iT Champion™

10 STEPS TO CYBER SECURITY

1 TEAM EDUCATION

Implement a staff training programme which ensures all users are using the company systems in a secure and acceptable way.

2 CONTROL USER PRIVILEGES

Build account management practices and limit the number of privileged accounts. Restrict user privileges and keep an eye on user activity.

3 PROTECT AGAINST MALWARE

Make sure your anti-malware defences are up to date and that they're right for all areas of your business.

4 INCIDENT RESPONSE & DISASTER RECOVERY

Create and provide training to an incident management team, implement incident management plans and establish your disaster recovery capability.

5 CONTROL REMOVEABLE MEDIA

All removable media should be monitored for malware before being imported. Create a policy limited media types and handling and limit access

6 CHECK NETWORK SECURITY

Frequently check your networks for unauthorised access or malicious content and ensure you're protected against internal or external attack.

7 WORKING FROM HOME OR MOBILE

Implement a policy for anyone working from home or mobile to comply with and ensure that data is protected at all times.

8 MONITORING

Create a monitoring policy and implement it consistently across all ICT systems and networks. Check for any unusual activity that could be the first sign of an attack.

9 SECURE CONFIGURATION

Apply security patches and ensure that the secure configuration of all ICT systems is maintained. Create a system inventory and define a baseline build for all ICT devices.

10 INFORMATION RISK MANAGEMENT REGIME

Ensure you have up to date risk management policies and that all staff are always engaged with them, and enforce an effective order of command.