Information Security Policy

Introduction

1.1. Background

This Information Security Policy is based upon the International Standard ISEC/ISO 270001 the Code of Practice for Information Security Management and ISEC/ISO 270002.

1.2. Requirements for policy

Intech Centre has an obligation to clearly define requirements for the use of its information technology (IT) facilities and its information systems (IS) to all staff, learners and partners.

The objective of this requirement is to ensures that users of IT/IS facilities do not unintentionally place themselves, or the Centre, at risk of prosecution or disciplinary action, by carrying out computer related activities which contravene current policy or legislative restrictions.

Information within the Centre is intended to be openly accessible and available to all members of the organisation for sharing and processing. Certain information (sensitive information) has to be processed, handled and managed securely and with accountability.

This policy outlines the control requirements for all information contained within the Centre network and IT systems.

1.3. Policy Structure

This document forms the Centre's Electronic Information Security Policy. Its purpose is to provide an overarching framework (a commitment of undertaking) to apply information security controls throughout the Centre.

1.4. Purpose and scope

All processing of data and collection of information will be processed in accordance with UK law.

This policy defines how the Centre will secure electronic information, which is found within:-

- The Centre's IT infrastructure
- CMS data and information systems.
- Security of information held in electronic form on any Centre computer.

And is processed or used by:

- Centre Staff and learners who have access to or administer the Centre network or IT systems.
- External users, agents and guest users authorised to use Centre network or IT Systems.
- Individuals who process key data and information within CMS.

1.5. Objectives

Information Security controls are designed to protect members of the Centre and the Centre's reputation through the preservation of:

- Confidentiality - knowing that key data and information can be accessed only by those authorised to do so;
- Integrity - knowing that key data and information is accurate and up-to-date, and has not been deliberately or inadvertently modified from a previously approved version; and,
- Availability - knowing that the key data and information can always be accessed.

V6 May 2024
By Network Engineer
Signed by MDS

362 Essex Road • Islington • London • N1 3PD
Tel: 020 7354 5655
info@intechcentre.com • www.intechcentre.com

1

The Centre is committed to protecting its members and CMS. Controls will therefore be deployed that mitigate the risk of vulnerabilities being exploited which adversely affect the efficient operation of the Centre.

1.6. Applicability

This policy applies to all users of the Centre network and IT Services and includes:

- all full-time, part-time and temporary staff employed by, or working for or on behalf of the Centre;
- learners studying at the Centre;
- Third party contractors and consultants working for or on behalf of the Centre;
- All other individuals and groups who have been granted access to the Centre's network or IT Services.

These categories of persons and agencies are collectively known as the 'user' in this policy document

Senior Manager is ultimately responsible for ensuring that adherence to this policy, overseeing compliance by users and control or supervision.

Each user is responsible for their own actions and must ensure all actions relating to using the Centre network and IT Services adheres to the principles and requirements of this policy.

2. Legislation and policy

2.1. Legislation

Supply and use of the Centre network and IT Services is bound by UK law. A list of current legislative requirements relating to the use and provision of IT Services is contained in the Policy for using Centre IT Resources; this is not an exhaustive list of relevant legislation.

2.2. Associated Policies

The Centre is also governed by external policies which impose responsibilities on the provision of IT Services and network access, these include:

- Acceptable Use Policy

The principles in this policy support and enhance the requirements contained within these documents and ensure compliance with contractual agreements.

3. Information Security - risk management

Information security governance is the structure which supports the implementation of this policy. An IT infrastructure will be implemented within the Centre to ensure the effective and efficient implementation of this policy across the Centre.

3.1. Ownership and maintenance of policy

This policy is owned by IT Services and is maintained, reviewed and amended by the Network Engineer in accordance with Centre policy, procedures and guidance.

This policy will be subject to annual review and will be submitted to the Director if substantial amendment or redrafting is required in order to maintain relevance and effectiveness.

V6 May 2024
By Network Engineer
Signed by MDS

362 Essex Road • Islington • London • N1 3PD
Tel: 020 7354 5655
info@intechcentre.com • www.intechcentre.com

2

3.2. Risk management and Electronic Service Incidents

The IT Services will be responsible for raising an incident message in relation to any reported security incident at the Centre. These incidents will be recorded as "Electronic Security Incidents".

