

Szczególne wymagania bezpieczeństwa systemów i sieci teleinformatycznych Firmy

Formalności

Na podstawie ustawy z dnia 22 stycznia 1999 r., o ochronie informacji niejawnych (Dz. U. Nr 11, poz. 95 z późniejszymi zmianami) i rozporządzenia Prezesa Rady Ministrów z 25 lutego 1999 r. w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformatycznych (Dz. U. Nr 18, poz. 162) jest opracowana instrukcja służbowa - **Szczególne Wymagania Bezpieczeństwa Systemów i Sieci Teleinformatycznych w Firmie zwane SWB.**

Regulacje prawne

- Ustawa o ochronie danych osobowych z 29 sierpnia 1997
- Zgłoszenie bazy do GIODO
- Rozporządzenie MSWiA z 29 kwietnia 2004 w sprawie dokumentacji przetwarzania danych osobowych
 - **Dane osobowe:** wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej
 - **Co identyfikuje?** Cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe bądź społeczne lub nr identyfikacyjny np. PESEL
 - **Zgoda** na przetwarzanie musi być dobrowolna

Czego dotyczą SWB?

Instrukcja ta dotyczy wymagań związanych z ochroną kryptograficzną, elektromagnetyczną, techniczną i organizacyjną eksploatowanych w Firmie systemów teleinformatycznych, w których są wytwarzane, przetwarzane, przechowywane i przekazywane informacje niejawne stanowiące tajemnicę służbową (art. 60, ust. 4).

Kogo dotyczą SWB?

Zapisy niniejszej instrukcji obowiązują wszystkich pracowników, których zakres obowiązków związany jest z korzystaniem z usług systemów teleinformatycznych lub z nadzorem formalnym i/lub merytorycznym nad tymi systemami.

SWB?

SWB zawierają administracyjno-organizacyjne ustalenia dotyczące ochrony informacji niejawnej przetwarzanej, przechowywanej i przesyłanej w systemach teleinformatycznych Firmy oraz określają podział obowiązków i odpowiedzialności pracowników realizujących funkcje z zakresu bezpieczeństwa i ochrony informacji

Indywidualizacja SWB

Zróżnicowanie systemów teleinformatycznych wykorzystywanych w Firmie, zarówno w aspekcie techniczno-technologicznym jak też aplikacyjnym (zakresu i rodzaju realizowanych w nich aplikacji użytkowych) powoduje, że zapisy poszczególnych punktów SWB są ogólne i powinny być uszczegółowione w instrukcjach (Instrukcje szczegółowe) opracowanych dla konkretnych systemów teleinformatycznych.

Co w indywidualnych SWB?

- zasady postępowania z zewnętrznymi maszynowymi nośnikami informacji;
- zasady wyboru i trybu zmiany haseł dostępu;
- zasady ochrony przed wirusami komputerowymi;
- zasady wyprowadzania informacji z systemu na papierowe, magnetyczne, optyczne nośniki informacji oraz zasad postępowania z tymi nośnikami i wydrukami;
- zasady składowania informacji i przechowywania kopii;
- zasady utrzymywania kopii archiwalnych systemu (programy, pliki);
- plany postępowania awaryjnego i odtwarzania stanu systemu po zaistniałej awarii z punktu widzenia ochrony,
- plany postępowania awaryjnego i odtwarzania stanu systemu po zaistniałej katastrofie wykluczającej poprawne funkcjonowanie oddziału lub całej Firmy w jej siedzibie.

Kto jest kto?

- *Administrator bezpieczeństwa systemu teleinformatycznego*
- *Inspektor bezpieczeństwa teleinformatycznego (BTI)*
- *Pełnomocnik Ochrony Informacji Niejawnych w Firmie* – osoba powołana zarządzeniem Prezesa Firmy odpowiadająca za zapewnienie przestrzegania przepisów o ochronie informacji niejawnych;
- *Pracownicy strony trzeciej*

Kontrola przestrzegania SWB

Nadzór i kontrolę nad przestrzeganiem postanowień SWB sprawuje BO, a w nim inspektor BTI

SWB przeznaczone są do użytku służbowego i nie mogą być, bez zgody Dyrektora BO, udostępniane osobom nie będącym pracownikami Firmy

Instrukcja szczegółowa

Integralną częścią każdego eksploatowanego lub wdrażanego systemu teleinformatycznego powinien być podsystem ochrony, a jego formalnym uzupełnieniem jest *Instrukcja szczegółowa*.

