodano pkt 13, zmiana wprowadzona Zarządzeniem nr 100/2022 z dnia 3 listopada 2022 r

   a. w przypadku ustania stosunku pracy – wniosek odbierający wszystkie uprawnienia – natychmiast, najpóźniej ostatniego dnia pracy zatrudnionego,
   b. długotrwałe zwolnienie lekarskie – wniosek odbierający wszystkie uprawnienia – natychmiast po upływie 30 (trzydziestu) dni kalendarzowych od dostarczenia zwolnienia lekarskiego,
3. Po spełnieniu powyższych wymagań wniosek zostaje przekazany do służb informatycznych.
4. Służby informatyczne przyjmują wniosek o odebranie uprawnień do systemu informatycznego spełniający wymogi opisane powyżej.
5. Służby informatyczne dokonują weryfikacji poprawności wniosku o odebranie uprawnień do systemu informatycznego.
6. Służby informatyczne bezzwłocznie realizują otrzymany wniosek.
7. Wniosek o odebranie uprawnień może zostać sporządzony i przekazany służbom informatycznym w formie papierowej lub elektronicznej.

UŻYTKOWANIE SPRZĘTU KOMPUTEROWEGO

1. Służby informatyczne przekazuj pracownikowi służbowy sprzęt komputerowy po podpisaniu przez niego protokołu przekazania i odebrania mienia pracownikowi.
2. Protokół przygotowywany jest w dwóch jednobrzmiących egzemplarzach po jednej dla każdej ze stron.
3. Przekazanie sprzętu to czynność polegająca na dostarczeniu sprzętu komputerowego wraz z odpowiednio skonfigurowanym oprogramowaniem.
4. Służby informatyczne odpowiadają za poprawne działanie oraz skonfigurowanie sprzętu komputerowego.
5. Sprzęt komputerowy przetwarzający dane osobowe należy skonfigurować w ten sposób, aby możliwość instalowania lub odinstalowania oprogramowania miały tylko służby informatyczne.
6. Przed przekazaniem użytkownikowi komputera przenośnego cała powierzchnia dysku twardego urządzenia musi zostać zaszyfrowana.
7. Służby informatyczne mają obowiązek przechowywać karty gwarancyjne, klucze i licencje do oprogramowania.
8. Służby informatyczne prowadzą rejestr wydanego sprzętu komputerowego wraz z wyszczególnieniem użytkownika.
9. W przypadku ustania stosunku pracy pracownika lub potrzeby przekazania sprzętu w użytkowanie innej osobie pracownik zobowiązany jest do zwrotu używanego urządzenia do Służb informatycznych wraz z protokołem przekazania.
10. W przypadku braku uszkodzeń i kompletności zestawu Służby informatyczne podpisują protokół przekazania i odebrania mienia pracownikowi.

UŻYTKOWANIE MOBILNYCH NOŚNIKÓW DANYCH

1. W celu ograniczenia możliwości utraty informacji zaleca się uwzględnienie rejestrowania mobilnych nośników danych.
2. Przed przekazaniem użytkownikowi mobilnego nośnika danych musi zostać on zaszyfrowany, zgodnie z przyjętym oprogramowaniem do stosowania zabezpieczeń kryptograficznych.
3. Czytniki nośników wymiennych komputerów użytkowników udostępniane są tylko dla zautoryzowanych nośników danych.
4. Jeśli mobilny nośnik danych zostanie uszkodzony i nie można go odczytać ani usunąć z niego danych, należy go zniszczyć mechanicznie np. przy użyciu niszczarki spełniającej wymagania normy DIN 66399 na poziomie bezpieczeństwa nie niższym niż 3 lub przy pomocy zewnętrznego podmiotu realizujący tego typu czynności w sposób profesjonalny uwzględniając zapisy wewnętrznej dokumentacji w zakresie usuwania danych.
5. Po przeprowadzonej utylizacji przez podmiot zewnętrzny Służby informatyczne są obowiązane odebrać i zarchiwizować protokół zniszczenia.

