ISO 27001

…bezpieczeństwo informacji
w organizacji

Czym jest INFORMACJA dla organizacji?

DANE
(uporządkowane, przefiltrowane, oznaczone, pogrupowane …)

Składnik aktywów,
które stanowią wartość i znaczenie dla organizacji i muszą być zabezpieczone.

INFORMACJA ma postać:

- *Papierową*
- *Elektroniczną*

(to również nagrania filmowe, zdjęcia)

i jest podatna na zagrożenia

Kradzież, zniszczenie, sfałszowanie, zagubienie….

co może powodować:

- ***Straty finansowe,***
- ***Utratę konkurencyjności***
- ***Reputacji***

Większa ilość INFORMACJI ***to większe ryzyko ich utraty!***

Dużą ilość danych, aplikacji, nośników …
Brak świadomości pracowników

- *Karteczki z hasłami, przekazywanie loginów i haseł*
- *Ekrany widoczne przez klientów*
- *Zostawianie niezablokowanego stanowiska,*
- *Brak prawidłowego niszczenia danych (dokumentacja papierowa, dyski twarde…)*

Bezpieczeństwo informacji, a prawo…..

- Ustawa o ochronie danych osobowych
- Ustawa o ochronie informacji niejawnych
- Ustawa o dostępie do informacji publicznej
- Ustawa o zwalczaniu nieuczciwej konkurencji
- Ustawa o prawie autorskim i prawach pokrewnych,

W Polsce istnieje ponad dwieście aktów prawnych, które dotyczą ochrony informacji.

Dodatkowe wymagania dotyczące „tajemnicy zawodowej"

Zarządzanie bezpieczeństwem informacji … i pojawia się ISO 27001

Bezpieczeństwo informacji jest realizowane poprzez wdrażanie odpowiedniego systemu zabezpieczeń, w tym polityki, procesów, procedur, struktury organizacyjnej, funkcji oprogramowania i sprzętu.

Zabezpieczenia te muszą zostać ustanowione, wdrożone, monitorowane, sprawdzone i udoskonalone, w razie potrzeby, w celu zapewnienia, że bezpieczeństwo i cele biznesowe organizacji są spełnione.

W praktyce bezpieczna informacja oznacza, że muszą być spełnione ***trzy zasadnicze atrybuty ochrony****:*

Poufność – czyli informacje są dostępne tylko dla osób uprawnionych do ich dostępu *(loginy, karty, zasoby wspólne..)*

Integralność – *czyli dane są nienaruszalne przez uprawnionych i nieuprawnionych* (Dane są integralne wtedy, kiedy nie zostały zmodyfikowane, dodane lub usunięte przez osobę nieupoważnioną, w nieautoryzowany, celowy sposób)

Dostępność *– czyli każdy ma dostęp dokładnie do tego, do czego jest uprawniony*

Po co właściwie zarządzać bezpieczeństwem informacji? Jaki jest cel? Jakie korzyści?

Potrzeba wdrożenia systemu zarządzania bezpieczeństwem może wyniknąć z wielu źródeł.

„Polak mądry po szkodzie”

Organizacja, która doświadczyła przykrego incydentu związanego
np. z utratą danych,
będzie szukała metody na zminimalizowanie prawdopodobieństwa wystąpienia podobnego zdarzenia w przyszłości.

„czynniki wewnętrzne”

- *spełnione są obowiązkowe wymagania prawne dotyczące bezpieczeństwa informacji,*

- *zarządzanie bezpieczeństwem informacji odbywa się w sposób sformalizowany i przewidywalny,(mamy porządek)*

- *zwiększenie bezpieczeństwa ważnych zasobów informacyjnych spółki, których utrata może przynieść poważne straty finansowe, wizerunkowe i czasu,*

- *szybki dostęp do informacji niezbędnych do wykonywania codziennych zadań,*

„czynniki zewnętrzne”

•*pokazanie , że odpowiedzialnie chronimy informacje należące do klientów oraz własnych*

