Information Security Document

Access Control Policy

Version History			
Version	**Date**	**Detail**	**Author**
1.0		Completed for distribution	
1.0		Agreed by Information Governance Group	
2.0		Reviewed by Information Governance Group	
3.0		Reviewed by Information Governance Group	
4.0		Approved by Information Governance Group. Renamed from Information and Systems Access Procedures.	
5.0		Reviewed by Information Governance Group	
6.0		Reviewed by Information Governance Group	
7.0		Reviewed by Information Governance Group.	

This document has been prepared using the following ISO27001:2013 standard controls as reference:

ISO Control	Description
A.7.1.1	Screening
A.7.2.2	Information security awareness, education and training.
A.9.2.6	Removal or adjustment of access rights.
A.9.2.1 > 2	User registration and de-registration/User access provisioning
A.9.2.3	Management of privileged access rights
A.9.2.4	Management of secret authentication information of users
A.9.4.1	Information access restriction
A.18.2.2	Compliance with security policies and standards

1 Introduction

Availability**,** confidentiality and integrity are fundamental aspects of the protection of systems and information and are achieved through physical, logical and procedural controls. It is vital for the protection of systems and information authorised users who have access to Council systems and information are aware of and understand how their actions may affect security.

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

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

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

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 Council including:
    - Council employees
    - Elected Members
    - Third Parties
    - Full and part-time staff
    - Temporary staff
    - Agency staff
    - Partner organisations
    - Members of the public
    - Volunteers
    - Any other party utilising Council 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 Council 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 corporate 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.

SYSTEMS/INFORMATION ACCESS.

Information risk owners, as identified in the Council's ISO27001 Scope, or their delegate must explicitly define, document and keep up to date the access requirements for the specific roles which have access to the information.

A form exists on the SAP system for managers to complete if an employee's role within the organisation changes and access to systems needs to be updated or removed. Managers must contact the Service Desk 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. Users will need to apply to the relevant owners/senior custodian of the systems using the appropriate completed forms.
- Generic logons are not generally permitted across the Council, however, use of generic accounts under exceptional 'controlled' circumstances such as the Council's Libraries system, is permitted.
- To ensure relevant Council or national legislation security 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.
- Access for remote users shall be subject to authorisation by line managers via the Transformation Service. No uncontrolled external access shall be permitted to any network device or networked system.
- 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

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 by SAP processes.
- 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 Transformation 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 User name and a Password.
- Logon to systems/information should only be attempted using authorised and correctly configured equipment in accordance with Council policies.
- 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 Council ID badges and visitors must wear the Visitor ID badges which have been issued to them. People who are not displaying ID badges should be challenged. 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 security officer/manager should be contacted to confirm the individual's identity. Staff in residential establishments will need to check their local procedures whilst working inside the home.

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

Council personnel) to Council locations. All visitors must be issued with an authorised Council visitors badge when 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. Electronic access fobs must be issued to authorised staff on an individual basis. Staff issued with access fobs must have their names and employee numbers 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 Council must be deactivated and recovered immediately – a record of this action must be kept, using an official recording system

7. Locations housing critical or sensitive information and/or information processing facilities should have a secure, physically sound perimeter with suitable controls and restrictions allowing access to authorised staff only. CCTV and audible alarm systems should be active in areas where critical servers are located, such as in the data centre.

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/council checks. If required, usage policies will also need to be signed by staff.

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, door lock codes 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. Outside of County Hall a

record should be kept in a secure location of when the dates when the access codes are updated.

13. If electronic door locks/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.

15. All Council/Contracted Cleaners must have and display appropriate identification and be made aware of the requirements within this procedure.

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

Directors are 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 Council assets, or an event which is in breach of the Council's security procedures and policies.
All Council employees, elected members, partner agencies, Third Parties and vendors have a responsibility to report security incidents and breaches of this policy as quickly as possible through the Council's Incident Reporting Procedure. This obligation also extends to any external organisation contracted to support or access the Information Systems of the Council.

The Council 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.

This document forms part of the Council's ISMS Policy and as such, must be fully complied with.