ZASADY KORZYSTANIA Z POCZTY ELEKTRONICZNEJ

1. Użytkownikowi zostaje nadany dedykowany adres skrzynki poczty elektronicznej działający w domenie Administratora.
2. Informacja o służbowym adresie skrzynki pocztowej jest jawna i dostępna powszechnie, w tym może być dostępna na łamach witryny internetowej Administratora w postaci książki adresowej.
3. Nadany użytkownikowi adres skrzynki poczty elektronicznej służy wyłącznie do realizacji celów służbowych lub umownych. Korespondencja realizowana drogą elektroniczną z wykorzystaniem systemów informatycznych Administratora podlega rejestrowaniu i może być monitorowana. Informacje przesyłane za pośrednictwem sieci Administratora (w tym do i z Internetu) nie stanowią własności prywatnej użytkownika.
4. Wszelka korespondencja elektroniczna niezwiązana z działalnością Administratora powinna być prowadzona przez prywatną skrzynkę poczty elektronicznej użytkownika.
5. Użytkownicy dokonujący wysyłki korespondencji masowej poza organizację, obowiązani są do ukrywania odbiorów w kopii (pole BCC lub UDW).
6. Użytkownicy dokonujący wysyłki korespondencji z załącznikiem zawierającym w swojej treści dane osobowe, poufne informacje lub informacje mogące stanowić tajemnicę przedsiębiorstwa obowiązani są do opatrzenia takiego dokumentu hasłem autoryzacyjnym. Hasło do pliku powinno zostać przesłane za pomocą innej formy komunikacji np. krótkiej wiadomości tekstowej SMS.
7. Zabronione jest:

1) wysyłanie materiałów służbowych na konta prywatne (np. celem pracy nad dokumentami w domu),
2) otwieranie załączników od nieznanych nadawców, w szczególności z plikami samorozpakowującymi się bądź wykonalnymi typu exe, com, itp.,
3) czytanie, usuwanie, kopiowanie lub zmiana zawartości skrzynek pocztowych innego użytkownika,
4) posługiwanie się adresem służbowym e-mail w celu rejestrowania się na stronach handlowych, informacyjnych, chat'ach lub forach dyskusyjnych, które nie dotyczą zakresu wykonywanej pracy lub obowiązków umownych,
5) wykorzystywanie poczty elektronicznej do działalności innej niż wynikającej z potrzeb Administratora Danych Osobowych.

ZARZĄDZANIE DOSTĘPEM ZDALNYM

1. Zdalny dostęp wykonawcy zewnętrznego do systemów informatycznych Administratora przy wykorzystaniu elektronicznych kanałów dostępu, powinno podlegać ewidencji i monitorowaniu.
2. Przed udzieleniem dostępu, parametry takie jak: czas zalogowania się, przewidywany czas pracy, jej zakres oraz niezbędny zakres dostępu do systemów informatycznych, są określone, zaplanowane i zatwierdzone przez osobę upoważnioną.
3. Przekazanie konta dostępu do systemów powinno odbywać się z zachowaniem szczególnej ostrożności, w sposób dający pewność przekazania go upoważnionemu przedstawicielowi wykonawcy usługi.
4. Podstawowym sposobem ewidencji wykonanych zdalnie czynności są logi z systemów, do których wykonawca miał dostęp i przetwarzał zgromadzone w nich dane.
5. Po wykonaniu usługi przez wykonawcę zewnętrznego Służby informatyczne zobowiązane są do odebrania tymczasowo przydzielonego dostępu.

