IT Security Policy and procedure

1. Policy Statement

1.1. Protecting access to IT systems and applications is critical to maintain the integrity of the organisation's information, technology and data and prevent unauthorised access to such resources.

1.2. Access to the organisation systems is restricted to authorised users or processes only, based on the principle of strict ***need to know and least privilege***. Access controls are necessary to ensure that only authorised users can obtain access to the organisation's information and systems and they manage the admittance of users to system and network resources by granting access only to the specific resources they require to complete their job related duties.

1.3. The organisation will use an IT Permissions Form to identify and agree individual access to systems, applications and firewalls and identify who should be given administrator privileges.

1.4. Because of the nature of this Policy and the potential risks to the organisation, it will be reviewed on an annual basis.

2. Policy objective

2.1. The objective of this policy and related procedure is to ensure that the organisation has adequate controls to restrict access to its systems and data.

3. Access to confidential and restricted information

3.1. Access to confidential and restricted information will be limited to authorised persons whose job role require it, or, is determined by law or a contractual agreement. (See Data Protection Policy.)

3.2. Access to any of these resources will be restricted by the use of firewalls, network segregation, secure log-on procedures, access control list restrictions and other controls as appropriate.

3.3. The responsibility to implement access restrictions lies with data processors and data controllers but must be implemented in line with this policy. The ~~Head Office~~ Development Manager for the organisation is the Data Protection Officer (DPO)

3.4. There are no restrictions on the access to "Public" information.

4. *Areas of activity*

4.1. This policy applies to:

- The creation, amendment and deletion of individual user accounts and access permissions.
- The creation and deletion of administrator permissions.
- Cloud computing.
- Firewall security.
- Access for remote users.
- Addition and removal of approved applications.
- Related policy and procedure.

5. *Scope*

5.1. This Policy applies to:

- All schemes, offices and sites.
- All members of core staff, all Bank Workers, all volunteers and student placements, consultants, contractors, agents and authorised users accessing the organisation's IT systems and applications.
- All IT systems or applications managed by the organisation that store, process or transmit information, including network and computer hardware, software and applications, mobile devices, and telecommunication systems.

Procedure

1. Introduction

1.1. This document provides the framework and process for how user accounts and privileges are created, managed and deleted. It includes how new users are authorised and granted appropriate privileges, as well as how these are reviewed and revoked when necessary and includes appropriate controls to prevent users obtaining unauthorised privileges or access.

2. Definitions

Users

2.1. The collective term used to describe all those who have access to the organisation's information and information systems as outlined in the Scope of this Policy.

Privileged Users

2.2. A privileged user is a user who has an elevated level of access to a network, computer system or application and is authorised to perform functions that standard users are not authorised to perform.

2.3. This includes a "standard user" with approved elevated privileges that allows equivalent access to that of a privileged user.

2.4. Examples of user accounts with privileges include:

- Administrators.
- Super users.

2.5. *Access Control*

"Access Control" is the process that limits and controls access to resources of a computer system.

2.6. *Access privileges*

"Access Privileges" are systems permissions associated with an account, including permissions to access or change data, to process transactions, create or change settings, etc.

2.7. *Administrator Account*

An "Administrator Account" is a user account with privileges that have advanced permissions on an IT system that are necessary for the administration of this system. For example, an administrator account can create new users, change account permissions, modify security settings such as password settings, modify system logs, etc.

2.8. *Application and Service Accounts*

"Application and Service Accounts" are user accounts that are not associated with a person but an IT system, an application (or a specific part of an application) or a network service.

2.9. *Nominative User Accounts*

"Nominative User Accounts" are user accounts that are named after a person.

2.10. *IT Support Team*

The company contracted by the organisation to provide IT support to the organisation.

2.11. *Low Risk Data*

"Low risk data" refers to:

- Data that is intended for public disclosure, or
- The loss of confidentiality, integrity, or availability of the data or system would have no adverse impact on our mission, safety, finances, or reputation.

2.12. *Medium Risk Data*

"Medium risk data" refers to:

- Data that is not generally available to the public, or
- The loss of confidentiality, integrity, or availability of the data or system could have a mildly adverse impact on the organisation's mission, safety, finances, or reputation.

2.13. *High Risk Data*

"High risk data" refers to:

- Data that is required to be protected by GDPR (General Data Protection Regulation), or some other law.

- the organisation is required to self-report to the Information Commissioners Office (ICO), commissioners of its services and / or provide notice to an individual if the data is inappropriately accessed.
- The loss of confidentiality, integrity, or availability of the data or system could have a significant adverse impact on the organisation's mission, safety, finances, or reputation.

