Cyber Security Policy

1st February 2022

Prepared by:
Graham Morgan
Managing Director
Spatial Consultants Ltd

Tel 07717 539412
gmorgan@spatialconsultants.com

Contents

Release Notes

Version	Date	Notes
V1	01/12/2021	First version
V2	01/02/2023	Revised to align with v3 of the NCSC 'Cyber Essentials: Requirements for IT infrastructure'

References

Title	Source
NCSC Cyber Essentials: Requirements for IT Infrastructure, v3	https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-0-January-2022.pdf
Microsoft Privileged Identity Management	https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/
NCSC Password Administration	https://www.ncsc.gov.uk/collection/passwords/updating-your-approach

Cyber Security Policy

Spatial Consultants Ltd is committed to managing client and company information safely and securely. Responsibility for Cyber Security ultimately lies with the Managing Director, however, all personnel have a responsibility to do everything practicable to prevent a cyber security breach.

The Cyber Security Policy of the company is:

- maintain our data and IT infrastructure securely and in alignment with the requirements of the UK Cyber Essentials programme as described by the National Cyber Security Centre.

a) Purpose

i) This policy outlines our guidelines and provisions for preserving the security of our data and technology infrastructure.

b) Scope

i) This policy applies to our entire IT infrastructure and all our employees, contractors, volunteers remote or onsite, and anyone who has permanent or temporary access to our data, systems and hardware.
ii) Mobile phones
iii) Bring your Own Devices (BYOD)
iv) Home working
v) Wireless devices
vi) Externally managed services such as Microsoft Office 365

c) Policy Elements

The company has outlined security measures that may help mitigate cyber security risks.

- Firewalls
- Secure configuration
- User access control
- Malware protection
- Security update management

Firewalls

Applies to: boundary firewalls; desktop computers; laptop computers; routers; servers.

Objective: Ensure that only safe and necessary network services can be accessed from the Internet.

Every device must be protected by a correctly configured firewall (or equivalent network device).

For all firewalls (or equivalent network devices), the organisation must routinely:

- change any default administrative password to an alternative that is difficult to guess (see Password-based authentication) — or disable remote administrative access entirely
- prevent access to the administrative interface (used to manage firewall configuration) from the Internet, unless there is a clear and documented business need and the interface is protected by one of the following controls:
    - a second authentication factor, such as a one-time token
    - an IP allow list that limits access to a small range of trusted addresses
- block unauthenticated inbound connections by default
- ensure inbound firewall rules are approved and documented by anauthorised individual; the business need must be included in the documentation
- remove or disable permissive firewall rules quickly, when they are no longer needed.
- use a host-based firewall on devices which are used on untrusted networks, such as public Wi-Fi hotspots.

Secure Configuration

Applies to: email, web, and application servers; desktop computers; laptop computers; tablets; mobile phones; firewalls; routers.

Objective: Ensure that computers and network devices are properly configured to:

- reduce the level of inherent vulnerabilities
- provide only the services required to fulfil their role

Computers and network devices

- The Company will be active in its management of computers and network devices. It will routinely:
  remove and disable unnecessary user accounts (such as guest accounts and administrative accounts that won't be used)
- change any default or guessable account passwords to something nonobvious
- remove or disable unnecessary software (including applications, system utilities and network services)
- disable any auto-run feature which allows file execution without user authorisation (such as when they are downloaded from the Internet)
- authenticate users before allowing Internet-based access to commercially or personally sensitive data, or data which is critical to the running of the organisation

Password-based authentication

The Company will make good use of the technical controls available to it on password-protected systems. As much as is reasonably practicable, technical controls and policies will shift the burden away from individual users and reduce reliance on them knowing and using good practices.

