ELCAP
Cyber Security Policy Guidance for Management

Cyber and Fraud Centre Scotland

Table of Contents

Cyber Security Policy Template

1. Document Control

Organisation Name: ELCAP

Creation/Last Edit Date: January 2026

Version: 2

Author: Lara Ritchie

Approval:

2. Revision History

Version	Date	Description of Changes	Author
1	August 2025	Initial population of document	Lara Ritchie - ELCAP
2	September 2025	Update on details through discussion with Mother Technologies	Lara Ritchie - ELCAP Mother Technologies - IT

3. Policy Statement

The purpose of this document is to define guidelines and rules regarding the security of this organisation. It is based on a template which is the property and intellectual property of the Cyber and Fraud Centre. It is intended for use exclusively by Centre members.

4. Stakeholders/Roles

CEO or Deputy: Claire Macdonald

Policy Manager or Deputy: Lara Ritchie

Risk Manager or Deputy: Lara Ritchie

Information Security Manager or deputy:

IT Provider: Mother Technologies

Legal Advisor: Navigator Ltd

Human Resources: Navigator Ltd

Public Relations: Navigator Ltd

5. Risk Assessment

5.1 IT Estate Auditing

5.1.1 Estate Inventory

Identifying the devices present on the networks and devices of the organisation is key in identifying vulnerabilities and building, planning cybersecurity improvements, etc.

This inventory will be conducted by the Information Security Manager, in this case,
Business Manager - ELCAP
and the results will be given to the Risk manager, in this case,
Navigator Ltd & ELCAP SMT
or their equivalent deputy. After the inventory has been completed, the Risk and Information Security manager, or their equivalent deputies, will use the information acquired to run Data, Vulnerability and Access Control Audits.

5.1.2 Vulnerability Auditing

Identifying the vulnerabilities present on the networks and devices of the organisation is key in building an incident response plan, planning cybersecurity improvements, etc. This audit should build off the results from the estate inventory.

This audit will be conducted by the Risk Manager, in this case,
IT Provider - linking with ELCAP SMT.

or by their equivalent deputy, and the results will be given to the Policy Manager, in this case, Business Manager - ELCAP.
or their equivalent deputy. After the audit has taken place the Policy Manager or their equivalent deputy will take necessary actions. Actions taken could be, updating incident response policy, pushing for any immediate fixes, etc.
This audit will take the form of a Vulnerability Report Scan and will repeat every Month

5.2 Data Auditing

Identifying what data is stored and where is a critical part of the policy creation. This will be conducted by the Information Security Manager, in this case, Business Manager - ELCAP (Share Point / Access Care Planning & Access People Planner /
or their equivalent deputy. This audit will build off the Estate inventory and will identify data present and stored on all devices.

The results of the Data Audit should be provided to the Policy Manager, in this case, Business Manager - ELCAP
or their equivalent deputy, after which the Policy Manager or their equivalent deputy will take the actions outlined in this policy document. Actions taken could be modifying the data management policy such as changing where the data identified is stored, etc.

A data audit will be run every Annually or when a device prompts a change
and will fill the table in the Appendix A with each device identified in the organisation.

5.3 Access Control Auditing

Identifying what each person has access to, within the organisation is key to ensuring the security of the organisation. It will build off the Estate Inventory and Data Audit to identify which members of the organisation have access to which data and which devices.

This audit will be conducted by the Risk Manager, in this case, Business Manager
or their equivalent deputy, in communication with the IT Provider. The results will be given to the Policy Manager, in this case, Business Manager
or their equivalent deputy. After the audit has taken place, the Policy Manager or their equivalent deputy will take necessary actions. Actions taken could be removing privileges from individuals that shouldn't have them, adding privileges to those who should, etc.

This audit will repeat every Year

6. Contents

6.1 Device Management

Devices provided by ELCAP to the staff are subjected to the following policies.

6.1.1 Acceptable Use Policy

When using the device provided by the organisation these policies and rules apply:

- Staff may not install external software without prior approval that isn't present in the whitelisted software in section 6.1.2
- No copy of company software, files or data may be copied or removed from company devices without prior authorization.
- ELCAP is not responsible for any messages or actions taken online while using company devices
- All staff are required to comply with ELCAP policies when carrying out work, and in particular the following policies: Bring your Own Device Policy, Home working/Hybrid working Policy, Computers Internet and Email Policy, and our Data Protection Policy.

Failure to adhere by these rules may result in disciplinary actions.

