Information Security Management System (ISMS) Policy

1 Version History details and author

1.0 01/08/2012 Approved by Information Governance Group Jo White
2.0 31/07/2013 Reviewed by Information Governance Group. No amendments. Jo White
3.0 11/08/2014 Reviewed by Information Governance Group Jo White
4.0 14/09/2015 Reviewed by Information Governance Group Jo White
5.0 10/10/2016 Reviewed by Information Governance Group. Update to scope statement. Jo White
6.0 04/12/2017 Reviewed by Information Governance Group. No changes. Jo White
7.0 11/06/2018 Reviewed by Information Governance Group. DPA 2018 added. Jo White
8.0 08/07/2019 Reviewed by Information Governance Group. No changes. Jo White
9.0 11/08/2020 Reviewed by Information Governance Group. No changes. Jo White
10.0 07/09/2021 Reviewed by Information Governance Group. No changes. Jo White
11.0 08/11/2022 Approved by Information Governance Group. Scope changed in line with Derbyshire scope. Jo White
12.0 12/12/2023 Approved by Information Governance Group. Volunteers added. Jo White

2 Introduction

Derbyshire County Council provides essential services and functions which rely on resources including information. The use of information assets must be in line with good professional working practices and procedures as well as statutory, regulatory and contractual requirements and must ensure the confidentiality, integrity and availability of all Council information assets.

Information is an extremely important Council asset and enables the council to fulfil its business functions and obligations to citizens. ISO/IEC 27001:2013, the international security standard for information security management systems provides mandatory requirements for implementing, reviewing and continuously improving an Information Security Management System (ISMS).

The Council's ISMS shall ensure the Council meets its statutory, regulatory and contractual information security requirements including those provided by the Data Protection Act 2018 and the Information Commissioner's Office (ICO). The ICO is the UK's independent authority established to uphold information rights in the public interest, promoting openness by public bodies and data privacy and security for individuals. To this end it has imposed fines on public bodies for not protecting information satisfactorily. Further to this, some external partners are only willing to deal with other partner agencies which adhere to high information security standards and this increasingly means achieving and maintaining ISO 27001 compliance.

The DCC Scope Statement:-

"The protection of all Derbyshire County Council (DCC) owned and or controlled information assets inclusive of hard copy data, electronic data, Council records, policies and procedures, software and licences and physical IT hardware. The boundaries of this Information Security Management System encompass the above protection when interacting with offsite locations, authorised mobile workers and the endpoints of the organisational networks and scope of activities. Supporting technology includes server platforms, network devices and organisational networks within the control of Derbyshire County Council, operated from DCC's head office in Matlock. In accordance with the current Statement of Applicability Ver 5"

3 Purpose

This policy defines the ISMS policy in terms of the characteristics of the business, the organisation and its assets. It establishes the Council's principles, ambitions and objectives when utilising a management system for information security.

4 Scope

The scope of this policy extends to all Derbyshire County Council departments, employees, elected members, volunteers, contractors, vendors and partner agencies who use/access the Council's information assets. This ISMS scope excludes schools and associated school maintained premises and resources.

5 Policy statement

- The Information Governance Group (IGG), incorporating senior representatives from all Council departments, is charged with the management and approval functions associated with the ISMS.

- The IGG is charged with establishing and continually improving the ISMS.

- The IGG will provide the framework for setting objectives and establish an overall sense of direction of principles for action with regard to security.

- The ISMS will take into account business and legal or regulatory requirements and contractual security obligations.

- The approach to information security will be based on risk, as per the ISO 27001 standard and best practice.
.
- The ISMS procedures will establish risk evaluation criteria that are aligned with the current Derbyshire County Council approved corporate strategic risk management procedures and policies. The 'Risk Treatment Guidance for DCC Asset Owners' outlines this in conjunction with the 'Risk Management Strategy and Policy Statement' and 'Risk Management Awareness Toolkit For Employees'.

- The creation of the ISMS will include listing all information assets and the security risks that may arise for each. The resultant information will inform IGG of prospective mitigation priorities.

- This ISMS policy covers all policies and procedures material to security including those listed in appendices A-C of the Information Security Policy.

- The IGG will periodically review the Council's current practices, policies and guidance to recommend any changes or improvements to ensure we apply appropriate security measures.