Instrukcja szczegółowa dla starych systemów

W stosunku do już eksploatowanych systemów, nie zawierających mechanizmów ochrony, zleceniodawca/użytkownik systemu jest zobowiązany zapewnić budowę takiego podsystemu i opracowanie *Instrukcji szczegółowej* w terminie uzgodnionym z Dyrektorem BO

Jak bez kryptografii?

Do czasu wdrożenia kryptograficznych mechanizmów ochrony przesyłanych danych zakazuje się wymiany informacji niejawnych w sieciach transmisji danych; informacje te należy przekazywać zgodnie z obowiązującymi w Firmie zasadami wymiany korespondencji niejawnej.

Internet w Firmie?

Systemy teleinformatyczne Firmy wykorzystywane są do realizacji zadań służbowych i nie mogą być fizycznie połączone z systemami teleinformatycznymi (teletransmisyjnymi) publicznego użytku ani też z systemami teleinformatycznymi innych użytkowników niż Firma dopóki nie zostaną zastosowane odpowiednie mechanizmy ochrony zapewniające systemom teleinformatycznym Firmy bezpieczną współpracę z systemami zewnętrznymi

Internet z wydzielonych stanowisk

Pracownicy Firmy mogą korzystać z dostępu do usług świadczonych przez sieci publiczne (np. Internet) lub prywatne sieci innych (niż Firma) operatorów wyłącznie z wydzielonych stanowisk komputerowych, które nie mogą być używane do realizacji zadań służbowych (nie mogą w nich być utrzymywane programy użytkowe Firmy, jak również przechowywane dokumenty zawierające informacje niejawne).

Strona trzecia

Przygotowanie współpracy ze stroną trzecią odnośnie dostępu tej strony do systemów teleinformatycznych Firmy musi opierać się na formalnej *Umowie o Współpracy* zawierającej odniesienie do obowiązujących w Firmie uregulowań prawnych w zakresie ochrony i bezpieczeństwa informacji przetwarzanej, przechowywanej i przesyłanej w systemach teleinformatycznych Firmy oraz do postanowień niniejszych SWB.

Ochrona przed niepożądanym dostępem do informacji

- **Monitory powinny być ustawione tak, aby ograniczyć możliwość odczytu zawartości ekranu przez osoby postronne.**
- **Użytkownik ma obowiązek zachowania poufności haseł i identyfikatorów osobistych. Zabrania się udostępniania hasła i identyfikatora innym osobom.**

Ustalenia odnośnie użytkowania zewnętrznych nośników informacji

- **Do przechowywania informacji o różnych klauzulach tajności należy stosować odrębne nośniki magnetyczne (np. różne dyskietki)**
- **W systemach teleinformatycznych należy stosować znakowanie nośników magnetycznych. Znacznik musi wskazywać klauzulę tajności informacji utrzymywanej na tym nośniku:** znacznik czerwony stosuje się do rejestrowania informacji tajnych, żółty - informacji poufnych, niebieski – zastrzeżonych i zielony - informacji jawnych.
- **Wszystkie nośniki używane w systemach teleinformatycznych powinny być etykietowane**

Kontrola antywirusowa

**W każdym systemie
teleinformatycznym powinna być
dostępna aktualna wersja
rezydentnych programów
wykrywania wirusów
komputerowych.**

Zasady składowania i archiwizacji

Administrator systemu teleinformatycznego powinien utrzymywać aktualne kopie archiwalne oprogramowania systemowego i użytkowego, a także aktualne kopie baz danych.

Nośniki z kopiami archiwalnymi powinny być zabezpieczone przed nieupoważnionym dostępem, zniszczeniem lub kradzieżą, a sposób ich przechowywania powinien być zgodny z obowiązującymi przepisami o

ochronie informacji niejawnych.

Częstotliwość tworzenia kopii archiwalnych

- w odniesieniu do oprogramowania określa Dyrektor DI,
- w odniesieniu do baz danych określa Dyrektor Oddziału,
- w Centrali nadzorujący DI członek Zarządu lub Dyrektor Firmy

Zapasowe wersje

- **Za utrzymywanie zapasowej wersji własnych plików danych, które przechowywane są na indywidualnych komputerach, odpowiadają ich użytkownicy**
- **Jeśli pliki zawierają informacje niejawne, to do przechowywania zapasowych wersji plików należy również używać nośników zaewidencjonowanych.**

