Information Systems Development and Maintenance Policy

1 Version History details and author

1.0	25/03/2011	Completed for distribution	Jo White
1.0	26/04/2011	Approved by Information Governance Group	Jo White
2.0	26/05/2011	Reviewed by Information Governance Group	Jo White
3.0	30/05/2012	Reviewed by Information Governance Group	Jo White
4.0	27/06/2013	Reviewed by Information Governance Group	Jo White
5.0	14/07/2014	Reviewed by Information Governance Group	Jo White
6.0	14/09/2015	Reviewed by Information Governance Group	Jo White
7.0	10/10/2016	Reviewed by Information Governance Group. Changed from procedures to policy.	Jo White
8.0	06/11/2017	Reviewed by Information Governance Group. Information on PIAs added.	Jo White
9.0	03/12/2018	Reviewed by Information Governance Group. No changes.	Jo White
10.0	14/01/2020	Reviewed by Information Governance Group. System Monitoring Plan at award stage removed.	Jo White
11.0	09/02/2021	Reviewed by Information Governance Group.	Jo White
12.0	09/02/2022	Reviewed by Information Governance Group. PIA changed to DPIA.	Jo White
13.0	10/05/2023	Reviewed by Information Governance Group. Live data environment amended to match Operational Management Policy.	Jo White
14.0	09/07/2024	Reviewed by Information Governance Group. Paragraph added regarding not testing if live data is contained in the test environment.	Jo White

This document has been prepared using the following ISO27001:2022 standard controls as reference:

A.5.2 - Information security roles and responsibilities
A.5.4 - Management responsibilities
A.5.8 - Information security requirements analysis and specification
A.5.18 - User access management
A.6.3 - Information security awareness, education and training
A.8.3 - Information access restriction
A.8.4 - Access control to program source code
A.8.6 - Capacity management
A.8.13 - Information backup
A.8.18 - Use of privileged utility programs
A.8.19 - Installation of software on operational systems
A.8.31 - Security in development and support processes
A.8.32. - Change management
A.8.33 - Protection of test data

2 Introduction

The need to secure information is a legal requirement, rather than an option. The consideration and inclusion of security controls within information systems from design to decommission is essential to ensure the secure operation, management and protection of the Council's information and information systems.

This policy outlines controls which must be in place to ensure security is built into information systems and that they are developed and supported in a consistent way, ensuring that the business needs of end users and customers are met. Systems development, upgrades and maintenance should all be considered with regard to their possible effects upon confidentiality, integrity and availability of the system concerned and any linked systems - the aim being to provide seamless and robust access to the assets and information of Derbyshire County Council.

3 Purpose

The purpose of this policy is to ensure that controls and processes for the security of information and systems are in place during all phases of the systems development lifecycle - including decommission. It is essential that all staff involved in systems development and maintenance have an understanding of the Council's IT security policies and procedures and ensure that they are adhered to.

4 Scope

The scope of this policy includes all individuals who design, build, commission, purchase, modify, maintain, update and/or who have systems development and maintenance access to Council information and ICT systems. This policy applies throughout the information lifecycle from acquisition, creation, through to utilisation, storage and disposal.

5 Responsibilities

Directors are responsible for ensuring that staff and managers are aware of the Council's IT security policies and that they are complied with. Managers need to be aware that they have a responsibility to ensure staff have the relevant knowledge concerning security of information and systems which they develop or maintain. Staff involved within the ICT systems development lifecycle need to be aware of their responsibilities toward security of both systems and information. 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.

The County Council's Financial Regulations require that

The Chief Financial Officer is responsible for the operation of the Council's accounting systems, the form of accounts and the supporting financial records. Any proposed changes by Strategic Directors to existing financial and/or control systems or the establishment of new systems must be reported to and considered by the Assistant Director of Finance (Audit) who will consider the potential impact on the Internal Control framework and report to the Chief Financial Officer, raising any concerns as appropriate. The Chief Financial Officer will then formally consider the proposed changes. No changes may be actioned without the formal approval of the Chief Financial Officer.