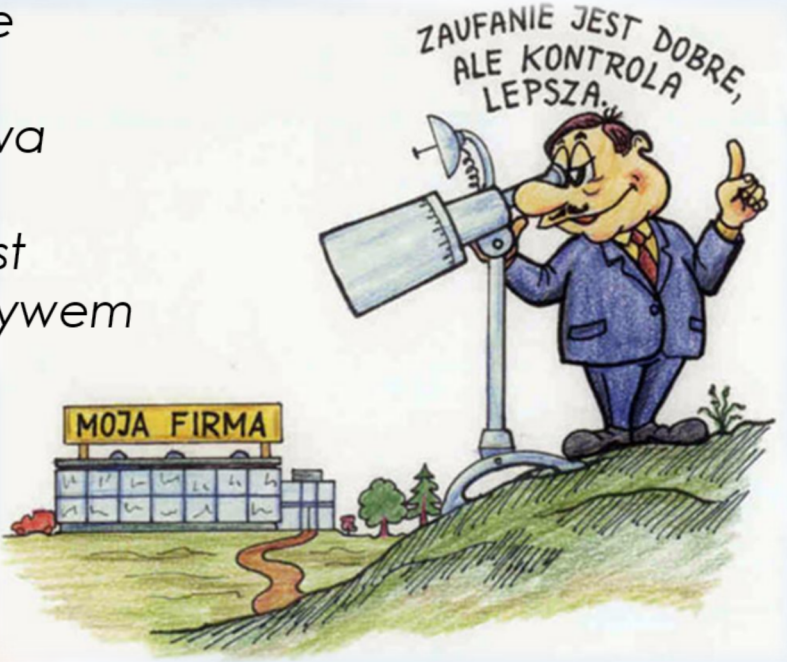
•*podnosi wiarygodność, zaufanie i daje zapewnienie, że powierzone i przetwarzane informacje są w odpowiedni sposób chronione*

•*zwiększa szanse na pozyskanie nowych rynków i klientów*
•*zobowiązania wynikające z umów lub oczekiwania w relacjach biznesowych*

•*otwiera drogę do klientów o nieprzeciętnych wymaganiach, dla których spełnienie określonych norm jest podstawowym warunkiem do rozpoczęcia współpracy*

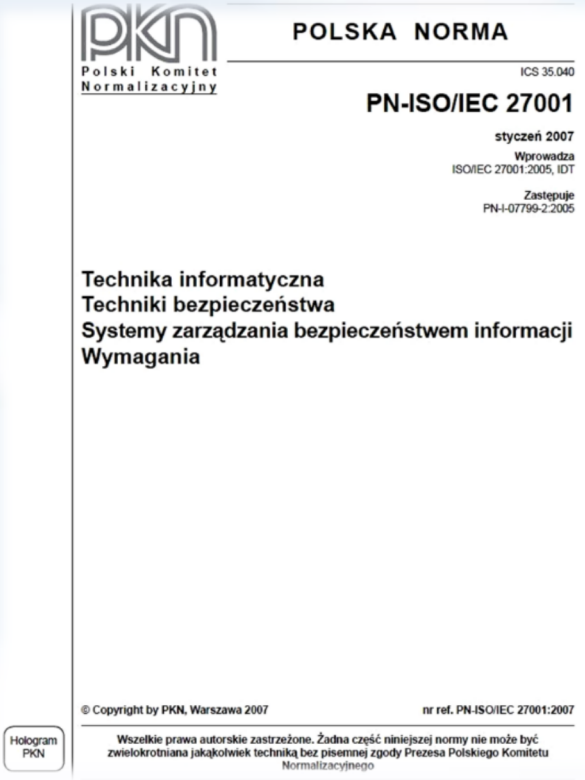
„czynniki uniwersalne”

Kierownictwo organizacji chce mieć ***kontrolę*** *nad poziomem bezpieczeństwa informacji, która w obecnych czasach jest najbardziej wartościowym aktywem każdej organizacji.*



ISO 27001 to norma....

