БЕЗБЕДНОСТ НА ИНФОРМАЦИИ, CYBER БЕЗБЕДНОСТ И ЗАШТИТА НА ПРИВАТНОСТА – КОНТРОЛИ ЗА БЕЗБЕДНОСТ НА ИНФОРМАЦИИ

МОБЕС КВАЛИТЕТ

Подетални информации на:

тел: +389 2 3103 671
+389 2 5297 705
+389 75 531 077

e-mail:
info@mobeskvalitet.mk
biljana@mobeskvalitet.mk

Exemplar Global

mobes QUALITY

Што е ISO 27002?

ISO/IEC 27002:2022 е стандард за безбедност на информациите објавен од Меѓународната организација за стандардизација (ISO) и Меѓународната електротехничка комисија (IEC). Стандардот ISO 27002 е тесно поврзан со ISO 27001. Општо земено, обезбедува упатства за имплементација на ISO 27001 (ISMS).

ISO/IEC 27002 обезбедува референтен збир на контроли за безбедност на информации, cyber безбедност и заштита на приватноста, вклучувајќи упатства за имплементација засновани на меѓународно признати најдобри практики.

Иако ISO 27002, сам по себе, не е стандард за сертификација, усогласувањето со неговите упатства за безбедност на информации, физичка безбедност, cyber безбедност и управување со приватноста, ја доведува Вашата организација чекор поблиску до исполнување на барањата за добивање на ISO 27001 сертификат.

Што треба да знаете за ISO/IEC 27002?

ISO/IEC 27002:2013 Информатичка технологија – техники на безбедност – кодекс на практики за контроли на безбедност на информации е ревидиран и објавен во февруари 2022 година согласно ISO/IEC 27002:2022 Безбедност на информации, cyber безбедност и заштита на приватноста – контроли за безбедност на информации. Сите организации со добра ISMS практика или безбедност на информации мора да ги мапираат и ажурираат своите контроли според новите упатства од ажурираниот ISO/IEC 27002, согласно организациските потреби и контекст.

Што е ново за ISO/IEC 27002:2022?

ISO/IEC 27002:2022 е ревизија на BS EN ISO/IEC 27002:2013. Клучните промени во ISO/IEC 27002:2022 се:

- Фразата "кодекс на практики" е изоставена за подобро одразување на целта на стандардот да биде референтен збир на контроли за безбедност на информации.
- Бројот на наведени контроли за безбедност е намален од 114 на 93, при што некои контроли се отстранети бидејќи повеќе не ја одразуваат најдобрата практика.
- Претставени се 11 нови контроли, кои го одразуваат развојот на технологии и индустриски практики, вклучувајќи известување на податоци за закана, безбедност на информации за користење на услуги во cloud и спречување на истекување на информации.
- Изданието од 2022 година обезбедува референци за контролните идентификатори на изданија од 2013 година со цел да им олесни на компаниите да се префрлат на најновото издание.

Зошто е важен ISO/IEC 27002:2022?

Ако Вашата организација собира, користи или обработува податоци, секогаш ќе постојат безбедносни ризици и закани на кои треба да внимавате.

За да се заштитите од овие ризици, треба да имате имплементирано Систем за управување со безбедност на информации (ISMS) за да се обезбеди доверливост, достапност и интегритет на сите информации и информатички средства.

Главниот предизвик со кој се соочуваат компаниите кои се нови во делот за управување со безбедноста на информации е широкиот опсег. Имплементацијата и одржувањето на ISMS опфаќа толку широк опсег што дури и менаџерите не се сигурни од каде да почнат.

Ако ова Ви звучи реално или ако сакате да го подобрите Системот за безбедност на информации, тогаш одлична почетна точка е Имплементација на контролите предложени во ISO/IEC 27002.

Како ISO/IEC 27002:2022 може да му помогне на Вашиот бизнис?

- Идентификување на соодветните и пропорционални безбедносни контроли во рамките на процесот на поставување Систем за управување со безбедноста на информации (ISMS).
- Постигнување на најдобрите практики во управувањето со безбедноста на информации.
- Исполнување на законските, статутарните, регулаторните и договорните барања во врска со безбедноста на информации.
- Зајакнување на управувањето со ризик и намалување на веројатноста за прекршување на безбедноста на информации.
- Зголемување на довербата во организациите кои имаат Систем за управување со безбедност на информации (ISMS).
- Зголемување на севкупната робусност и еластичност на IMS и зајакнување на управувањето со ризик.