Thistle Initiatives

Guiding you through compliance

NCSC 10 steps to Cyber Security

020 7436 0630 | info@thistleinitiatives.co.uk

Thistle Initiatives

Guiding you through compliance

Defining and communicating your Board's Information Risk Regime is central to your organisation's overall cyber security strategy.

The National Cyber Security Centre recommends you review this regime and the ten associated security areas described below to protect your business against the majority of cyber attacks.

Set up your Risk Management Regime	Assess the risks to your organisation's information and systems with the same vigour you would for legal, regulatory, financial or operational risks. To achieve this, embed a Risk Management Regime across your organisation, supported by the Board and senior managers.
Network Security	Protect your networks from attack. Defend the network perimeter and filter out unauthorised access and malicious content. Monitor and test security controls.
User education and awareness	Produce user security policies covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks.
Malware prevention	Produce relevant policies and establish anti-malware defences across your organisation.
Removeable media controls	Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing it onto the corporate system.
Secure configuration	Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices.
Managing user privileges	Establish effective management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

Thistle Initiatives

Guiding you through compliance

Incident management

Establish an incident response and disaster recovery capability. Test your incident management plans. Provide specialist training. Report criminal incidents to law enforcement.

Monitoring

Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack.

Home and mobile working

Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and build to all devices. Protect data both in transit and at rest.

Our Cyber Essentials programme provides a team of Cyber Experts, certified by various cyber security bodies, supporting companies battling cyber crime for many years.

We also offer the following services to enhance your cyber awareness:

- Cyber Insurance to cover your company's costs should you experience a breach
- Awareness training and threat briefings to staff members
- Cyber risks analysis based on the National Cyber Security Centre 10 Steps to Cyber Security, with pragmatic, affordable remediation roadmaps to ensure the company is protected from emerging cyber threats
- Business continuity and disaster recovery plans

020 7436 0630 | info@thistleinitiatives.co.uk

Part of the Thistle Group