WYMAGANIA DOTYCZĄCE BEZPIECZEŃSTWA URZĄDZEŃ MOBILNYCH

1. Skonfigurowanie smartfonu lub tabletu powinno odbyć się przed przekazaniem sprzętu użytkownikowi.
2. Za odpowiednie skonfigurowanie urządzenia odpowiedzialne są Służby informatyczne.
3. Zaleca się wdrożenie zabezpieczeń w postaci ograniczenia instalacji jakiegokolwiek oprogramowania na urządzeniach mobilnych przez użytkownika.
4. Wobec urządzeń mobilnych wymaga się szyfrowania nośników pamięci, w tym kart pamięci.
5. Na wszystkich urządzeniach mobilnych zapewnia się oprogramowanie antywirusowe.
6. Wobec urządzeń mobilnych wymaga się skonfigurowania ekranu blokady (pin/ hasło/ symbol graficzny).
7. Wobec użytkowników urządzeń mobilnych wymaga się wyłączania nieużywanych usług (Wi-Fi, GPRS, Bluetooth, NFC).

8. Wobec urządzeń mobilnych wymaga się możliwości zdalnego usunięcia danych na skutek kradzieży, zagubienia urządzenia.
9. W przypadku utraty urządzenia mobilnego przez pracownika, w szczególności na skutek kradzieży lub zgubienia urządzenia, obowiązany jest on o tym fakcie bezzwłocznie powiadomić ASI.

ZASADY TELEPRACY

1. W przypadku, gdy jest to konieczne dopuszcza się zdalny dostęp do sieci komputerowej Administratora dla pracowników, współpracowników oraz podwykonawców.
2. W takich przypadkach stosowane są następujące mechanizmy zabezpieczające:
    1) silne uwierzytelnianie użytkowników,
    2) szyfrowane połączenie (VPN/SSL).
3. Praca zdalna wykonywana przez pracowników może być realizowana na komputerach, tabletach, smartfonach służbowych. Służbowe urządzenia mobilne mogą być wykorzystywane tylko i wyłącznie do użytku służbowego, a ich użytkownicy powinni być świadomi odpowiedzialności za przechowywane na nich informacje.
4. Każdy użytkownik zobowiązany jest do przestrzegania zakazu prowadzenia rozmów, podczas których może dochodzić do wymiany informacji, danych osobowych lub informacji poufnych będącego własnością Administratora, jeśli rozmowy te odbywają się w miejscach publicznych, otwartych pomieszczeniach biurowych lub takich, które nie gwarantują zachowania poufności rozmów.

BEZPIECZEŃSTWO FIZYCZNE I ŚRODOWISKOWE

1. Dostęp do pomieszczeń, w których znajdują się systemy informatyczne wysokiej istotności, oraz systemy wspomagające takie jak UPSy, generatory prądu i inne, mogą posiadać wyłącznie osoby upoważnione.
2. W pomieszczeniach, w których ulokowane są systemy informatyczne wysokiej istotności, nie powinno się zezwalać przebywającym tam osobom na fotografowanie ani rejestrowanie głosu oraz obrazu bez odpowiedniego zezwolenia.
3. Pomieszczenia, w których pracują serwery, mają zapewnione stałe utrzymywanie temperatury, wilgotności i innych parametrów określonych przez producenta sprzętu komputerowego.
4. Szafy, w których przechowywane są nośniki informacji powinny zapewniać ochronę przed czynnikami zewnętrznymi mogącymi doprowadzić do utraty lub ujawnienia danych.
5. Wszystkie prace remontowe, konserwacyjne, naprawcze, a także porządkowe na terenie obszaru przetwarzania danych osobowych są nadzorowane przez osobę upoważnioną.