Electronic Security Incidents will be recorded with a unique reference number; a review of incidents will be conducted at six monthly intervals. Incidents considered to be exhibiting unacceptable levels of risk to the Centre network or IT Services will be subject to an investigation to identify the inherent vulnerabilities exposed by this incident. A report will be submitted to the Senior Manager for consideration of the question of suitable remedial action which may be effectively implemented to mitigate future risks.

3.3. Security of Third Party Access

Procedures will be developed to regulate access to the Centre's information processing facilities by third parties. Such access will be controlled and regulated in order to protect information assets and prevent loss or damage to data through unauthorised access.

3.4. Identification of risk from third party access

Third parties who require access to the Centre's IT infrastructure will be bound by contracts which define Centre security requirements. Prior to being granted any network connectivity they will be required to sign an undertaking to adhere to the requirements of the ICT Acceptable Use Policy and where sensitive information or sensitive business information is involved, they will be required to sign a non-disclosure agreement prior to access to the IT network.

4. Asset Clarification

Information assets will be categorised and recorded to enable appropriate management and control.

4.1. Inventory of assets

IT Services will maintain an inventory, subject to audit, of assets in three categories:-

- Centre Business Systems
- Hardware inventory
- Software inventory

An inventory of electronic learning resources is maintained by Learning Information Systems.

5. Personnel Security Issues – roles and access levels

Controls will be deployed to reduce the risks of human error, theft, fraud, nuisance or malicious misuse of facilities.

IT Services maintains the directory of people and accounts which are authorised to use the Centre network, IT Services and applications. All users, Staff, learners, external users and guest users are subject to the principles of this policy and must certify that they agree to the terms, conditions and acceptable use policy contained within the ICT Acceptable Use Policy and the Policy for using IT resources.

For the purposes of this policy authorised users of the Centre network and IT Services will belong to one of the following groups:

- Centre staff - those people registered on Centre Personnel/Payroll systems
- Centre learners - those people registered on the Centre Client Management System
- Guest users - people permitted temporary access to Centre public IT facilities

V6 May 2024
By Network Engineer
Signed by MDS

362 Essex Road • Islington • London • N1 3PD
Tel: 020 7354 5655
info@intechcentre.com • www.intechcentre.com

3

- External users - all other people permitted access to Centre IT systems for a predefined time.

The above list will be reviewed periodically to ensure the authorised user list maintains relevance to the business model of the Centre.

If a user's relationship with the Centre alters, due to a change in role or employment relationship, then the revised level of access must match both the new role and relationship with the Centre. All IT account access levels must comply with the requirements of the ICT Acceptable Use policy.

5.1. Security in job descriptions

Security roles and responsibilities will be included in job descriptions where appropriate. These will include any specific responsibilities for the protection of particular assets, or the execution of particular processes or activities such as data protection.

5.2. Confidential personal data – sensitive information

All data which identifies any individual will be handled in accordance with the Data Protection Act 1998. All personal details will be held securely and in accordance with current UK legislation.

Data transferred to external organisations should be encoded using the current recommendations in the Personal Responsibilities for Electronic Information Security.

All data classified as Sensitive Data will be processed and stored in compliance with the current Sensitive Information guidelines and Centre policies and procedures.

5.3. Confidentiality undertaking

All learners, members of staff and partners are reminded of their obligation to protect confidential information in accordance with the Centre's standard terms and conditions of employment.

All users will be bound by the confidentiality agreement in either their contract or terms of employment.

5.4. Employee responsibilities

All staff (including agency and casual staff) must agree to written terms and conditions contained within the ICT Acceptable Use Policy when they register to use an IT account.

Casual staff accounts will be set to expire at the end of the staff contract period; this period should only exceed 6 months in exceptional circumstances and a request for an extension must be accompanied by the business case for such an extension.