3. *Guiding principles*

3.1. The organisation will provide access privileges to its IT services and equipment (including networks, systems, applications, computers and mobile devices) based on the following principles:

- ***Need to know*** – users or resources will be granted access to systems that are necessary to fulfil their roles and responsibilities.
- ***Least privilege*** – users or resources will be provided with the minimum privileges necessary to fulfil their roles and responsibilities.

3.2. Requests for users' accounts and access privileges must be formally documented and appropriately approved.

3.3. Requests for special accounts and privileges (such as system administration accounts, shared / generic accounts, test accounts and remote access) must be formally documented and approved by a Head Office Manager via the IT Permissions Form.

3.4. Accounts for services or applications (apps) must only be used by staff who are required to use them as part of their job role; access to the passwords must be restricted to authorised staff only.

3.5. Where possible, the organisation will set user accounts to automatically expire at a pre-set date. More specifically:

- When temporary access is required, such access will be removed immediately after the user has completed the task for which the access was granted.
- User accounts assigned to temporary staff will be set to expire according to their contract's expiry date.

- User accounts will be disabled when they leave the organisation:
  - User accounts will be transferred to the Head Office Manager when individual leaves the organisation.
  - Head Office Manager will record the date of resignation and contact the user's Head Office Manager after 3 months to confirm that the account can be deleted before asking the IT Support Team to do so.

3.6. Access rights will be disabled or removed when the organisation's IT Support Team receives notification that a user is terminated or ceases to have a legitimate reason to access the organisation systems.

3.7. Verification of each user's identity must be performed by a Head Office Manager or designate, before granting a new password (i.e. the organisation must be satisfied that they are being contacted by the user when a request for a new password is made, if this is not done in person).

3.8. Existing user accounts and access rights will be reviewed at least annually to detect dormant accounts; which will then be deleted. The privileges attached to accounts will also be checked:

- Active accounts assigned to external contractors, vendors or employees that no longer work for the organisation will be deleted.
- Active accounts with access rights for which the user's role and responsibilities do not require access will be revised. E.g. users that do not have authority or responsibility to approve expenses should not have access with approval permissions within a financial system.
- System administrative rights or permissions (including permissions to change the security settings or performance settings of a system) granted to a user who is not an administrator will be amended. (See Paragraph 5.3.)
- Unknown active accounts will deleted.

3.9. All access requests for system and application accounts and permissions will be documented using the most current version of the IT Permissions Form.

4. Creation, amendment and deletion of individual user accounts and access permissions

Creation of new accounts

4.1. On the appointment of every new employee, the Head Office Manager will complete the most current IT Permissions Form ensuring that the following sections are completed in full (where applicable):

- Name.
- Start date.
- Staff member.
- Change of responsibilities.
- Date of change.
- Locations of work.
- Drive access.
- Email distribution groups.
- Administrator permissions or access to cloud services.
- Access to applications.
- Other requests.

4.2. Once completed the Head Office Manager will sign and date the form and forward to a senior manager for approval. A senior manager for this approval is:

- Area Manager
- Regional Director
- Development Director

4.3. The senior manager will confirm the details listed on the form and if satisfied with the permissions requested will sign and date the form.

4.4. The senior manager will then forward the form to the Head Office Manager

4.5. Head Office Manager will record the information on the form in the database.

4.6. located at Champness hall, Drake Street Rochdale and email the completed form to the IT Support Team.

4.7. IT Support Team will complete the work requested on the form. Once complete the IT Support Team will reply to Head Office Manager by email and, if applicable, provide the username and password for a new user.

Amendment of accounts

4.8. The IT Permissions Form must be used to advise the IT Support Team of employees who have changed:

- Job role.
- Job location.
- Responsibilities within their current role

And should include the following:

- Name.
- Staff member.
- Date of change.
- Change of responsibilities.
- Locations of work.
- Drive access.
- Email distribution groups.
- Administrator permissions or access to cloud services.
- Access to applications.
- Other requests.

4.9. When amending accounts, the whole of the IT Permission Form must be completed, and the IT Support Team should not be asked to just add or delete access to certain folders or email groups.

Deletion of accounts

4.10. The IT Permissions Form must be used to advise the IT Support Team of employees who are leaving the organisation in order for permissions to be removed and access to the organisation's server and systems removed as necessary. The following must be provided:

- Name.
- Staff member.
- Leaver notification
- Date of termination
- Date of change.
- Other requests.