The *'Protocol for the Approval of New Systems or Changes to Existing Systems by the Chief Financial Officer'* outlines how the process will be conducted to enable compliance with the Council's Financial Regulations.

6 Policy statement

Assurance and security requirements need to be captured at the start of any project to ensure that they are effective. Security requirements should not be considered in isolation of the systems functional requirements.

To effectively consider security, it should be planned from the beginning of the development and/or maintenance process to ensure it is embedded within the context of the environment of the system.

All departments requesting a new (internal) ICT system/solution must have completed an in-depth business plan and risk assessment prior to the allocation of a project manager. The risk assessment should include a completed Data Protection Impact Assessment (DPIA). A review should be undertaken as part of the initial business plan scoping, to assess whether service or business needs could be delivered using existing Council ICT systems and solutions.

6.1 SYSTEMS DEVELOPMENT AND MAINTENANCE

The consideration of security during systems development and maintenance is a mandatory information security Council requirement. The following processes and activities must be in place in order to ensure the protection of information and information systems.

1. The development and maintenance of information systems must include adequate consideration of:
    - Efficient installation of vendor security updates and patches
    - Business continuity,
    - Backup and recovery,
    - System access controls, including two factor authentication
    - Data processing controls,
    - Level of encryption applied to data in transit and at rest,
    - Transactional audit trail.
    - Exception reporting
    - Documentation of security measures and user guidance.
    - Suitability of off-site storage for backup recovery and emergency equipment.
2. Information systems development and maintenance must be carried out in accordance with the Council's ISO27001 certification, current legislation including the Data Protection Act 2018 and approved ICT Security policies, using identified controls for development processes and environment.
3. Systems must be coded to ensure only valid and accurate data is processed.
4. Internal Audit should be notified at the start of the information systems development to ensure that the required control framework can be implemented as part of the early development work

5. All development code must be checked for errors, bugs and malware and the use of any proprietary code must be checked using industry standard malware and antivirus scanning techniques.
6. Functional testing must be undertaken during the development of systems to ensure processes behave as expected and within design criteria.
7. Procedures to back up and secure information and data against loss or damage must be in place.
8. Archiving or “housekeeping” functions must be in place for system performance or data retention purposes.
9. Back-up strategies and business continuity plans need to be included into the project plan and approved by the system owner.
10. Disaster recovery arrangements must be in place to recover developed systems, information, software dependencies and/or patches applied – including the availability of media formats required for the recovery. This may include the use of escrow agreements which must be considered in order to ameliorate possible problems that may be encountered with third-party suppliers of code/systems.
11. The criticality and maximum tolerable times for the restoration and recovery of information systems must be established and agreed with the system owner in accordance with business continuity and recovery plans.
12. Adequate assurance of availability must be provided and identified at the start of the development lifecycle.
13. Compliance with any legal, statutory and regulatory requirements must be ensured during the development lifecycle and adhered to.
14. Systems must ensure the security of communications using recognised, up to date security protocols and standards relevant to the communication technologies employed.
15. All development staff must be provided with relevant security awareness and training specific to the secure development of information systems including the Council’s Information Security policies and procedures.
16. Changes within the development lifecycle must be controlled by the use of formal change control procedures to ensure the security and integrity of information and information systems.
17. Effective auditing of activities which include change requests, modifications and privileged access activities must be established to enable full monitoring throughout the development lifecycle of systems.
18. All ICT systems and solutions must have an active audit trail in place that captures key transactional details including:
    - Date and time of transaction;
    - User ID and name of the individual undertaking the transaction;
    - Details of the data before and after the transaction;
    - Details of user ‘logins’, ‘logouts’ and failed user connections; and details of the user’s device IP address making the connection
19. Effective reporting mechanisms must be established and enabled for systems to fulfil internal audit requirements for reporting on user, administrative and other security related activities which include system access, connections and client computer access details.
20. All systems development undertaken by the Council, including systems commissioned or purchased and any subsequent maintenance, should be assessed for appropriate levels of security as identified in the Council’s information security policies and information security best practices.
21. Subsequent maintenance of developed systems must maintain the original security and integrity of the system unless the maintenance is required due to identified security risks or vulnerabilities.

