Instrukcja zarządzania Systemami Informatycznymi

—

Wykaz zabezpieczeń RODO

w Państwowej Wyższej Szkole Techniczno-Ekonomicznej im. ks. Bronisława Markiewicza w Jarosławiu

REKTOR

prof. ucz. dr hab. Krzysztof Rejman

Spis treści

1. Wstęp

Instrukcja stanowi wykaz procedur oraz stosowanych środków technicznych i organizacyjnych mających na celu, zgodnie z Art. 32 RODO, zabezpieczyć przetwarzane dane osobowe przed: przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych oraz nieuprawnionym dostępem do danych osobowych.

2. Zabezpieczenia fizyczne

1. zabezpieczono dostęp do kluczowej infrastruktury w postaci budynków/ pomieszczeń biurowych /archiwum/serwerowni, miejsc przechowywania kopii bezpieczeństwa,
2. funkcjonuje portiernia,
3. wdrożono zasadę dostępu osób nieupoważnionych do miejsc przetwarzania danych wyłącznie w obecności osoby upoważnionej (praca personelu sprzątającego w godzinach pracy i w obecności osób upoważnionych),
4. rozmieszczenie komputerów /drukarek ogranicza dostęp osób nieupoważnionych,
5. ograniczenie fizycznego dostępu do miejsc, gdzie znajdują się nienadzorowane gniazdka sieciowe (np. sale konferencyjne, korytarze),
6. krytyczne elementy infrastruktury zabezpieczono w zamykanych na klucz szafach serwerowych,
7. rozdzielnie elektryczne zabezpieczono w szafach zamykanych na klucz,
8. dostęp do pomieszczeń (w tym biurowych) zabezpieczono drzwiami zamykanymi na klucz,
9. dostęp do serwerowni zabezpieczono drzwiami zamykanymi na klucz,
10. dostęp do archiwum zabezpieczono drzwiami zamykanymi na klucz,
11. dostęp do dokumentacji/danych w pomieszczeniach zabezpieczono w zamkniętych metalowych szafach,
12. obiekt/pomieszczenia chronione są przez system monitorujący,
13. zapewniono ochronę obiektu - ochrona własna / firma ochroniarska,
14. stosowana jest Polityka kluczy.

3. Zabezpieczenia techniczne

1. Zastosowano UPS podtrzymujący zasilanie serwerów oraz UPS dla kluczowych urządzeń sieciowych.
2. Zastosowano monitoring wizyjny w obrębie obiektu i w otoczeniu.
3. Serwerownia wyposażona w gaśnice.
4. Monitoring środowiskowy w serwerowni – czujnik temperatury.
5. Powiadamianie administratora systemu informatycznego o alertach temperatury.
6. Klimatyzacja w serwerowni.

PR

7. Monitoring środowiskowy w archiwum – czujnik wilgotności.
8. Digitalizacja dokumentów archiwalnych.

4. Procedura nadawania uprawnień do przetwarzania danych osobowych.

Celem procedury jest minimalizacja ryzyka przetwarzania danych przez osoby nieupoważnione.

1. Dostęp do systemu informatycznego (np. stacji roboczej, dysku sieciowego, programu lub aplikacji, poczty elektronicznej) nadawany jest każdemu użytkownikowi w formie indywidualnego identyfikatora (loginu) oraz hasła.
2. Każdemu użytkownikowi uprzywilejowanemu (administratorowi) nadawane jest indywidualne konto administracyjne. Nadawanie uprawnień administratora wynika z zakresu czynności Działu Informatyki.
3. Nadawanie, zmiana, odbieranie uprawnień użytkownika do zasobów i aplikacji odbywa się na pisemne polecenie kierownika komórki organizacyjnej.
4. Za wykonanie czynności nadawania, zmiany, odbierania uprawnień użytkownikowi odpowiada administrator systemu informatycznego.
5. Obowiązuje zasada minimalizacji uprawnień.
6. Identyfikator użytkownika po wyrejestrowaniu z systemu informatycznego nie może być przydzielany innej osobie.
7. Użytkowników obowiązuje zasada pracy na własnym koncie. Zabronione jest umożliwianie innym osobom pracy na koncie innego użytkownika. Zasada ta obowiązuje również administratorów systemów
8. W przypadku pracy z uprawnieniami użytkownika uprzywilejowanego, każdy Administrator systemu zobowiązany jest do bieżącej pracy na koncie roboczym. Użycie tzw. konta administracyjnego (np. "root" lub "admin") dopuszczalne jest jedynie w sytuacjach awaryjnych lub podczas poważnych zmian wprowadzanych w administrowanym systemie.

5. Metody i środki uwierzytelnienia

Celem procedury jest zapewnienie, że do systemów informatycznych przetwarzających dane osobowe mają dostęp jedynie osoby do tego upoważnione.

