Ethical Standards Commissioner

Commissioner for Ethical Standards in Public Life in Scotland
Thistle House
91 Haymarket Terrace
Edinburgh
EH12 5HE

Information Technology Policy

- Date policy first adopted: 01/04/2011
- Review period: Annually or when changes are required
- Date of last review: 25/01/2024
- Date of next review: 31/01/2025

Index

Section 1 - Introduction

1.1 - Purpose

This Information Technology (IT) Policy outlines the guidelines and principles governing the use of all IT resources within the Ethical Standards Commissioner (ESC) as well as ensuring compliance with all relevant UK laws and legislation, including the Computer Misuse Act (1990) and Data Protection Act (2018).

The integrity and security of these resources, including the information they hold, are critical to the effective operation and reputation of the ESC, as well as protecting the personal data and rights of all individuals involved within the organisation's remit.

All staff are trusted to use IT systems in a sensible and responsible manner as well as exercising good judgement, and ensuring they comply with the ESC Code of Conduct.

1.2 - Scope

This policy is applicable to:

- All individuals who have access to any information or technologies within the ESC.
- All systems managed by the ESC that are used to access or process its information.
- All external parties, including contractors, that provide services to the ESC but do not have their own equivalent terms and conditions to this policy.

Everyone covered by this scope must adhere to this policy regardless of role or location, and any changes will be communicated as soon as possible.

1.3 - Implementation and Review

Overall responsibility for implementation of this policy lies with the Information Management and IT Officer (IMITO) and Head of Corporate Services (HCS).

This policy will be reviewed according to the scheduled timescale by the IMITO, and more frequent reviews may take place to accommodate changes to ensure the policy:

- Remains operationally fit for purpose.
- Reflects changes in technology or software implementations.
- Is aligned with current industry standards and best practices.
- Complies with all relevant UK and Scottish laws and legislation.

1.4 - Monitoring

All IT facilities used by the ESC automatically log all system and user activity which includes, but is not limited to, internet traffic, communications, device usage and location data.

The systems are monitored for the following purposes:

- To detect or investigate unauthorised, unacceptable, or criminal activity.
- To ensure the security of our IT systems and devices.
- To protect the data held by the ESC and record how it is processed.
- To maintain a complete and accurate representation of our records management.

Activity can be attributed to an individual device or staff member, and so all users must expect any interactions with ESC IT resources to potentially be reviewed.

This data is only accessible by staff with system administrator privileges and must not be accessed without a specific purpose.

In the event of an emergency, it may be necessary for the ESC to access an employee's personal data such as email or file storage, but this access must be authorised by an employee's line manager or the HCS.

Monitoring tools must never be used to breach the personal privacy of any staff through real time observation such as accessing their camera, microphone, or live calls, without their express permission.

1.5 - Breaches of policy

Any employee of the ESC who wilfully or repeatedly fails to comply with this policy may be subject to disciplinary action with the possibility of dismissal from the organisation.

Any other individual or external party covered by this policy will be reported to their relevant office or employer, which may also result in the ESC terminating any contract which has been affected by the breach.

Any suspected illegal activity will be reported directly to the police or other relevant authority.

1.6 - Queries

Any queries or concerns regarding any details of this policy, or the use of IT systems, should be directed to the IMITO or HCS.

Section 2 - Acceptable Use

2.1 - Business and Personal Use

All ESC IT systems must be used primarily for business purposes; however, employees may use the systems for limited personal or emergency use provided the terms of this policy are observed and this does not interfere with business operations.

2.2 - Unacceptable Material

IT systems must not be used for the creation, access, transmission, or reproduction of any material that is illegal or otherwise unacceptable to the ESC, unless it is relevant to an employee's duties, such as investigative work.

"Material" should be interpreted as information in any form.

All staff should use good judgement in determining what material is relevant to their work and should refer to their line manager or HCS if clarification is required.