22. All systems developed must be risk assessed and placed on the relevant departmental risk register where identified risks must be recorded and treated, mitigated or accepted accordingly.
23. A Data Protection Impact Assessment (DPIA) must be completed in all cases.
24. Risks to information security must be assessed for the likelihood and potential impact on confidentiality, integrity and availability. Categories or levels of risk (such as low, medium, high) can be assigned. A risk assessment should also define the level of threat to the system in the environment in which it will operate.
25. The development and maintenance of systems must be considered for its potential effects on the confidentiality, integrity and availability of information, both directly and indirectly in conjunction with other systems and assets.
26. Separate test environments must be used wherever possible to replicate the live system to allow for the assessment of system modifications, updates, patches and other work to be carried out without the risk of adverse effect or impact on the live system and/or the information held within it.
27. A risk assessment should be undertaken in instances where 'real' personal, sensitive and special category data is used in a test environment. Such development facilities may not be subject to the full security features inherent in the live/production system and thus should not be used for training purposes.
28. Systems development and maintenance roles and responsibilities must be clearly defined. System owners and administrators overseeing day-to-day security management throughout the development lifecycle must be identified and appointed.
29. Development standards must prompt consideration of the need to notify the legal department when new products/services are developed so that patents and trademark searches can be undertaken and new trademarks and patents can be filed.
30. Controls should consider the embedding of Digital Watermarks in Web Content and using sophisticated search engines to locate illegal copies and notify the owner.
31. Access to development tools and system utilities must be restricted to authorised staff only and must not be accessible from operational systems. Access to program source code must be restricted.
32. Both logical and physical security controls must be identified for the environment in which the system is to be deployed.
33. Access to the development environment must be controlled and restricted to authorised staff only to ensure the security of access to code, documentation, media and systems. Physical controls must be in place to control access to development working environments where necessary – including physical controls for the storage of development documentation and/or media.
34. Secure coding standards and conventions must be used for systems processing restricted information and for systems which could affect the security of the Council's computer network and information assets.
35. Development standards documents and coding guidelines developed by the Council's Business Applications team must be made available to development staff and continually updated as required to maintain secure coding standards and must be regularly reviewed to ensure accuracy and up-to-date secure coding practices.
36. Development coding must be regularly reviewed using security checkpoints throughout the development lifecycle to ensure the consistent application of security for developed systems.

37. Version control for development code must be used to identify the stages of the development lifecycle to mitigate risks associated with incorrect code implementation and identification.
38. Version history control for accompanying development documentation must be up-to-date and maintained.
39. Guidelines and procedures for the implementation of version control of code and version control for documentation must be maintained and made available to authorised development staff.
40. Training for development staff must be provided to ensure skills for finding and fixing vulnerabilities are available throughout the development lifecycle – including appropriate training for secure coding techniques.
41. Disposal of systems at the end of the implementation lifecycle must be carried out securely – in accordance with the Council's secure disposals procedures.
42. During disposal of any system, if required, data and information may need to be archived in line with statutory requirements and internal/external audit requirements. The archiving of data will need to be overseen and signed off by system owners to ensure requirements have been fulfilled.
43. The integrity, confidentiality and availability of data from decommissioned systems and translation to new systems needs to be assured during and after the archive process.
44. Prior planning and actual decommissioning of systems needs to be undertaken and must include removal of access rights and removal of software from PCs and servers.

7 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, contractors 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. Where it becomes apparent that there may have been a breach of this policy by an employee then the matter may be dealt with under the disciplinary process.

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