SYSTEM BEZPIECZEŃSTWA
Akademii WSB

POLITYKA BEZPIECZEŃSTWA
Akademii WSB

Spis treści

I. POLITYKA BEZPIECZEŃSTWA

Polityka Bezpieczeństwa jest dokumentem nadrzędnym Systemu Bezpieczeństwa Akademii WSB. Dokument spełnia wymagania 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).

1. SŁOWNIK POJĘĆ

Administrator Danych /AD/ - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania; W Akademii WSB funkcję Administratora Danych pełni Rektor.

Podmiot przetwarzający - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora

Odbiorca - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania

Zgoda osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;

Inspektor Ochrony Danych – Akademia WSB wyznaczyła Inspektora Ochrony Danych w osobie: .....

Administrator Systemu Informatycznego /ASI/ - osoba odpowiedzialna za przestrzeganie zasad ochrony danych osobowych w systemach informatycznych.

Dane osobowe - oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;.

Przetwarzanie danych - oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką 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.

Ograniczenie przetwarzania - oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania

Profilowanie - oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji,

zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;

Pseudonimizacja - oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

Zbiór danych - oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

Naruszenie ochrony danych osobowych - oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

Naruszenie Systemu Bezpieczeństwa - działanie niezgodne z przyjętymi dokumentami Systemu Bezpieczeństwa.

Identyfikator - ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym

Hasło - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

Incydent - jedno lub seria niepożądanych lub niespodziewanych zdarzeń, które ze znacznym prawdopodobieństwem mogą zakłócić działania Akademii WSB i oraz zagrozić bezpieczeństwu informacji.

Podatność - słabość zasobu lub grupy zasobów, która może być wykorzystana przez zagrożenie.

System informatyczny - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

Zabezpieczanie danych w systemie informatycznym - wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.

Przegląd Systemu Bezpieczeństwa – cykliczna weryfikacja skuteczności przyjętych rozwiązań związanych z bezpieczeństwem informacji

Aktywa - jest to wszystko, co ma wartość dla organizacji (administratora danych lub podmiotu przetwarzającego), np. dane osobowe.

Aktywa podstawowe – są to procesy, działania biznesowe oraz informacje związane z funkcjonowaniem organizacji (w tym dane osobowe).

Aktywa wspierające – są to środki umożliwiające korzystanie z aktywów podstawowych. Przykładem aktywów wspierających jest sprzęt, oprogramowanie, sieć, pracownicy.

Anonimizacja – oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było przypisać konkretnej osobie, której dane dotyczą, za pomocą dodatkowych informacji lub wszelkich innych środków, jakimi dysponuje administrator lub podmiot przetwarzający. Zabieg ten ma charakter trwały i nieodwracalny, powodujący, że po jego przeprowadzeniu nie mamy do czynienia z danymi osobowymi.

Grupa Robocza Art. 29 - Grupa Robocza Art. 29 to powołany na mocy Dyrektywy 95/46 zespół roboczy do spraw ochrony osób fizycznych mający charakter doradczy i działający w sposób całkowicie niezależny. Jej misją jest służenie radą Komisji Europejskiej i przyczynianie się do jednolitego stosowania przepisów krajowych przyjętych na mocy dyrektywy. Grupę tworzą przedstawiciele krajowych organów nadzorczych, przedstawiciele organów ustanowionych dla instytucji i organów unijnych (po jednym dla każdej z

instytucji i organu) oraz przedstawiciele Komisji Europejskiej. Działania Grupy sprowadzają się głównie do wydawania niemających mocy wiążącej zaleceń, rekomendacji oraz opinii w sprawach unijnych aktów normatywnych z zakresu ochrony prywatności.

Identyfikowanie ryzyka – jest to czynność polegająca na określeniu, co może się zdarzyć (kiedy, gdzie, jak i dlaczego) i spowodować stratę.

Kontekst – są to wszystkie informacje wiążące się z działaniem organizacji, m.in. informacje dotyczące środowiska prawnego, społecznego, politycznego, finansowego czy też technologicznego, np. przepisy dotyczące ochrony danych osobowych.

Kryteria akceptacji ryzyka – są to kryteria, które określają dopuszczalność danego ryzyka.

Kryteria oceny ryzyka - są to kryteria, które określają poziomy odniesienia, względem których określa się ważność ryzyka.

Ocena ryzyka – jest to czynność polegająca na porównaniu wyników uzyskanych podczas analizy ryzyka z kryteriami oceny ryzyka określonymi na etapie ustanawiania kontekstu działania organizacji.

Operacja przetwarzania danych osobowych - każda czynność wykonywana na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka 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.

Podatność - jest to słabość, która może być wykorzystana przez zagrożenie, powodując niekorzystne skutki, np. luka w systemie informatycznym.

Proces przetwarzania danych osobowych – zespół operacji (czynności) wykonywanych na danych osobowych lub zestawach danych osobowych w celu osiągnięcia określonego celu przetwarzania.

Pseudonimizacja - oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji. Te dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. W przeciwieństwie do anonimizacji, której skutkiem jest nieodwracalne uniemożliwienie identyfikacji osoby, pseudonimizacja jest procesem odwracalnym.

RODO - Rozporządzenie 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), które będzie stosowane od 25 maja 2018 r.; jego celami są skuteczna ochrona podstawowych praw i wolności osób fizycznych, w szczególności prawa do ochrony danych osobowych osób fizycznych oraz uregulowanie zasad i zapewnienie swobodnego przepływu danych osobowych w UE w taki sposób, by ochrona praw jednostki nie stała temu na przeszkodzie.

Ryzyko – wpływ niepewności na cele. W przypadku ryzyka naruszenia praw i wolności osób, których dane dotyczą, celem będzie ochrona tych praw i wolności.

Szacowanie ryzyka – całościowy proces identyfikacji ryzyka, analizy ryzyka oraz oceny ryzyka (definicja przyjęta zgodnie z normą PN-ISO/IEC 27005:2011). W ramach procesu „szacowanie ryzyka" ujęto takie zadania, jak: ustalenie kontekstu, ocena ryzyka, postępowanie z ryzykiem oraz jego monitorowanie i przegląd.

Właściciel aktywów – jest to osoba odpowiedzialna w danym podmiocie za konkretny proces przetwarzania danych i mająca prawo do podejmowania w tym zakresie decyzji, np. dyrektor departamentu, kierownik określonej komórki w organizacji.

Zabezpieczenie - jest to środek, którego celem jest zmniejszenie ryzyka poprzez obniżenie prawdopodobieństwa zrealizowania zagrożenia (czyli wykorzystania istniejącej podatności) lub też minimalizację potencjalnych strat związanych ze zrealizowanym zagrożeniem, np. program antywirusowy, drzwi antywłamaniowe, stosowanie procedury bezpieczeństwa.

