Mid Devon District Council

Information Security Management Policy

Policy Number: IM 003

October 2018

Version Control Sheet

Title: **Information Security Policy**

Purpose: **To detail the Information Security Standards for Mid Devon District Council in the protection of all Information Assets. These standards apply to all officers, Councillors, Third Party Contractors and Partner Organisations sharing Mid Devon District Council's information.**

Owner: **Group Manager for Performance, Governance and Data Security**
cyandle@middevon.gov.uk
01884 234975

Date: **October 2018**

Version Number: **2.0**

Status:

Review Frequency: **Every three years**

Next review date: **October 2021**

Consultation **This document was sent out for consultation to the following:**
Leadership Team
Cabinet Member

Document History
This document obtained the following approvals.

Title	Date	Version Approved
Group Manager for ICT & GMS Services	**12/10/2018**	**2.0**
Leadership Team		**2.0**
Cabinet		**2.0**

Contents

Information Security Policy

1. Introduction

1.1 Mid Devon District Council has a duty and responsibility to protect all its Information Assets in whatever form they exist and wherever they are located. Mid Devon District Council will protect information as directed by national government standards as set by National Cyber Security Centre (NCSC) and in collaboration with Devon Information Security Partnership.

1.2 This policy provides a framework for the management of information assets to ensure that they are kept secure, are available when needed, maintains integrity and, where necessary, remains confidential ensuring compliance with all laws, regulations and other obligations.

2. Scope

2.1 These standards shall apply to all officers, Councillors, third party contractors and partner organisations sharing Mid Devon District Council's information.

3. Risks

3.1 Failure to adequately manage information security can lead to:

- Damage to Mid Devon District Council's reputation
- Disclosure of confidential or personal information
- Misuse of Mid Devon District Council's information for personal gain, e.g. fraud
- Theft of data and other assets
- Loss or damage to data due to infection by malicious attacks
- Breaches of legislation and legal action against Mid Devon District Council
- Electronic eavesdropping or interception of communications
- Inaccuracies in data processing
- Failure to deliver critical services to Mid Devon District Council's customers.

4. Identification of roles and responsibilities

4.1 Leadership Team are the lead group for Information Security, with specific duties as follows:

- Director of Corporate Affairs and Business Transformation as Senior Risk Information Officer (SIRO)
- Group Manager for Performance, Governance and Data Security as Data Protection Officer and Information Management and Security Officer (DPO)
- Group Manager for ICT & GMS Services as Information Technology Security Officer (ITSO)
- Information Asset Owners (IAO) are the key system owners

5. Training and Awareness

5.1 Training will be carried out through use of the Learning Management System (LMS), Induction training and update briefings.

5.2 References to security protocols will be in tenders, contracts and agreements.

5.3 Adhering to security measures will be a condition of any sharing, partnerships, contractors and third party agreements.

6. Review of Policy

6.1 This policy will be reviewed in 2021 and in accordance with NCSC and the Devon Information Security Partnership.

Standard 1: Organisation of Information Security

1.1 Introduction

1.1.1 This standard sets out Mid Devon District Council's commitment to manage information security.

1.2 Control Objective

1.2.1 This standard is intended to ensure that Mid Devon District Council manages the security of information within a clear and agreed framework which shall be applied across the organisation and in its dealings with third parties.

1.3 Policy

1.3.1 Mid Devon District Council will manage the security of information within an approved framework through assigning roles and co-ordinating implementation of this security policy across the organisation and in its dealings with third parties, where necessary drawing upon specialist external advice so as to maintain the security policy and thus address new and emerging threats and standards.

1.4 Internal Security Organisation

1.4.1 Leadership Team will give clear direction and support for information security initiatives.

1.4.2 Group Managers Team acting as a cross-functional forum will co-ordinate security measures.

1.4.3 Responsibilities for the protection of individual assets and for carrying out specific processes are clearly defined.

1.4.4 A process is in place for data protection impact assessments to be done before the installation of new information processing facilities.

1.4.5 Mid Devon District Council requires confidentiality and non-disclosure agreements to be completed where appropriate.

1.4.6 Information security advice will be sought from in-house or external specialist advisors and communicated throughout the organisation.

1.4.7 Mid Devon District Council maintains contacts with external security specialists, e.g. law enforcement and regulatory bodies.

1.5 Third Party Access

1.5.1 All third party access to Mid Devon District Council information systems must be risk assessed and appropriate counter measures applied to mitigate the risk.

1.5.2 Suppliers given access to Mid Devon District Council information or assets must comply with Mid Devon District Council's Information Security Policy.

