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-