URBAN
IT SOLUTIONS

Cyber Security Controls

IT Support | System Monitoring & Maintenance | Infrastructure and Cloud Services | Data Backup Services | Cyber Security Solutions | Telephony & Connectivity | IT Compliance | IT Consultancy

Firewalls & Boundaries

Strong □ **5.** Firewall equipment in place with policy-led passwords. Necessary services enabled with a documented business case.

□ **4.** Firewall equipment in place with policy-led passwords. Necessary services enabled without a documented business case.

□ **3.** Firewall equipment in place with default passwords. Necessary services enabled without a documented business case.

□ **2.** Firewall equipment in place with default passwords. Unnecessary services enabled.

Weak □ **1.** No firewall protection in place.

Secure Configuration

Strong □ **5.** IT equipment is used with policy-led configuration definitions. All unrequired default software services are removed or disabled. Secure configuration is audited regularly as part of a defined policy.

□ **4.** IT equipment is used with policy-led configuration definitions. All unrequired default software services are removed or disabled.

□ **3.** IT equipment is used with non-default settings without any policy-led configuration definitions. All unrequired default software services are removed or disabled.

□ **2.** IT equipment is used with non-default settings without any policy-led configuration definitions. Unrequired default software and services are still in place.

Weak □ **1.** IT equipment is used with default factory settings and unrequired default software and services.

Worried about your cyber security?
Get in touch > joanna@urbanitsolutions.co.uk

www.urbanitsolutions.co.uk

Access Controls

Strong □ **5.** Technically controlled system access rights in place along with published policies and processes.

□ **4.** Technically controlled system access rights without published policies in place.

□ **3.** System Admin access rights assigned to specific users with policies in place but without technical controls.

□ **2.** System Admin access rights assigned to specific users without technical controls or policies in place.

Weak □ **1.** System Admin access rights assigned to all users as default.

Malware Protection

Strong □ **5.** Malware protection in place and up to date. Monitored updates mandated at group policy level with published policies in place.

□ **4.** Malware protection in place and up to date. Monitored updates mandated at user level.

□ **3.** Malware protection in place and up to date but unmonitored.

□ **2.** Malware protection in place but out of date.

Weak □ **1.** No malware protection in place.

Patch Management

Strong □ **5.** All operating systems, applications and firmware are supported and in receipt of regular security patches, which are installed within 14 days of release. A published policy is in place.

□ **4.** All operating systems, applications and firmware are supported and in receipt of regular security patches, which are installed within 14 days of release.

□ **3.** All operating systems, applications and firmware are supported and in receipt of regular security patches.

□ **2.** All operating systems, applications and firmware are supported but regular patching is not mandated.

Weak □ **1.** All operating systems, applications and firmware are unsupported and do not receive any regular security patches.