Examples of unacceptable material:

- Offensive, obscene, or indecent.
- Designed to cause annoyance, inconvenience, or disruption.
- Intended to harass, threaten, bully, or discriminate.
- Defamatory or likely to bring the ESC into disrepute.
- Likely to cause damage or exploit IT systems or data.

2.3 - Unacceptable Activities

Staff are not permitted to:

- Attempt unauthorised access of another user's account or personal data.
- Corrupt or destroy organisational or any other users' data.
- Violate the privacy of other individuals.
- Impersonate another employee or act on their behalf without explicit permission.
- Disrupt or hinder the work of any others.
- Download, install, or run any software without permission.
- Knowingly infringe any software or hardware license agreements.
- Access any systems or devices they are not permitted to use.
- Connect unregistered devices or storage to the ESC network or systems.
- Modify systems or hardware in any way without approval.
- Willingly void the warranty of any hardware, through misuse, or unapproved repair.
- Allow any third party to use ESC devices.
- Bypass copyright or intellectual property laws.
- Share confidential data with unauthorised individuals or parties.
- Store personal data unrelated to their work or role at the ESC unless in exceptional circumstances and for a short period of time, and this is at staff members own risk as the ESC cannot guarantee the security and privacy of personal data.
- Commit the ESC to any decisions or initiatives without explicit authorisation.
- Use ESC branding or resources for personal gain or activity conflicting with the ESC.

Section 3 - Accounts

3.1 - Allocation

IT accounts will be created for employees and authorised users as required by their job roles and responsibilities.

Separate accounts will be created for every individual where possible, but shared accounts are permitted with authorisation of the IMITO or HCS.

Usernames should be created using one of the following formats:

- FirstInitial.LastName
- FirstName.LastInitial
- email@ethicalstandards.org.uk

3.2 - Permissions

Account permissions will be assigned based on the principle of least privilege, ensuring that users have access only to the resources and functions necessary for their role.

3.3 - Deletion

When a user leaves the ESC, all associated IT accounts will be immediately deactivated, pending deletion after a specified period.

Data associated with deactivated accounts will be retained for a specified period in accordance with data retention policies and after this period the data will be deleted.

3.4 - Passwords

All users are responsible for selecting strong and unique passwords for their accounts.

All passwords must contain the following:

- A minimum of twelve characters.
- A mix of uppercase and lowercase letters.
- Both numbers and special characters.

Where possible, users should be able to reset their own passwords, and passwords should never expire to keep in line with current best practices.

All users are strongly recommended to use a password management tool, such as Google Chrome, to generate and store their account credentials.

3.5 - Multi Factor Authentication

Where possible, all accounts should have Multi Factor Authentication (MFA) enabled.

MFA must only be used with the following applications on a personal mobile phone:

- Google Authenticator
- Microsoft Authenticator
- Salesforce Authenticator
- Passly Authenticator

If a supported phone is not available, text or email approval is an acceptable alternative.

3.6 - Administrators

Specific users may be given administrator accounts to manage systems or services, which must always be a separate account from their standard account.

Administrator accounts of any kind must only be used when required, never for routine use, and logged out of when work is complete.

Global Administrators will have full control of the entire ESC infrastructure and so there should be as few of these as possible, and currently these accounts must only be provided to the IMITO and the third-party IT Managed Service Provider (MSP).

Local Administrators will have limited and specific controls of the services they are required to manage, and permissions should be removed if there is no longer a required need for them.

A backup Global Administrator account should be created as a fall back in the event all other accounts are unavailable – this account must never be used unless there is an emergency.

Log in details for this backup account should be provided to the MSP, IMITO, HCS, and Commissioner, and then stored securely.

Administrator accounts must only be provided with approval of the HCS.

3.7 - Security

Personal account details must never be shared with anyone.

Shared account passwords must only be shared with staff approved by the IMITO or HCS.

If an account is suspected of being compromised, users must reset their password immediately and notify the IMITO or HCS.

The ESC may suspend access to any accounts at any time to ensure systems and data are protected.