Norma określa wymagania związane z ustanowieniem, wdrożeniem, eksploatacją, monitorowaniem, przeglądem, utrzymaniem i doskonaleniem SZBI (systemu zarządzania bezpieczeństwem informacji)



Polski Komitet Normalizacyjny

POLSKA NORMA

ICS 35.040

PN-ISO/IEC 27001

styczeń 2007

Wprowadza
ISO/IEC 27001:2005, IDT

Zastępuje
PN-I-07799-2:2005

Technika informatyczna
Techniki bezpieczeństwa
Systemy zarządzania bezpieczeństwem informacji
Wymagania

Hologram PKN

© Copyright by PKN, Warszawa 2007 nr ref. PN-ISO/IEC 27001:2007

Wszelkie prawa autorskie zastrzeżone. Żadna część niniejszej normy nie może być zwielokrotniana jakąkolwiek techniką bez pisemnej zgody Prezesa Polskiego Komitetu Normalizacyjnego

Norma ISO 27001 składa się z części podstawowej oraz załączników.

Część podstawowa normy definiuje wymagania związane z:

- *ustanowieniem i zarządzaniem SZBI,*
- *wymaganą dokumentacją,*
- *odpowiedzialnością kierownictwa,*
- *wewnętrznymi audytami SZBI, przeglądami SZBI*
- *oraz ciągłym doskonaleniem SZBI.*

Wszystkie wymagania zdefiniowane w części podstawowej powinny być spełnione. Podstawą ustanowienia oraz utrzymania SZBI jest określenie metody oraz przeprowadzenie analizy ryzyka.

Rola kierownictwa, czyli „góra” wie czego chce….

Podstawa to *świadomość kierownictwa*, którą budujemy przez:

- wskazanie aktualnych luk bezpieczeństwa,
- zagrożeń dla bezpieczeństwa informacji
- praktycznych zabezpieczeń
- uświadomienie ewentualnych zysków i strat

„Kasa misiu, kasa”

Analiza ryzyka, czyli przewidujemy przyszłość

Ryzyko – wypadkowa prawdopodobieństwa wystąpienia zagrożenia, które, wykorzystując podatności aktywu, może doprowadzić do jego uszkodzenia lub zniszczenia

Aktyw - wszystko to, co ma wartość dla organizacji (ludzie, sprzęt)

Kroki szacowania ryzyka

- *Identyfikacja aktywów (wg ich ważności)*
- *Identyfikacja zagrożeń (głównie rzeczywistych, konkretnych)*
- *Określenie prawdopodobieństwa (częstości)*
- *Określenie podatności*
  (cechy i/lub właściwości aktywu, które mogą zostać wykorzystane przez zagrożenie)
- *Wpływ/skutek wystąpienia zagrożenia (efekt, skala, zasięg)*

Audyt, czyli badanie….

Czym jest audyt:

- *JEST BADANIEM SYSTEMU (nie konkretnych osób!)*

- *SZUKANIEM konkretnych dowodów na działanie systemu zarządzania*

- *Odpowiedzią na pytanie*
- *„Czy jest tak jak to sobie ustanowiliśmy?”*

- *NIE JEST KONTROLĄ !*
- *Jest raczej „dyżurnym kijem”*

Wracamy do konkretów. Załącznik normy.

Załącznik A. normy określa:
Cele stosowania zabezpieczeń i zabezpieczenia w organizacji

18 stron w normie,
ponad 150 pozycji

Załącznik A. tej normy, zawierający wymagane zabezpieczenia podzielone na 11 obszarów, mających wpływ na bezpieczeństwo informacji w organizacji:

Znajdziemy tam wszystko co się tyczy przetwarzania danych w systemach informatycznych,

1. *Polityka bezpieczeństwa*
2. *Organizacja bezpieczeństwa informacji*
3. *Zarządzanie aktywami*
4. *Bezpieczeństwo zasobów ludzkich*
5. *Bezpieczeństwo fizyczne i środowiskowe*
6. *Zarządzanie systemami i sieciami*
7. *Kontrola dostępu*
8. *Pozyskiwanie, rozwój i utrzymanie systemów informacyjnych*
9. *Zarządzanie incydentami związanymi z bezpieczeństwem informacji*
10. *Zarządzanie ciągłością działania*
11. *Zgodność*

A.6.2 Strony zewnętrzne

Cel: Utrzymanie bezpieczeństwa informacji należących do organizacji oraz środków przetwarzania informacji, do których mają dostęp, za pomocą których przetwarzają, komunikują się lub którymi zarządzają strony zewnętrzne.