Zagrożenie - jest to źródło potencjalnej szkody, np. zagrożenie naruszenia integralności danych.

2. DEFINICJA BEZPIECZEŃSTWA INFORMACJI

Bezpieczeństwo informacji postrzegane jest przez pryzmat zachowania jego podstawowych cech, definiowanych jako:

- **Poufność** – cecha informacji określająca, że do informacji mają dostęp tylko osoby uprawnione, a wszelkie próby nieuprawnionego dostępu są uniemożliwione dzięki wdrożeniom odpowiednich zabezpieczeń.
- **Integralność** – cecha informacji, dzięki której informacje pozostają kompletne i prawidłowe (pozbawione błędów i przekłamań).
- **Dostępność** – cecha informacji określająca, że informacja jest dostępna dla uprawnionych użytkowników wtedy, gdy mają uzasadnioną potrzebę skorzystania z niej. Celem zarządzania bezpieczeństwem informacji jest zachowanie wszystkich wyżej wymienionych cech. Utrata dowolnej z powyższych cech stanowi naruszenie bezpieczeństwa informacji.

3. PRAWA OSÓB WYNIKAJĄCE Z RODO

Każda osoba powinna mieć kontrolę nad dotyczącymi jej danymi osobowymi, niezależnie od tego kto i w jakim celu te dane przetwarza. Ogólne rozporządzenie o ochronie danych (RODO) przyznaje szereg uprawnień podmiotom danych:

- prawo do bycia poinformowanym o operacjach przetwarzania
- prawo dostępu,
- prawo do sprostowania/uzupełnienia danych,
- prawo do usunięcia danych (prawo do bycia zapomnianym),
- prawo do ograniczenia przetwarzania,
- prawo do przenoszenia danych,
- prawo do sprzeciwu,
- prawo do tego, by nie podlegać profilowaniu.

Prawo dostępu do Danych

Każda osoba, której dane są przetwarzane, ma prawo do wystąpienia do administratora z wnioskiem, o wydanie jej informacji o tym, czy jej dane są przetwarzane, a jeżeli tak, to do uzyskania dostępu do tych danych lub uzyskania ich kopii.

Administrator Danych jest zobowiązany do udzielenia stosownych informacji wnioskodawcy bez nadmiernych opłat oraz bez zbędnej zwłoki, najpóźniej w terminie 1 miesiąca od otrzymania wniosku.

Prawo do poprawienia Danych

Osoba, której dane są przetwarzane przez administratora ma prawo, w razie stwierdzenia nieścisłości w zgromadzonych danych, w każdej chwili spowodować, żeby jej dane zostały poprawione przez administratora bez zbędnej zwłoki.

Ponadto, jeżeli jest to uzasadnione z uwagi na cel przetwarzania jej danych, osoba, której dane dotyczą, ma prawo żądać od administratora uzupełnienia niekompletnych danych.

Prawo do ograniczenia przetwarzania danych

Każda osoba, której dane są przetwarzane, ma prawo żądać ograniczenia ich przetwarzania w następujących przypadkach:

1. jeżeli kwestionuje prawidłowość danych (ograniczenie następuje na okres sprawdzenia prawidłowości danych przez administratora),
2. wniosła sprzeciw wobec przetwarzania (ograniczenie następuje do czasu stwierdzenia czy podstawy administratora do przetwarzania są nadrzędne wobec podstaw sprzeciwu),
3. przetwarzanie jest niezgodne z prawem, a osoba, której Dane dotyczą, sprzeciwia się ich usunięciu, żądając w zamian ograniczenia ich przetwarzania,
4. dane nie są już potrzebne administratorowi do celów przetwarzania, jednakże osoba, której dane dotyczą potrzebuje ich do ustalenia, dochodzenia lub obrony roszczeń prawnych.

W razie ograniczenia przetwarzania danych na wniosek osoby, której dane dotyczą, administrator będzie uprawniony wyłącznie do przechowywania danych tej osoby. Jakiekolwiek przetwarzanie wybiegające poza ich przechowywanie będzie wymagało odrębnej zgody, chyba że przetwarzanie jest niezbędne z uwagi na ochronę roszczeń lub praw innej osoby lub z uwagi na ważne przesłanki interesu publicznego. W takiej sytuacji, przed uchyleniem ograniczenia przetwarzania, administrator jest zobowiązany poinformować o tym fakcie osobę, która żądała ograniczenia.

Prawo do sprzeciwu

Każda osoba, której dane są przetwarzane może w dowolnym momencie wnieść sprzeciw wobec przetwarzania jej danych.

W razie wniesienia takiego sprzeciwu administrator nie może dalej przetwarzać danych osoby, która wniosła sprzeciw, chyba że wykaże on istnienie ważnych, prawnie uzasadnionych, podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, która wniosła sprzeciw.

W przypadku przetwarzania danych do celów marketingu bezpośredniego, osoba, której dane są przetwarzane ma prawo wnieść sprzeciw wobec przetwarzania jej danych w tym celu. Powyższe dotyczy również sprzeciwu wobec profilowania. Administrator jest zobowiązany poinformować osobę o ww. przysługującym jej uprawnieniu najpóźniej przy okazji pierwszego kontaktu, przy czym wspomniana informacja powinna być przedstawiona w sposób wyraźny i łatwy do zrozumienia - odrębnie od innych informacji.

Prawo do bycia zapomnianym (prawo do usunięcia danych)

Każda osoba, której dane są przetwarzane ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych, a administrator ma obowiązek jej dane usunąć bez zbędnej zwłoki, jeżeli zachodzi przynajmniej jedna z następujących okoliczności:

1. dane nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
2. osoba, której dane dotyczą, cofnęła zgodę na przetwarzanie jej danych i nie ma innej podstawy do ich przetwarzania;
3. osoba, której dane dotyczą wniosła sprzeciw wobec przetwarzania jej danych i nie istnieją nadrzędne prawnie uzasadnione podstawy przetwarzania;
4. dane były przetwarzane niezgodnie z prawem;

5. dane muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator;
6. dane zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego.

Ponadto, jeżeli administrator upublicznił dane, to na wniosek osoby, której dane dotyczą - biorąc pod uwagę dostępną technologię i koszt realizacji - jest zobowiązany do podjęcia rozsądnych działań, w tym środków technicznych, by poinformować administratorów przetwarzających te dane, że osoba, której dane dotyczą, żąda, aby administratorzy ci usunęli wszelkie łącza do tych danych, a także kopię lub replikacje tych danych.