Section 4 - Email

4.1 - Allocation and Access

All ESC staff will be provided with a personal email address with the format:

- FirstInitial.LastName@ethicalstandards.org.uk

Staff are only permitted to access email from Outlook (Desktop Client or Mobile App) or M365 Webmail on provided or authorised personal devices.

4.2 - Shared Mailboxes

Staff will be provided full access and “send as” permissions to any shared mailboxes relevant to their role.

Shared mailboxes will be provided as delegate accounts and have sign in blocked to avoid remote log in.

4.3 - Multiple Recipients

In the interest of transparency, the Blind Carbon Copy (BCC) feature should never be used.

Carbon copy (CC) should not be used to send material to a large number of recipients due to the risk of personal information being released and instead a mail merge should be used.

4.4 - Storage and Filing

Staff mailboxes will have a limit of 0.5 GB, and shared mailboxes a limit of 1.0 GB.

Storage increases may be requested on a temporary basis with permission from line managers.

The HCS and IMITO will arrange a phased move for staff to these new limits.

All email pertinent to the business must be regularly filed according to the ESC Records Management Plan and not stored within individual or shared mailboxes long term.

4.5 - Signatures

All staff must use the ESC email signature templates provided to them for all email.

4.6 - Attachments

Please refer to the secure transfer methods detailed in Section 6.5 Sharing for more information on using Email Attachments.

4.7 - Unsolicited or Malicious messages

All staff must ensure they engage in relevant training and use good practice to identify messages which are unsolicited or malicious.

Staff are permitted to flag unsolicited email as Junk and delete them immediately.

Any malicious messages must be reported to the IMITO or HCS as soon as possible.

Staff must never block any legitimate senders, instead the HCS can invoke the Unacceptable Behaviour Policy when required.

Any suspected phishing accounts not detected automatically may be blocked by the IMITO.

Section 5 - Conferencing and Messaging

5.1 - Allocation

All ESC staff will be provided with Microsoft Teams for internal and external communication.

If a staff member is required to make and receive phone calls, they will be provided with a personal Teams Voice phone number.

5.2 - Instant Messaging

Staff must only use Teams instant messaging for brief day to day communications, as anything pertinent to the business should be conducted by email and filed as a record.

Third party instant messaging services must not be used to conduct ESC work or discussions under any circumstances.

5.3 - Phone Calls

Teams Voice Calling is intended for business use.

5.4 - Meetings and Conferences

Meetings and conferences are configured to only allow invited members to participate, anonymous joining must be disabled.

5.5 - External Parties

Voice and Video conferencing with external parties should be conducted using Teams in the first instance, but Zoom is permitted only if Teams is not feasible.

If neither Teams or Zoom are a possibility and another third-party application is the only option, authorisation must be granted from the IMITO or HCS.

5.6 - Recording and Transcription

All Teams text-based chat is retained for one month before being automatically deleted.

Video and Audio calls may be recorded with approval of the HCS for transcription purposes and the recordings must be deleted once this task is completed.

Complaint interviews involving Members of the Scottish Parliament may be recorded and retained to comply with legislation and associated directions.

Automatic and real time transcriptions of audio or video calls are permitted to be used by staff to assist in the creation of minutes or call reports, provided the transcription text is deleted once the task is completed.

Section 6 - Data

6.1 - Access

Staff will be given access only to the storage areas required for their role.

ESC storage access should be restricted to authorised devices and network connections.

Personal storage areas must only be accessible by the individual the area is assigned to.

Shared storage areas should be accessible by all staff, aside from the sensitive areas detailed below.

The following sensitive areas will be restricted to the Senior Management Team, HR and Facilities Officer, and Governance and Finance Officers:

- Finance - Payroll
- Staff - Personnel Files

6.2 - Permissions

Where possible, staff should be given “modify” permissions for files and folders they have access to, and only administrators should have “full control” permissions.

“Modify” will allow staff to create, edit, and delete files and folders whereas “full control” also allows changes to file permissions.

