Information Security Document

Physical and Environmental Infrastructure Procedures

Version 9.0

Version History			
Version	**Date**	**Detail**	**Author**
1.0	20/05/2011	Completed for Distribution	Jo White
1.0	28/06/2011	Approved by Information Governance Group	Jo White
2.0	06/07/2012	Reviewed by Information Governance Group	Jo White
3.0	27/09/2013	Reviewed by Information Governance Group	Jo White
4.0	03/11/2014	Reviewed by Information Governance Group	Jo White
5.0	15/12/2015	Reviewed by Information Governance Group. No changes.	Jo White
6.0	09/01/2017	Reviewed by Information Governance Group	Jo White
7.0	05/03/2018	Reviewed by Information Governance Group. Transformation changed to ICT.	Jo White
8.0	08/04/2019	Reviewed by Information Governance Group. Juniper replaced by Direct Access.	Jo White
9.0	12/05/2020	Reviewed by Information Governance Group. Volunteers added.	Jo White

This document has been prepared using the following ISO27001:2013 standard controls as reference:	
ISO Control	**Description**
A.9.1.1	Access Control Policy
A.9.2	User access management
A.11.1 > A.11.2	Physical and environmental security / Equipment
A.12.1.1	Documented operating procedures
A.12.2.1	Controls against malware

1 Introduction

Derbyshire County Council has a large and complex ICT infrastructure. The foundation of this structure is the Data and Communications Network which is facilitated and supported by many types of hardware including extensive cabling and supporting systems installed throughout the Council's various buildings and offices across Derbyshire.

Physical and environmental security often provides the first line of defence of information and information systems with what might be called geographic or area security, with equipment security and general controls to protect physical assets.

2 Purpose

These procedures define the requirements to ensure that the Council's critical or sensitive information processing facilities are in secure areas and protected by a well-defined, secure perimeter. Appropriate security and controls provide protection against unauthorised access or damage to information available within processing facilities.

3 Scope

The scope of these procedures includes all persons/parties who have access to Council buildings, locations, information and ICT systems belonging to or under the control of Derbyshire County Council including:

- Council employees
- Elected Members
- Third Parties
- Temporary staff
- Partner organisations
- Members of the public
- Volunteers
- Any other party utilising Council ICT resources

4 Procedures

There are three spheres of principal control that are available and when used in conjunction can supplement and enhance the overall assurance of Council's physical and environmental infrastructure.

The three controls are:-

- Physical
- Technical
- Procedural.

1. Physical controls rely on the presence of physical limitations to secure the perimeter or environment (buildings and locations) containing information and information processing facilities. Stopping unauthorised people from entering/breaking into buildings (fire escapes, back doors), the use of locks on offices, server rooms, other sensitive areas and the willingness to challenge those who aren't wearing badges. Further to this, what to do if something does go wrong e.g. there is a break in, a location suffers a fire or the power supply fails.

2. Technical security involves security measures that employ technology in some way. Usually they are related to computers and software techniques but can equally apply to technical locks such as tokens or biometric techniques such as fingerprints. They can extend to hardware through locking of ports or to some other technological solution for a specific application (e.g. Derbyshire Direct Access).

3. Procedural security covers the rules, regulations and policies that an organisation puts in place to help reduce the risk of issues arising e.g. obligatory policies such as internet and email, safe haven, password protection, PC and network security.

A layered approach using all three types of security provides the best solution. A set of controls need to be effectively implemented such as:-

- Controls getting into the site, buildings or locations (procedural and physical)
- A set of well drafted and effectively policed policies, of which staff are well aware. For example, staff are aware of where and how to store, send or copy sensitive information and ensure encryption is used if necessary (procedural and technical) e.g. Council's Safe Haven Guidelines.
- Physical, technical and procedural controls surrounding access to information processing systems. For example Specific logons/access technology to ICT equipment, systems and applications
- Physical, technical and procedural controls to ensure safety, security and integrity of information and locations e.g. fire procedures, power failures, eating and drinking, back-up equipment, location of critical equipment.
- Business continuity plans and disaster recovery plans must exist to counteract any loss of critical equipment, infrastructure and/or data.
- Maintenance contracts and service level agreements that incorporate, for example: antivirus software, encryption and security breach reporting mechanisms.