Postanowienia administracyjne

- **Każdy pracownik, korzystający służbowo z komputerów powinien odbyć odpowiednie przeszkolenie w zakresie bezpieczeństwa i ochrony informacji, a przestrzeganie zasad bezpieczeństwa i ochrony informacji powinno być wpisane w zakres jego obowiązków.**
- **Za zorganizowanie szkoleń odpowiadają przełożeni**

Komputery tylko do pracy

**Systemy teleinformatyczne Firmy
powinny być wykorzystywane
wyłącznie do realizacji zadań
służbowych. Za wykorzystywanie
systemów teleinformatycznych
zgodnie z ich przeznaczeniem
odpowiedzialni są użytkownicy tych
systemów**

Odpowiedzialni

**Za bezpieczeństwo sieci i systemów
teleinformatycznych Firma
odpowiada Administrator ABI
oraz pracownik BO
odpowiedzialny za sprawy
bezpieczeństwa systemów
teleinformatycznych w Firmie –
inspektor BTI**

Niektóre zadania inspektora BTI

- Kontrolowanie przestrzegania ustaleń organizacyjno-administracyjnych dotyczących bezpieczeństwa i ochrony informacji niejawnych w systemach teleinformatycznych
- Ustalanie programu i inicjowanie/prowadzenie szkoleń dotyczących bezpieczeństwa i ochrony danych w systemach teleinformatycznych
- Przeprowadzanie okresowych testów kontrolno-szkoleniowych (po zakończonych szkoleniach, po wystąpieniu poważnych incydentów, ale nie rzadziej niż raz w roku) sprawdzających znajomość i zrozumienie przyjętych procedur i zasad postępowania w sytuacjach normalnych i awaryjnych (zaistnienia zasymulowanego incydentu).
- Opiniowanie projektów systemów teleinformatycznych przewidywanych do wdrożenia w objętych nadzorem jednostkach organizacyjnych Firmy

Wybrane zadania administratora systemu teleinformatycznego (ochrona informacji niejawnych)

- **Ustalenie zasad tworzenia i zmiany haseł**
- **Przydzielanie użytkownikom uprawnień dostępu**
- **Uruchamianie zainstalowanych systemowych mechanizmów ochrony,**
- **Zapewnienie wszystkim użytkownikom dostępu do aktualnych wersji programów antywirusowych**
- **Wyznaczenie drukarek systemowych, które mogą być używane do wydruku danych niejawnych**
- **Ustalanie wykazu programów, które mogą być użytkowane w systemie**
- **Ustalenie zasad archiwizacji zbiorów danych,**
- **Udostępnianie (na żądanie) wyznaczonym osobom odpowiedzialnym za bezpieczeństwo i ochronę informacji niejawnych systemowych plików audytu (logów systemowych).**

Obowiązek stosowania się do zakazów:

- pozostawiania bez nadzoru pomieszczeń, w których zainstalowany jest sprzęt komputerowy,
- pozostawiania bez nadzoru komputera (terminala) bez wcześniejszego zakończenia pracy w systemie,
- udostępniania komputera osobistego osobom nieuprawnionym
- udostępniania innym użytkownikom swoich haseł i identyfikatorów,
- dokonywania prób uzyskania nielegalnego dostępu do plików innych użytkowników,
- propagowania przypadkowo uzyskanej informacji o istniejących w systemie możliwościach nielegalnego dostępu do informacji lub nieuprawnionego korzystania z zasobów teleinformatycznych;
- wykorzystywania komputera do celów innych niż realizacja zadań służbowych (np. uruchamianie gier komputerowych)

Użytkownik systemu teleinformatycznego jest odpowiedzialny za:

- **nadanie (zgodnie z kompetencjami) generowanej informacji, właściwej klauzuli tajności;**
- **przestrzeganie przyjętych procedur postępowania z nośnikami informacji (np. dyskietki, wydruki papierowe);**
- **respektowanie zasad tworzenia haseł i trybu ich zmiany, utrzymywanie poufności haseł dostępu do systemu;**
- **przestrzeganie przyjętych procedur postępowania (określonych w instrukcjach) odnośnie składowania przetwarzanych danych;**
- **bezzwłoczne powiadamianie wyznaczonej osoby odpowiedzialnej za bezpieczeństwo i ochronę informacji w systemach teleinformatycznych Firmy o wszelkich zauważonych próbach nieuprawnionego korzystania z zasobów systemu lub naruszenia mechanizmów i zasad jego bezpieczeństwa;**
- **przestrzeganie obowiązujących w danym systemie teleinformatycznym procedur postępowania (określonych w instrukcjach) w zakresie ochrony antywirusowej.**