Personnel Services shall ensure that:

- Confidentiality agreements form part of the terms and conditions of employment
- Awareness training about electronic information security forms part of Centre staff induction programmes
- Information for all staff on electronic information security is maintained in the staff handbook.
- All references for a period extending to 3 years prior to the recruitment date are checked by Personnel prior to a member of staff's commencement of employment.

Schools and Services must ensure that where there are specific security roles and responsibilities that these are documented in all relevant job descriptions and that there is appropriate screening of applicants.

5.5. Staff leaving employment

On termination of employment with the Centre the user account will be managed in accordance with the procedure detailed in the ICT Acceptable Use Policy.

V6 May 2024
By Network Engineer
Signed by MDS

362 Essex Road • Islington • London • N1 3PD
Tel: 020 7354 5655
info@intechcentre.com • www.intechcentre.com

4

In accordance with the ICT Acceptable Use policy, except where a strong business case exists, which meets the needs of the Centre, all user accounts will be closed at the termination of employment. Files and folders will be deleted shortly after the user leaves the Centre.

5.6. Responding to security incidents

5.6.1. Suspected security breach

Staff or learners using or administering the Centre network or IT Services must not in any circumstances try to prove or collect evidence in relation to any suspected or perceived security breach. The exception to this rule is where staff has been granted a specific policy exemption which allows them to do so as part of their role. IT Services will be responsible for identifying members of staff who are responsible for security breach investigations.

A security incident is any incident which alters, destroys or amends data within the Key Business Systems without authority. May cause damage to or reduces the efficiency of the Centre network or IT Services. This includes any actions or behaviour which contravenes Centre policy, statutory or common law legal requirement or professional regulation or guidance.

5.6.2. Reporting Security incidents

All suspected security incidents are to be reported in the first instance to the Network Engineer.

The IT Service Desk system will be used to record suspected security incidents through the service desk. Unless the initial risk assessment indicates that such a recording process will put the investigation in jeopardy or alert the persons involved in criminal activity.

All reported security incidents and active investigations will be monitored by the Senior Manager. An appropriate investigation and action plan will be prepared and agreed the Senior Manager.

Within the provisions of UK law, the Centre reserves the right at any time to intercept and monitor communications in accordance with the Regulation of Investigatory Powers Act; The Telecommunications (Lawful Business Practise) and (Interception of Communications) Regulations. The above legislation will be implemented in compliance with the monitoring provisions contained within the ICT Acceptable Use Policy

Monitoring and recording of electronic communication and data will be carried out in accordance with current Centre policy and interception/monitoring of individual activity shall normally only take place with the prior express approval of the Senior Manager, but may be undertaken without any prior notice to the users of Centre systems. Permission for undertaking monitoring or surveillance of user activity may in the first instance be given verbally; any such permission must be recorded in writing as soon as practicable, this requirement is to ensure an auditable investigatory process exist for any subsequent disciplinary or criminal proceedings.

5.6.3. Security Incident management/ investigation

Security Incidents will be processed in accordance with the CSIRT Information Security Procedure. The senior member of staff identified as being responsible for investigating the incident will ensure that all steps are taken to limit damage and loss of data whilst preserving the reputation of the Intech Centre.

IT Services will maintain written procedures for the operation (e.g. start up, backup, shut down and change control) of those Centre Key Business Systems where threat, risk and organisational impact would adversely the operational effectiveness or organisational reputation.

V6 May 2024
By Network Engineer
Signed by MDS

362 Essex Road • Islington • London • N1 3PD
Tel: 020 7354 5655
info@intechcentre.com • www.intechcentre.com

5

5.6.4. Investigating Information Security Incidents

On receipt of information indicating that a security incident may have taken place the Senior Manager will nominate a member of staff to coordinate the investigation. The investigation will follow the CSIRT Information Security Procedure.

5.6.5. Network isolation and reconnection

Any device perceived as placing the integrity of the Centre IT network at risk to harm or service interruption will be isolated from the main network domain. Suspension of network connectivity will remain in force until the issue has been investigated and a plan of action agreed with the Senior Manager. Subsequent reinstatement will only be permitted once the requirements of that action plan have been met, verified and authorised by the Director.