4.11. Where employees are absent from work on long-term sickness absences, stress, subject to disciplinary proceedings, or on "garden leave", etc. access may be temporarily removed on the advice of the organisation's HR advisors.

5. Creation and deletion of administrator permissions

5.1. An administrator has complete and unrestricted access to create, delete, and modify files, folders, and settings on a particular computer or site. This is in contrast to other types of user accounts that have only been granted specific permissions and levels of access. An administrator account is used to make system-wide changes to the computer, such as:

- Creating or deleting user accounts on the computer.
- Creating account passwords for other users on the computer.
- Changing others' account names, pictures, passwords, and types.

5.2. Administrative rights are permissions granted by administrators to users which allow them to create, delete, and modify items, system and settings, install software or changing network settings.

5.3. Because of this, administrative privileges are not granted to all staff; after a request to become an administrator has been made, it must be approved by a Director or the CEO. Head Office Manager will hold a central record of all administrators.

6. *Cloud Computing*

6.1. Cloud services are services provided by an external supplier and made available to organisations, or individuals, on terms and conditions, which are defined by that supplier. Cloud services are provided outside the organisation's data domain and allow files to be shared and make data available over a range of computers and other mobile devices.

6.2. Cloud services provide convenient and on-demand access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services). Examples of cloud storage providers include

- Microsoft 365
- Quickbooks
- Breathe

6.3. The use of cloud services may involve risks to the confidentiality, availability and integrity of the organisation's data, in particular:

- They do not necessarily provide data protection, retention or backup.
- The cloud provider may store data outside the UK or EU and not be bound by UK / EU laws relating to the protection of personal data.
- Terms and Conditions in relation to the following will need to be checked by the organisation's IT Support Team and legal advisers:
  - Account termination and potential loss of data.
  - Provider's liability for negligence with respect to misuse, exposure, loss or damage of data.
  - Confidentiality of data with respect to provider's data mining activities and potential resale of information for advertising, user tracking and user profiling purposes.
  - Considerations about who actually owns the data and therefore has full rights over it. Some cloud providers may assert ownership of any data stored in the provider's cloud, or reserve the right to do so in future

- The financial stability / instability of cloud providers should be considered to avoid the potential of end of service with no or little notice.

6.4. These risks will be recorded on the organisation's Risk Register.

6.5. Only low risk data may be stored or processed on cloud services aimed at consumers. Medium or high risk data may only be stored or processed using business-oriented cloud services, where the requirements of this Policy have been met and risks considered and addressed.

6.6. The following requirements must be met, before a cloud service or application can be signed up to, or procured, for use with Medium or High risk data and before any data are stored or transferred:

- Risks to security, including confidentiality, integrity and availability of data, and risks to privacy have been considered and addressed.
- A Data Protection Impact Assessment (DPIA) must be carried out a service contract is entered into.
- The contract must satisfy the organisation's requirements for information guardianship, as well as its legal and contractual obligations.
- The contract must be shared with the organisation's IT Support Team and their opinion as to risk assessed.
- the organisation must retain management control of the user accounts associated with cloud service subscriptions.
- The contract must address the timely recovery of lost or damaged data.
- The contract must address they timely application of critical security updates.

Signing into Cloud Services

6.7. Staff are not permitted to sign into any of the organisation's Cloud Services using their personal accounts. Administrative accounts will be issued to staff who them and a central record will be held by Head Office Manager (see paragraph 5.3). Staff must use an organisation device to access these accounts.

Sharing responsibilities

6.8. Where there is a requirement to share information with others using a cloud storage service, it is important that individuals who enable the sharing of data do so with the following safeguards:

- Grant access only to the specific folders and files that are required to support the collaboration or information sharing. Ensure that no other folders or files are made available.
- Take care to ensure access is granted to the correct individuals.
- Inform all individuals involved in the collaboration or information sharing that they have a duty of care for the information provided and must honour all security requirements as well as privacy and confidentiality commitments.

6.9. Cloud services with insecure APIs (that is the definitions and protocols for building and integrating application software) threaten the confidentiality and integrity of information and risk the exposure of the organisation data and systems to brute force attacks, denial-of-service attacks and man-in-the-middle attacks, amongst others.

6.10. Because of these risks, individual members of staff can only use Cloud Service where approved by Head Office Manager.

6.11. All cloud computing services are to be recorded on the organisation's Cloud Computing Register.

7. Firewall security

7.1. A Firewall is a computer security device that monitors and filters information coming into and leaving an organisation's network; it is the barrier that sits between a private internal network and the public Internet designed to allow only non-threatening traffic into a computer system.

