Przez bezpieczeństwo informacji w systemach IT PRIS SYSTEM Sp. z o.o. rozumie się zapewnienie:

1. Poufności informacji (uniemożliwienie dostępu do danych osobom trzecim).
2. Integralności informacji (uniknięcie nieautoryzowanych zmian w danych).
3. Dostępności informacji (zapewnienie dostępu do danych, w każdym momencie żądanym przez autoryzowanego użytkownika)
4. Rozliczalności operacji wykonywanych na informacjach (zapewnienie przechowywania pełnej historii dostępu do danych, wraz z informacją kto taki dostęp uzyskał).

Zarząd Firmy stosuje adekwatne do sytuacji środki aby zapewnić bezpieczeństwo informacji w Firmie.

- Oznaczanie danych

Jako dane podlegające szczególnej ochronie (informacje poufne) rozumie się:

- informacje o realizowanych kontraktach (zarówno planowane, bieżące jak i historyczne),
- informacje finansowe Firmy,
- dane dostępowe do systemów IT,
- dane osobowe,
- informacje stanowiące o przewadze konkurencyjnej Firmy,
- inne informacje oznaczone jako „informacji poufne" lub „dane poufne".

Zasada minimalnych uprawnień:

W ramach nadawania uprawnień do danych przetwarzanych w systemach IT Firmy należy stosować zasadę „minimalnych uprawnień", to znaczy przydzielać minimalne uprawnienia, które są konieczne do wykonywania pracy na danym stanowisku.

Zasada wielowarstwowych zabezpieczeń:

System IT Firmy powinien być chroniony równolegle na wielu poziomach. Zapewnia to pełniejszą oraz skuteczniejszą ochronę danych.

Zasada ograniczania dostępu

Domyślnymi uprawnieniami w systemach IT powinno być zabronienie dostępu. Dopiero w przypadku zaistnienia odpowiedniej potrzeby, administrator IT przyznaje stosowne uprawnienia.

Dostęp do danych poufnych na stacjach PC.

- Dostęp do danych poufnych w LAN realizowany jest na przeznaczonych do tego serwerach.
- Dostęp do danych poufnych (udany lub nieudany) na serwerach jest odnotowywany.
- Jeśli stacja PC jest komputerem przenośnym (laptopem) to musi ona być dodatkowo.
- Dostęp do danych poufnych z zewnątrz firmy powinien odbywać się z wykorzystaniem kanału szyfrowanego (np. VPN, dostęp do e-mail poprzez protokół szyfrowany).
- Dostęp do danych poufnych poprzez firmową sieć WiFi powinien odbywać się z wykorzystaniem kanału szyfrowanego (np. VPN).

Zabezpieczenie stacji roboczych

- Stacje robocze powinny być zabezpieczone przed nieautoryzowanych dostępem osób trzecich.
- Minimalne środki ochrony to:
    - zainstalowane na stacjach systemy typu: firewall oraz antywirus,
    - wdrożony system aktualizacji systemu operacyjnego oraz jego składników,
    - wymaganie podania hasła przed uzyskaniem dostępu do stacji,
    - niepozostawianie niezablokowanych stacji PC bez nadzoru,
    - bieżąca praca z wykorzystaniem konta nieposiadającego uprawnień administracyjnych.

Wykorzystanie haseł

- Hasła powinny być okresowo zmieniane.
- Hasła nie mogą być przechowywane w formie otwartej (nie zaszyfrowanej).
- Hasła nie powinny być łatwe do odgadnięcia, to znaczy:
    - powinny składać się z minimum 9 znaków, w tym jeden znak specjalny
    - nie mogą przybierać prostych form, np. 123456789, stanislaw, dom99, haslo, Magda8, itp.

- Hasła mogą być tworzone według łączenia „losowych” (tj nie istniejących w popularnych słownikach) sylab/słów, np,: mal-tra-laza-#topa. W ten sposób można uzyskać długie hasło stosunkowo proste do zapamiętania.

Odpowiedzialność pracowników za dane poufne

Każdy pracownik odpowiada za utrzymanie w tajemnicy danych poufnych, do których dostęp został mu powierzony.

Monitoring bezpieczeństwa

W celu zapewnienia ochrony informacji Zarząd może stosować monitoring wykorzystania firmowej infrastruktury informatycznej, w szczególności obejmujący następujące elementy:

- analiza oprogramowania wykorzystanego na stacjach roboczych,
- analiza stacji roboczych pod względem wykorzystania nielegalnego oprogramowania / plików multimedialnych oraz innych elementów naruszających Prawo Autorskie,
- analiza odwiedzanych stron WWW,
- analiza godzin pracy na stanowiskach komputerowych,
- analiza wszelakich dostępów (autoryzowanych oraz nieautoryzowanych) do systemów IT będących w posiadaniu Firmy,
- analiza ruchu sieciowego pod względem komunikacji, szkodliwej dla bezpieczeństwa danych Firmy.

Monitoring bezpieczeństwa musi odbywać się z zachowaniem obowiązującego prawa.