Prawo do bycia zapomnianym może zostać ograniczone w sytuacji, gdy przetwarzanie będzie niezbędne z uwagi na:

1. korzystanie z prawa do wolności wypowiedzi i informacji;
2. wywiązanie się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
3. względy interesu publicznego w dziedzinie zdrowia publicznego;
4. cele archiwalne w interesie publicznym, cele badań naukowych lub historycznych lub cele statystycznych, o ile prawdopodobne jest, że prawo do usunięcia danych uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania;
5. ustalenie, dochodzenie lub obronę roszczeń.

Prawo do przenoszenia danych

Osoba, której dane dotyczą, ma, co do zasady, prawo do uzyskania od administratora kopii przekazanych mu danych, w formacie

ustrukturyzowanym, powszechnie używanym i maszynowo czytelnym oraz do żądania przesłania tych danych innemu administratorowi.

4. ZASADY PRZETWARZANIA DANYCH

Główne zasady postępowania przy przetwarzaniu danych osobowych wyznacza art. 5 RODO. Z treści art. 5 RODO wynika, iż Administrator Danych przetwarzający dane powinien dokonywać tego zgodnie z poniższymi zasadami.

Zasada zgodności z prawem, rzetelności i przejrzystości

Zgodnie z nią dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą

a) dla osób fizycznych powinno być przejrzyste, że dotyczące ich dane osobowe są zbierane, wykorzystywane, przeglądane lub w inny sposób przetwarzane oraz w jakim stopniu te dane osobowe są lub będą przetwarzane

b) wszelkie informacje i wszelkie komunikaty związane z przetwarzaniem tych danych osobowych mają być łatwo dostępne i zrozumiałe oraz sformułowane jasnym i prostym językiem,

c) osoby których dane dotyczą należy informować o tożsamości administratora i celach przetwarzania oraz innych informacji mających zapewnić rzetelność i przejrzystość przetwarzania w stosunku do nich,

d) osobom których dane dotyczą należy zapewnić możliwość uzyskania potwierdzenia i informacji o przetwarzanych danych osobowych ich dotyczących,

e) osobom fizycznym należy uświadomić ryzyka, zasady, zabezpieczenia i prawa związane z przetwarzaniem danych osobowych oraz sposoby wykonywania praw przysługujących im w związku z takim przetwarzaniem,

f) konkretne cele przetwarzania danych osobowych powinny być wyraźne, uzasadnione i określone w momencie ich zbierania,

Zasada ograniczenia celu

Zgodnie z nią dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami:

a) dane osobowe powinny być przetwarzane tylko w przypadkach, gdy celu przetwarzania nie można w rozsądny sposób osiągnąć innymi sposobami,

b) dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami,

Zasada minimalizacji danych

Zgodnie z nią dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane,

Zasada prawidłowości

Zgodnie z nią dane osobowe muszą być prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane,

Zasada ograniczenia przechowywania

Dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane:

a) dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem, że wdrożone zostaną odpowiednie środki

techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą,

b), aby zapobiec przechowywaniu danych osobowych przez okres dłuższy, niż jest to niezbędne, administrator powinien ustalić termin ich usuwania lub okresowego przeglądu,

Zasada integralności i poufności

Dane osobowe muszą być przetwarzane w sposób zapewniający im odpowiednie bezpieczeństwo i poufność, w tym ochronę przed:

a) niedozwolonym lub niezgodnym z prawem przetwarzaniem- czyli nieuprawnionym dostępem do nich i do sprzętu służącego ich przetwarzaniu oraz przed nieuprawnionym korzystaniem z tych danych i z tego sprzętu,

b) przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych,

Zasada rozliczalności

Administrator jest odpowiedzialny za przestrzeganie powyższych zasad. Musi on być także w stanie wykazać ich przestrzeganie (to po stronie AD leży ciężar dowodu, że przestrzega zasad rozporządzenia RODO) - wynika stąd, że administrator musi być w stanie udowodnić przestrzeganie, opisanego w art. 25 RODO, obowiązku uwzględniania ochrony danych w fazie projektowania oraz zapewnienia domyślnej ochrony danych.

5. POZOSTAŁE ZASADY BEZPIECZEŃSTWA STOSOWANE W AKADEMII WSB

Poniższe zasady stanowią podstawę dla skutecznego zarządzania bezpieczeństwem informacji i są brane pod uwagę przy wprowadzaniu Systemu Bezpieczeństwa w Akademii WSB:

1. **Zasada uprawnionego dostępu**. Każdy pracownik przeszedł szkolenie z zasad ochrony informacji, spełnia kryteria dopuszczenia do informacji i podpisał stosowne oświadczenie o zachowaniu poufności.

2. **Zasada przywilejów koniecznych**. Każdy pracownik posiada prawa dostępu do informacji, ograniczone wyłącznie do tych, które są konieczne do wykonywania powierzonych mu zadań.

3. **Zasada wiedzy koniecznej**. Każdy pracownik posiada wiedzę o systemie, do którego ma dostęp, ograniczoną wyłącznie do zagadnień, które są konieczne do realizacji powierzonych mu zadań.

4 **Zasada świadomości zbiorowej**. Wszyscy pracownicy są świadomi konieczności ochrony zasobów informacyjnych i aktywnie uczestniczą w tym procesie.

5. **Zasada indywidualnej odpowiedzialności**. Za bezpieczeństwo poszczególnych elementów odpowiadają konkretne osoby.

6. **Zasada obecności koniecznej**. Prawo przebywania w określonych miejscach mają tylko osoby upoważnione.

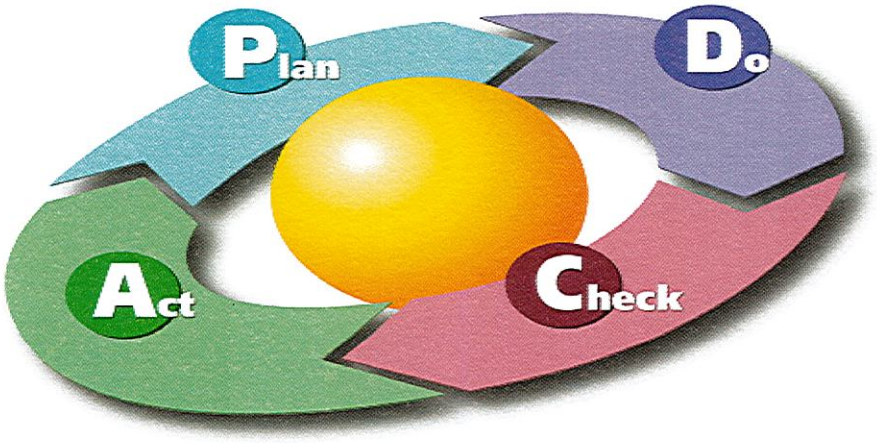
7. **Zasada stałej gotowości**. System jest przygotowany na wszelkie zagrożenia. Niedopuszczalne jest tymczasowe wyłączanie mechanizmów zabezpieczających.