6.1.2 Whitelist of Software

The following is a list of acceptable software:

- All software from the Microsoft 365 Product Suite
- Adobe Acrobat
- Microsoft Edge

-Sage 50 Accounts, -Sage 50 Payroll / Edge / Acrobat / Access Care Planning / Access People Planner / Microsoft 365 / Microsoft Teams / Google Docs

The software listed above has been approved by

ELCAP SMT

in their function as Policy Manager and

ELCAP CEO

in their function as CEO or by their equivalent deputies.

6.1.3 Antivirus Policy

Antivirus software must be present and active on company provided devices. The antivirus used by the organisation is

Microsoft Defender

Each company device must have this antivirus software that has been updated or is being updated to the latest version.

6.1.4 Update Policy

Company provided devices need to be updated to the latest version of firmware and software as quickly as possible. This is handled by the IT Provider, in this case,

RMM agent with Patch management / Windows Update Ring Policies from M365

Updates are done routinely every 3 times per week and offer the user 2 chances at installing the updates after which the device is forcefully rebooted and updates installed.

6.2 Access Controls

This section defines the rules on who is allowed to access certain data, applications, resources, and services. In most organisations, access rights should be assigned per role (Role-Based Access Control), where for example, a staff member in finance will only have access to folders and files related to finance or the project they are involved with. No staff accounts should have administrator access on the network or company devices. This permission should only be reserved to the IT or Cyber teams; however, it should be a separate account that is common to all staff and must not be used by the staff on day-to-day actions.

This section would also define the protocol that needs to be followed when a member of staff leaves the organisation or role is terminated. There have been cases of an individual being terminated from the organisation, not having their access revoked in due time and causing damage to the organisation by deleting or leaking documents. To avoid this, it is imperative to revoke access to accounts used by the staff member for their activities in the organisation. Some accounts to think about:

- MS Office suite
- Company password manager
- Admin account (if they're in IT)
- VPN and remote access
- Removal from Active Directory
- Emails
- Any other services staff have access to

While revoking access to accounts is the first step, it is important to retrieve all company devices such as phones, computers, USBs or anything that is owned by the company and may have company data stored on it.

6.3 Password Management

6.3.1 Password Creation

Passwords used to access any organisational device or account used for the purposes of the organisation must follow these guidelines:

- Length of 12-16 characters
- Use of numbers
- Use of special characters
- Use of both small and large caps
- Randomised

When processing requests to establish and change memorized passwords, verifiers SHALL compare the prospective password against a list that contains values known to be commonly used, expected, or compromised. For example, the list MAY include, but is not limited to:

- Passwords obtained from previous breach corpuses.
- Dictionary words.
- Repetitive or sequential characters (e.g. 'aaaaaa', '1234abcd').
- Context-specific words, such as the name of the service, the username, and derivatives.

If the chosen password is found in the list, the CSP or verifier SHALL advise the subscriber that they need to create a different password, SHALL provide the reason for rejection, and SHALL require the subscriber to choose a different value.

NIST Guidance: https://pages.nist.gov/800-63-3/sp800-63b.html#sec5

6.3.2 Password Managers

ELCAP does not currently use any password manager.

6.3.3 Authentication Applications

An authenticator application should be used for all business related accounts. The one used by the organisation is Microsoft Authenticator

6.3.4 Password Renewals

Passwords for company provided devices and accounts must be renewed only when:

- The user has lost or forgotten the password
- The account has been compromised
- The account has been found in a database leak

Staff can request password reset via The Admin Team at ELCAP who will link with IT Provider to reset the password following authentication checks.

Staff must immediately inform the Information Security Manager or their equivalent deputy if any of those options have happened. If the reason for password renewal does not fall under the listed above, the Information Security Manager and Policy Manager or their equivalent deputies must agree to the renewal and should consider adding said reason to the list above.

6.4 Incident Response

Incident Response policies have been written and created in a separate document. One of those is our Breach Reporting procedure. Please contact the Business Manager if you have not already received it.

The Incident Response policies must have an updated and printed copy located in key areas of the organisation, such as:

- Offices
- Incident Manager's home
- Policy Manager's Home

These must be ready to use and available in the event of an emergency.

6.5 Data and Backups

6.5.1 Backup Strategy

The business-critical data of the organisation should be stored and backed up according to the following instructions.