PROCEDURES

Council Infrastructure equipment is maintained and installed across most Council buildings and locations e.g. network cables in cupboards, network connection points, PCs and printers, servers, internet routers. Access to computers and devices must be controlled using secure methods and procedures in order to prevent damage to council assets and reputation.

1. 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 and upon leaving any badges issued should be collected to prevent access by the employee / visitor at a later date.

2. At all times staff and visitors must wear their Council and visitor ID badges which have been issued to them and visitors must be supervised at all times when visiting and leaving secure areas. People who are not displaying ID badges must be challenged in order to establish why they are not wearing an ID badge, 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.

3. 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, and should be periodically reviewed to ensure they are operating as intended.

4. 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.

5. Council ICT equipment may only be used by authorised parties for authorised Council business or purposes in accordance with the Council's Acceptable Use policy and associated security policies.

6. Desktop PCs, laptops and mobile devices which have not been provided by the Council but have been approved for use may be subject to the relevant security checks and procedures by the ICT Service and Internal Audit.

7. All ICT equipment, data and communication networks must be installed and maintained according to the manufacturer's guidelines and in line with all relevant Council policies and procedures.

8. All Council PCs, laptops and mobile devices will be encrypted or password protected when issued to employees and will be maintained to ensure the best standards of software and hardware integrity and security. This will include the correct security configuration and initial and regularly updated protection from viruses, spyware/malware.

9. Network Support staff working remotely must observe the same controls and procedures as when working within the Council campus in order to ensure security and integrity and to prevent loss and/or damage to Council assets and reputation.

10. 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.

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

12. Maintenance of Council equipment and infrastructure will be carried out by ICT Services authorised staff.

13. 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.

14. ICT equipment should be taken off site only if permission for this has been agreed and the device has been encrypted with the approved encryption software by the ICT Service. Extreme care regarding loss, damage or theft needs to be employed whilst the equipment is off site. Staff must adhere to any relevant procedures and guidance regarding the use of and security of ICT equipment being used off site.

15. Access codes used for secure locking mechanisms must be changed on a regular basis as specified by the location manager in line with professional best practice - especially in instances where there has been a change in personnel, for example, staff leaving or being suspended during the course of a disciplinary investigation.

16. 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 and returned immediately when no longer required and registration details updated accordingly. Any key fobs that are not being used should be securely stored and a separate record maintained of these fobs.

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

18. Doors which provide access to ICT Network Infrastructure equipment must not to be left/wedged open unless for the purpose of taking delivery of new equipment, to accommodate the movement of existing equipment, transportation of maintenance or cleaning equipment – an authorised member of staff must be present at all times to supervise access when doors are left open.

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

20. 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.

21. Consideration and understanding of health and safety guidelines/procedures should be followed to ensure security, integrity and safety of the Council's data and communications infrastructure. Smoke detectors should be located

within the areas housing critical system and applications with firefighting equipment maintained and periodically tested. Local operations staff should be provided with basic training in the use of fire suppressant equipment.

22. If it is suspected that any of the above procedures have been broken or compromised, then the concern should be placed before a senior manager or use the Security Incident Form: https://staff.derbyshire.gov.uk/information-security/report-a-security-incident/report-a-security-incident.aspx to report the matter.

23. A business continuity plan and disaster recovery procedures must be in place in the event of the loss of a part, or the whole Council Data and Communications Network infrastructure. Procedural documentation must be regularly updated to include any changes/updates to existing procedures or processes involved.

24. Procedures for network infrastructure fault tolerance and redundancy must be in place and tested for effectiveness on a regular basis. Procedural documentation must be regularly updated to include any changes or updates.

25. 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.

26. ICT property and equipment should be indelibly marked. A full inventory of assets and their location must be kept to ensure effective asset maintenance identifying each item where items are lost or stolen, disposal of asset equipment and ensuring that confidential information and software is properly removed from all devices.

This document is owned by the Information Governance Group and forms part of the Council's ICT Security Policy and as such, must be fully complied with.