6. Physical and Environmental Security

Controls will be implemented as appropriate to prevent unauthorised access to, interference with, or damage to information assets.

6.1. Physical security

Computer systems and networks will be protected by suitable physical, technical, procedural and environmental security controls.

File servers and machines that hold or process high criticality, high sensitivity or high availability data will be located in physically secured areas. All Key Business Systems will be subject to security measures which supports the Centre Business Continuity Plan.

6.2. Data Storage Facility Security

Access to the server rooms and rooms containing data communications or telephone equipment will be controlled and restricted. Authority to access these areas will be controlled by the Network Engineer. Records of authorisation will be maintained by IT Services. Access control will be by smart card, key lock or digital lock as appropriate.

6.3. Equipment Security

Servers holding corporate information will be held in a secure environment protected by:-

- Physical security and access control
- Fire detection and extinguishing systems
- Temperature and humidity control
- Water sensors
- Stable, conditioned electrical supply protected by uninterruptible power supply (UPS) and standby generator
- Centre electronic information will be held on servers approved by IT Services. External hosting must not take place without prior approval from the Senior Manager.
- Key communications equipment will also be protected by UPS.

IT Services must ensure the IT Infrastructure is covered by appropriate hardware and software maintenance and support.

Workstations must be appropriately secured and operated by Centre staff who must be trained in and fully conversant with this policy and their personal responsibilities for confidentiality of information displayed on the screen or in printed output.

Backup media must be retained in accordance with Centre policy on retention of records and the Data Protection Act 1998.

V6 May 2024
By Network Engineer
Signed by MDS

362 Essex Road • Islington • London • N1 3PD
Tel: 020 7354 5655
info@intechcentre.com • www.intechcentre.com

6

All Centre data must be cleared securely from Centre IT equipment and media on disposal. All IT equipment must be disposed of via the Centre's appointed WEEE contractor; this contract includes secure erasure and destruction of data.

7. Communications and Operations Management

Controls will be implemented to enable the correct and secure operation of information processing facilities.

7.1. Documented operating procedure

Design, build and configuration documentation will be produced in respect of system platforms. Sensitive documentation will be held securely and access restricted to staff on a need to know basis.

7.2. Segregation of duties

Access to Key Business Systems and key data and information will only be granted based on the user role and access classification.

Segregation of duties between operations and development environment shall be strictly maintained and all work on Key Business Systems will be strictly segregated.

Permanent and full access to live operating environments will be restricted to staff on role-based requirements.

Sensitive operations will be identified and action taken to implement split functional controls where appropriate

7.3. System planning and acceptance

7.3.1. System changes

All changes to live Key Business Systems will follow a pre-defined change management process, to ensure that activities are undertaken in accordance with stringent change control processes.

7.3.2. Controls against malicious software

Controls will be implemented to check for malicious or fraudulent code being introduced to Key Business Systems.

Source code written by contractors and staff will be subjected to security scrutiny before being installed on any live Key Business system.

All systems will be protected by a multi-level approach involving firewall, router configuration, e-mail scanning, and virus and spy/malware protection on all workstations on the Centre network.

All Centre workstations will have appropriate anti-virus software installed by IT Services set up to update anti-virus signatures automatically. This must not be turned off by users with unlocked desktops. Any device found to pose a threat to data or the provision of the Centre network will be isolated from the Centre network until the security issues are resolved.

Staff and learners may use their own PC hardware to connect to the Centre WiFi network. Equipment so used will be subject to security checks and a number of pre-requisites before being allowed to establish a connection with the Centre network.

Network traffic will be monitored for any anomalous activity which may indicate a security threat to the network.

V6 May 2024
By Network Engineer
Signed by MDS

362 Essex Road • Islington • London • N1 3PD
Tel: 020 7354 5655
info@intechcentre.com • www.intechcentre.com

7

7.3.3. Virus protection

A Virus Protection procedure will be implemented to prevent the introduction and transmission of computer viruses both within and from outside the Centre. Failure to maintain a device in a state which prevents or detects virus infection will leave the device liable to exclusion from the Centre network until the security issue is resolved.