8. **Zasada adekwatności**. Używane środki techniczne i organizacyjne muszą być adekwatne do sytuacji.

9. **Zasada świadomej konwersacji**. Nie zawsze i wszędzie trzeba mówić, co się wie, ale zawsze i wszędzie trzeba wiedzieć co, gdzie i do kogo się mówi.

6. PROCESOWE PODEJŚCIE DO BEZPIECZEŃSTWA INFORMACJI

Zarządzanie bezpieczeństwem informacji jest stałym procesem, wykonywanym zgodnie z cyklem PDCA, opisanym między innymi w normie ISO/IEC 27001:2013 a pierwotnie opisanym przez dr W. Edwarda Deminga.



Rys: Karn G. Bulsuk (http://karnbulsuk.blogspot.com)

Cykl PDCA zakłada cztery powtarzające się fazy ciągłego doskonalenia procesu:

- Faza P (Plan) – planowanie wdrożenia lub doskonalenia polityki bezpieczeństwa, analiza procesów, planowanie budżetu na bezpieczeństwo itp.
- Faza D (Do) – implementacja, wdrożenie polityki bezpieczeństwa, wdrożenie zmian wynikających z procesów pokontrolnych.
- Faza C (Check) – kontrola stanu faktycznego i porównanie go z planowanym, analiza różnic, identyfikacja źródeł niezgodności.
- Faza A (Act) – działanie, wdrożenie potencjalnych działań naprawczych i doskonalenia.

7. PRZEGLĄDY SYSTEMU BEZPIECZEŃSTWA

Zakłada się, że pełen cykl PDCA dla Systemu Bezpieczeństwa nie powinien przekroczyć jednego roku. Założenie to będzie spełnione przez zrealizowanie przeglądu Systemu Bezpieczeństwa raz na 12 miesięcy. Przegląd Systemu Bezpieczeństwa będzie dokonywany przez Administratora Danych oraz Inspektora Ochrony Danych.

8. CELE POLITYKI BEZPIECZEŃSTWA INFORMACJI

Celem Polityki Bezpieczeństwa Informacji jest wskazanie działań, jakie należy wykonać oraz ustanowienie zasad i reguł postępowania, które należy stosować, aby właściwie wykonać obowiązki w zakresie bezpieczeństwa danych.

9. DEKLARACJA REKTOR AKADEMII WSB.

Kierownictwo Akademii WSB mając na uwadze wartość przetwarzanej w Akademii WSB informacji oraz dobro i prawa osób, których dane osobowe przetwarza, pragnie dołożyć szczególnej staranności w ochronę ich interesów. Propaguje aktywne podejście do zarządzania bezpieczeństwem informacji. Kierownictwo deklaruje zaangażowanie w realizację postanowień polityki i propagowanie bezpieczeństwa, w tym bezpieczeństwa informacji wewnątrz organizacji.

10. ZAKRES OBOWIĄZYWANIA POLITYKI BEZPIECZEŃSTWA INFORMACJI

Polityka bezpieczeństwa jest zestawem praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji informacji - danych osobowych. Odnosi się ona do problemów zabezpieczania danych osobowych, zarówno przetwarzanych tradycyjnie, jak i przy wykorzystaniu systemów i technik informatycznych. Polityką Bezpieczeństwa Informacji objęte są wszystkie dane przetwarzane przez organizację, w szczególności dane osobowe zawarte w urządzeniach ewidencyjnych prowadzonych w Akademii WSB, zarówno w formie papierowej, jak i w systemach informatycznych oraz informacje niejawne.

Polityką Bezpieczeństwa Informacji objęte są wszystkie osoby dopuszczone do przetwarzania danych osobowych tj. pracownicy, osoby świadczące pracę na podstawie umowy zlecenia lub o dzieło, praktykanci, stażyści i podmioty zewnętrzne.

11. ODPOWIEDZIALNOŚĆ ZA BEZPIECZEŃSTWO INFORMACJI

Zarządzanie bezpieczeństwem informacji w Akademii WSB opiera się na następującym podziale odpowiedzialności:

1. **Rektor Akademii WSB -** odpowiedzialny jest za zapewnienie zasobów niezbędnych dla opracowania, wdrożenia, funkcjonowania, utrzymania i doskonalenia Systemu Bezpieczeństwa Akademii WSB oraz stosowania poszczególnych zabezpieczeń. Rektor Akademii WSB wykonuje czynności wynikające z RODO i przypisane Administratorowi Danych, w tym zakresie odpowiada za zarządzanie ryzykiem w zakresie naruszeń oraz czynów zabronionych.

2. **Kierownicy komórek organizacyjnych** odpowiadają za:

a. Przestrzeganie zasad ochrony informacji przez nich samych, jak i przez podległych im pracowników.
b. Identyfikowanie i dokumentowanie zagrożeń dla bezpieczeństwa informacji.
c. Definiowanie oraz realizację działań zapobiegających zagrożeniom.
d. Zapoznanie pracowników z obowiązkami związanymi z ochroną informacji na stanowiskach pracy.
e. Przeszkolenie pracowników w zakresie przepisów prawa oraz wewnętrznych zasad przyjętych w pracy Akademii WSB, dotyczących ochrony informacji.

3. W Akademii WSB odpowiedzialność za bezpieczeństwo informacji ponoszą wszyscy pracownicy zgodnie z posiadanymi zakresami obowiązków.
4. Każdy pracownik obowiązany jest dbać o bezpieczeństwo powierzonych mu do przetwarzania, archiwizowania lub przechowywania informacji zgodnie z obowiązującymi w Akademii WSB przepisami wewnętrznymi w tym m. in:

a. Stosować zasady opisane w polityce oraz innych dokumentach wewnętrznych Akademii WSB.
b. Chronić informacje podlegające ochronie przed dostępem do nich osób nieuprawnionych.
c. Chronić dane przed przypadkowym lub umyślnym zniszczeniem, utratą lub modyfikacją.
d. Chronić sprzęt, wydruki komputerowe i inne nośniki zawierające dane chronione,
e. Utrzymywać w tajemnicy powierzone hasła, częstotliwości ich zmiany oraz szczegóły technologiczne systemów także po ustaniu zatrudnienia w Akademii WSB.
f. Stosować się do szczegółowych zaleceń w zakresie ochrony antywirusowej, a także do innych zaleceń wynikających z Systemu Bezpieczeństwa Akademii WSB.
g. Powiadomić Inspektora Ochrony Danych lub bezpośredniego przełożonego o:

- Ujawnieniu lub możliwości ujawnienia informacji chronionych osobom nieupoważnionym.
- Nieautoryzowanej zmianie informacji chronionych lub możliwości wprowadzenia nieautoryzowanych zmian.
- Zniszczeniu lub możliwości zniszczenia informacji chronionych.
- Zablokowaniu lub możliwości zablokowania pracy systemu informatycznego przetwarzającego informacje chronione lub uniemożliwienia innego dostępu do informacji chronionych.