DOBÓR I KONFIGURACJA KOMPONENTÓW INFRASTRUKTURY TELEINFORMATYCZNEJ

1. Zasady doboru komponentów infrastruktury i ich konfiguracji:
    1) rodzaj i konfiguracja każdego z komponentów infrastruktury teleinformatycznej wynika z analizy funkcji, jaką dany element pełni w środowisku teleinformatycznym oraz poziomu bezpieczeństwa wymaganego przez systemy informatyczne lub przesyłane dane,
    2) komponenty są dobierane z uwzględnieniem ich wad i zalet z perspektywy potrzeb i wymagań obszaru infrastruktury, w którym mają być ulokowane,
    3) ustalając sposób konfiguracji komponentu Organizacja kieruje się zasadą minimalizacji zakresu udostępnianych przez dany komponent usług.
2. Weryfikacja predefiniowanych ustawień:
    4) organizacja weryfikuje przed dopuszczeniem do produkcji, czy na urządzeniach lub systemach nie pozostawiono ustawień fabrycznych (domyślnych) wprowadzonych przez ich producentów,
    5) w szczególności weryfikacją objęte są ustawienia urządzeń sieciowych, urządzeń biurowych, serwerów fizycznych (w tym wirtualnych), systemów informatycznych oraz konfiguracja serwerów bazodanowych.
    6) Zasady dokonywania zmian w konfiguracji komponentów informatycznych:
    7) realizację zmian przeprowadza się w sposób zaplanowany i kontrolowany, biorąc pod uwagę wpływ zmiany na inne komponenty. W tym celu należy zastosować również odpowiednie zasady w zakresie „privacy by design” oraz „privacy by default”,
    8) komponenty infrastruktury są zabezpieczone przed wprowadzaniem nieuprawnionych zmian w ich konfiguracji,
    9) zmiany w konfiguracji uwzględniają możliwość wycofania zmiany,
    10) zapewnia się kopie bezpieczeństwa konfiguracji zmienianych komponentów,
    11) w przypadku zmian wprowadzanych w serwerach aplikacji, mogących skutkować utratą danych lub utratą dostępności do usługi, zapewnia się kopie bezpieczeństwa zmienianych systemów,
    12) zapewnia się możliwość identyfikacji osób wprowadzających oraz zatwierdzających poszczególne zmiany w konfiguracji poprzez analizę logów oraz poprzez pracę na indywidualnych kontach administracyjnych jednoznacznie identyfikujących osobę.

ZAKUP LUB ROZWÓJ SYSTEMÓW INFORMATYCZNYCH

1. Zakup nowego lub rozwój zasobu informatycznego jest realizowany zgodnie z zasadą „privacy by design” oraz „privacy by default” (art. 25 RODO).
2. W organizacji przeprowadza się testy bezpieczeństwa oprogramowania niezależnie od testów wytwórcy oprogramowania.
3. Celem testów jest weryfikacja, walidacja oraz wyłapanie usterek i błędów oprogramowania.

4. Testy bezpieczeństwa oprogramowania składają się z trzech etapów:
    1) etap przygotowania testów,
    2) etap przeprowadzenia testów,
    3) etap zamknięcia testów.
5. Wynikiem realizacji działań objętych testami jest:
    1) wykonanie działań niezbędnych do sprawdzenia wszystkich przypadków testowych,
    2) monitorowanie postępów testów (uwzględniające rejestrację zidentyfikowanych błędów),
    3) ponowne testowanie poprawek do zarejestrowanych błędów,
    4) dokumentacja potwierdzająca weryfikację poprawności działania, zaplanowanego
       i zweryfikowanego zakresu testów.