1.5.3 Contracts with third parties set out the security conditions and controls that they are required to adhere to.

Standard 2: Asset Management

2.1 Introduction

2.1.1 This standard sets out Mid Devon District Council's commitment to protect information and related information processing assets.

2.2 Control Objective

2.2.1 This standard is intended to ensure that Mid Devon District Council achieves and maintains an appropriate level of protection of its organisational assets.

2.3 Policy

2.3.1 Mid Devon District Council requires that all assets are accounted for and have a nominated person made responsible for their safekeeping, ie the IAO. The IAO shall be responsible for the maintenance and protection of the asset(s) concerned.

2.4 Responsibility for assets

2.4.1 An inventory of assets is maintained which includes: software, databases, information stores, physical assets, services, people and intangibles.

2.4.2 An IAO, either an individual or a section, must be formally assigned to all information and assets connected with information processing. The IAO has responsibility for controlling the production, development, maintenance, use and security of a named asset.

2.5 Information classification

2.5.1 Information classification and associated protective controls must be applied to facilitate sharing or restricting information.

2.5.2 Mid Devon District Council maintains procedures for information labelling and handling in accordance with its classification scheme.

Standard 3: Human Resources

3.1 Introduction

3.1.1 This standard sets out Mid Devon District Council's commitment to reduce the risk of employee, contractor or third party user theft, fraud or misuse of information and information processing facilities.

3.2 Control Objective

3.2.1 This standard is intended to ensure that Mid Devon District Council's officers, contractors and third party organisations understand their responsibilities, having been assessed as suitable for their role and provided with adequate resources to safeguard Mid Devon District Council's information assets.

3.3 Policy

3.3.1 Mid Devon District Council requires that employee, contractor and third party terms and conditions of employment/working and any supporting documents, e.g. job descriptions, set out security responsibilities with an adequate screening and declaration process in place. These shall be supported by an adequate training and awareness programme with recourse to disciplinary/contract action if necessary.

3.4 Prior to Employment

3.4.1 Background (screening) checks are carried out in respect of officers, employment candidates, contractors and third party users, relevant to the classification of information they will access.

3.4.2 Mid Devon District Council's officers, contractors and third parties sign security confidentiality and data protection agreements as part of their initial terms and conditions of employment.

3.5 During Employment

3.5.1 Mid Devon District Council's Councillors, officers, contractors and third party users receive appropriate training and mandatory updates in policies and procedures.

3.5.2 Mid Devon District Council may invoke the formal disciplinary process for officers who commit an information security breach.

3.6 Termination or Change of Employment

3.6.1 Mid Devon District Council maintains clearly defined and assigned procedures in respect of leavers, which must be followed at all times.

3.6.2 Councillors, officers, contractors and third party users must return all information assets in their possession upon termination of their employment, contract or agreement.

3.6.3 The access rights of all Councillors, officers, contractors and third party users to information and information processing facilities are terminated upon termination of their employment, contract or agreement.

Standard 4: Physical and Environmental Security

4.1 Introduction

4.1.1 This standard sets out Mid Devon District Council's commitment to preventing unauthorised access.

4.2 Control objective

4.2.1 This standard is intended to ensure that Mid Devon District Council takes adequate steps to prevent unauthorised physical access and damage or interference to its premises, information, assets or people therein.

4.3 Policy

4.3.1 Mid Devon District Council requires that physical security is commensurate with the risks faced for the area concerned. In particular, critical or sensitive information processing is carried out in appropriately secure environments.

4.4 Secure Areas

4.4.1 Areas that contain information and information processing facilities have access restricted to only authorised personnel.

4.4.2 Mid Devon District Council must design facilities with regard to protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster.

4.5 Equipment Security

4.5.1 Information processing equipment is sited with a view to minimise loss or damage from environmental threats and hazards or opportunities for unauthorised access.

4.5.2 Key items of equipment are protected from power failures and other disruptions caused by failures in supporting utilities.

4.5.3 Data carrying cabling is protected from interception or damage.

4.5.4 Equipment is maintained in accordance with manufacturer's recommendations to ensure continued availability and integrity.

4.5.5 Due consideration is taken for equipment removed from Mid Devon District Council premises in terms of its security and any information held on it.

4.5.6 Equipment is checked prior to disposal to remove or overwrite any sensitive data and/or licensed software.

4.5.7 Mid Devon District Council equipment, information or software must not be taken off site without prior risk assessment.

