

Understanding Information Security

What exactly is Information security?

From the position of any public or private organization, information has some kind of value and is therefore an asset. Information assets, just like any corporate asset, need to be protected along with the infrastructure that supports the information. This infrastructure includes all the networks, systems, and functions that allow an organization to store, manage and control information assets.

But why should information assets need to be protected?

Information needs to be protected because most modern organizations can be faced with a wide range of security threats at any unforeseen moment.

These threats can include anything from human error and equipment failure to theft, fraud, vandalism, targeted damage and fire or water damage.

And because most modern organizations operate in an intricate, interconnected, technological world, information is also vulnerable to an entirely new set of high-tech threats such as hacking and virus attacks.

So how exactly can an organization protect its information assets?

This can be done by using a variety of controls provided by a professional information security services provider.

In addition to hardware and software functions, controls include things like policies, procedures, processes, and organizational structures. In order to protect information, organizations must seek professional assistance to develop, implement, monitor, evaluate, and improve these types of security controls.

This is where **infoShield comes in.**

We can explain what you can do to protect your organization's information assets via our recurring training courses and conferences as well as provide the tools and expertise to implement the best information security plan for your organization, whether it is via our 24 hour monitoring surveillance, ISO certification and auditing or architecting an infrastructure design that is safe against risks and threats.