Система менеджменту інформаційної безпеки **ISO / IEC 27001**

Менеджмент інформаційної безпеки

Забезпечення безпеки інформації та інших об'єктів, що відносяться до інформації - вкрай важливе завдання для будь-якого бізнесу. Кожен власник бізнесу і призначене ним керівництво вже не може закривати очі на поточний стан інформаційних систем, вони повинні бачити і розуміти потреби підприємства в інформаційному забезпеченні, вирішувати існуючі інформаційні проблеми.

У загальному розумінні інформаційна безпека пов'язана з обмеженням доступу третіх осіб до інформації. Крім конфіденційності стандарт чітко вказує на обов'язковість роботи над іншими, часто більш важливими властивостями. Ці властивості - доступність і цілісність інформації.

Кращі світові практики в галузі управління інформаційною безпекою описані в міжнародному стандарті на системи менеджменту інформаційної безпеки **ISO / IEC 27001**

Опис стандарту ISO / IEC 27001

Міжнародний стандарт **ISO / IEC 27001 «Системи менеджменту інформаційної безпеки. Вимоги»** встановлює вимоги до системи менеджменту інформаційної безпеки для демонстрації здатності організації захищати свої інформаційні ресурси.

Основа стандарту ISO / IEC 27001 - система управління ризиками, пов'язаними з інформацією.

Система управління ризиками дозволяє отримувати відповіді на наступні питання:

- На якому напрямку інформаційної безпеки потрібно зосередити увагу
- Скільки часу і коштів можна витратити на дане технічне рішення для захисту інформації

Метою інформаційної безпеки є забезпечення безперервності бізнесу компанії і мінімізація бізнес-ризиків шляхом попередження інцидентів безпеки і зменшення розмірів потенційного збитку.

Напрями інформаційної безпеки.

Щоб досягти рівня інформаційної безпеки, який задовольняє потреби компанії, необхідно більше, ніж просто купити антивірус, систему мережевого захисту або систему резервування даних. Необхідна чітка і злагоджена система.

Вимоги стандарту **ISO / IEC 27001** покривають весь спектр необхідних напрямків безпеки:

- Менеджмент ризиків
- Нормативне забезпечення інформаційної безпеки
- Внутрішній аудит
- Моніторинг та аналіз стану безпеки

- Політика в області безпеки
- Організація системи безпеки
- Класифікація інформаційних активів і управління
- Безпека і персонал
- Фізична та зовнішня безпека
- Менеджмент комп'ютерів і мереж
- Управління доступом до системи
- Придбання, розробка та підтримка інформаційних систем
- Менеджмент інцидентів інформаційної безпеки
- Забезпечення безперервності бізнесу
- Відповідність законодавству та іншим нормам

Система менеджменту інформаційною безпекою дозволить вирішувати і попереджати проблеми підприємства, пов'язані з інформацією. При цьому важливо розуміти, що для бізнесу важливі як паперові, так і електронні документи. Правильно налагодити управління інформаційною безпекою дозволять вимоги міжнародного стандарту ISO / IEC 27001 і німецькі методики впровадження.

Вигоди впровадження та сертифікації по ISO / IEC 27001

- Зрозумілість інформаційних активів для менеджменту компанії
- Систематичне виявлення загроз інформаційної безпеки для існуючих бізнес-процесів. Розрахунок ризиків і прийняття рішень на основі бізнес-цілей компанії
- Зниження і оптимізація вартості підтримки системи інформаційної безпеки
- Забезпечення ефективного управління інформацією в критичних ситуаціях
- Міжнародне визнання і підвищення авторитету компанії, як на внутрішньому ринку, так і на зовнішніх ринках
- Демонстрація клієнтам, партнерам, власникам бізнесу своєї прихильності до інформаційної безпеки

Пропозиції по стандарту

- Навчання фахівців
- Діагностика системи менеджменту
- Сертифікація системи менеджменту
- Підтримка при впровадженні

Контакти

04071, м. Київ,
вул. Воздвиженська, 44

+380 44 500 3345
+380 44 500 3346

info@tms-ua.com