A.6.2.1	Określenie ryzyk związanych ze stronami zewnętrznymi	*Zabezpieczenie* Ryzyka dla informacji należących do organizacji i środków przetwarzania informacji, związane ze stronami zewnętrznymi, należy zidentyfikować przed przyznaniem dostępu tym stronom.
A.6.2.2	Bezpieczeństwo w kontaktach z klientami	*Zabezpieczenie* Wszystkie zidentyfikowane wymagania bezpieczeństwa powinny być wprowadzone przed przyznaniem klientom dostępu do informacji lub aktywów należących do organizacji.
A.6.2.3	Bezpieczeństwo w umowach ze stroną trzecią	*Zabezpieczenie* Umowy ze stronami trzecimi, dotyczące dostępu, przetwarzania, przekazywania lub zarządzania informacjami organizacji lub środkami przetwarzania informacji, lub dodania produktów lub usług do środków przetwarzania informacji, powinny obejmować wszystkie stosowne wymagania bezpieczeństwa.

A.8.3 Zakończenie lub zmiana zatrudnienia

Cel: Zapewnienie, że pracownicy, wykonawcy i użytkownicy reprezentujący stronę trzecią odchodzą z organizacji lub zmieniają stanowisko w sposób zorganizowany.

A.8.3.1	Odpowiedzialność związana z zakończeniem zatrudnienia	*Zabezpieczenie* Odpowiedzialność związaną z zakończeniem lub zmianą zatrudnienia należy jasno określić i przypisać.
A.8.3.2	Zwrot aktywów	*Zabezpieczenie* Wszyscy pracownicy, wykonawcy i użytkownicy reprezentujący stronę trzecią powinni zwrócić wszystkie posiadane aktywa organizacji w momencie zakończenia stosunku pracy, kontraktu lub umowy.
A.8.3.3	Odebranie praw dostępu	*Zabezpieczenie* Prawa dostępu pracowników, wykonawców, użytkowników reprezentujących stronę trzecią do informacji i środków przetwarzania informacji, należy odebrać w momencie zakończenia stosunku pracy, kontraktu lub umowy, lub zmodyfikować zgodnie z zaistniałymi zmianami zatrudnienia.

A.9.2 *Bezpieczeństwo sprzętu*

Cel: Zapobieganie utracie, uszkodzeniu, kradzieży lub naruszeniu aktywów oraz przerwaniu działalności organizacji.

A.9.2.1	Lokalizacja i ochrona sprzętu	*Zabezpieczenie* Sprzęt należy rozlokować lub chronić w taki sposób, aby redukować ryzyka wynikające z zagrożeń i niebezpieczeństw środowiskowych oraz możliwości nieautoryzowanego dostępu.
A.9.2.2	Systemy wspomagające	*Zabezpieczenie* Sprzęt należy chronić przed awariami zasilania lub zakłóceniami spowodowanymi awariami systemów wspomagających.
A.9.2.3	Bezpieczeństwo okablowania	*Zabezpieczenie* Okablowanie zasilające i telekomunikacyjne służące do przesyłania danych lub wspomagające usługi informacyjne należy chronić przed przejęciem lub uszkodzeniem.
A.9.2.4	Konserwacja sprzętu	*Zabezpieczenie* Sprzęt należy prawidłowo konserwować, aby zapewnić jego ciągłą dostępność i integralność.
A.9.2.5	Bezpieczeństwo sprzętu poza siedzibą	*Zabezpieczenie* Sprzęt pozostający poza siedzibą należy chronić przy uwzględnieniu ryzyk związanych z pracą poza siedzibą organizacji.
A.9.2.6	Bezpieczne zbywanie lub przekazywanie do ponownego użycia	*Zabezpieczenie* Wszystkie składniki sprzętu zawierające nośniki informacji należy sprawdzić, aby przed jego zbyciem upewnić się, że wszelkie informacje wrażliwe i licencjonowane oprogramowanie zostały usunięte lub bezpiecznie nadpisane.
A.9.2.7	Wynoszenie mienia	*Zabezpieczenie* Sprzęt, informacje lub oprogramowanie nie powinny być wynoszone bez uprzedniego zezwolenia.