Access Control Policy

1. Introduction

Confidentiality, integrity and availability are fundamental aspects of the protection of systems and information and are achieved through physical, logical and procedural controls. It is vital that authorised users who have access to Centre systems and information are aware of and understand how their actions may affect security.

Confidentiality - systems and information will only be accessible to authorised persons.

Integrity – the accuracy and completeness of systems and information are safeguarded.

Availability – systems and information are physically secure and will be accessible to authorised persons when required.

Authorised users referred to in this document are members of the following groups: -

All parties (either as part of a contract of employment or third-party contract) who have access to, or use of ICT systems and information belonging to, or under the control of the Centre including:

- Employees
- Learners
- Temporary staff
- Agency staff
- Partner organisations
- Members of the public
- Any other party utilising Centre ICT resources

2. Purpose

The purpose of this policy is to ensure that both logical and physical access to information and systems is controlled and procedures are in place to ensure the protection of information systems and data.

3. Scope

The scope of this policy includes all access to Centre information, ICT systems and physical access to areas and locations where information and data is located. This policy applies throughout the information lifecycle from acquisition/creation, through to utilisation, storage and disposal.

4. Policy Statement

On-going education featuring induction programmes, eLearning, line manager training, specific training and awareness programmes must be undertaken by staff to enable them to be aware of their responsibilities towards systems and information security,

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

4.1 Generic identities

Generic or group IDs shall not normally be permitted as means of access to Centre data, but may be granted under exceptional circumstances if sufficient other controls on access are in place. Centre currently has limited access generic account for learners where all data gets deleted after each sign-off.

Under all circumstances, users of accounts must be identifiable by Intech Centre. Generic identities will never be used to access Confidential data or Personally Identifiable Information, including data supplied to Intech Centre.

Privileged accounts

The allocation of privilege rights (e.g. local administrator, domain administrator, super-user, root access) shall be restricted and controlled and not provided by default.

Authorisation for the use of such accounts shall only be provided explicitly, upon written request from a senior manager.

Technical teams shall guard against issuing privilege rights to entire teams to prevent potential losses of confidentiality and / or integrity.

Privileged accounts must not be used for standard activities; they are for program installation and system reconfiguration, not for program use, unless it is otherwise impossible to operate the program.

Least privilege and need to know

Access rights to both physical and logical assets will be accorded following the principles of least privilege and need to know.

Maintaining data security levels

Every user must understand the sensitivity of their data and treat them accordingly. Even if technical security mechanisms fail or are absent, every user must still maintain the security of data commensurate to their sensitivity.

This policy enables users to classify data appropriately and give guidance on how to store it, irrespective of security mechanisms that may or may not be in place. Users electing to place information on non-centre based systems and databases, digital media, cloud storage, or removable storage devices are advised by Intech Centre only do so where:

- such an action is in accord with the information's security classification
- the provision meets any research data supplier or other contracts,
- other protective measures (such as the use of encryption) have been implemented.

Users are consequently responsible in such situations for ensuring that appropriate access to the data are maintained in accord with the Information Security Policy and any other contractual obligations from data providers they may have to meet.

Access Control Authorisation

4.2 User accounts

Access to Intech Centre IT resources and services will be given through the provision of a unique user account and complex password.

Our accounts include, superusers, managers, staff, learner admin and learner.

Password creation

As a best practice guide, passwords must be created in the following format:

- A minimum of 8 characters long.
- Not contain a dictionary word of more than 4 characters.
- Contain at least one uppercase letters.
- Contain at least one lower case letters.
- Contain at least one number.
- Contain at least one special characters or non-alphanumeric characters, such as ! ” £ $ % & @

Password security

All passwords must be protected to the same level as that afforded to the system or information that they provide access to.

Users must ensure that passwords are not shared with other users.

Users must ensure that passwords are never revealed to any other persons. This includes system administrators, security staff and management.

All Manager and Superuser passwords must be changed every 90 days.

If there is any indication that a password has been compromised that password must be changed immediately and reported as a security incident.

The Superuser passwords must differ from domain administration.

Separate login and passwords is required for administrators to undertake normal day to user functions.

Password management

All passwords must meet the required criteria (such as length, complexity).

All new or reset passwords must be changed immediately upon 1st log on.