BEZPIECZEŃSTWO SIECI

1. Sieć, w której pracują urządzenia komputerowe Administratora Danych Osobowych musi być odseparowana od sieci publicznej zaporą ogniową.
2. Wszelkie wykryte incydenty mogące powodować naruszenie poufności, integralności, dostępności systemów i usług przetwarzania natychmiastowo należy natychmiastowo zgłaszać do IODO.
3. Zdalny dostęp do serwerów w celach administracyjnych może mieć miejsce po zastosowaniu systemu uwierzytelniania użytkownika i szyfrowanego kanału transmisji.
4. Systemy informatyczne powinny korzystać z szyfrowanych protokołów wymiany danych, w szczególności połączeń sftp i https.
5. Zabrania się wykorzystywania przez użytkowników dostępu do sieci publicznej (Internet) do celów innych niż wynikających z rzeczywistych potrzeb Administratora Danych Osobowych.
6. Zabrania się korzystania z treści uznanych za pornograficzne, rasistowskie, traktujące o przemocy, przestępstwach, jak również do protokołów umożliwiających wymianę plików w sieciach z naruszeniem przepisów prawa.
7. Zabrania się przetwarzania treści niezgodnych z prawem polskim za pomocą służbowych urządzeń elektronicznych.
8. Zaleca się regularnie badać podatności usług i systemów pod kątem występowania luk pozwalających na nieuprawniony dostęp lub ujawnienie danych osobowych przetwarzanych w systemie administratora danych osobowych. Powyższe na potrzeby kontroli należy dokumentować.
9. System poczty elektronicznej wykorzystywany do wymiany wiadomości:
    1) gwarantuje poufność przesyłanych danych - transmisja jest szyfrowana,
    2) zapewnia ochronę antywirusową,
    3) jest odporny na ataki phishingowe,
    4) posiada ochronę antyspamową,
    5) uniemożliwia/ogranicza przesyłanie spamu przez serwer pocztowy,

6) umożliwia sprawowanie kontroli nad przesyłanymi wiadomościami
7) zapewnia rozliczalność przesyłanych wiadomości.

10. Zabrania się uruchamiania aplikacji deszyfrujących hasła, prowadzenia działań mających na celu podsłuchiwanie lub przechwytywanie informacji przepływającej w sieci bez uprzedniej zgody Administratora Danych Osobowych.
11. Zabrania się uruchamiania aplikacji, które mogą zakłócić i destabilizować pracę systemu lub sieci komputerowej, bądź naruszyć prywatność zasobów systemowych bez uprzedniej zgody Administratora Danych Osobowych.

WERYFIKACJA MECHANIZMÓW KONTROLNYCH, BADANIE PODATNOŚCI

1. Za identyfikowanie podatności technicznych odpowiedzialny jest IODO i służby informatyczne.
2. Informacje o podatnościach technicznych są uzyskiwane w szczególności poprzez:
    1) testy podatności,
    2) testy penetracyjne,
    3) niezależne wewnętrzne lub zewnętrzne audyty ochrony danych osobowych lub bezpieczeństwa informacji,
    4) w oparciu o analizę incydentów bezpieczeństwa informacji.
3. Podatności zasobów uczestniczących w przetwarzaniu danych osobowych są uwzględniane
   w czasie procesu zarządzania ryzykiem w organizacji.
4. Proces wyszukiwania podatności powinien być realizowany cyklicznie, przynajmniej raz w roku.
5. Każde poszukiwanie podatności w zasobach Administratora musi być na potrzeby kontroli udokumentowane.

ZASADY ZARZĄDZANIA ELEKTRONICZNYMI KOPIAMI DANYCH OSOBOWYCH

1. Zbiory danych, oprogramowanie oraz konfiguracja systemów operacyjnych serwerów Administratora powinny być zabezpieczone w postaci cyklicznie wykonywanych kopii bezpieczeństwa lub kopii archiwalnych.
2. Za tworzenie kopii zapasowych przy użyciu narzędzi systemowych i systemów do tego przystosowanych odpowiedzialne są Służby informatyczne.
3. Kopie zapasowe są wykonywane zgodnie z opracowanym, aktualizowanym i przyjętym harmonogramem wykonywania i testowania kopii zapasowych.
4. Oprócz wykonywania kopii archiwalnych zgodnie z opracowanym, aktualizowanym i przyjętym harmonogramem wykonywania i testowania kopii archiwalnych, wykonuje się kopie bezpieczeństwa zawsze przed:
    1) dokonaniem zmian w konfiguracji systemów operacyjnych lub oprogramowania,
    2) dokonaniem zmian w programach (np. zmiana wersji lub aktualizacja oprogramowania),
    3) każdą istotną zmianą danych w bazie danych.