6.3 - Storage Areas

ESC data must only be stored in the following areas:

- ESC file server
- ESC file backup system
- Microsoft 365 (Includes Email, OneDrive, SharePoint, Teams)
- Salesforce Content Management System
- ESC Drupal 10 Website
- Appointments Knowledge Hub
- Sage Accounts
- MyePay Payroll
- Pension Portal
- Internal and External Auditor platforms

The following areas are permitted for short term temporary storage:

- ESC laptop hard drive
- Authorised external storage devices

6.4 - Processing

ESC data must only be read or processed by authorised platforms and applications and must not be entered into third party Artificial Intelligence systems.

6.5 - Sharing

To ensure good version control, data should be shared internally by creating a direct link to the original file, and not by creating a copy for distribution.

Data transfers to external parties must be sent only to specific individuals or groups.

When sharing sensitive data with external parties, there is a risk that email may be inadvertently sent to the wrong address or that email may be intercepted in transit.

We intend to move away from sharing confidential, sensitive, special category and personal data by email attachment and will aim to use the secure transfer systems detailed below.

Until then, staff should consider whether the content of an attachment is sufficiently sensitive to warrant being password-protected, and passwords must be sent in a separate email to the same recipient.

Secure data transfer systems currently authorised by the ESC are:

- Microsoft OneDrive
- WeTransfer
- Egress
- Authorised external storage devices

Anonymous or open sharing methods must not be used.

6.6 - Filing and Retention

Data pertinent to the ESC must be filed according to the ESC Records Management Plan, which dictates the storage locations and retention periods for specific data types.

6.7 - Deletion

Filed data must not be deleted until the relevant retention period has been exceeded, unless the data is being deleted to remove a duplicate or old data is being replaced with an updated version such as a new draft.

Where possible, automated schedules should be used to delete filed data.

If filed data must be deleted manually, this must be authorised by the asset owners described in the ESC File Plan and Retention Schedule. Otherwise, asset owners may delegate the management and deletion of records to relevant staff members.

All filed data deletions must be recorded in the data destruction log prior to deletion.

Temporary data, empty folders, or data created in error, may be deleted without permission or logging.

6.8 - Backups

The ESC file server must be backed up daily to an off-site location using a secure solution.

Backup integrity must be tested regularly.

6.9 - Data Breaches

All suspected data breaches must be reported immediately to the IMITO and HCS for investigation.

All breaches must be entered into the Data Breach Log.

Section 7 – Hardware

7.1 - Allocation

All ESC staff will be provided with the necessary equipment allowing them to work both at home and in the office:

- A laptop preconfigured with Windows 10 or later, and all necessary software.
- A monitor, mouse, and keyboard for home use.
- A keyboard and mouse for office use.

7.2 - Requesting

If an employee wishes to request additional or specialist hardware, they must make a request with reasoning to their line manager who will consult with the IMITO or HCS, who can then review and determine what is possible.

Hardware not related to the business function of the ESC or to support reasonable adjustments are unlikely to be considered.

7.3 - Procurement

Hardware, supplies, and parts must only be purchased with approval of and by the HCS, through a genuine and authorised vendor.

7.4 - Replacements

Provided laptops are expected to last for five years before being replaced.

If a laptop is rendered unusable before this time, a suitable alternative will be provided depending on available budget and specific user requirements, unless there are reasons not to (e.g. the staff member is absent or a disciplinary process has been engaged).

Other equipment and devices will be replaced when required or at end of life.

7.5 - Security

All laptops must be encrypted to secure data on the local hard drive, and staff should be required to enter a unique PIN to unlock the laptop at startup.

All staff must manually lock their devices when they are not in use, and devices should auto lock after 15 minutes of inactivity.

All ESC computers must have endpoint security, firewall, and anti-virus solutions installed.

ESC hardware firmware updates will be applied by the MSP or IMITO when appropriate.

ESC equipment must only be used by authorised staff, and never be left unattended in a public area.

Any suspected or confirmed illegitimate access to ESC devices must be reported to the IMITO, HCS and relevant line manager as soon as possible.