System will force the change of passwords every 6 months for the standard accounts.

Previously used passwords cannot be reused.

New passwords should not just be a recycled password with the addition of a number of new characters or the changing of a number of characters.

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

Following the incorrect entering of a password a specified number of times, the account is locked and can only be opened/reset through a system administrator process.

Access to Confidential, Restricted and Internal Use information

Access to 'Confidential', 'Restricted' and 'Internal Use' information will be limited to authorised persons whose job or study responsibilities require it, as determined by law, contractual agreement with interested parties.

Access to any of these resources will be restricted by use of firewalls, network segregation, secure log-on procedures, access control list restrictions and other controls as appropriate.

The responsibility to implement access restrictions lies with the data processors and data controllers, but must be implemented in line with this policy.

Role-based access control (RBAC) will be used as the method to secure access to all file-based resources contained within Intech Centre's Active Directory domains.

There are no restrictions on the access to 'Public' information.

SYSTEMS/INFORMATION ACCESS

Information risk owners, have a responsibility to keep information access requirements for specific roles up to date and regularly reviewed.

If an employee's role within the organisation changes and access to systems needs to be updated or removed, managers must contact the IT Department to ensure access to other systems and programs are updated if a user's role or the business need changes.

- For systems containing restricted and personal information and data, an access control matrix must be developed to record role based authorised access recorded on an individual basis. Authorisation procedures must be in place for managers to authorise all access (including short term and temporary access) recorded on the matrix. The access matrix must be continually updated and maintained to reflect accurate records of access.
- To gain access to specific systems and information, a member of staff will need to follow a formal application process.
- Generic logons are not generally permitted, however, use of generic accounts under exceptional 'controlled' circumstances such as the learner computer logins, is permitted.
- To ensure relevant Centre or Prime contractor standards are adhered to, personnel checks, such as DBS and Baseline Personnel Security Standard checks may be undertaken if required.
- The appropriate level of access to systems and information will be determined upon the prospective users required business need, job function and role.
- A signed confirmation by the user may be required indicating that they understand and appreciate the conditions of access and security.
- If authorisation to use systems and information is granted, unique logon credentials and password will be provided to the applicant. Further instruction on how to maintain the security of systems and information with due regard to the procedures below may be given.

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

- The application and all other documentation should be maintained in line with the safe haven guidance.
- Login banners should be used to remind users of their obligations when using the system

Login/Welcome banners should be used to remind users of their obligations when using the system. The Login/Welcome banners must consist of the below approved corporate wording:-

Access to this system, data and associated networks are for authorised users only. Unauthorised access, or modification of data without authority, is unlawful, and could result in disciplinary or legal action being taken. Access to this system is monitored for both audit purposes in order to prevent unauthorised access attempts, and, to ensure compliance with current information security procedures.

It is essential that you keep your login details secret, and take reasonable steps to keep them secure, for example, by using a strong password. You should not re-use your login details for this system on other web sites or share them with other individuals. By continuing to use this system, you accept these conditions of use.

SYSTEMS/INFORMATION DE-REGISTRATION

- If a member of staff changes role or their contract is terminated, the manager should ensure that a user's access to the system/information has been reviewed or, if necessary, removed as soon as possible by the standard leavers/change process performed.
- Relevant prime contractor must be informed to cease access to their systems.
- If a member of staff is deemed to have contravened any of the Information Security policies or procedures, potentially jeopardising the availability, confidentiality or integrity of any systems or information, their access rights to the system/information should be reviewed by the system owners.
- If a specific access limit is exceeded or control circumvented several times by a user the manager should review the access rights of the user and if necessary remind the user of the relevant access and security.
- If a number of unsuccessful log-on attempts is exceeded, the user will be informed that they need to contact the system owners or the ICT Service desk to ask for access rights to be re-established. In these circumstances, access rights may need to be reviewed.
- If it is deemed that it is no longer appropriate or necessary for a user to have access to systems and/or information then the user's manager will need to inform the owners of the system/information that access rights should be altered/removed immediately.
- If any system/information rights are altered or removed, the relevant documentation will need to be updated accordingly.

LOG-ON CONSIDERATIONS

- All systems should be accessed by secure authentication of user validation. As a minimum this should entail use of a Username and a Password.
- Logon to systems/information should only be attempted using authorised and correctly configured equipment in accordance with Centre policies.