Users are still expected to pick sensible passwords. For password-based authentication in Internet-facing services the Company will:

- protect against brute-force password guessing, by using at least one of the following methods:
  - lock accounts after **no more** than 10 unsuccessful attempts
  - limit the number of guesses allowed in a specified time period to **no more** than 10 guesses within 5 minutes
- set a **minimum** password length of at least 8 characters
- **not** set a maximum password length
- change passwords promptly when the Company knows or suspects we have been compromised

- adopt the National Cyber Security Centre's password policy https://www.ncsc.gov.uk/files/password_policy_infographic.pdf
- advise our users:
    - how to avoid choosing obvious passwords (such as those based on easily discoverable information like the name of a favourite pet)
    - not to choose common passwords — this could be implemented by technical means, using a password blacklist
    - not to use the same password anywhere else, at work or at home
    - where and how they may record passwords to store and retrieve them securely — for example, in a sealed envelope in a secure cupboard
    - if they may use password management software — if so, which software and how which passwords they really must memorise and not record anywhere

Device Unlocking: For physical laptops, PCs, etc. users must unlock their device using a credential such as a biometric, password or PIN of at least 6 characters in length.

Multi Factor Authentication

For access to cloud services, all users are required to use Multi Factor Authentication, preferably through an Authenticator app.

User Access Controls

Applies to: email, web and application servers; desktop computers; laptop computers; tablets; mobile phones.

Objective: Ensure user accounts:

- are assigned to authorised individuals only
- provide access to only those applications, computers and networks actually required for the user to perform their role

The Company will be in control of its user accounts and the access privileges granted to each user account that has access to the organisation's data and services. Importantly, this includes accounts that third parties use for access (for example, device management or support services). It must also understand how user accounts authenticate and control the strength of that authentication. This means the Company will:

- have a user account creation and approval process
- authenticate users before granting access to applications or devices, using unique credentials (see Password-based authentication)
- remove or disable user accounts when no longer required (when a user leaves the organisation or after a defined period of account inactivity, for example)
- implement two-factor authentication, where available
- use administrative accounts to perform administrative activities only (no emailing, web browsing or other standard user activities that may expose administrative privileges to avoidable risks)
- remove or disable special access privileges when no longer required (when a member of staff changes role, for example)

Administrative Access

The company policy is that system access should be granted on the basis of least privilege. This protects networked assets in the event of the execution of malicious code. Administrative roles will only be granted for specific purposes, and only with the authorisation of the Managing Director.

Privileged Identity Management (PIM) will be used when available, with administrators needing to elevate their permissions for limited durations to perform specific tasks.

Malware Protection

Applies to: desktop computers; laptop computers; tablets; mobile phones.

Objective: Restrict execution of known malware and untrusted software, to prevent harmful code from causing damage or accessing sensitive data.

The Company will implement a malware protection mechanism on all devices. For each device, the Company will use at least one of the three mechanisms listed below:

Anti-malware software

- The software (and all associated malware signature files) must be kept up to date, with signature files updated at least daily. This may be achieved through automated updates, or with a centrally managed deployment.
- The software must be configured to scan files automatically upon access. This includes when files are downloaded and opened, and when they are accessed from a network folder.
- The software must scan web pages automatically when they are accessed through a web browser (whether by other software or by the browser itself).
- The software must prevent connections to malicious websites on the Internet (by means of deny listing, for example) — unless there is a clear, documented business need and the Company understands and accepts the associated risk.

Application allow listing

- Only approved applications, restricted by code signing, are allowed to execute on devices. The Company will:
    - actively approve such applications before deploying them to devices
    - maintain a current list of approved applications Users must not be able to install any application that is unsigned or has an invalid signature.

Application sandboxing

- All code of unknown origin must be run within a ‘sandbox’ that prevents access to other resources unless permission is explicitly granted by the user. This includes:
    - other sandboxed applications
    - data stores, such as those holding documents and photos
    - sensitive peripherals, such as the camera, microphone and GPS
    - local network access

Security Update Management

Applies to: web, email and application servers; desktop computers; laptop computers; tablets; mobile phones; firewalls; routers.

Objective: Ensure that devices and software are not vulnerable to known security issues for which fixes are available.

The Company will keep all its software up-to-date. Software will be:

- licensed and supported
- removed from devices when no longer supported
- have automatic updates enabled where possible updated, including applying any manual configuration changes required to make the update effective, within 14 days of an update being released, where:
    - the update fixes a vulnerability with a severity the product vendor describes as 'critical' or 'high risk'
    - there are no details of the vulnerability severity level the update fixes provided by the vendor

The Company will strive to ensure that all released updates be applied within 14 days

Signature of person responsible for policy:-

Graham Morgan

Managing Director

1st December 2021