10 Steps to Cyber Security

NETWORK SECURITY

This is about setting up security controls and monitoring and testing them.

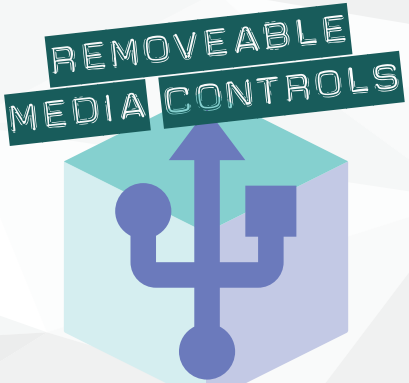
SECURE CONFIGURATION

This means making sure any patches or updates are installed. It's a good idea to create a system inventory and define a baseline build for all devices.

MALWARE PROTECTION

This is the overall defence against malware, stopping malicious content from getting in – ensuring anti-virus and anti-malware is up-to-date on every entry point in a system.

REMOVEABLE MEDIA CONTROLS



Produce a policy to control access to removeable media and scan all media for malware before importing data from it into a system.

USER EDUCATION AND AWARENESS

This is all about creating policies and providing training to all employees.

INFORMATION RISK REGIME

This is an organisation's overall cyber security strategy and encompasses the other 9 steps. The whole strategy should be reviewed regularly.

MANAGING USER PRIVILEGES

Limit access to authorised people only.
Keep logs and monitor access to sensitive areas.

INCIDENT MANAGEMENT

Produce a policy explaining what do you do if you have a security breach. This step is about how you respond to an incident, how it's reported and who to.

MONITORING

Continuously monitor all systems and networks. Look for any unusual activity that might indicate an attack.

HOME AND MOBILE WORKING

Produce a policy for all employees who work away from the office. It needs to protect data in use, in transit and at rest.

iHASCO

+44 (0)1344 867 088 hello@ihasco.co.uk www.ihasco.co.uk