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

- After successful logon users should ensure that equipment is not left unattended and active sessions are terminated or locked as necessary. Systems should be logged off, closed down or terminated as soon as possible.
- System logon data should not be copied, shared or written down.

PHYSICAL ACCESS AND CONTROLS

Maintaining the physical security of offices and rooms where information, data and processing facilities are accessed and located is vitally important. There must be methods of physically securing access to protect information and data:

1. Staff should wear their Centre badges and visitors must sign-in. Any person not known to location personnel must be challenged in order to establish who they are and whether authorisation has been provided for them to be there. If there is any doubt about the identity of the individual, the appropriate manager should be contacted to confirm the individual's identity.

2. Appropriate recording mechanisms need to be in place to record the names, dates, times and signatures for the signing in and out of visitors (including Centre staff). All visitors must be directed to appropriate department/person after signing in.

3. The use of keys to buildings, rooms, secure cabinets, safes etc. must be controlled and recorded. Keys must be stored in secure areas/locked cabinets when not in use and must be identifiable by recording serial/ID markings of all keys. The location of keys must be known at all times and a signing in/out recording mechanism must be maintained to record the serial/ID of keys against individual names when keys are used.

4. Security access fobs must be issued to authorised staff on an individual basis. Staff issued with access fobs must have their names recorded against the registered access fob number including date and time of issue

5. Access fobs should only be used by the registered user and must not be lent out or given to other staff, regardless of their seniority. In emergency situations, authorised personnel may be permitted to use another authorised person's fob if available with permission of the line manager and the recorded user must either be present or be made aware that their fob is being used. Any such use must be recorded and maintained in a logging system for this type of event

6. Access fobs issued to personnel who no longer work for the Centre must be deactivated and recovered immediately.

8. Observance and maintenance of the physical security of rooms and offices where PCs and/or critical information processing equipment is located needs to be a paramount consideration. For example, do not house critical equipment in publicly accessible locations, close to windows, in areas where theft is a high risk. Locate servers and business critical equipment in locations with adequate environmental and fire controls.

9. Access to information processing systems will only be allocated to staff following any required legal checks. If required, usage policies will also need to be signed by staff.

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

10. All interfaces used for managing system administration and enabling access to information processing must be appropriately secured.

11. Access to and knowledge of key fobs or access to keys for locks, are restricted to authorised personnel only and must not be shared with any unauthorised person.

12. Access codes used for secure locking mechanisms must be changed every three months as a minimum or more regularly as specified by the location manager in line with professional best practice.

13. If electronic key fobs are in use they must be issued to authorised staff on an individual basis, be fully registered to that individual and only used by that individual. The key fob must be deactivated immediately when no longer required and registration details updated accordingly.

14. Direct access to secure locations, or access to adjoining offices which could provide access, must be locked and secured using appropriate locking mechanisms.

16. Personal, special access visits from relatives or acquaintances of personnel are not permitted within secure areas. There must be a valid reason for all visits and any such visitors must go through the standard signing in/out procedure.

17. Equipment should be sited to minimise unnecessary, unauthorised access into work areas. For example, refreshment units or office machinery designed for visitors should be placed in public accessible areas only.

5. Responsibilities

Senior Manager responsible for ensuring that all staff and managers are aware of security policies and that they are observed. Managers need to be aware they have a responsibility to ensure staff have sufficient, relevant knowledge concerning the security of information and systems. Designated owners of systems, who have responsibility for the management of ICT systems and inherent information, need to ensure that staff have been made aware of their responsibilities toward security.

Designated owners of systems and information need to ensure they uphold the security policies and procedures.

6. Breaches of Policy

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to Centre assets, or an event which is in breach of the Centre's security procedures and policies.

All Centre employees, learners, partner agencies and third parties have a responsibility to report security incidents and breaches of this policy as quickly as possible through the Centre's Incident Reporting Procedure. This obligation also extends to any external organisation contracted to support or access the Information Systems of the Centre.

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

The Centre will take appropriate measures to remedy any breach of the policy and its associated procedures and guidelines through the relevant frameworks in place. In the case of an employee then the matter may be dealt with under the disciplinary procedures.

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