HANDFORTH TOWN COUNCIL
Here for the whole community
Town Clerk: Ashley Comiskey Dawson
Tel: 01625 523330
Email: clerk@handforthtowncouncil.gov.uk

IT Access control policy

Purpose

The objective of this policy is to minimise accidental or unauthorised access to the organisation systems, networks, drives, applications, electronic folders and electronic information. It is therefore applicable to all forms of logical access. The organisation requires that all employees and members comply with the directives presented within this policy. This document supports the organisation's IT and Data Protection Policies. It provides direction and support for the implementation of access controls and is designed to help organisation employees carry out the business of the organisation in a secure manner.

Introduction

Individuals who are not explicitly granted access to organisation information or information systems are prohibited from using such systems.

Individuals employed by or under contract to the organisation shall be granted access only to information and information systems that are required to fulfil their duties.

Access will be granted only to those individuals who have formally agreed to comply with the organisation's Information Security Policy and have signed the organisation's Code of Conduct or a confidentiality/non-disclosure agreement (agency workers).

This policy applies to:

- all employees including temporary and agency workers, independent consultants and contractors
- trustees and/or members
- third party organisations who require access to the organisation's information systems and facilities should also be aware of the contents of this policy

The policy is not designed to be obstructive. If you consider that any element of this policy hinders or prevents you from carrying out your duties, please contact the organisation clerk

This policy should be read in conjunction with all other IT and Data Protection policies

Access to IT network and drives

Access to information and information systems will be controlled on the basis of business and security requirements.

Each business application run by, or on behalf of the organisation, will have a nominated system administrator who is responsible for managing and controlling access to the application and associated information.

Access to information must be based on roles and responsibilities, 'need to know' and segregation of duties and roles. The appropriate information, system, database, or application owner is the only individual that can authorise a systems administrator to grant or update access via the formal access management process.

Special attention is given, where appropriate, to the need to control the allocation of privileged access rights, which allow users to override system controls.

Access control requirements are clearly defined, documented and maintained within an Access Policy Matrix, which specifies the rights of individuals or groups of users.

The organisation has adopted common Windows-based operating systems, and predefined user profiles will be maintained to restrict access. The matrix will be approved and reviewed by the data controller.

Remote access to systems

Work is recognised as an activity rather than a specific place. Therefore, the locations in which work is carried out can include places away from the office such as home. Or the work could involve dealing with the public and/or customers in the community or where our services are based and/or delivered. The Organisation's flexible working policy sets out the criteria and arrangements

Requests for remote access to be established will be assessed using a consistent set of criteria regardless of the remote location:

- Compliant with flexible working policy
- Physical security of site
- Provision of firewall, or firewall router/modem
- Suitability of ISP – (this is of particular relevance if remote site is outside of UK)

User access management

User access management covers all stages of user access, from initial registration, through changes in role, to deregistration and revocation of access.

The security of systems, networks, applications and databases is heavily dependent on the level of protection of user IDs, passwords, and other credentials that provide access to it. Hence, protecting the credentials that provide access to information is indirectly protecting the information.

Identification and authentication of users and systems enables the tracking of activities to be traced to the person responsible.

All employees shall have a unique identifier (user ID) for their personal and sole use. Shared, group and generic user IDs are not permitted unless they are used to access the intranet only. Employees must be educated that they are not permitted to allow their user ID to be used by anyone else. Employees must be made aware of this and how to store them.

A process must exist for issuing and revoking the user IDs. Redundant user accounts must be monitored and managed.

User registration

A process for user registration and granting access rights exists and includes:

- line managers request correct access controls for new users. A ‘New User Request’ should be completed using the organisation's Service Desk
- unique user IDs assigned so that access and modifications can be traced
- authorised users are aware of their responsibilities for the protection of information within the application and where applicable users sign an appropriate agreement
- ensuring access is granted once authorisation is obtained
- maintaining a record of all registered users
- Change of role

Where an employee changes role within the organisation the following process is followed:

- Line Managers must inform all relevant information owners/system administrators of the names of employees that have transferred to different job/roles within 24 hours of transfer
- Information owners must review the transferee’s access rights to their systems to ensure that they are still valid
- Where relevant, an ‘Amend User Request’ should be completed by line managers using the organisation's Service Desk available on the staff intranet
- A process must be in place for HR departments/officers to communicate transfers to system administrators.