12. STRUKTURA SYSTEMU BEZPIECZEŃSTWA

Administrator Danych

a) wprowadza, zarządza i sprawuje nadzór nad działaniem Systemu Bezpieczeństwa,

b) określa rodzaje zasobów podlegających ochronie,

c) decyduje o celach i środkach przetwarzania danych.

Inspektor Ochrony Danych

a) pełni rolę Inspektora Ochrony Danych zgodnie z RODO

b) analizuje ryzyko bezpieczeństwa danych osobowych,

c) sprawuje nadzór nad realizacją zapisów Polityki Bezpieczeństwa Informacji,

d) analizuje raporty z wszelkich zdarzeń związanych z bezpieczeństwem wszystkich zasobów chronionych,

e) monitoruje zachowanie właściwego poziomu bezpieczeństwa informacji,

f) przedstawia okresowy raport o stanie bezpieczeństwa informacji.

g) wykonuje czynności wynikające z zapisów RODO

Administrator Systemu Informatycznego

a) monitoruje oraz zapewnia ciągłość działania systemu IT,

b) utrzymuje rejestr ważnych aktywów w zakresie systemu informatycznego,

c) utrzymuje konfigurację i wydajność systemu teleinformatycznego,

d) instaluje i konfiguruje sprzęt, systemy i aplikacje,

e) odpowiada za administrację oprogramowaniem systemowym w stopniu umożliwiającym zachowanie bezpieczeństwa systemu i zabezpieczenie danych przed nieupoważnionym dostępem,

f) współpracuje z dostawcami aplikacji,

g) nadzoruje wdrożone aplikacje,

h) zarządza kopiami awaryjnymi danych

i) opracowuje dokumentacje dla systemów teleinformatycznych,

j) opracowuje standardy dotyczące systemów teleinformatycznych,

k) opracowuje procedury określające zarządzanie systemem teleinformatycznym.

13. MIEJSCE /OBSZARY/ PRZETWARZANIA DANYCH OSOBOWYCH

Jako miejsce przetwarzania danych osobowych wyznacza się wszystkie budynki Akademii WSB, w tym pomieszczenia, w których umożliwiono pracę w systemie informatycznym Akademii WSB.

14. PRZETWARZANIE DANYCH OSOBOWYCH

1. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych, nadane przez Administratora Danych. Upoważnienie do przetwarzania danych osobowych uzyskuje osoba, której stanowisko pracy wymaga takiego upoważnienia.
2. Upoważnienie do przetwarzania danych osobowych muszą uzyskać również osoby, pracujące na terenie Akademii WSB, nie będące etatowymi pracownikami Akademii WSB: w tym stażyści i praktykanci, pracownicy podmiotów zewnętrznych oraz inne osoby krótkoterminowo upoważnienie.
3. Zmiana stanowiska pracy, związana z koniecznością uzyskania dostępu do przetwarzania danych osobowych w innych celach niż dotychczas, wymaga unieważnienia dotychczasowego upoważnienia do przetwarzania danych osobowych oraz nadania nowego upoważnienia do przetwarzania danych osobowych. Każdy pracownik Akademii WSB ,który otrzyma upoważnienie do przetwarzania danych osobowych, zobowiązuje się pisemnie do zachowania w tajemnicy tych danych oraz sposobów ich zabezpieczania.

15. WYDAWANIE UPOWAŻNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH

Upoważnienia do przetwarzania danych osobowych w Akademii WSB wydaje Administrator Danych. Upoważnienia dla wszystkich pracowników wydawane są za pośrednictwem Działu Kadr. Upoważnienia dla osób krótkoterminowo upoważnionych mogą być wydawane za pośrednictwem

Inspektora Ochrony Danych. Wydane upoważnienie jest jednocześnie dokumentem upoważniającym Administratora Systemu Informatycznego do założenia profilu użytkownika w ramach danej komórki organizacyjnej w której pracownik będzie wykonywał czynności służbowe.
Upoważnienie wygasa z momentem rozwiązania stosunku pracy lub odpowiedniej umowy oraz z upływem czasu na jaki zostało wydane. Z momentem złożenia podpisu na karcie obiegowej Administrator Systemu Informatycznego usuwa przyznane użytkownikowi uprawnienia do korzystania z systemu, nie usuwając konta i informacji zgromadzonych przez pracownika.

16. SZKOLENIA

Wszyscy pracownicy Akademii WSB przechodzą szkolenia z zakresu bezpieczeństwa informacji, w tym z ochrony danych osobowych. Inspektor Ochrony Danych) lub Administrator Systemu Informatycznego najpóźniej w dniu dopuszczenia do pracy w systemie prowadzi indywidualne szkolenie dla dopuszczanego pracownika. W trakcie szkolenia pracownik zostaje zapoznany z zakresem swoich uprawnień (dotyczy również systemu informatycznego) wynikających z pełnionego stanowiska i potwierdza zrozumienie warunków dostępu do systemu.

17. OPIS SYSTEMÓW INFORMATYCZNYCH

W Akademii WSB funkcjonuje system informatyczny, przetwarzający informacje, w tym dane osobowe, w formie elektronicznej. Przez obszar systemu objęty niniejszą Polityką rozumie się wszelkie urządzenia techniczne niezbędne do funkcjonowania systemu informatycznego w danej jednostce organizacyjnej, w którym wykonywane są zadania związane z wprowadzaniem, przetwarzaniem oraz archiwizowaniem danych osobowych lub korzystaniem ze zbiorów zawierających dane osobowe oraz pomieszczenia, w których te urządzenia się znajdują.