5. Nośniki zawierające kopie zapasowe szyfruje się zawsze w przypadku, gdy kopie opuszczają obszar przetwarzania lub istnieje ryzyko, że miejsce ich przechowywania nie gwarantuje dostępu tylko i wyłącznie osobom upoważnionych.
6. Tworzenie kopii zapasowych podlega rejestracji.
7. Po utworzeniu kopii automatycznie (jeżeli jest technicznie realizowalne) jest generowany raport o przebiegu wykonania kopii. Raport podlega weryfikacji przez Służby informatyczne.
8. Miejsce przechowywania kopii jest zabezpieczone przed nieuprawnionym dostępem oraz skutkami zdarzeń takich, jak pożar, zalanie, oddziaływanie silnego pola elektromagnetycznego, promieniowanie, zanieczyszczenie środowiska na takim poziomie, jak jest zabezpieczony system, z którego kopia zapasowa została wykonana.
9. Kopie są przechowywane w bezpiecznej odległości (co najmniej w innej strefie pożarowej) od miejsca, w którym jest prowadzona eksploatacja systemów, chyba że do tego celu wykorzystuje się sejf ogniotrwały.
10. Nośnik, z którego przeniesiono zapis, niszczony jest w sposób uniemożlwiający odzyskanie danych na nim zgromadzonych.
11. Regularnie, co najmniej cztery razy w roku, Służby informatyczne przeprowadzają testowe sprawdzenie odtworzenia systemu, aplikacji, bazy danych lub dokumentów z kopii. Testowe odtworzenie podlega udokumentowaniu w dzienniku pracy systemu, jeżeli jest prowadzony.
12. Po upływie wymaganego okresu przechowywania kopie archiwalne są niszczone zgodnie z zasadami obowiązującymi u Administratora Danych Osobowych.

OCHRONA PRZED SZKODLIWYM OPROGRAMOWANIEM

1. Zidentyfikowanymi obszarami systemu informatycznego Administratora narażonymi na ingerencję wirusów oraz innego szkodliwego oprogramowania są wszelkie elektroniczne nośniki danych.
2. Stacje robocze, komputery przenośne, smartfony, tablety oraz serwery są objęte ochroną w czasie rzeczywistym za pomocą oprogramowania antywirusowego oraz zapory (firewall), zapewniających integralność zasobów przechowywanych i przetwarzanych w systemie informatycznym Administratora.
3. Oprogramowanie antywirusowe automatycznie uruchamiane jest przy starcie systemu, a użytkownik nie posiada uprawnień do jego jakiejkolwiek konfiguracji lub wyłączenia.
4. Zarówno oprogramowanie jak i baza wirusów oprogramowania antywirusowego jest stale aktualizowana.
5. Należy regularnie weryfikować skuteczność mechanizmów aktualizujących oprogramowanie antywirusowe.
6. Za prawidłowe i efektywne funkcjonowanie oprogramowania antywirusowego odpowiadają Służby informatyczne.

