Herefordshire Council

Reference number	
Approved by	**Information Management and Technology Board**
Date approved	**30 April 2013**
Last revised	**August 2018**
Review date	**August 2021**
Category	**Information Assurance**
Owner	**Information Governance**
Target audience	**All staff**

IT ACCESS CONTROL POLICY

Document Control

This is a CONTROLLED document and updates or changes to this document are authorized and then advised by email to the relevant document holders.

It is UNCONTROLLED when printed. You should verify that you have the most current issue.

DOCUMENT HISTORY

Author(s)

Names	Role
Helen Worth	Information Governance Manager

Document Log

Version	Status	Date Issued	Description of Change	Pages affected	Review
0.1	Draft		Approval to use of WM template obtained from KI Steering Group 12/02/2013	All	
1.0	Issued	30/04/2013	Approved by IM&T Board	All	March 2014
1.1	Issued	22/04/2014	ISO27001 Logo Removed and policy reviewed	All	March 2015
1.1	Issued		Annual review October 2014 – no changes made	All	November 2015
1.2			Annual Review Nov 2015 – no changes made	All	December 2016
1.3	Issued	22/02/2016	Updated to reflect policy changes	All	January 2019
1.4	Issued	25/04/2016	Updated due to recommendations from internal audit.	All	January 2019
1.5	Issued	08/08/2018	Updated in line with GDPR	All	August 2021

Contents

Policy Statement

Herefordshire Council will establish specific requirements for protecting information and information systems against unauthorised access.

Herefordshire Council will effectively communicate the need for information and information system access control.

Purpose

Information security is the protection of information against accidental or malicious disclosure, modification or destruction. Information is an important, valuable asset of Herefordshire Council which must be managed with care. All information has a value to the Council. However, not all of this information has an equal value or requires the same level of protection.

Access controls are put in place to protect information by controlling who has the rights to use different information resources and by guarding against unauthorised use.

Formal procedures must control how access to information is granted and how such access is changed.

This policy also mandates a standard for the creation of strong passwords, their protection and frequency of change.

Scope

This policy applies to all Herefordshire Council Councillors, Committees, Departments, Partners, and Employees of the Council (including system support staff with access to privileged administrative passwords), contractual third parties and agents of the Council with any form of access to Herefordshire Council's information and information systems.

Definition

Access control rules and procedures are required to regulate who can access the Council's information resources or systems and the associated access privileges. This policy applies at all times and should be adhered to whenever accessing Herefordshire Council information in any format, and on any device.

Risks

On occasion business information may be disclosed or accessed prematurely, accidentally or unlawfully. Individuals or companies, without the correct authorisation and clearance may intentionally or accidentally gain unauthorised access to business information which may adversely affect day to day business. This policy is intended to mitigate that risk.

Non-compliance with this policy could have a significant effect on the efficient operation of the Council and may result in financial loss and an inability to provide necessary services to our customers**.**

System Administration Standards

The password administration process for individual Herefordshire Council systems is well-documented and available to designated individuals.

All Council IT systems will be configured to enforce the following:

- Authentication of individual users, not groups of users - i.e. no generic accounts.
- Protection with regards to the retrieval of passwords and security details.
- System access monitoring and logging - at a user level.
- Role management so that functions can be performed without sharing passwords.
- Password admin processes must be properly controlled, secure and auditable.

User Access Management

Formal user access control procedures must be documented, implemented and kept up to date for each application and information system to ensure authorised user access and to prevent unauthorised access. They must cover all stages of the lifecycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access. These must be agreed by Herefordshire Council. Each user must be allocated access rights and permissions to computer systems and data that:

- Are commensurate with the tasks they are expected to perform.
- Have a unique login that is not shared with or disclosed to any other user.
- Have an associated unique password that is requested at each new login.

User access rights should be reviewed at regular intervals to ensure that the appropriate rights are still allocated. System administration accounts must only be provided to users that are required to perform system administration tasks.

User Registration

A request for access to the Council's computer systems must first be submitted to the Hoople IT Service Desk. Applications for access must only be submitted if approval has been gained from the information asset owner.

When an employee leaves the Council, their access to computer systems and data must be suspended at the close of business on the employee's last working day. It is the responsibility of the employee's line manager to request the suspension of the access rights via the Hoople IT Service Desk.

User Responsibilities

It is a user's responsibility to prevent their user ID and password being used to gain unauthorised access to Council systems by:

- Following the Password Policy Statements outlined In the Handling Information Personal Responsibilities document

- Ensuring that any PC they are using that is left unattended is locked or logged out.
- Leaving nothing on display that may contain access information such as login names and passwords.
- Informing Hoople IT Service Desk of any changes to their role and access requirements.

Privilege Management

Inappropriate use of system privileges is often found to be a major contributory factor to breaches of system security. To address this concern, the allocation of privileges shall be managed through a formal authorisation process as follows:

- Privileges shall be allocated on a need to know basis. Where privilege based activities are not a primary function of the (privileged) user, privileges shall be allocated on a specific, event basis;
- A Privileged Access register shall be maintained by information asset owners to include the ID of an individual allocated privileges and the level of access rights granted;
- The allocation of privileges shall be kept to a minimum;

Network Access Control

The use of modems on non-Council owned PC's connected to the Council's network can seriously compromise the security of the network. The normal operation of the network must not be interfered with. Specific approval must be obtained from Information Governance before connecting any equipment to the Council's network.

