The Moray Council

Access Control Policy

EDRMS

2013

Name of Document:	**The Moray Council Electronic Document and Records Management System (MCEDRMS) Access Control Policy – SharePoint 2010**
Author:	Eleanor Rowe
Description of Content:	Under the Data Protection Act personal and sensitive personal records require protection to ensure correct levels of permission, access, security, disposal, administrative or editorial rights are assigned to users of the system. To comply with records management policies it is important that records held in the system maintain their authenticity, reliability and integrity (ISO 15489).
Distribution:	
Embargoed?	
Status:	Version 1.0
Approved by:	
Date of Approval:	

Table of Contents

1. Introduction

Many of the electronic documents and records held within The Moray Council Electronic Document and Records Management System (MCEDRMS) are confidential and/or personal and sensitive. Under the Data Protection Act they require protection to ensure correct levels of permission, access, security, disposal, administrative or editorial rights are assigned to users of the system. To comply with records management policies it is important that records held in the system maintain their authenticity, reliability and integrity (ISO 15489). The Moray council have adopted the Document and Records Management elements of SharePoint 2010 as its corporate EDRMS

In order to maintain the security of electronic records, it is essential to control the process of allocating rights to staff and of changing the security levels of confidential or personal information.

Access, security, editorial and administrator rights must be authorised by the Service and created by the SharePoint Implementation Team during the development of the MCEDRS and then by the Customer Services Support Team once in Support. Changes to permissions, access, security and editorial rights must be confirmed in writing by a senior manager in the Service.

The identification of correct levels of access, security and editorial rights for staff rests with service managers. Information about access control will be sought during the development of the MCEDRMS and confirmed in writing by senior service managers.

Service managers with responsibility for the allocation of security rights for their staff must be aware of the wider implicationsof an open access policy. The Information Commissioner responsible for Data Protection poses this question in the Privacy Impact Assessment:-

Does the proposal involve personal data of particular concern to individuals? Does the proposal involve the linkage of personal data with data in other collections, or any significant change to existing data links or holdings?'

It is the linking of information and the ability to build up knowledge about an individual client or customer of the Council across services which needs to be managed carefully.

2. Policy summary

For all electronic documents and records held in MCEDRMS and any supporting systems – scanning software, Lagan, bespoke systems – it is required that:-

no unauthorised information flows from a higher to a lower level of security access
integrity, reliability and authenticity of information within the system is preserved over very long periods of time
access control is managed securely by the Customer Services Manager as holder of the Service Level Agreement (SLA) with the service
access control will be set up by the SharePoint Implementation Team and then passed to the SharePoint Customers Service Support Team – both managed by the Customer Services Manager.
an audit log of access requests and changes to permissions is to be maintained
Managers are responsible for informing the Customer Services Support Team about changes in staff and permission requirements post implementation.
Post implementation, reviews are held regularly by the Customer Services Support Team to audit security permission
Internal audit may do checks of security permissions

In support of these requirements, there shall be:

Business processes which clearly define and identify roles
Correct access, security and editorial permissions will be assigned to these roles within the business processes

These general access control principles shall be applied in support of the policy:

Read Only access is the standard access assigned to staff
Staff see what they need to see [principle of least privilege]
Permissions are assigned to groups and job descriptions not to individuals
Permissions are normally assigned to SharePoint Libraries and Document sets
Permissions may be used to restrict access to individual documents, especially in cross service processes
Permissions are consistent within the group and process i.e. different members of a group do not have different permission
The number of administrators who have control over access policy will be restricted to members of the ICT SharePoint Infrastructure Team, Customer Service Support Team and authorised by the Customer Services Manager

3. Policy

3.1 Open Material

Open material for which there exists no explicit restriction on public read access shall be termed fully open material.
Information which is publicly available to read by some method (even if some restrictions apply) shall be termed open material.
Open material for which there exists some explicit restriction on public read access shall be termed partially open material.

3.2 Closed Material

Information not intended to be publicly available by any method shall be termed closed material.

3.3 Flow of Information

No unauthorised information flow from a higher to a lower level
By default, all users have read rights to fully open material unless explicitly restricted. This constitutes a mandatory access control policy for record confidentiality.
All other rights and permissions must be agreed by senior managers and the SharePoint Implementation Team

3.4 Integrity of service

Preserve integrity of the system and the information it contains
It is essential to ensure that information in a system possesses both internal and external integrity.
Rights that allow the creation, modification or destruction of controlled information rests with the service.
The administrator's role must be limited to members of the SharePoint Implementation Team and the Customer Services Support team under the Customer Services Manager.
By default, no member of staff has any administrator rights; they must be explicitly assigned to roles and the roles to the users – controlled by explicit permission.
The identification and separation of the duties of staff who need access to the information should ensure staff have the correct permissions and the risk of security breaches can be lessened.

3.5 Management of secure access control

Access rights must not be allocated directly to staff without permission and agreement between senior managers and the SharePoint Implementation Team and the Customer Services Support Team, post implementation.

Specific access rights shall be allocated to defined roles and roles then allocated to staff.
Role based access control simplifies security management and allows for quick and easily reversible assignment of additional rights to another user, for example, when a member of staff is away.

3.6 Audit of access requests and changes

All changes in role e.g. moving across services, including secondments, need to be communicated to the Customer Services Support Team who will make the necessary changes in permissions, post implementation.
All changes to administrative, editorial, permission and execute roles, or their allocation to staff shall be audited.
All access requests by a staff for administrative, editorial, permission and execute rights shall be audited.
All access request failures shall be audited.
Any creation, modification, or destruction of a controlled object by staff shall be audited
Audit logs are themselves controlled objects and shall be protected from unauthorised observation, modification or deletion.
Audit logs shall carry the maximum security level of the information audited.

3.7 Principle of least privilege

The principle of least privilege requires that staff be granted the most restrictive set of privileges needed for the performance of their authorised tasks.
Application of this principle limits the damage that can result from accident, error or unauthorised use of the information system.

4. For Future Consideration - Protective markings

Central Government currently operates a system of protective marking classifications. The council network may not currently be configured to cope with these classifications and the introduction of such a government scheme will have implications for ICT and the council ICT network.

This section is, therefore, for information only at the current time.

Security levels may not be a simple linear classification, such as Unclassified, Restricted, or Classified, but would be able to accommodate a complex, multi-dimensional structure, for example, also allowing for the control of Freedom of Information, Sensitivity and Copyright, by the assignment of sets of security labels.

The UK Government defines 4 hierarchical security classifications for the protective marking of records:

Top secret
Secret
Confidential
Restricted

Any remaining information is classified as unrestricted

The Council may also want to consider the use of classifications which identify the following information:
Personal
Sensitive Personal

The Council is also investigating the use of warning markers (which would show e.g. if a client has a preference as to who should visit) to assist staff [under development by Human Resources]

5.Reference

TMC Information Security Policy
http://intranet.moray.gov.uk/documents/central_services/corporate_information_security_policy.pdf

TMC Information Management Strategy
http://intranet.moray.gov.uk/documents/InformationManagementStrategyv12March2011.pdf

Data Protection Act
http://www.moray.gov.uk/moray_standard/page_41220.html

Freedom of Information (Scotland) Act
http://www.moray.gov.uk/moray_standard/page_41220.html

Public Records (Scotland) Act
http://www.legislation.gov.uk/asp/2011/12/contents/enacted