1. Pierwsze (pierwotne) hasło użytkownika nadawane jest przez Administratora i przekazywane mu w poufny sposób.
2. Obowiązuje polityka haseł opisana w Regulaminie Ochrony Danych.
3. Zastosowano mechanizm blokady dostępu po 10 próbach nieudanego logowania się.
4. Hasła administracyjne zdeponowane są w sejfie (lub w innym bezpiecznym miejscu).
5. W przypadku utraty uprawnień przez osobę administrującą systemem należy niezwłocznie zmienić hasła, do których miała dostęp.

06

6. W przypadkach awaryjnych (np. nieobecność administratora) hasło może być przekazane decyzją Kierownika Działu Informatyki osobie zastępującej administratora.
7. Po ustaniu sytuacji awaryjnej, Administrator jest zobowiązany do zmiany hasła.

6. Procedura tworzenia kopii zapasowych

1. Kopie zapasowe serwera (z zawartością plików i baz danych) tworzone są w sposób zautomatyzowany w oparciu o system kopii przyrostowych.
2. Kopie przyrostowe tworzy się codziennie po godzinie 22:00
3. Kopie całościowe sporządzane zgodnie z regułami tworzenia kopii przyrostowych nie rzadziej, niż co 14 dni.
4. Dane z bazy danych, w formacie exportu są sporządzane, co miesiąc i zapisywane na nośniku optycznym.
5. Kopie sporządzane są na wydzielonym serwerze NAS.
6. Dział Informatyki sprawuje nadzór nad prawidłowością wykonania kopii zapasowych.
7. Kopie zapasowe przechowywane są w zabezpieczonym miejscu, innym niż miejsce przechowywania oryginału.
8. Niszczenie nośników z kopiami odbywa się komisyjnie. Nośniki niszczone są przez fizyczne zniszczenie.

7. Utylizacja elektronicznych nośników i wydruków oraz czyszczenie danych

1. Podlegające likwidacji uszkodzone lub przestarzałe nośniki a szczególności macierze dyskowe/twarde dyski z danymi osobowymi ze stacji roboczych i laptopów/ pendrive /pamięci flash / dyski SSD / płyty DVD / telefony komórkowe / smartfony są niszczone w sposób fizyczny w tym również komisyjnie, zakończone sporządzeniem protokołu (wzór protokołu niszczenia dokumentów stanowi załącznik do niniejszej instrukcji). Stosowana metoda niszczenia, to fizyczne niszczenie (pocięcie, nawiercenie, młotkowanie) wymontowanych nośników / użycie degaussera /zmielenie w specjalistycznej firmie potwierdzone protokołem zniszczenia lub certyfikatem bezpieczeństwa firmy utylizacyjnej lub nagraniem z procesu transportu i utylizacji.
2. Nośniki informacji zamontowane w sprzęcie IT a w szczególności twarde dyski muszą być wyczyszczone specjalistycznym oprogramowaniem zanim zostaną przekazane poza obszar organizacji (np. sprzedaż lub darowizna komputerów stacjonarnych/ laptopów/smartfonów).
3. Dokumentacja papierowa niszczona jest w niszczarkach.

PR

8. Procedura zabezpieczenia systemu informatycznego

8.1. Ochrona przed nieautoryzowanym dostępem do sieci lokalnej

Stosowane zabezpieczenia mają na celu zabezpieczenie systemów informatycznych przed nieautoryzowanym dostępem do sieci lokalnej.

1. Dokonuje się aktualizacji oprogramowania (firmware / sterowniki) urządzeń sieciowych oraz innych (np. w urządzeniach jak: routery, switche, access pointy, firewalle, macierze, dyski NAS, drukarki, skanery)
2. Dokonywana jest konfiguracja urządzeń sieciowych oraz innych (routery, switche, access pointy, firewalle, macierze, dyski NAS, drukarki, skanery) w celu zabezpieczenia przed nieuprawnionym dostępem do nich (np. zmiana domyślnych haseł na urządzeniach, zmiana domyślnych nazw kont administratora w urządzeniach, konfiguracja portów na routerze).
3. Dokonuje się aktualizacji oprogramowania systemów i aplikacji (systemy operacyjne) na stacjach roboczych/ systemy operacyjne serwerów/przeglądarki www. Aktualizacja dokonywana jest zgodnie z zaleceniami producentów oraz opinią rynkową, co do bezpieczeństwa i stabilności nowych wersji (np. aktualizacje, service pack-i, łatki).
4. Monitoring usług sieciowych, np.: DHCP, DNS, SSH, htpp, telent, FTP, SMTP, SNMP oraz utrzymuje się niezbędne usługi oraz dezaktywuje pozostałe.
5. Zastosowano system antywirusowy (na serwerze, na stacjach roboczych).
6. Zastosowano filtr antyspamowy.
7. Stosowany jest Firewall sprzętowy zintegrowany z routerem oraz programowy na serwerach.
8. Zastosowano mechanizmy kontroli dostępu do sieci w postaci IDS/IPS do wykrywania i blokowania ataków do sieci komputerowej, technikę NAT.
9. Sieć bezprzewodową zabezpieczono.
10. Zabezpieczenie baz i katalogów webowych przed indeksacją wyszukiwarek.