7. Wszelkie systemy informatyczne są na bieżąco aktualizowane, a w szczególności natychmiast po opublikowaniu krytycznych luk czy błędów.
8. Za aktualizacje wykorzystywanego oprogramowania odpowiedzialne są Służby informatyczne.
9. Stacje robocze i komputery przenośne przynajmniej raz w miesiącu automatycznie skanowane są pod kątem występowania na nich oprogramowania złośliwego.
10. Serwery plikowe podlegają automatycznemu skanowaniu pod kątem występowania na nich oprogramowania złośliwego przynajmniej raz w tygodniu.
11. Użytkownicy systemu w przypadku stwierdzenia pojawienia się wirusa na wykorzystywanym sprzęcie komputerowym i braku możliwości usunięcia go przez program antywirusowy są obowiązani niezwłocznie odłączyć urządzenie od sieci Internet oraz niezwłocznie skontaktować się w przedmiotowej sprawie z IODO i Służbami informatycznymi.
12. W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy, Służby informatyczne podejmują działania zmierzające do usunięcia zagrożenia. W szczególności działania te mogą obejmować:
    1) usunięcie zainfekowanych plików, o ile jest to akceptowalne ze względu na prawidłowe funkcjonowanie systemu informatycznego,
    2) odtworzenie plików z kopii zapasowych, po uprzednim sprawdzeniu, czy dane zapisane na kopiach zapasowych nie są zainfekowane,
    3) samodzielną ingerencję w zawartość pliku – w zależności od posiadanych kwalifikacji lub skonsultowanie się z odpowiednim serwisem,
    4) zmianę wszystkich haseł stosowanych przez użytkownika zainfekowanego sprzętu komputerowego
13. Wszelkie czynności, o których mowa powyżej należy wykonywać w trybie offline.

PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY

1. Użytkownik przed przystąpieniem do pracy w systemie informatycznym zobowiązany jest dokonać sprawdzenia stanu sprzętu informatycznego oraz oględzin swojego miejsca pracy, obejmującej weryfikację podłączonych urządzeń nieznanego pochodzenia.
2. W przypadku stwierdzenia podłączenia urządzeń niewiadomego pochodzenia zabrania się uruchamiania systemu informatycznego do momentu ich usunięcia.
3. Rozpoczęcie pracy w systemie informatycznym następuje po wprowadzeniu unikalnego identyfikatora i hasła.
4. Zabrania się zapisywania dokumentów zawierających dane osobowe, poufne informacje lub inne dane mogące stanowić tajemnice przedsiębiorstwa na pulpicie komputera, w tym w szczególności sugerowania nazwą ich zawartości.
5. Dokumenty zawierające dane osobowe, poufne informacje lub inne dane mogące stanowić tajemnicę przedsiębiorstwa użytkownik obowiązany jest do przechowywania na dedykowanych zasobach sieciowych.

6. Zawieszenie pracy w systemie informatycznym, tj. brak wykonywania jakichkolwiek czynności przez okres 5-10 minut w systemie informatycznym, powoduje automatycznie uruchomienie systemowego wygaszacza ekranu blokowanego hasłem.
7. Zastosowanie powyższego mechanizmu nie zwalnia użytkownika z obowiązku każdorazowego blokowania ekranu przed odejściem od stanowiska („ctrl + alt + del" i wybranie „zablokuj komputer" lub skrótem klawiszowym „Win + L").
8. Po zakończeniu pracy, użytkownik obowiązany jest wylogować się z systemu informatycznego przetwarzającego dane osobowe i z systemu operacyjnego, zabezpieczyć nośniki informacji (elektroniczne i papierowe) oraz każdorazowo wyłączyć komputer, chyba że użytkownik otrzymał informację od Administratora zasobu o planowanych pracach serwisowych.
9. W celu zabezpieczenia elektronicznych oraz papierowych nośników danych pracownik obowiązany jest umieścić je w przydzielonych meblach biurowych, zamknąć na klucz, a przedmiotowy klucz przechowywać w miejscu uniemożliwiającym dostęp osobom nieupoważnionym.

POSTANOWIENIA KOŃCOWE

1. Dokumentacja przetwarzania danych osobowych stanowi wewnętrzną regulację Administratora i obowiązuje wszystkich pracowników i współpracowników Administratora.
2. Dokumentacja przetwarzania danych osobowych obowiązuje od dnia jej wprowadzenia w życie w sposób przyjęty u Administratora. Wszelkie zmiany niniejszej dokumentacji obowiązują od dnia ich wprowadzenia w życie w sposób przyjęty u Administratora.
3. Dokumentacja przetwarzania danych osobowych podlega przeglądowi co najmniej raz w roku. Każdy kto przetwarza dane posiadane przez Administratora zobowiązany jest do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej dokumentacji przetwarzania danych osobowych.
4. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych lub rażące naruszenie staranności w wykonaniu zobowiązania w przypadku stosunku prawnego innego niż stosunek pracy.
5. W sprawach nieuregulowanych w niniejszej dokumentacji przetwarzania danych osobowych mają zastosowanie przepisy powszechnie obowiązującego prawa, w tym w szczególności przepisy RODO oraz ustawy o ochronie danych osobowych.