6.5.1.1 Local Copy

Staff can only use ELCAP data on authorised devices. What qualifies as ELCAP data is:

- Relevant reports, images or documents relating to projects the organisation is or has

worked on

- Relevant customer data

Staff should only save such data on One Drive or Sharepoint (Office 365). Desktop, documents, pictures and downloads are synced to One Drive and configured appropriately.

6.5.1.2 Local Backup

All files and data stored by staff should be transferred to a local backup for safekeeping and version control.

Local Backups must be stored on a local server or hard drive that is securely stored in a locked place, the structure of these files must abide by the ISO 15689-1:2016 international standard. More information regarding this standard can be found here: https://static1.squarespace.com/static/5a1c710fbce17620f861bf47/t/5a45d41353450a6f05e9b138/1514525716795/ISO+15489-1-2016.pdf

6.5.1.3 Offsite Backup

Offsite Backups are handled by the IT Provider, these backups are used to store:

- Client data
- Reports for projects
- Contracts
- Financial details

Microsoft 365 is backed up by IT Provider. Sage is also backed up manually via Share Point.

These backups are stored on the cloud and secured by the IT Provider.

6.5.2 Data Backup Procedures

Data destined for the local must be encrypted, transferred and stored securely according to the recommendations given by ISO 15689-1:2016. After the transfer is completed the server or drive used for the backups must be stored in a secured place with an access log kept up to date on who accesses the key and at what time.

Offsite Backups being handled by the IT Provider, the protocol used is guaranteed secure by them and include these steps:

- Encryption

Encryption, MFA

6.5.3 Backup Schedule

Local Backups are scheduled to be completed every: Daily

Offsite backups should be completed every: Day

6.5.4 Data Recovery

During an incident or outage, the sectors of the organisation will be brought back up in a certain order. This is to ensure that the organisation is brought up swiftly and ensure that no other issues can resurface. Services and data will be brought up in this order:

Order	Service	Data Needed	Location of Data
1	Finance	Client data, financial details	Local backup and offsite backup
2	Client Facing Website	Website code, account information databases	Local backup and offsite backup
2	Sharepoint - Office 365	Staff, Individuals ELCAP supports & Organisational Data	Off-site back up hosted by Mother Technologies
3	Access Care Planning	Individual ELCAP supports and staff files including reports and submitted forms	Access Host Backup
4	Access People Planner	Rota Planning, payroll and finance exports including staff and individual ELCAP	Access Host Backup
	Direct Care Services	All data relating to service provision to individuals that ELCAP supports and the	Off-site back up hosted by Mother Technologies
	Business Services	Operational information, policies & Procedures and all records held on Sharepoint /	Off-site back up hosted by Mother Technologies
	HR	All personel Documentation including data held on sharepoint / Microsoft 365	Off-site back up hosted by Mother Technologies
	IT	Access to email via Microsoft 365, website and access to Sage	Off-site back up hosted by Mother Technologies
	Board of Directors Governance	Committee Meeting minutes, Action Plans and data required for governance and	

A proper protocol needs to be put in place to verify that the issue has been resolved. This may be a service provided by the IT Provider and should be discussed.

6.5.4 Data Retention

Client data and reports must be deleted in an appropriate timeline which is detailed in the following table:

Type of Data	Location	Retention Period
Client Reports	Local devices, local backups, offsite backups	6 months
Customer Data	Local devices, local backups, offsite backups	5 years
Individual Data	Sharepoint, Local Devices, offisite back ups	
Staff / Employee Data	Sharepoint, Local Devices, offisite back ups	
Policies and Procedures	Sharepoint, Local Devices, offisite back ups	
Committee Meetings	Sharepoint, Local Devices, Microsoft Teams	
Operational Meetings	Sharepoint, Local Devices, Microsoft Teams	
Incident Reports	Sharepoint, Local Devices, offisite back ups	Forever

7. Training and Awareness

Training must follow the following periodicity and objectives.

Training/Test	Objective	How Often
Phishing Test	Evaluate the organisational preparedness to phishing attacks	Every year
Phishing awareness training	Train and inform staff on regular phishing techniques and ways to recognise them	Every year after Phishing Test
Cyber and Policy Education	Inform new staff on the policy around cybersecurity and the basic actions to take regarding cybersecurity	Every new onboarding
Policy Update Awareness	Inform current staff of changes made to the policy document	Every time the policy document is modified
Incident Response Plan testing	Test and evaluate the Incident Response Plan and remind the IR team of the steps and procedures part of the Incident Response Policy	Every year
Board member / Senior Executive Training	Remind and update board member and senior executives on the latest cyber threats that could affect the organisation or the members	Every year

8. Supply Chain Management

When onboarding a new third-party in the organisation's supply chain there will need to be a check of certain criteria that this new organisation would have to meet to be correctly onboarded.

