



ИНСТИТУТ ЗА АКРЕДИТАЦИЈА
НА РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА



Акредитација: ISO 27001

Систем за управување со
безбедноста на информациите

Што е информација и што се информациски безбедносни системи?

Податоците може да бидат трансформирани во нешто што има значење, вредност или релевантност за создавање информации. Деловните информации се податоци што имаат релевантност, вредност или значење за вашата компанија. Во овие таканаречени информации се вклучуваат сите извештаи, табеларни пресметки, аналитики, регулаторно известување, веб-локации, публикации, контролни табли итн. што ги исполнуваат критериумите да имаат релевантност, вредност или значење за вашата организација. Дури и групирањата на извори на податоци може да претставува деловна информација. На пример, вашиот склад за податоци се квалификува како деловна информација бидејќи ги интегрира вашите податоци за да произведе корисни информации. Информациите може да се чуваат и заштитуваат на различни начини, вклучително и со имплементирање на системи за сајбер безбедност, ажурирани системи за управување и прописи за претпазливост.

Од клучно значење е да се забележи дека безбедноста на информациите не подразбира само сајбер безбедност. Сајбер безбедноста е само еден дел од целиот систем за информациската безбедност и сите мерки кои се применуваат со цел да се засили севкупната безбедност на информациите. Поради тоа, мора да се разбере важноста за примена на мерки и прописи кои ќе го контролираат и заштитат протекувањето на знаењето и информациите кои ги поседува персоналот.

За кого е ISO 27001?

Барањата на ISO 27001 се генерички и се наменети да бидат применливи за сите организации (или делови од организација), без оглед на видот, големината и природата на активноста.

Стандардот е флексибилен и може да се прилагоди на широк спектар на организации, вклучувајќи:

- Големи организации
- Мали и средни претпријатија
- Организации од јавниот и приватниот сектор
- Невладини организации.

Стандардот може да го користат организации во која било земја.

Придобивките кои што следат од ISO 27001 ги имаат разубедено бизнисите во сите економски сектори (сите видови услуги и производство, како и примарниот сектор; приватни, јавни и непрофитни организации) да го воведат стандардот, иако информатичката, (ИТ) е индустријата во која најчесто се применува овој стандард (речиси една петтина од сите валидни сертификати за ISO/IEC 27001 според ISO истражувањето 2021 година). Овој стандард е исклучително важен, особено во денешно време кога скоро сите компании се склони кон сајбер-напади, кражба на податоци и истекување податоци. Сите овие потенцијални закани се огромен ризик за долговечноста на компаниите и е клучно да се контролираат.

На што се однесува ISO 27001?

Компаниите од секоја големина и од сите индустрии можат да го користат стандардот ISO/IEC 27001 како водич за креирање, имплементирање, одржување и континуирано подобрување на системот за управување со безбедноста на информациите.

За корпорација или организација се вели дека е во согласност со ISO/IEC 27001 ако има имплементирано систем за управување со ризици поврзани со безбедноста на податоците што ги поседува или ракува, и тој систем се придржува до сите најдобри практики и водечки принципи наведени во овој Меѓународен стандард.

Како стандардот ќе и придаде значење на една организација?

Според организацијата ISO, ISO/IEC 27001 во моментов е најдобриот светски стандард за системи за управување со безбедноста на информациите. Спроведувањето на рамката за безбедност на информациите специфицирана во стандардот ISO/IEC 27001 помага:

- Да се намали ранливоста на растечката закана од сајбер-напади;
- Да се реагира на развојните безбедносни ризици;
- Да се осигура дека средствата како што се финансиските извештаи, интелектуалната сопственост, податоците за вработените и информациите доверени од трети страни остануваат неоштетени, доверливи и достапни по потреба;
- Да се обезбеди централно управувана рамка која ги обезбедува сите информации на едно место;
- Да се подготват луѓе, процеси и технологија во вашата организација за да се соочите со ризици засновани на технологија и други закани;
- Да се заштитат информации во сите форми, вклучително и хартиени, во облак и дигитални податоци;
- Да се заштедат пари со зголемување на ефикасноста и намалување на трошоците за неефикасна одбранбена технологија.

Зошто е потребно да се користи акредитирано тело за сертификација?

Акредитираните тела за сертификација се непристрасни трети страни, кои независни од целта на сертификацијата мора да имаат компетентност наведена во меѓународните стандарди и други предуслови за нивното работење. Во повеќето случаи, сертификацијата е доброволна постапка што може да се користи за да се покаже дека сертифицираната цел е во согласност со барањата што и се наметнуваат. Сертификацијата може да се користи и за да се покаже усогласеноста со законските барања, вклучително и оние во директивите или регулативите на ЕУ.

Телото за сертификација врши ревизија за тоа дали системот е во согласност со барањата за сертификација. Врз основа на резултатите од ревизијата, сертификационото тело издава сертификат во кој потврдува дека системот за управување ги исполнува наведените барања. Сертификацијата важи во период од три години, а потоа може да се изврши и ресертификација. Одржувањето на сертификацијата вклучува годишни процедури за надзор што треба да се вршат за време на важноста на сертификацијата.





Како Институтот за акредитација на Република Северна Македонија го поддржува ISO 27001 сертификатот?

- Институтот за акредитација на Република Северна Македонија (ИАРСМ) е единственото национално тело за акредитација во нашата држава и работи на воведување и промовирање на системот за акредитација и доближување до економијата и граѓаните како крајни корисници.
- Институтот активно работи и на полето на меѓународното признавање. Имено, Институтот го задржува статусот потписник на трите најзначајни меѓународни договори за меѓусебно признавање на резултатите од акредитираните активности, договорот со Европската организација за акредитација (EA-MLA), договорот со Меѓународната организација за акредитација на лаборатории (ILAC-MRA) и договорот со Меѓународниот форум за акредитација (IAF-MLA).
- Главната цел на Институтот е да обезбеди еднаквост на домашните акредитирани тела со другите широм светот и да ги отвори вратите за домашните производи и услуги за непречен и сигурен пласман на европскиот и светскиот пазар. Како резултат на процесот на акредитација, потрошувачите и компаниите стекнуваат доверба во доверливоста, квалитетот и безбедноста на користењето на производите и услугите што ги користат во секојдневниот живот и работа.
- Институтот за акредитација на Република Северна Македонија ги препознава потребите на заинтересираните страни за акредитирана сертификација на системи за управување со информациска безбедност (ISO/IEC 27001).
- Институтот за акредитација на Република Северна Македонија е во процес на проширување на активностите за акредитација со развој и воведување на акредитација на сертификациони тела за системи за управување со информациска безбедност (ISMS).

Извори:

<https://www.iso.org/standard/27001>

<https://www.britannica.com/topic/information-system>



**ИНСТИТУТ ЗА АКРЕДИТАЦИЈА
НА РЕПУБЛИКА СЕВЕРНА МАКЕДОНИЈА**

Тел.: ++389 2 3293 080

Е-пошта: info@iarm.gov.mk

Веб страна: www.iarm.gov.mk

Кеј Димитар Влахов бр. 4

зграда 2, спрат 3

1000 Скопје, Р. С. Македонија