PROCEDURA ZARZĄDZANIA TOŻSAMOŚCIĄ DLA USŁUGI LOGOWANIA FEDERACYJNEGO

Konta użytkowników w Usłudze logowania federacyjnego zakładane, kasowane oraz użytkowane są zgodnie z zarządzeniami wewnętrznymi dotyczącymi poczty elektronicznej dla pracowników i studentów Uczelni.

Dostawca Tożsamości kontroluje ustawienie atrybutów typu *affiliation* i przypisuje je następująco: dla studentów - *student*, dla pracowników - *staff*, dla pozostałych grup - *member*.

Zasady zakładania, kasowania, okresu użytkowania kont dla systemu określa się zgodnie z poniższą tabelą:

	Grupa kont	**Podstawa do założenia/utrzymania konta**	**Okres użytkowania**	**Podstawa kasowania**	**Zgłaszający (forma zgłoszenia)**
1.	Pracownicy	Umowa o pracę, zgłoszenie przez Biuro Organizacji i Spraw Pracowniczych	Okres trwania umowy	Rozwiązanie umowy o pracę	Biuro Organizacji i Spraw Pracowniczych (informacja o pracowniku)
2.	Pracownicy zatrudnieni na umowy cywilnoprawne	Umowa na okres zamknięty, zgłoszenie przez Biuro Organizacji i Spraw Pracowniczych	Okres trwania umowy	Zakończenie okresu umowy	Biuro Organizacji i Spraw Pracowniczych (informacja o pracowniku)
6.	Funkcyjne	Stosownie do struktury uczelni/jednostki, na podstawie zgłoszenia kierownictwa jednostki.	Okres pełnienia funkcji	Zmiana organizacyjna uczelni	Rektor, Kanclerz, Zastępca Kanclerza, Prorektor (informacja o zmianach)

7.	Konferencyjne	Złożenie wniosku o założenie serwera wirtualnego do Specjalisty ds. informatyki	Do zakończenia konferencji (z możliwością przedłużenia na 12-mcy)	Zakończenie konferencji	Rektor, Kanclerz, Zastępca Kanclerza, Kierownik Jednostki (informacja)
7.	Koła Naukowe	Wniosek opiekuna koła, który jest pracownikiem uczelni. Konta pocztowe zakładane są w domenie koła naukowego (liczba kont jest ograniczona)	Konto jest aktywne na podstawie składanych sprawozdań z działalności do Działu Studenckiego.	Zakończenie działalności Koła Naukowego, wykreślenie z listy Kół Naukowych.	Opiekun koła, Prorektor, Dyrektor Instytutu (wykaz członków koła posiadających dostęp do konta)
8.	Organizacje uczelniane	Pisemna prośba zaakceptowana przez Rektora.	Okres użytkowania podany w podaniu.	Brak akceptacji przez Rektora lub zakończenie okresu użytkowania.	Rektor (informacja)
9.	Studenci	Wykaz studentów otrzymany z systemu USOS, konta zakładane są w domenie ans.edu.pl	Okres trwania studiów – od nadania statusu studenta na podstawie decyzji o przyjęciu na studia do utraty statusu studenta.	Zakończenie/skreślenie z listy studentów Uczelni	Administrator systemu USOS/ pracownicy Działu Nauczania i Spraw Studenckich (automatycznie z systemu USOS)