7.3.4. Security patches fixes and workarounds

The Desktop Management Team will be responsible for the day to day management of systems and are responsible for ensuring that security patches, fixes and workarounds are applied in a timely manner to reduce vulnerabilities to devices within the Centre network. Such patches, fixes and workarounds must be tested and approved before deployment and the efficiency of the deployment to the Centre IT estate will be monitored to ensure the effective mitigation of risk due to known vulnerabilities.

7.4. IT Housekeeping and storage

7.4.1. Data Storage

System backups will be performed by the relevant IT support staff in accordance with documented procedures. The procedure will include keeping backups off site in secure storage. Periodic checks will be made to ensure backup media can be read and files restored. Records of backups will be monitored by Network Engineer.

Backups of corporate data are taken on a daily basis for Key Business Systems or less frequently if appropriate. Backups protect electronic information from major loss or failure of system software and hardware. Backups are not designed to guard against accidental deletion or overwriting of individual user data files Backup and recovery of individual user files is the responsibility of the owner (see "Personal Responsibilities for Electronic Information Security").

7.5. Network management

Controls will be implemented to achieve, maintain and control access to computer networks, including wireless LANs.

The configuration of critical routers, firewall and other network security devices will be the responsibility of, maintained by, documented and kept securely by the Network Engineer.

No IT equipment may be connected to the Centre network without approval by IT Services. Any device found to be installed without prior authority from IT Services will be disconnected, the equipment removed and an investigation commenced to establish the cause of the network compromise. Users should be aware that installation of such devices is potentially a disciplinary and criminal offence under the Misuse of Computers Act 1990.

7.6. Device Disposal

Removable magnetic and optical media containing Key Business System data or Sensitive Information will be reused or disposed of through controlled and secure means when no longer required, in accordance with the Disposal of IT equipment advice. Redundant computer equipment will be disposed of in accordance with the Waste Electrical and Electronic (WEEE) Regulations and through secure and auditable means.

Procedures will be made available for the secure disposal of removable data storage media containing Key Business System data or sensitive information when these become defunct or unserviceable. Users should contact the IT Services, Service Desk for the current procedures.

7.7. Software usage and control

Software will be used, managed and controlled in accordance with legislative and Centre policy requirements in relation to asset management and licence agreements.

V6 May 2024
By Network Engineer
Signed by MDS

362 Essex Road • Islington • London • N1 3PD
Tel: 020 7354 5655
info@intechcentre.com • www.intechcentre.com

8

All major software upgrades and in-house systems development for Key Business Systems will be appropriately controlled and tested through a managed process before live implementation and deployment.

All software used on devices managed by IT Services must be installed in compliance with current software licensing policy and software deployment policy. Software installed without IT Services authority and agreement may leave a user liable to prosecution under the Misuse of Computers Act 1990 and disciplinary action.

8. Information Exchange Requests

Use of the Centre network will be governed by the Electronic Information Security Policy and the Policy for using IT Resources.

Failure to comply with these requirements will leave a user liable to disciplinary and/or possible criminal legal penalties.

8.1. Exchange of information with outside organisations

Requests by external bodies for the provision of electronic information from Key Business Systems will in all instances be referred to the system owner. This includes Data Subject Access Requests made under the auspices of the Data Protection Act 1998.

9. Access control

Policy Statement

Procedures for the registration and deregistration of users and for managing access to all information systems shall be established to ensure that all users access rights match their authorisations. These procedures shall be implemented only by suitably trained and authorised staff. A periodic review will be conducted to verify user access and roles.

9.1. Intech Centre Operational Policy

Access to Key Business Systems will be appropriately controlled and comply with the access rights of the user.

Access to the Centre network and IT Services will be restricted according to the access classification of the user.

Centre staff, learners and external users may use:

- Standard software portfolio
- Shared file store
- Email, calendar and public folders**
- Centre Business systems**
- Electronic learning resources
- Internet

**These services will not be provided to all EX account users (e.g. representatives of external organisations with their own email accounts).

9.2. User responsibilities

Users of the Centre network must comply with the ICT Acceptable Use Policy and the Personal Responsibilities for Electronic Information Security.