18. STANDARDY AKCEPTOWALNEGO WYKORZYSTYWANIA SPRZĘTU SŁUŻBOWEGO

Każdy pracownik zobowiązany jest do przestrzegania wszelkich regulacji dotyczących obszaru zarządzania bezpieczeństwem informacji. Pracownicy Akademii WSB muszą być świadomi faktu, że wszystkie systemy informatyczne, w tym telekomunikacyjne, są przeznaczone do użytku służbowego i nie zapewniają prywatności w przypadku wykorzystywania ich do celów pozasłużbowych. Obowiązkiem Administratora Systemu Informatycznego jest okresowe przeglądanie systemów, w tym sposobu wykorzystywania ich przez pracowników i działania pozasłużbowe nie są wyłączone z takich przeglądów. Zakłada się wykorzystanie systemów jedynie dla celów służbowych.

19. PRACOWNICY AKADEMII WSB NIE MOGĄ WYKORZYSTYWAĆ SPRZĘTU SŁUŻBOWEGO:

- Do działań sprzecznych z przepisami prawa, w tym do przechowywania, przetwarzania lub przesyłania materiałów nielegalnych (w rozumieniu prawa autorskiego, kodeksu karnego innych obowiązujących przepisów prawa).
- Do przesyłania lub wyświetlania materiałów, które mogą narazić inne osoby na otrzymanie lub zobaczenie treści dla nich obraźliwych lub krzywdzących.
- Do podszywania się pod inne osoby lub systemy.
- Do prób uzyskania informacji, do której nie mają dostępu z racji pełnionych funkcji i obowiązków na nich nałożonych (stanowi to naruszenie zasady wiedzy koniecznej).
- Do podłączania nieautoryzowanych urządzeń do sieci Akademii WSB.
- Do nieautoryzowanego (samodzielnego) odłączania lub przenoszenia urządzeń IT.
- Do samodzielnego instalowania nieautoryzowanego przez organizację oprogramowania.

20. OPIS ZAGROŻEŃ:

Do najważniejszych zagrożeń związanych z bezpieczeństwem informacji należą:

- Kradzież, zniszczenie lub zagubienie dokumentacji, w tym dokumentacji w formie elektronicznej, za pomocą której osoba nieuprawniona może doprowadzić do naruszenia lub czynu zabronionego, zgodnie z wytycznymi RODO
- Kradzież sprzętu elektronicznego: komputera, notebooka, pendrive'u zawierającego dane wrażliwe,
- Obecność wirusa komputerowego,
- Pozostawienie niezabezpieczonych dokumentów,
- Pozostawienie otwartego pomieszczenia podczas nieobecności pracowników,
- Włamanie do pomieszczenia Akademii WSB.
- Wyciek informacji do osób nieupoważnionych.
- Udostępnienie dokumentów osobie nieuprawnionej.

21. SPOSOBY ZABEZPIECZANIA INFORMACJI

21.1. KONTROLA DOSTĘPU DO SYSTEMU INFORMATYCZNEGO

1. Każda osoba upoważniona do przetwarzania danych w systemie informatycznym, posiada konto użytkownika zakładane przez Administratora Systemu Informatycznego
2. Każde nowe konto użytkownika systemu, jak również wszelkie zmiany w zakresie kont wykonywane są na pisemny wniosek Kierownika komórki organizacyjnej, kierowany do Administratora Systemu Informatycznego. Dopuszczalna jest informacja mailowa.
3. W ramach utworzonego konta, użytkownik otrzymuje identyfikator oraz hasło dostępu.

4. System informatyczny Akademii WSB wymusza zmianę haseł dostępu nie rzadziej niż co 30 dni.

5. Pracownik jest zobowiązany do zmiany hasła dostępu na kolejny miesiąc w odpowiednim terminie. Konieczność zmiany hasła jest sygnalizowana przez system

6. Hasło należy zachować w tajemnicy i zabezpieczyć przed dostępem osób trzecich.

7. Zabrania się przekazywania haseł dostępu innym pracownikom Akademii WSB, a także – zwłaszcza - osobom niezwiązanym z organizacją pod rygorem zastosowania odpowiedzialności dyscyplinarnej, wynikającej z przepisów określonych w Rozdziale IV Ustawy Kodeks Pracy.

8. Zabrania się zapisywania haseł w miejscach umożliwiających przejęcie przez osoby nieupoważnione oraz umożliwiających identyfikację właściciela, użytkownika systemu.

9. Konieczne jest wykonywanie swoich obowiązków pracy w ramach własnego konta użytkownika. Niedopuszczalne jest korzystanie z jednego konta użytkownika przez wiele osób.

10. Odpowiedzialność za wprowadzenie do systemu informacji błędnych, niezgodnych z prawem lub też zagrażających Akademii WSB, będzie nakładana na właścicieli kont, niezależnie od faktu, czy zostały one przez niego wprowadzone.

11. Administrator Systemu Informatycznego zobowiązany jest do niezwłocznego informowania Administratora Danych za pośrednictwem Inspektora Ochrony Danych o każdorazowym przypadku nieprzestrzegania powyższych zapisów.

21.2. ZASADY DOTYCZĄCE KONT I HASEŁ

- Minimalna długość hasła: 8 znaków
- Maksymalny czas życia hasła: 30 dni
- Ilość nieudanych prób logowania przed zablokowaniem konta: 5 prób
- Zasady złożoności hasła:

- Nie mogą zawierać nazwy konta użytkownika ani części jego pełnej nazwy dłuższej niż dwa kolejne znaki.
- Muszą zawierać znaki z trzech spośród następujących czterech kategorii:
- Wielkie litery angielskie (od A do Z)
- Małe litery angielskie (od a do z)
- Cyfry systemu dziesiętnego (od 0 do 9)
- Znaki niealfabetyczne (na przykład!, $, #, %)
- Wymagania dotyczące złożoności są wymuszane podczas zmienienia lub tworzenia hasła.

21.3. POLITYKA CZYSTEGO BIURKA I CZYSTEGO EKRANU

Obowiązkiem pracowników Akademii WSB jest zadbanie, aby informacje wrażliwe, w tym dane osobowe, nie były udostępnione osobom nieuprawnionym. Polityka czystego biurka oznacza, że informacje wrażliwe nie mogą zostać na biurku podczas nieobecności pracownika – musi on wcześniej odpowiednio je zabezpieczyć (np. przez schowanie ich w szafce zamykanej na zamek). Polityka czystego ekranu oznacza obowiązek zablokowania ekranu komputera przed odejściem od niego, poprzez stosowanie, wygaszacza ekranu chronionego hasłem z czasem ustawionym na okres nie dłuższy niż 10 minut.