Edukacja pracowników w zakresie bezpieczeństwa

Firma dba o cykliczną edukację pracowników w zakresie bezpieczeństwa informacji. Pracownicy w zależności od zajmowanego stanowiska mogą uczestniczyć w szkoleniach z zakresu:

- ochrony Danych Osobowych,
- świadomości istnienia problemów bezpieczeństwa,
- szczegółowych aspektów bezpieczeństwa.

Odpowiedzialność pracowników za dane dostępowe do systemów

Każdy pracownik zobowiązany jest do ochrony swoich danych dostępowych do systemów informatycznych. Dane dostępowe obejmują między innymi takie elementy jak:

- hasła dostępowe,
- klucze softwareowe (pliki umożliwiające dostęp – np. certyfikaty do VPN) oraz sprzętowe,
- inne mechanizmy umożliwiające dostęp do systemów IT.

Przykłady ochrony danych dostępowych:

- nieprzekazywanie dostępów do systemów IT innym osobom (np. przekazywanie swojego hasła dostępowego osobom trzecim),
- nieprzechowywanie danych w miejscach publicznych (np. zapisywanie haseł dostępowych w łatwo dostępnych miejscach),
- Ochrona danych dostępowych przed kradzieżą przez osoby trzecie.

Transport danych poufnych przez pracowników

Zabrania się przenoszenia niezabezpieczonych danych poufnych poza teren Firmy. W szczególności zabrania się przenoszenia danych poufnych na nośnikach elektronicznych (np.: pendrive, nośniki CD) poza teren Firmy.

Korzystanie z firmowej infrastruktury IT w celach prywatnych

Zabrania się korzystania firmowej infrastruktury IT w celach prywatnych.

Sieć lokalna (LAN).

Sieć lokalna musi być odpowiednio chroniona przed nieuprawnionym dostępem, przykładowo:

- istotne serwery muszą być odseparowowane od sieci klienckich,
- gniazdka sieciowe dostępne publiczne muszą być nieaktywne,
- goście nie mogą uzyskiwać dostępu do sieci LAN.

Szczegółowe informacje dotyczące przyjętych metod ochrony zostały zawarte w osobnej procedurze.

Systemy IT / serwery

- Systemy IT przechowujące dane poufne (np. dane osobowe) muszą być odpowiednio zabezpieczone.
- W szczególności należy dbać o poufność, integralność i rozliczalność danych przetwarzanych w systemach.

- Szczegółowe informacje dotyczące przyjętych metod ochrony zostały zawarte w osobnej procedurze.

Dokumentowanie bezpieczeństwa

Firma prowadzi dokumentacje w zakresie:

- obecnie wykorzystywanych metod zabezpieczeń systemów IT,
- budowy sieci IT,
- ewentualnych naruszeń bezpieczeństwa systemów IT,
- dostępów do zbiorów danych / systemów udzielonych pracownikom.

Wszelkie zmiany w obszarach objętych dokumentacją, uwzględniane są w tejże dokumentacji.

Dane osobowe

Szczegółowe wytyczne dotyczące przetwarzania danych osobowych zawarte są w osobnym dokumencie.

Publiczne udostępnianie infrastruktury IT

Infrastruktura udostępniona publicznie musi być szczególnie zabezpieczona. Przykładowe środki bezpieczeństwa:

- Separacja od sieci LAN (np. z wykorzystaniem strefy DMZ)
- Wykonanie hardeningu systemu (zwiększenia bezpieczeństwa oferowanego domyślne przez system)
- Wewnętrzna lub zewnętrzna weryfikacja bezpieczeństwa systemu (np. poprzez realizację testów penetracyjnych)

Kopie zapasowe.

- Każde istotne dane (w tym dane poufne) powinny być archiwizowane na wypadek awarii w firmowej infrastrukturze IT.
- Nośniki z kopiami zapasowymi powinny być przechowywane w miejscu uniemożliwiającym dostęp osobom nieupoważnionym.
- Okresowo kopie zapasowe muszą być testowane pod względem rzeczywistej możliwości odtworzenia danych.

Dostęp do systemów IT po rozwiązaniu umowy o pracę

W przypadku rozwiązania umowy o pracę z pracownikiem, dezaktywowane są wszelakie jego dostępy w systemach IT.

Naruszenie bezpieczeństwa

Wszelakie podejrzenia naruszenia bezpieczeństwa danych w Firmie należy zgłaszać w formie ustnej lub za pośrednictwem poczty elektronicznej do Zarządu Spółki.

Każdy incydent jest odnotowywany w stosownej bazie danych, a Zarząd Firmy podejmuje stosowne kroki zaradcze.

Weryfikacja przestrzegania polityki bezpieczeństwa.

Zarząd okresowo wykonuje szkolenie mające na celu wykrycie ewentualnych uchybień w realizacji założeń polityki bezpieczeństwa.

Ta polityka IT stanowi podstawę naszych działań i zobowiązuje wszystkich pracowników do przestrzegania jej zasad w celu osiągnięcia najwyższej jakości naszych usług dla klientów

Członek Zarządu

Krzeszowice, 30.10.2024 r.