V6 May 2024
By Network Engineer
Signed by MDS

362 Essex Road • Islington • London • N1 3PD
Tel: 020 7354 5655
info@intechcentre.com • www.intechcentre.com

9

All staff (including agency and temporary staff) must agree to written terms and conditions covering use of IT when they register to use Centre IT.

Personnel Services shall ensure that:

- Confidentiality agreements form part of the terms and conditions of employment
- Awareness training about electronic information security forms part of Centre staff induction programmes
- Information for all staff on electronic information security is maintained in the staff handbook.
- All references for a period extending to 3 years prior to the recruitment date are checked by Personnel prior to a member of staff's commencement of employment.

Access to Centre systems may be withdrawn and Centre disciplinary procedures will be invoked where a serious or deliberate breach of the policy is made.

9.3. Learner Responsibilities

In order to use the Centre network learners must agree to the terms and conditions contained within the ICT Acceptable Use Policy. To ensure all learners see and consent to these conditions learners must expressly register on-line in person. Proxy registration by others is not acceptable.

Centre disciplinary procedures including withdrawal of access to systems may be invoked if learners fail to carry out their responsibilities under the policy; this includes copyright infringement and any criminal behaviour or obfuscated behaviour which threatens the organisational reputation of the Centre.

9.4. External User Responsibilities

All external users and agency staff must be sponsored by a member of Centre staff. The procedure for registering such users is held on the IT Services web site. The external user must agree in writing to terms and conditions of the ICT Acceptable Use Policy. Records of these agreements and the sponsors are held by IT Services.

Examples of persons eligible for application for an EX account are:-

- Learners on courses not covered by SITS
- People teaching on Centre courses who are not employed by the Centre
- Staff who have left but have an on-going working relationship with the Centre
- External examiners
- Outside researchers collaborating with Centre researchers
- Auditors

EX accounts will be of limited duration (normally maximum of 12 months), extensions may be granted if there is a demonstrable business need for the account and the application is sponsored by the Senior Manager. By default the EX account will expire in twelve months from the date of initial creation.

Breach of terms and conditions may result in suspension of the account as well as possible disciplinary/legal proceedings against the user or sponsor.

9.5. Guest Users and Open Access

Guest user accounts and open access facilities may be used to allow visitors strictly limited access to public Centre IT. Written records of such IT use (who, when and where) must be maintained by the Network Engineer.

Access to corporate systems, protected electronic resources, Centre e-mail services and personal file store will not be permitted for guest users.

V6 May 2024
By Network Engineer
Signed by MDS

362 Essex Road • Islington • London • N1 3PD
Tel: 020 7354 5655
info@intechcentre.com • www.intechcentre.com

10

Guest Users will be encouraged to use the applications available to access the internet via Wi-Fi unless a specific need exists for the guest to be granted access the Centre network.

9.6. Centre Key Business System access

9.6.1. Subject access Management and administration

Formal procedures will be implemented for granting access to both the Centre network and IT Services. This will be supported by a formal review of user privileges on a regular basis to ensure that they remain appropriate to the role and relationship with the Centre. Accounts identified as dormant accounts will be closed in accordance with current procedures.

9.6.2. Remote access

Controls will be implemented to manage and control remote access to the Centre's network and IT Services. Key Business Systems will have controlled access in accordance with the Remote Access Policy and Agreement (2010).

Users should note that failure to comply with the Remote Access Policy and Agreement will leave the user liable to disciplinary action and possible criminal law prosecution under the appropriate legislation.

9.6.3. Mobile computing

The Centre recognisees the inherent dangers of information stored on portable computers (laptops, notebooks, tablets and smart phones) as well as removable media. IT Services will provide security advice to staff via the IT Security section of the ITS web site. This advice is issued as a guideline for users and failure to follow recommended guidance will leave a user vulnerable to disciplinary action should Key Business System data or sensitive information be lost or altered.

Wireless computer networks potentially introduce new security risks which are the subject of specific "Wireless Security Policy" which should be read in conjunction with this Electronic Information Security Policy.