7.6 - Personal Devices or peripheral

If a staff member wishes to use a personal device or peripheral an application form must be completed and sent to the HCS and a security check-up will be conducted by the IMITO where necessary. A peripheral is any external device that connects to a computer to allow data to be input, output, or stored. This includes but is not limited to printers, monitors, keyboards, mice, external storage, speakers etc.

Staff must only connect authorised peripherals to their laptop.

Unknown storage devices must never be connected to a device under any circumstances.

7.7 - Use and Care

Staff are responsible for safeguarding their allocated equipment, and ensuring devices are kept in a good and clean condition.

Equipment must not be operated, handled, or stored in a way that will risk damage.

When transporting equipment, it is strongly recommended to use a padded backpack or other suitable solution, as well as powering off any equipment before moving it.

To preserve the battery life of equipment, it is recommended to fully shut down any devices when they are not in use rather than using standby or hibernation modes.

Cables must be kept loose and free of tangles to avoid damage, and must never be used if there are any visible defects.

Food or liquids must not be stored or consumed near equipment.

7.8 - Damage, Loss, or Theft

Any damage, accidental or otherwise, must be reported to the IMITO or HCS, and the device should be disconnected from a power source immediately if it is safe to do so.

Staff must report missing or stolen equipment as soon as possible to the HCS and the police or other appropriate authorities and obtain a crime reference number.

7.9 - Repairs

Repairs must only be carried out by specialists with the approval of the IMITO or HCS.

Devices within warranty must be repaired by the original manufacturer or supplier, however, reputable third-party companies may be used if the device is out of warranty.

7.10 - Returning

All provided hardware must be returned by staff as soon as possible when it has been either replaced or they leave the organisation.

Staff must ensure that they have backed up any local data from any devices before they are returned, as all data will be wiped by the IMITO.

7.11 - Disposal

Hardware must only be disposed of through an authorised company that adheres to Waste Electrical and Electronic Equipment recycling (WEEE) regulations and have secure data destruction policies in place.

Section 8 - Software

8.1 - Availability

ESC devices will be provided with the general software necessary for all roles.

Specialist programs may only be accessible on specific devices or by users who require it.

ESC provided software must only be used on personal devices with explicit approval of the IMITO or HCS.

All approved applications will be listed on the Software Whitelist, which will be regularly reviewed by the IMITO.

8.2 - Requesting

If an employee wishes to request additional software, they must make a request with reasoning to their line manager who will consult with the IMITO or HCS, who can then review and determine what is possible.

Software not related to the business function of the ESC or to support reasonable adjustments are unlikely to be considered.

8.3 - Procurement

Software must only be purchased with approval of the IMITO or HCS, through a genuine and authorised vendor.

8.4 - Installing

Software must only be installed by the IMITO or the MSP with approval by the HCS.

8.5 - Updates

Where possible, automatic software updates will be enabled.

Manual updates must only be performed by the IMITO or MSP.

8.6 - Licensing

All software, from licensed to open source, is subject to terms and conditions which must be followed without exception.

Where possible, software should be licensed to individual user accounts.

If a software license or account permits sharing, and there is no individual user alternative available, a shared email address will be used to create the account.

8.7 - Removal

If software is no longer required, it will be removed.

If any software is found to contain security vulnerabilities which cannot be resolved, it may be removed without warning while an alternative is investigated.

8.8 - Remote Management

Remote desktop viewing and control must only be used by the IMITO or MSP to troubleshoot issues, and only with explicit confirmation from the end user.

Remote tools must never be used to access a staff member's camera or microphone without their permission.

Section 9 - Office Working

9.1 - Hot Desking

All desks within the office are to be shared by all staff, and all should be equipped with the same setup which will consist of a laptop dock connected to a monitor.

The office docking stations must only be used by ESC provided laptops.

All staff will be provided with a wireless mouse and keyboard to use when in the office.

9.2 - Clear Desk and Screen

At the end of an office shift, all desks must be cleared of personal equipment, belongings, and physical documents, and then returned to the original setup.