8.2. Zabezpieczenia infrastruktury IT

1. Zapewniono redundantne łącze internetowe.
2. Serwery wyposażono w macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej.
3. Zastosowano wirtualizację serwera.
4. Zastosowano redundantne serwery dla wirtualizacji.
5. Zastosowano blokadę zapisu na nośnikach wymiennych (USB, nośniki optyczne) na stacjach roboczych.
6. Dokonano dezaktywacji nieużywanych gniazd sieciowych (np. przez wypięcie przewodów lub wyłączenie portów na switchu).
7. Drukarki ogólnodostępne z funkcją kontroli wydruków (PIN).

8. Na stacjach roboczych zastosowano „zahasłowane wygaszacze ekranu", aktywowane po 5 minutach nieaktywności użytkownika.
9. Ustawienie monitorów uniemożliwiające wgląd w dane przez osoby postronne.

8.3. Zabezpieczenia aplikacji

1. Zapewniono rozliczalność operacji dla pracy w kluczowych aplikacjach / bazach / serwerach plików.
2. W ramach rozliczalności logowane są operacje tworzenia, zmiany (historii zmian), usuwania rekordu, wglądu w dane, eksportu danych do plików.
3. Zabezpieczono interfejsy programistyczne poprzez zmianę domyślnych loginów i haseł/ wyłączenie dostępu zdalnego, gdy nie jest wymagany.
4. Zabezpieczenie testowych wersji aplikacji poprzez zmianę domyślnych loginów i haseł/ wyłączenie dostępu zdalnego, gdy nie jest wymagany.
5. W kluczowych aplikacjach stosuje się terminację sesji.
6. Stosuje się szyfrowanie poczty wychodzącej (SSL).
7. Dla aplikacji webowych stosowane jest szyfrowanie połączeń internetowych z użyciem protokołu SSL.
8. Formularze kontaktowe na stronach www zabezpieczono protokołem SSL.

9. Procedura naprawy w serwisach zewnętrznych.

1. Dział Informatyki odpowiada za sprawdzenie poprawności działania systemu IT, w tym: stacji roboczych, serwerów, drukarek, baz danych, aplikacji, poczty elektronicznej.
2. Dział Informatyki odpowiada za identyfikację i przyjmowanie zgłoszeń o nieprawidłowościach w działaniu systemu informatycznego oraz oprogramowania celem ich niezwłocznego usunięcia.
3. W przypadku napraw dokonywanych na zewnątrz (z komputerów należy uprzednio wymontować dyski i wszelkie nośniki, z urządzeń mobilnych karty pamięci, usunąć dane z nośnika z użyciem specjalistycznego oprogramowania).
4. W przypadku naprawy sprzętu z danymi osobowymi na nośniku - rekomendowane jest zawarcie specjalnego zapisu w umowie serwisowej, gwarantującego bezpieczną naprawę (należy na to zwrócić uwagę przy zakupach sprzętu).
5. W przypadku naprawy sprzętu z danymi osobowymi na nośniku - rekomendowane jest przekazywanie do naprawy uszkodzonego sprzętu z danymi zaszyfrowanymi na dysku / karcie pamięci. Sprzęt przekazywany jest do serwisu bez podania hasła.
6. Rekomendowane jest korzystanie z serwisu, który dokonuje napraw u klienta (umowy gwarancyjne on-site).

PR

7. Czynności konserwacyjne i naprawcze wykonywane przez osoby nieposiadające upoważnień do przetwarzania danych (np. specjalistów z firm zewnętrznych) muszą być wykonywane pod nadzorem osób upoważnionych.
8. Wszelkie prace konserwacyjne i naprawcze sprzętu komputerowego oraz uaktualnienia systemu informatycznego wykonywane przez podmiot zewnętrzny, powinny odbywać się na zasadach określonych w szczegółowej umowie z uwzględnieniem klauzuli dotyczącej ochrony danych.

10. Procedura wykonywania przeglądów i konserwacji

1. Stosowany jest system wykrywania słabości i zagrożeń (Skanery podatności).
2. Stosowany jest system do monitoringu aktywności użytkowników.
3. Dział Informatyki jest odpowiedzialny za monitoring/przegląd logów aktywności aplikacji/baz.
4. Dział Informatyki jest odpowiedzialny za monitoring/przegląd logów aktywności oraz uprawnień użytkowników i administratorów.
5. Dział Informatyki odpowiada za optymalizację zasobów serwerowych, wielkości pamięci i dysków pamięci, optymalizację baz danych.
6. Dział Informatyki odpowiada za sprawdzanie poprawności działania systemu IT w tym: stacji roboczych, serwerów, drukarek, baz danych, aplikacji, poczty email.
7. Dział Informatyki odpowiada za identyfikację i przyjmowanie zgłoszeń o nieprawidłowościach w działaniu systemu informatycznego oraz oprogramowania celem ich niezwłocznego usunięcia.

PR