21.4. ZARZĄDZANIE INCYDENTAMI I NARUSZENIAMI

Wszelkie incydenty noszące znamiona naruszenia polityki bezpieczeństwa (a więc w szczególności noszące znamiona intencjonalnych działań mających na celu narażenie informacji wrażliwych na nieuprawnione ujawnienie, uniemożliwienie dostępu do nich lub spowodowanie naruszenia ich integralności) są zgłaszane przez pracowników Akademii WSB do Inspektora Ochrony Danych. Zgłoszenie incydentu może nastąpić w formie bezpośredniej wypowiedzi, telefonicznie lub mailowo. Inspektor Ochrony Danych weryfikuje czy zgłoszenie jest zgłoszeniem incydentu w myśl

przyjętego Systemu Bezpieczeństwa Akademii WSB. Po potwierdzeniu przez Inspektora Ochrony Danych, iż zgłoszone odstępstwo jest incydentem Inspektor Ochrony Danych, podejmuje następujące działania:

- Informuje kierownictwo Akademii WSB o zaistniałym incydencie.
- Weryfikuje przyczyny wystąpienia incydentu.
- Sprawdza czy podczas incydentu nie doszło do naruszenia danych osobowych wrażliwych opisanych w art. 9 i art. 10 RODO.
- Weryfikuje czy podczas incydentu nie doszło do czynu zabronionego w oparciu o dane osobowe Akademii WSB.
- Wprowadza działania korygujące mające na celu niedopuszczenie do powtórzenia incydentu.
- Informuję osobę zgłaszającą incydent o procedurze skorygowania incydentu.
- O ile to konieczne informuje pracowników Akademii WSB o zaistniałym incydencie i jego skutkach dla Systemu Bezpieczeństwa Informacji oraz dla Akademii WSB.

22. KONSEKWENCJE NARUSZANIA POLITYKI BEZPIECZEŃSTWA INFORMACJI

Przypadki nieuzasadnionego zaniechania obowiązków wynikających z obowiązującej Polityki Bezpieczeństwa Akademii WSB mogą być potraktowane jako celowe naruszenie obowiązków pracownika. Wyciągnięte konsekwencje służbowe nie wykluczają możliwości wniesienia sprawy z powództwa cywilnego o naprawienie szkody.

R E K T O R
dr Zdzisława Dacko-Pikiewicz, prof. AWSB

AKADEMIA WSB
ul. Cieplaka 1c
41-300 Dąbrowa Górnicza
Tel. 32 262 28 05
-1-

INSTRUKCJA BEZPIECZEŃSTWA SYSTEMU TELEINFORMATYCZNEGO AKADEMII WSB

II. INSTRUKCJA BEZPIECZEŃSTWA SYSTEMU TELEINFORMATYCZNEGO

Dokument spełnia wymagania 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).

1. CELE INSTRUKCJI BEZPIECZEŃSTWA SYSTEMU TELEINFORMATYCZNEGO

Celem Instrukcji jest wskazanie działań, jakie należy wykonać oraz ustanowienie zasad i reguł postępowania, które należy stosować, aby właściwie wykonać obowiązki w zakresie przetwarzania danych osobowych w systemach informatycznych Akademii WSB.

2. ODPOWIEDZIALNOŚĆ ZA BEZPIECZEŃSTWO I ZARZĄDZANIE SYSTEMAMI

Administrator Danych – odpowiedzialny jest za zabezpieczenia systemu informatycznego oraz dopuszczenie osób do pracy w systemie. Administrator Danych formalnie inicjuje kontrolę systemu informatycznego.

Administrator Bezpieczeństwa Informacji (docelowo Inspektor Ochrony Danych) jest upoważniony do:

a) prowadzenia kontroli prawidłowości przestrzegania Instrukcji Bezpieczeństwa Systemu Teleinformatycznego w całym zakresie jej obowiązywania,

b) wprowadzania zaleceń oraz wydawania poleceń dla wszystkich osób dopuszczonych do systemu – w zakresie niesprzecznym z niniejszą Instrukcją,

Inspektor Ochrony Danych odpowiada również za zabezpieczenie obsługi systemów przez **Administratora Systemu Informatycznego** w przypadku uszkodzenia, awarii lub naruszenia bezpieczeństwa systemu.

Obowiązki **Administratora Systemu Informatycznego**:

a) wykonywanie czynności wynikających z niniejszej Instrukcji w zakresie zabezpieczenia prawidłowego i bezpiecznego funkcjonowania bazy technicznej i oprogramowania, wykonywanie czynności wynikających z niniejszej Instrukcji, związanych z zapewnieniem bezpieczeństwa systemu informatycznego, w tym:

- wprowadzenia lub usuwanie prawa dostępu do systemu informatycznego dla poszczególnych pracowników na podstawie upoważnienia do przetwarzania danych osobowych,
- opracowania systemu haseł do poszczególnych obszarów systemu,
- zapewnienia konfiguracji systemu uniemożliwiającej wprowadzanie lub uzyskiwanie danych z systemu przez niepowołane osoby,
- przeprowadzanie kontroli systemu informatycznego z polecenia Inspektora Ochrony Danych,
- monitorowanie bezpieczeństwa dla serwerów oraz urządzeń aktywnych sieci,
- opracowywanie tematyki szkoleń z zakresu systemu oraz urządzeń dla użytkowników systemu – ze szczególną dbałością o wiedzę z zakresu bezpieczeństwa systemów.
- czuwanie zgodnie z wytycznymi niniejszej Instrukcji nad prawidłowością postępowania z nośnikami zawierającymi dane systemu,
- prowadzenie rzetelnej dokumentacji systemu i czuwanie nad prawidłowością sporządzania tej dokumentacji przez inne osoby,
- zapewnienie stałego kontaktu ze sobą lub osobą wskazaną, zaś w przypadku wyjazdów lub niemożności wykonywania swoich obowiązków, powiadomienie o tym fakcie Inspektora Ochrony Danych.

Administrator Systemu Informatycznego posiada następujące kompetencje:

a) przeprowadzanie kontroli systemu informatycznego,

b) podejmowanie kroków zaradczych, w tym wyłączanie systemu lub częściowe ograniczanie dostępu do niego, jeżeli w jego ocenie istnieje zagrożenie dla prawidłowego funkcjonowania systemu lub bezpieczeństwa danych w nim się znajdujących.

a) Użytkownik Systemu

Użytkownikiem systemu jest osoba, która w ramach swoich obowiązków służbowych korzysta z systemu informatycznego w Akademii WSB. Dopuszczenia użytkownika do systemu dokonuje Administrator Systemu Informatycznego.