Staff must ensure their screen cannot be viewed by unauthorised parties while working, and must lock their screen when away from their desk.

9.3 - Wireless Network Access

Two wireless networks are provided within the office.

- “ESC Secure” must only be used by ESC provided devices.
- “ESC Guest” is only to be used by personal or visitor devices.

Office wireless access must be encrypted, and password protected.

The ESC Guest connection must not allow access to any other devices on the network.

9.4 - Multi Function Printer

Staff must ensure that they do not leave printed materials or any other physical documents within the printer after using the MFP.

Sensitive materials that are no longer required must be immediately shredded or placed into the marked bag for future shredding which must be stored securely.

The MFP must be configured to not store print or scan details once a job is completed.

9.5 - Equipment Storage

Personally allocated IT equipment left on site must be kept within a staff member’s own designated storage unit and locked securely.

The IMITO and HCS will be responsible for all other IT inventory belonging to the business and must store this in a secure location.

9.6 - Infrastructure Access

Access to the ESC server room and equipment should be limited to the IMITO and HCS.

All other visitors or third-party support staff must be accompanied by the IMITO or HCS.

If both the IMITO or HCS are unavailable, a member of the SLAB Information Security team may accompany them.

Section 10 - Remote Working

10.1 - Working Abroad

Staff are not permitted to work remotely or take ESC IT equipment outside of the UK.

10.2 - Working in Public

Staff should not connect to open public (passwordless or password advertised openly) or unknown third-party internet for work purposes as security cannot be guaranteed and internet traffic could be monitored.

Staff may use connections hosted by reputable organisations such as large-scale businesses, local government, and education.

Using a personal mobile phone device as a hotspot for ESC devices is permitted.

10.3 - Home Working

Staff must ensure their home working environment passes a Display Screen Equipment risk assessment and equipment can be safely stored and secured.

10.4 - Clear Desk and Screen

Staff must keep their workspace clear of physical documents or any sensitive materials while not in use, and these must be securely stored otherwise.

Staff must ensure their screen or any other materials cannot be viewed by unauthorised parties while working remotely, and they must lock their screen when not actively working.

10.5 - Home Internet

It is the responsibility of staff to choose a reputable home broadband Internet Service Provider (ISP), and that the connection is sufficiently fast and stable enough to allow the following:

- Video Conferencing and Streaming
- File Transfer
- Remote Desktop

Minimum broadband speeds of 25 Mbps download and 5 Mbps upload will be sufficient.

If you have any concerns about implementing this requirement, the IMITO can provide advice regarding home networks, however the ESC will not be responsible for resolving faults with personal networks or equipment.

10.6 - Router Configuration

Most ISPs will supply a broadband router which will be preconfigured with industry standard security features and passwords in place, and it is strongly recommended to leave these features unaltered unless directed by the ISP.

At a minimum, a home router must have the following security features:

- Administrator settings access must require a password.
- Wi-Fi connections must require authentication.
- Firewalls are enabled.

All ISPs will be able to confirm if their router meets these requirements.

To improve security, a router should not be left in a public area and stored securely if possible.

Wi-Fi access should only be given to others who live within the premises or are trusted guests.

The IMITO must be informed of any changes to the default configuration of a supplied router, or if a third-party alternative router is used.

10.7 - Remote Desktop Server

When working remotely, staff must connect to the Remote Desktop Server (RDS) to gain access to the ESC file server as well as specialist applications that may not be available on their provided laptop.

The RDS may be taken offline at any time for maintenance or security reasons, and advance warning will be provided with as much notice as possible.

RDS users may be logged off remotely or have running applications terminated by the IMITO or MSP if there is a security or system concern.

Where possible, routine updates to the server and applications will be scheduled outside of standard working hours.

Staff should not engage in conferencing or streaming over the RDS as the quality may be poor and should instead do this directly on their laptop.

As the RDS is a shared resource, staff should close any applications not in use to free up memory and be aware of how many active internet browser tabs they have open.