User Authentication for External Connections

Where remote access to the internal network resources is required, an application must be made via the It Service desk who will then contact Information Governance to ensure that correct agreements are held on file. Remote access to the network must be secured by two factor authentication consisting of a username and one other component, for example a Crypto Card.

Suppliers and Partner Agencies Access to the Network

A guest wireless network is available for suppliers and third parties at our premises. Access must be sponsored by an existing employee and must be in adherence to the acceptable use policy.

Connectivity by means other than guest wireless which permits access to the internal network by partner agencies or 3rd party suppliers must not be given without authorisation from Hoople Transformation and Technology.

Accounts for Suppliers and Partner Agencies will be restricted in what they can access, only enabled for a time to complete the required work, have a business sponsor and be subject to periodic review. Any changes to supplier's connections must be immediately sent to the IT Service Desk so that access can be updated or ceased. All permissions and access methods must be registered with Information Governance and controlled by Transformation and Technology.

Partners or 3rd party suppliers must contact our Service Desk before connecting to the network and a log of activity must be maintained. Remote access must be disabled when not in use.

Operating System Access Control

Access to operating systems is controlled by a secure login process. The access control defined in the User Access Management section in this policy must be applied. The login procedure must also be protected by:

- Not displaying any previous login information e.g. username.
- Limiting the number of unsuccessful attempts and locking the account if exceeded.
- The password characters being hidden by symbols.
- Displaying a general warning notice that only authorised users are allowed.

All access to operating systems is via a unique login ID that will be audited and can be traced back to each individual user. The login ID must not give any indication of the level of access that it provides to the system (e.g. administration rights).
System administrators must have individual administrator accounts that will be logged and audited. The administrator account should not be used by individuals for normal day to day activities.

Use of System Utilities

System utilities and tools can be capable of over-riding both system and application level security controls and their use shall be strictly controlled in accordance with the following criteria:

- System utilities and tools shall only be available to authorised users and only after users have undertaken appropriate training, to ensure the safe use of the utility;
- The use of system utilities shall be limited to the minimum practical number of trained, authorised users;
- The ID and authorisation level for authorised user of system utilities shall be recorded and retained with the respective system documentation;
- System utilities and tools shall be removed from systems where their use is not explicitly required for normal operations;
- Individuals using system utilities and tools shall be responsible for taking appropriate precautions to protect the security of the system and any information within the system.

Session Time Outs

Sensitive systems and terminals in high risk locations, e.g. public or external areas shall incorporate a time-out facility which will clear the terminal screen and close both application and network sessions after a defined period of inactivity. Individual Services will be expected to identify which of their systems and terminals are classed as sensitive.

Limitation on Connection Time

Limiting the period during which access is allowed for sensitive computer operations reduces the window of opportunity for unauthorised access. Where justified by business requirements and the sensitivity of information, the following controls may be established:

- Predetermined time slots may be used for batch file transmissions;
- Regular interactive sessions may be restricted to short durations;
- Connection times may be restricted to normal office hours, where there is no requirement for out-of-hours operation.

Application and Information Access

Access within software applications that process sensitive information must be restricted using the security features built into the individual product. The Information Asset Owner of the software application is responsible for granting access to the information within the system. The access must:

- Be compliant with the User Access Management section of this policy.
- Be separated into clearly defined roles.
- Give the appropriate level of access required for the role of the user.
- Be unable to be overridden (with the admin settings removed or hidden from the user).
- Be free from alteration by rights inherited from the operating system that could allow unauthorised higher levels of access.
- Be logged and auditable.

Sensitive Systems Isolation

For highly sensitive applications where security breaches may result in an unacceptable impact and where justified by risk analysis, specific security measures shall be deployed to prevent unauthorised access to the application and information contained within it, particularly:

- The sensitivity or security classification of such applications shall be explicitly identified and documented by the application owner;
- In circumstances where a sensitive application is to run in a shared environment, the network controls and the application systems with which it will share resources shall be identified and agreed with the owner of the sensitive application.

Policy Compliance

If any user is found to have breached this policy, they may be subject to Herefordshire Council's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).

If you do not understand the implications of this policy or how it may apply to you, seek advice from your Line Manager

Policy Governance

The following table identifies who within Herefordshire Council is Accountable, Responsible, Informed or Consulted with regards to this policy. The following definitions apply:

- **Responsible** – the person(s) responsible for developing and implementing the policy.
- **Accountable** – the person who has ultimate accountability and authority for the policy.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

Responsible	Information Governance
Accountable	Data Protection Officer
Consulted	Information Governance Steering Group
Informed	All Staff, Councillors, Contractors and Partners

Review and Revision

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 3 years.

Policy review will be undertaken by Information Governance.