Skillzminer Limited
163 Bath Street
Glasgow
G2 4SQ
www.skillzminer.com

Title	IT Security Policy
Version	1.1
Authorized by	Kirsty Mitchell
Published date	27/6/2022
Next review date	27/6/2023

IT Security Policy

The company's IT security policy is to achieve and maintain security in line with the UK governments Cyber EssentialsScheme, as laid out by GCHQ.

This policy will be reviewed annually, in line with IT policies and procedures.

1. Boundaries and Firewall

1.1. The default administrative passwords for all firewall (or equivalent network devices) are changed to analternative strong password.

1.2. Each rule that allows network traffic to pass through the firewall is subject to approval by an authorisedindividual and documented (including an explanation of the business need)

1.3. Unapproved services or services that are typically vulnerable to attack (such as SMB, Net-Bios, tftp, RPC,rlogin, rsh or rexec) are disabled (blocked) at the boundary firewall by de-fault.

1.4. Firewall rules that are no longer required are removed or disabled in a timely manner.

1.5. The administrative interface used to manage boundary firewall configuration is not acces-sible from theinternet.

1.6. The corporate policy 1.4 has been adhered to – meaning there are currently no open ports or services thatare not essential for the business.

1.7. When there is no requirement for a system to have internet access, a Default Deny policy is in effect whichhas been applied correctly, preventing the system from making connections to the internet.

2. Secure Configuration

2.1. Unnecessary user accounts (e.g. Guest accounts and unnecessary user accounts) are removed or disabled.

2.2. Unnecessary software (including applications, system utilities and network services) are removed ofdisabled.

2.3. The auto-run feature is disabled (to prevent software programs running automatically when removable storage media is connected to a computer of when network folders are ac-cessed).

2.4. A personal firewall (or equivalent) is enabled on desktop PCs and laptops and configured to disable (block)unapproved connections by default.

2.5. New workstations are configured securely and that build instructions are kept up to date with corporatepolicies.

2.6. The backup policy is reviewed and that backups are regularly taken to protect against threats such asransomware.

2.7. Event logs are maintained on servers, workstations and laptops.

3. User Access Control

3.1. All users account creation is subject to a provisioning and approval process.

3.2. Special access privileges are restricted to a limited number of authorised individuals.

3.3. Details about special access privileges (e.g. the individual and purpose) are documented, kept in a securelocation and reviewed on a regular basis.

3.4. Administrator accounts are only used to perform legitimate administrative activities and are not grantedaccess to email of the internet.

3.5. Administrative accounts are configured to require a password change on a regular basis (at least every 60days).

3.6. Each user authenticates using a unique username and strong password before being granted access toapplications, computers and network devices.

3.7. User accounts and special access privileges are removed or disabled when no longer required (e.g. when anindividual changes role or leaves the organisation)

4. Malware Protection

4.1. Malware protection software is installed on all computers that are connected to or capable of connecting tothe internet.

4.2. Malware protection software scans files automatically upon access (including when downloading and opening files, accessing files on removable storage media or a network folder) and scan web pages whenbeing accessed (via a browser).

4.3. Malware protection software is configured to perform daily scans on all files.

4.4. Malware protection software is able to prevent connections to malicious websites on the internet (e.g. byusing website blacklisting).

4.5. Corporate policy regarding malware is reviewed and requires all malware protection software to have allengine updated applied and this is applied rigorously.

4.6. Malware signature files are kept up to date (through automatic updates or through centrally manageddeployment)

4.7. Users are prevented from running executable code or programs from any folder to which there is also writeaccess.

5. Patch Management

5.1. Software running on computers and network devices that are connected to or capable of connecting to theinternet is supported by the software vendor or supplier of the software) to ensure security patches for known vulnerabilities are made available.

5.2. Updates to software (including operating system software and firmware) running on computers and networkdevices that are connected to or capable of connecting to the internet are installed in a timely manner (30 days of release)

5.3. Out of date software (i.e. software that is no longer supported) is removed from computer or networkdevices that are connected to or capable of connecting to the internet.

5.4. All security patches for software running on computers and network devices that are connected to ofcapable of connecting to the internet are installed in a timely manner (14 days of release)

5.5. A mobile working policy is in force that requires mobile devices (including BYOD) to be kept up to date withvendor updates and application patches.