Criteria	Priority
Secure Backups	1
MFA	2
Single Sign On	3
Encrypted Data	4
Geo Redundant Data Centre	5
Secure Data Handling & Retention	6
NDA / Data Protection Agreements / GDPR	7
Cyber Essentials - Supplier Assessment Questionnaire	8

Organisations currently part of the supply chain will be re-evaluated every Year

If an organisation evaluated does not fit the criteria defined above, the following actions can be taken depending on the priority of the organisation and the replies to the criteria above:

- Removing the organisation from the supply chain
- Conversing with the organisation to see if an agreement / action can be made to improve on the overall security

9. Regulatory Compliance

The organisation aims to be compliant with;

Cyber Essentials & UK data protection law, including the UK GDPR

The criteria to be met and how the organisation will or has met these are listed below.

Criteria	How is it met
Training for staff	Phishing training is provided every year to staff
Safe backup procedures	Organisation follows the 3, 2, 1 backup rule
Care Inspectorate	Compliance with regulations for data protection, data handling, data processing.
Data protection laws, including the UK GDPR and other legislation, and ICO guidance on those compliance requirements	Compliance with regulations
East Lothian Council	
Midlothian Council	
Scotland XL Framework	

10. Updating/Reviewing Template

This document must be tested and updated every year.

To test the policies, the policy team will meet and work through a scenario that will test various aspects of the policy. This should be conducted by an exterior consultant to avoid any bias to give the most precise results.

Following this test, the policy team will meet to discuss the results and provide insight into improvements for the document. From there the policy document is updated and staff are made aware of the change.

11. Culture Statement

Guidance is clear that no user should ever be punished for falling for a phishing attack, simulated or real. Punishment discourages users from coming forward and delays the response to the attack, likely leading to greater damage. Aim instead to increase transparency in security processes, encouraging users to report attacks and ensuring incidents are identified and mitigated as quickly as possible. This applies to multiple aspects of the policy.

An organisation's users are the most important part of its cyber resilience, and for that reason, they should be involved in the process as far as possible.

12. Appendices

12.1 Appendix A - Data Audit Table

Software/ Hardware/System/ Device	Asset official use	Asset Administor/ Owner	Identify sensitive data the asset has access to	Is muti-factor authentication required to access this asset?	Risk to business if we lose access to this asset
Sage	Finance processing for accounts and payroll	ELCAP Heather O'Reilly - Finance Officer	Payroll sensitive data, salaries, bank details etc. Account numbers for	Yes	Significant impact as payroll could not be implemented and invoices paid or sent
Share Point	Data Store for staff, individuals and business records	All Head Office staff who have a Premium Licence	Personnel files for staff and individuals. Business / Operational files are	Yes - through Microsoft 365 Accounts	Significant - loss of access would prevent business functionality
Access Care Planning	Platform for individuals & Staff personal data	HQ Staff	Staff and individual records	No - App generated credentials including username and PIN	Significant loss of operational data
Access People Planner	Platform for individuals and staff data including rota processing and	HQ staff	Staff and individual records, including hours worked and rota processing	No - App generated credentials including username and PIN	Significant loss of operational data
Microsoft 365	HQ Personnel & Support Practitioners including Board Members		Access to email content & sharepoint documents	Yes	Significant loss of operational data
Microsoft Teams	All personnell		Confidential files are stored within specific Team Group Files	Yes - through Microsoft credential log in	Loss of minutes, actions and agenda items
Individual Devices - Ref Asset list			Devices are protected by log in credentials	Yes - through Microsoft credential log in	No information should be saved local to the device
Mobile Phones - Ref Mobile Asset List			Telephone numbers of staff and individuals and external contacts	No - PIN protected to mobile device	Loss of contact details
	Refer to full asset list				

Cyber and Fraud Centre Scotland

Incident Response Helpline

0800 167 0623

Cyber and Fraud Centre Scotland
19 Rutland Square
Edinburgh
EH1 2BB

01786 447 441
enquiries@cyberfraudcentre.com
cyberfraudcentre.com
@cyberfraudcen
cyber-and-fraud-centre

A company limited by guarantee and registered in Scotland
No. SC170241 | VAT Registration No. 717 2746