When a user has finished for the day, they must use the “sign out” option on the RDS and not use “disconnect” or just close the RDS window, as this leaves their session active.

Section 11 - Social Media

11.1 - Conduct and Risk

Staff must adhere to the Social Media guidelines detailed within the ESC Code of Conduct at all times.

All social media activity has the risk of being made publicly visible at any time now or in the future, regardless of the current safeguards or rules in place.

11.2 - Personal Accounts

The ESC will not monitor personal social media accounts; but it is important that staff make a clear distinction between their personal activity and work activity.

Staff must not use personal accounts to engage with individuals involved in an investigation or engaging with any other ESC function.

11.3 - Investigative Work

Social media accounts provided for investigative work are intended solely for observation and gathering evidence and must not be used to post items or interact or communicate with the site or other users in any way.

11.4 - Official Communications

Social media accounts provided for official communications are solely intended for highlighting services or reports for the ESC, or hosting accessibility related materials such as British Sign Language videos.

All official communications must be authorised by the relevant line manager and follow the ESC corporate identity and design guidelines.

If an external individual submits a query to our social media accounts, they should be directed to the official channels on our website and not be answered either publicly or by direct messaging.

The safest practice will be to minimise engagement unless necessary.

11.5 - Reporting

Any concerns regarding social media activity should be reported to the IMITO and HCS.

Section 12 – Fault, Incident and Disaster Response

12.1 - Fault Response

All IT faults or concerns should be reported as soon as possible.

Problem resolution will be prioritised based on the severity and urgency of the issue.

General issues should be reported directly to the MSP.

Requests for change should be reported to the IMITO.

Critical or urgent issues should be reported to both the IMITO and HCS.

12.2 - Business Continuity

If key staff are temporarily or permanently unavailable, responsibilities and decision-making regarding ESC IT systems will fall to others to ensure the organisation can still function.

These considerations are set out in the Scheme of Delegation.

12.3 - Incident and Disaster Response

In the event of a serious failure or risk to ESC systems, the ESC Contingency Plan must be followed.

In summary, the following steps will be taken:

- Notify the IMITO, SMT, and MSP by phone.
- Report any criminal activity to the police.
- Contact the Scottish Cyber Co-ordination Centre (SG3).
- Advise all staff to stop using their accounts and power off ESC devices.
- Disable any compromised accounts.
- Remotely force all users to log out of from any cloud or remote services.
- Obtain and secure access to the physical network and server infrastructure.
- Physically disconnect all equipment and services from the network and internet.
- Power down any damaged equipment if it is safe to do so.
- Run offline security scans on any compromised systems.
- If a threat cannot be safely removed, wipe all data and software from device and reset the firmware to factory defaults.
- Re-install a clean version of the relevant Operating System to any wiped devices.
- Repair or replace any damaged equipment.
- Ensure systems are functioning correctly and run further threat scans until clear.
- Reset the password for any compromised accounts and ensure accounts are secure.
- Reconnect systems to the network and internet.
- Restore backups to clean systems.
- Advise staff they can re-connect to ESC systems and services.
- Monitor all systems and logs closely for any issues.

Section 13 - Impact Assessments

Equality Impact Assessment

Does this policy comply with the general Public Sector Equality Duty (s149 Equality Act 2010)?

This policy applies to all employees. We recognise that those with certain disabilities, such as visual impairments or mobility issues may have difficult with some requirements of this policy. Where possible, the Commissioner will make reasonable adjustments to the policy to accommodate these.

Data Protection Impact Assessment

Have we considered any effect the policy may have on the collecting, processing, and storing of personal data?

This policy aims to strengthen the protection of our personal data assets.

Information Security Impact Assessment

Have we considered the impact any policy may have on our cyber-resilience?

This policy aims to strengthen the protection of all our information assets.

Records Management Impact

Have we considered the impact any policy may have on our ability to manage our records?

This policy encourages the correct use and storage of our information assets.

Section 14 - Policy Versions

Version	Description	Author	Date
3.0	Full rewrite of original Information Security Policy	IMITO	##/03/2024