Review of access rights

- The clerk should review access lists to ensure they are still applicable.
- The data controller must approve access rights prior to set up by the system administrator.
- The system administrator does not have the authority to decide who should have access to what information. This is a organisation decision.

Removal of access

On resignation of employment, the worker's line managers, (and in conjunction with HR provider guidance where required), will undertake a risk assessment and determine whether existing access rights of an individual should be reviewed and reduced whilst working out their notice. Hostile terminations must be communicated to system administrators immediately and access immediately disabled.

Access rights should be disabled within 24 hours on the employee’s final working day.

If the leaver has been provided with any equipment and access to systems and buildings, it is important that all organisation assets are returned on the workers last working day and access to buildings and systems removed.

It is the responsibility of line managers to ensure that leavers return their entry ID pass at the end of their last working day.

It is important that all assets are returned to the organisation on the workers last working day.

Privilege management

A process is in place for the allocation and removal of system administration level access or increased user privilege. This will primarily be to provide access to systems and specific drives/folders where a staff member is off on sickness or other absence, or extended sickness absence, to permit temporary access, allowing essential organisation business to continue. Privilege management includes the control that every level of privilege within each application and the categories of staff to which they need to be allocated are identified and recorded:

- Privileges are allocated to an individual as an event requires
- Authorisation is recorded for each allocated level of privilege and only granted once authorisation is obtained
- The development of system routines are identified and implemented to avoid the use of privileged access
- Privileges are assigned to a different user ID from those used for normal business use and a log of increased user privilege is recorded

Monitoring system access and use

Systems will be monitored to detect deviation from the Access Control Policy and record events to provide evidence in case of security incidents.

The application business owner/system administrator must establish the logging and monitoring requirements for auditing trail purposes.

Audit and event logs will need to be adequately secured, possibly centrally and separately from privileged-level employees (separation of duties). Tools may be required for log analysis.

Exceptions

In the following exceptional cases compliance with some parts of the policy may be relaxed. The parts that may be relaxed will depend on the particular circumstances of the incident in question:

- If complying with the policy would lead to physical harm or injury to a member of staff
- If complying with the policy would cause significant damage to the company's reputation or ability to operate
- If an emergency arises, for instance due to staff absence/sickness access needs to be allocated to ensure organisation business can continue uninterrupted – see' Privilege' section above

In such cases, the staff member concerned must take the following action:

- Ensure that their manager and the clerk is aware of the situation and the action to be taken

- Ensure that the situation and the actions taken are recorded in as much detail as possible on a non-compliance report

Failure to take these steps may result in disciplinary action:

In addition, a list of known exceptions and non-conformities to the policy should be maintained. This list contains:

- known breaches that are in the process of being rectified
- minor breaches that are not considered to be worth rectifying
- any situations to which the policy is not considered applicable

The organisation will not take disciplinary action in relation to known, authorised exceptions to the information security management system.

Non -compliance

Non-compliance is defined as any one or more of the following:

- Any breach of policy statements or controls listed in this policy
- Unauthorised disclosure or viewing of confidential data or information belonging to the organisation or partner organisation
- Unauthorised changes to information, software or operating systems
- The use of hardware, software, communication networks and equipment, data or information for illicit purposes which may include violations of any law, regulation or reporting requirements of any law enforcement agency or government body
- The exposure of the organisation or partner organisation to actual or potential monetary loss through any compromise of security

Any person who knows of or suspects a breach of this policy must report the facts immediately to the clerk

Any violation or non-compliance with this policy may be treated as serious misconduct.

Penalties may include: Up to Final Written Warning.

Adopted by HTC on 13th January 2026.