3. OPIS SYSTEMU

1. Przez obszar systemu objęty niniejszą Instrukcją rozumie się wszelkie urządzenia techniczne, systemy oraz aplikacje niezbędne do funkcjonowania systemu informatycznego w Akademii WSB, w którym wykonywane są zadania związane z wprowadzaniem, przetwarzaniem oraz archiwizowaniem danych osobowych lub korzystaniem ze zbiorów zawierających dane osobowe oraz pomieszczenia, w których te urządzenia się znajdują.

4. SPOSÓB UŻYTKOWANIA SYSTEMU

1. System informatyczny eksploatowany jest na komputerach wolnostojących i przenośnych podłączonych do sieci lokalnej Akademii WSB.
2. Dołączanie do systemu innych urządzeń teletransmisyjnych, nie należących do struktury sieci musi zostać zgłoszone do Administratora Systemu Informatycznego.
3. Podłączenie prywatnego komputera lub komputera przenośnego wymaga uzyskania zezwolenia Administratora Danych.
4. Dostęp do poszczególnych obszarów systemu jest zabezpieczony za pomocą haseł według hierarchii dostępu opracowanej przez Administratora Systemu Informatycznego, sprawdzonej pod względem formalnym przez Administratora Bezpieczeństwa Informacji.

5. W szczególności zabezpieczeniom za pomocą haseł podlega:

a) dostęp do serwerów sieciowych,

b) dostęp do urządzeń aktywnych sieci,

c) dostęp do konfiguracji serwerów,

d) dostęp do konfiguracji stacji roboczych,

e) dostęp do systemu dla poszczególnych użytkowników systemu,

6. Konfiguracja serwerów oraz aplikacji zapewniają odporność systemu na zanik zasilania energetycznego lub inne przypadkowe uszkodzenia poszczególnych stacji roboczych.

7. W szczególności:

a) Serwery są zasilane wyłącznie przez urządzenia zasilające UPS.

b) Za prawidłowość podłączenia, monitorowanie stanu baterii odpowiada Administrator Systemu Informatycznego.

c) Konfiguracja serwerów zapewnia automatyczne bezpieczne wyłączanie serwera w wypadku zaniku zasilania energetycznego, dłuższego niż czas podtrzymania dobranego UPS.

d) Administrator Systemu Informatycznego odpowiedzialny jest za wykonanie przynajmniej jednego próbnego zamknięcia awaryjnego systemów w kwartale.

8. Konfiguracja w systemie musi zapewnić odnotowanie w systemie faktu rozpoczęcia pracy przez każdego z użytkowników, Wykaz logów podlega zabezpieczeniu łącznie z danymi systemu.

9. Konfiguracja systemów powinna zapewniać możliwość pozyskania informacji o realizacji praw osób fizycznych, w tym prawa do: dostępu do danych, modyfikacji danych, kopiowania danych, przenoszenia danych, usunięcia danych.

5. BEZPIECZEŃSTWO ZARZĄDZANIA SYSTEMU TELEINFORMATYCZNEGO:

5.1. KOPIE BEZPIECZEŃSTWA

1. Użytkownicy są świadomi, że archiwizacji podlegają dane zapisane na dyskach sieciowych udostępnianych na potrzeby poszczególnych komórek organizacyjnych oraz dysków prywatnych użytkowników zlokalizowanych na dysku sieciowym. Z dysków tych wykonywana jest codzienna pełna kopia.
2. Administrator Systemu Informatycznego konfiguruje kopie w ten sposób, że po zakończeniu pracy Akademii WSB dane z serwera plików i serwerów bazodanowych są przenoszone na serwer kopii zapasowych. Z serwera kopii zapasowych prowadzony jest pełen zapisanych na dysk zewnętrzny.
3. Wszystkie kopie bezpieczeństwa i backupy powinny być zlokalizowane w innej strefie pożarowej budynku Akademii WSB.

5.2. ZABEZPIECZENIE ANTYWIRUSOWE

1. Za politykę antywirusową odpowiedzialny jest Administrator Systemu Informatycznego.
2. Program antywirusowy i konfiguracja systemu zapewniają kontrolę całego systemu informatycznego:
   a) na bieżąco,
   b) przynajmniej raz dziennie, jeżeli z przyczyn technicznych nie możliwe jest jej zapewnienie na bieżąco,
   c) każdorazowo przy korzystaniu z nośników wymienialnych,

5.3. KORZYSTANIE Z POCZTY ELEKTRONICZNEJ

1. Poczta elektroniczna może być wykorzystywana tylko do celów służbowych.
2. Zabrania się rozsyłania m.in.:
   a) ogłoszeń komercyjnych,

b) tzw. łańcuszków szczęścia (listów, które wykorzystując elementy socjotechniki generują niepożądany ruch na serwerach poczty elektronicznej),
c) treści wulgarnych,
d) materiałów erotycznych,
e) treści niezgodnych z obowiązującymi przepisami prawa,
f) treści prawem chronionych bez odpowiedniego zabezpieczenia np. szyfrowanie.

3. Korespondencja, którą przechowuje i dostarcza system pocztowy jest własnością Pracodawcy. Pracodawca w celach dowodowych oraz bezpieczeństwa systemów ma prawo do kontroli skrzynek pocztowych użytkowników. O wynikach kontroli powinien być poinformowany użytkownik.

4. Korespondencja elektroniczna, jak i pliki mogą zostać udostępnione innemu pracownikowi. Czynności tej dokonać można na pisemny wniosek przełożonego pracownika, którego dane mają zostać udostępnione. We wniosku wskazuje się powód udostępnienia oraz osobę, której udostępnia się opisywane zasoby.

5. Pracodawca rezerwuje sobie prawo natychmiastowej blokady skrzynki pocztowej w uzasadnionych przypadkach. Nadzór i opiekę techniczną nad systemem poczty elektronicznej sprawuje ASI.

5.4. KORZYSTANIE Z SIECI INTERNET

1. Użytkownicy mogą korzystać z dostępu do Internetu tylko w celach służbowych a praca w sieci Internet nie może zagrażać bezpieczeństwu systemów informatycznych.

2. Pracodawca może wprowadzić kategoryzację stron internetowych oraz zablokować dostęp do wybranych kategorii.

3. Zabrania się:
a) wykorzystywania sieci Internet w sposób, który mógłby narazić organizację na utratę dobrego imienia,

b) pobierania oprogramowania (w tym w wersjach darmowych), nie związanego z wykonywanymi obowiązkami służbowymi,

c) instalowania urządzeń udostępniających Internet na sprzęcie Pracodawcy bez zgody Administratora Systemu Informatycznego.

R E K T O R
dr Zdzisława Dacko-Pikiewicz, prof. AWSB

AKADEMIA WSB
ul. Cieplaka 1c
41-300 Dąbrowa Górnicza
Tel. 32 262 28 05
-1-