ISO/IEC 27001:2005
Systemy Zarządzania Bezpieczeństwem Informacji

W czasach gospodarki wolnorynkowej główną wartością każdej firmy są informacje i dane stanowiące know-how. Informacje będące w posiadaniu firm i urzędów posiadają swoją realną wartość i mogą być podatne na zagrożenia takie jak, np.: **kradzież**, **zniszczenie** czy **zafałszowanie**.

Często **pozyskanie lub ujawnienie informacji** może stanowić o „**być albo nie być**" firmy.
Wraz z rozwojem technik przetwarzania informacji istotnym zagadnieniem w dzisiejszym świecie jest **zapewnienie bezpieczeństwa informacji**.
Zarządzanie bezpieczeństwem informacji to nie tylko problem wewnętrzny firmy.
To także bardzo często problem partnerów w biznesie. **Każdy jest odbiorcą i dostawcą informacji**.
I każdy chce zapewnienia, że proces wzajemnej **wymiany informacji** będzie się odbywał **zgodnie z ustaleniami** oraz, że będzie **kontrolowany**.

Firmy świadomie zarządzające informacją i jej bezpieczeństwem poszukują partnerów stojących na podobnym poziomie rozwoju. To naturalny proces znany z systemów zarządzania jakością. Eliminuje on z rynku tych, którzy pozostali w tyle i nie wprowadzili zarządzania informacją i jej bezpieczeństwem.
Model zawarty w normie pozwala efektywnie zarządzać wieloma aspektami przetwarzania informacji w firmie. **Dobrze zaprojektowany i wdrożony system po prostu usprawnia pracę porządkując proces przetwarzania informacji w firmie.**

Wymagania prawne to chyba najsilniejszy i bezdyskusyjny argument za wprowadzeniem systemu zarządzania bezpieczeństwem informacji. Szereg przepisów, aktów prawnych **wymaga bezwzględnie ochrony pewnych informacji**.
W naszym kraju obowiązuje co najmniej kilkanaście aktów prawnych związanych z ochroną pewnych informacji, do których musi się stosować każda nawet mała firma (np.: rachunkowość, dane osobowe). Brak takiej ochrony może skutkować ciężkimi sankcjami finansowymi, karnymi czy to w stosunku do organizacji czy do osób odpowiedzialnych i może doprowadzić nawet do zamknięcia działalności.

ISO/IEC 27001:2005 pomaga w ochronie zasobów informacji i daje pewność wszystkim zainteresowanym stronom, w szczególności Państwa klientom.

Norma ISO/IEC 27001 pomaga chronić informacje zapewniając:

Poufność - informacje są dostępne wyłącznie dla autoryzowanego personelu;
Integralność - zintegrowanie wszystkich działań w zakresie ochrony informacji od świadomości, poprzez organizację pracy, zabezpieczenia fizyczne, skończywszy na narzędziach informatycznych;
Dostępność - autoryzowani użytkownicy mają dostęp do informacji i zgromadzonych zasobów wtedy, kiedy jest to wymagane.

Bezpośrednie korzyści z wdrożenia i certyfikacji ISO 27001:

- Podnosi wiarygodność organizacji i daje zapewnienie, że powierzone, przetwarzane informacje są w odpowiedni sposób chronione.
- Pozyskanie nowych rynków i klientów. Podobnie jak certyfikat ISO 9001:2008, ISO 27001 otwiera drogę do klientów o nieprzeciętnych wymaganiach, dla których spełnienie określonych norm jest podstawowym warunkiem do rozpoczęcia współpracy.
- Zapewnienie, że spełnione są wymogi prawne, do których przestrzegania zobowiązana jest organizacja.
- Zarządzanie bezpieczeństwem informacji odbywa się w sposób sformalizowany, przewidywalny.

Pracownicy, partnerzy wiedzą **kto za co odpowiada** i **jak** mają **postępować w zakresie ochrony informacji**, z którą mają do czynienia. Jasno określone są odpowiedzialność, procedury, podejmowane działania.
Sam proces zarządzania zawiera mechanizmy kontroli, oceny i doskonalenia funkcjonowania.

Dzięki podejściu procesowemu (P-D-C-A) oraz oparciu o strukturę ISO 9001, norma ISO/IEC 27001:2005 pozwala w sposób efektywny zbudować narzędzie do zarządzania w organizacją.