9.6.4. Password management

Users are required to follow good security practices in the selection, use and management of their passwords and to keep them confidential in accordance with the ICT Acceptable Use Policy.

The Control of network passwords is the responsibility of IT Services. Network passwords are stored in encrypted form.

IT Services maintains records of the issue of system administrator passwords and ensures they are stored securely. System administrator passwords will be issued on the express authority of the Network Engineer on a need to know basis. Such passwords will be changed regularly and when authorised system administrator staff leaves.

For Windows operating systems the following will be enforced

- network passwords must be a minimum of 6 characters
- Network passwords will be subject to enforced periodic change, the life of a chosen password will be 6 months.
- network password history will prevent reuse of the last 3 password changes
- accounts will be locked on the third failed login attempt

Policy on network password complexity will be reviewed periodically.

V6 May 2024
By Network Engineer
Signed by MDS

362 Essex Road • Islington • London • N1 3PD
Tel: 020 7354 5655
info@intechcentre.com • www.intechcentre.com

11

The account type should at all times reflect the business relationship existing with the member of staff. As a staff member moves to a less formal relationship with the Centre then the account associated with that person should reflect this new relationship.

IT Services will maintain a list of staff with access to key business systems and services. A password matrix will be maintained to ensure business continuity and mitigate risk. This password matrix will be kept securely to ensure swift response to critical incidents.

9.6.5. Unattended user equipment

Users of the Centre network and IT Services are responsible for safeguarding Key Business System data and sensitive information. In order to protect these information assets users are required to ensure that devices are not left logged-on when unattended and that portable equipment in their custody is not exposed to opportunistic theft, unauthorised access or observation of sensitive information.

Where available, password protected screen-savers and automatic log-out mechanisms are to be used on office based systems to prevent individual accounts being used by persons other than the account holders, but not on cluster computers that are shared by multiple users.

Users will utilise the following security features of the system:

- Keyboard lock
- Logging out of sessions when session finished.
- Logging out of sessions when a computer is to be left more than 15 minutes.
- Whenever possible and at the end of the working day switch off computers when not in use.

Users are required to follow the guidance on user responsibilities Personal Responsibilities for Electronic Information Security failure to adhere to these recommendations will leave the user liable to possible disciplinary or criminal prosecution.

9.6.6. Monitoring systems access and use

Access to and use of the Centre network and IT Systems will be monitored in accordance with the provisions of the Policy for Using IT Resources.

Remote access by third party contractors to maintain and support Centre IT systems will be subject to appropriate monitoring and control measures defined by IT Services. Third Party access will only be granted where the applicant has agreed to the terms and conditions of the ICT Acceptable Use Policy.

10. Compliance

10.1. Compliance with legal and Centre policy

Supply and use of the Centre network and IT services is bound by UK law current at the time of any reported incident. The Policy for using IT resources provides guidance on the most common legal and policy requirement pertaining to Centre network use.

IT Services will maintain and monitor, at six-monthly intervals, reports of records of electronic security incidents, Reports will be considered by the Network Engineer, who will decide if further action or investigation is required.

The IT Services password matrix, listing members of staff with access to key systems and services, will be maintained by the Network Engineer.

V6 May 2024
By Network Engineer
Signed by MDS

362 Essex Road • Islington • London • N1 3PD
Tel: 020 7354 5655
info@intechcentre.com • www.intechcentre.com

12

All Centre Staff and Learners have a right, subject to Centre regulations, to use relevant centre IT systems as defined by the Acceptable Use Policy and Policy for Using centre IT Resources, including a duty to use IT responsibly.

People who are neither staff nor learners do not normally have an automatic right to use the centre network or IT Services. Authorisation for such external users will be subject to sponsorship from a member of centre staff along with written agreement from the user to abide by the ICT Acceptable Use Policy.

Any outsourcing agreements must include express provisions with respect to IT security and control and any applicable UK Law in relation to data processing and confidentiality.

- ICT Acceptable Use Policy
- Code of Conduct

V6 May 2024
By Network Engineer
Signed by MDS

362 Essex Road • Islington • London • N1 3PD
Tel: 020 7354 5655
info@intechcentre.com • www.intechcentre.com

13