Standard 5: Communications and Operations Management

5.1 Introduction

5.1.1 This standard sets out Mid Devon District Council's commitment to ensure the correct and secure operation of information processing facilities within, between and outside of Mid Devon District Council.

5.2 Control Objective

5.2.1 This standard is intended to ensure that Mid Devon District Council's processing facilities are secure and allow for the correct processing of data.

5.3 Policy

5.3.1 Mid Devon District Council requires that responsibilities and procedures for the management, operation, ongoing security and availability of all information processing facilities, data being stored and destroyed in a controlled manner.

5.4 Procedures and Responsibilities

5.4.1 Detailed operating procedures are documented and maintained through formal change control processes covering:

- Information processing and handling
- Error handling/exceptions
- Support contracts
- Restart and recovery procedures
- Back up/maintenance
- System start up/close down

5.4.2 Formal change control procedures for information processing facilities and systems are in place with audit logs stamped with the date and time and a roll-back capability.

5.4.3 The duties of those involved with the handling and processing of data and of subsequent output are wherever possible segregated and/or compensating controls adopted.

5.5 Third Party Service Delivery Management

5.5.1 Security controls, service definitions, data sharing and delivery levels included in third party service agreements are implemented, operated and maintained by the third party.

5.5.2 Third party services, reports and records may be monitored and reviewed with periodic audits being undertaken.

5.5.3 Changes to the provision of third party services, including maintaining and improving existing information security policies, procedures and controls are managed taking into account the risks involved.

5.6 Protection Against Malicious Code

5.6.1 Preventative, detective and recovery controls are implemented to protect against malicious code with appropriate user awareness procedures having been implemented.

5.7 Back-up

5.7.1 Back-up copies of essential business information and software are regularly taken and tested in accordance with a back-up policy.

5.8 Network Security Management

5.8.1 A range of controls has been implemented to achieve and maintain security across Mid Devon District Council networks and data whilst in transit.

5.8.2 The network meets the criteria and is regularly tested for Public Sector Network compliance.

5.9 Media Handling

5.9.1 The management of removable computer media, e.g. tapes, disks, data sticks and printed reports is adequately controlled.

5.9.2 Procedures are in place for the secure and safe disposal of media.

5.9.3 System documentation is protected from unauthorised access.

5.10 Exchange of Information

5.10.1 Data sharing agreements are in place between Mid Devon District Council and other organisations with regard to the exchange of information and software.

5.10.2 Electronic messaging systems, e.g. email, are appropriately protected.

5.10.3 Policies and procedures are in place and implemented to protect information accessed.

5.11 Electronic Commerce Services

5.11.1 Information used in the conduct of electronic commerce passing over public networks is protected from fraudulent activity, contract dispute, unauthorised disclosure and modification.

5.11.2 Information transmitted in respect of on-line electronic services is protected against incomplete transmission, mis-routing, unauthorised alteration and disclosure, duplication or replay.

5.12 Monitoring

5.12.1 Audit logs recording user activities, exceptions and security events are produced and retained as required.

Standard 6: Access Control

6.1 Introduction

6.1.1 This standard sets out Mid Devon District Council's commitment to control access to its information and information systems so as to safeguard its information against deliberate or accidental damage, disclosure or misuse.

6.2 Control Objective

6.2.1 This standard is intended to ensure that Mid Devon District Council allows appropriate access to information.

6.3 Policy

6.3.1 Mid Devon District Council requires that access to information and information systems shall be driven by business requirements. Access shall be granted to personnel, Councillors and contractors to a level that will allow them to carry out their duties and shall not be excessive.

6.4 Business Requirement for Access Control

6.4.1 An access control policy is established, documented and reviewed periodically.

6.5 User Access Management

6.5.1 A formal user registration and de-registration is in place for granting and revoking access to information systems and services.

6.5.2 The allocation of user rights to information and information systems is controlled and in accordance with the individual's authorised operational role.

6.5.3 The allocation of passwords for information and information systems is controlled.

6.5.4 Information system user's access rights are reviewed at regular intervals.

6.6 User Responsibilities

6.6.1 Users of information systems must follow good security practices in the selection and use of passwords.

6.6.2 The Council operates a clear desk policy and computer screens must be locked when left unattended.

6.7 Network Access Control

6.7.1 Users are only provided with access to services that they have specifically been authorised to use.

6.7.2 Appropriate authentication methods are used to control access by remote users, e.g. vpns, fobs etc.

6.7.3 Equipment connected to networks is authenticated using automatic equipment identification.

6.7.4 Access to physical and logical diagnostic and configuration ports is controlled.

6.7.5 Information services and systems are adequately segregated on the network.

6.7.6 The capability of users to connect to the network outside of Mid Devon District Council's boundaries is restricted.

6.8 Operating System Access Control

6.8.1 Access to operating systems is controlled through a secure log-on procedure.

6.8.2 Operating system users are provided with a unique identifier (user ID) so that activities are traceable to the individual concerned.

6.8.3 An effective password management system is in place for the selection of quality passwords.

6.8.4 Access to system utility programs is restricted and tightly controlled.

6.8.5 Procedures and mechanisms are in place to ensure that inactive systems time out after a defined period of inactivity.

6.9 Mobile and Home Working

6.9.1 Mid Devon District Council maintains a formal policy on the appropriate security measures that should be adopted to protect against risks of using mobile computing and communication facilities.

6.9.2 Mid Devon District Council maintains a working policy with supporting procedures to allow homeworking on request.

6.9.3 However, at present formal home working is not a requirement. If this situation changes formal home working policies will be required in consultation with HR and Unison.

Standard 7: Information Systems Acquisition, Development and Maintenance

7.1 Introduction

7.1.1 This standard sets out Mid Devon District Council's commitment to ensure that security is an integral part of its information systems.

7.2 Control Objective

7.2.1 This standard is intended to ensure that Mid Devon District Council maintains an adequate level of security in its information processing systems.

7.3 Policy

7.3.1 Mid Devon District Council requires that the information security risks, controls and requirements are identified at the earliest stage in the development or acquisition cycle, with controls to mitigate against them being identified. Controls should cover user access, data input, data processing, transmission, storage, system changes and known vulnerabilities.

7.4 Security Requirements of Information Systems

7.4.1 Security requirements are set out in statements of business requirements of new or enhanced information processing systems.

7.5 Correct Processing in Applications

7.5.1 Validation checks are incorporated into applications, where appropriate, to detect any corruption of information through processing errors or deliberate acts.

7.5.2 Data output from the application is validated.

7.6 Encryption

7.6.1 Encryption is a requirement under certain circumstances according to the DPA 2018.

7.7 Security of File Systems

7.7.1 Mid Devon District Council maintains procedures for the installation of software for operational systems.

7.7.2 Test data is carefully selected protected and controlled.

7.7.3 Access to program source code is restricted.

7.8 Security in the Development and Support Processes

7.8.1 Charges to systems are implemented under a formal change control procedure.

7.8.2 The impact of changes to operating systems on business critical applications is formally reviewed and tested to ensure that there has been no adverse effect on operations or security.

7.8.3 Modifications to software packages are generally discouraged and limited to necessary and strictly controlled changes.

7.8.4 Mid Devon District Council minimises the opportunities for the leakage of information e.g. by scanning outbound media, regular monitoring, etc.

7.8.5 Outsourced software development is supervised and monitored.

7.9 Technical Vulnerability Management

7.9.1 Information systems are assessed for technical vulnerabilities in a timely manner.

Standard 8: Compliance

8.1 Introduction

8.1.1 This standard sets out Mid Devon District Council's commitment to avoid breaches of any statutory, regulatory or contractual obligation arising out of the management of information assets.

8.2 Control Objective

8.2.1 This standard is intended to ensure that Mid Devon District Council avoids breaches of any statutory, regulatory or contractual obligation and any security requirements concerning the collection, processing, holding and dissemination of information assets whether they be communicated on paper, electronic or in verbal format.

8.3 Policy

8.3.1 Mid Devon District Council requires that the design, operation, use and management of information systems observe all statutory, regulatory and contractual security requirements.

8.4 Compliance with Legal Requirements

8.4.1 Procedures are in place to ensure compliance with legislative, regulatory and contractual requirements on the use of material in respect of which there may be intellectual property or copyrights.

8.4.2 Important records are protected against loss, destruction and falsification in accordance with statutory, regulatory and contractual requirements.

8.4.3 Data protection and privacy is ensured, as required, by relevant legislation, regulation and, where applicable, contractual obligations.

8.4.4 Controls are in place to deter users from using information processing facilities for unauthorised purposes.

8.4.5 Encryption is used in compliance with relevant laws, agreements and regulations whenever special category data is shared with third parties.

8.5 Compliance with Security Policies and Standards

8.5.1 Managers will ensure that all security procedures within their area of responsibility are carried out correctly in compliance with this and other Mid Devon District Council policies.

8.5.2 Information systems are regularly checked for compliance with security implementation standards.