7.2. Firewalls provide protection against cyber attackers by:

- Shielding computers or networks from malicious or unnecessary network traffic.

- Preventing malicious software from accessing a computer or network via the internet.
- Blocking data from certain computer network addresses and locations, applications, or ports while allowing relevant and necessary data through.

7.3. As such, it is essential that where organisations configure Firewalls to allow access to their network by external systems, they have clear and agreed reasons for doing so and have assessed potential risks.

Installation of a new firewall or replacement of an existing firewall

7.4. Before a new firewall device is put into use the IT support team will be consulted by a senior manager to determine what external services should be allowed to pass through the firewall.

7.5. For the purpose of this section of the Policy and Procedure, a senior manager is the CEO or a Director.

7.6. The senior manager and the IT support team will determine whether a new business case is required to authorise a new externally accessible service.

7.7. If no change is required to the business case the senior manager will instruct the IT support team by email to configure the firewall device as approved by the existing business case. The IT support team will also change the default password on a new firewall device (the new password is to comprise 12 characters with a random selection of numbers, capital letters and lower case letters). Once the new firewall device is put into service the IT support team will update the records it holds about the firewall device configuration and send an email to the senior manager to confirm that the work is complete.

7.8. If a change is required to the business case:

- The senior manager in consultation with the IT support team will amend the "Externally Accessible Services Business Case" document.
- The amended Business Case will be presented to the next Board of Trustees meeting for discussion and approval. Such approval is to take the form of a minuted action point.
- When the senior manager is provided with a copy of the Board Meeting minutes and action point referencing the Business Case, they will instruct the

IT support team by email to configure the firewall device as approved by the amended business case. The IT support team will also change the default password on a new firewall device (the new password is to comprise 12 characters with a random selection of numbers, capital letters and lower case letters). Once the new firewall device is put into service the IT support team will update the records it holds about the firewall device configuration and send an email to the senior manager to confirm that the work is complete.

7.9. The following steps are to be followed to maximise firewall security:

- All firewalls and equivalent network devices are recorded on the organisation's Firewall Asset Register.
- All points of access between the internet and the organisation's network must be controlled by at least one firewall or equivalent network device.
- All points of access between different networks used within the organisation are controlled by at least one firewall or equivalent network device. These points of access are recorded on the Firewall Asset Register.
- The default administrative account password for all firewalls or equivalent network devices is changed to a password that complies with section 7.7 above.
- All the organisation owned or managed laptop and desktop computers will be configured with a host based firewall with profiles suitable for when the device is connected to both trusted and untrusted networks.
- Firewalls and equivalent network devices should limit network traffic to only that which is needed. These points of contact and associated rules should be recorded in the Firewall Asset Register.
- Firewalls and internet gateways are deployed with specific configurations defined, including a set of default rules that block all network traffic.
- Default rules that specifically allow network traffic to pass should be subject to approval by Head Office Manager and IT Support Team and listed within the business justification section of the Firewall Asset Register.
- Additional firewall rule requests should be submitted to the IT Support Team on the IT Permissions Form. Approved and implemented requests will be recorded on the Firewall Asset Register.
- Temporary rule additions should be removed within 7 days of the supplied end date.
- Vulnerable services should be blocked (denied) by default on all firewalls and equivalent network devices unless approved by the Director of Business and IT Support Team. Approved use of these services should be recorded on the Firewall Asset Register.

7.10. All firewalls and equivalent network devices are reviewed monthly by the IT Support Team to ensure that the configuration is accurate and that rules that are no longer required are either disabled or removed.

8. Access for remote users

8.1. Members of staff may need to access the organisation's IT resources when not on site:

- Regularly as part of their job role in the case of Head Office Manager
- Occasionally in the case of Managers / Directors who need to work from home in order to complete specific pieces of work.

8.2. In all cases, access will be limited to the organisation devices – ***staff are not permitted to access the organisation's IT resources on their personal devices, unless agreed by*** Head Office Manager .

8.3. Secure remote access shall be strictly controlled.

8.4. Secure remote access will be strictly controlled with encryption through our Virtual Private Networks (VPNs) and strong passwords or pass-phrases.

8.5. All members of staff granted remote access to the organisation's IT resources shall protect their login and password, even from family members and people they live with.

8.6. While using computers to remotely connect to the organisation's network, staff must ensure that the remote host is not connected to any other network at the same time.

8.7. Use of external resources to conduct the organisation business must be approved in advance.

8.8. All devices (including personal devices where permission has been agreed) that are connected to the organisation's internal networks through remote access technologies must use the most up-to-date anti-virus software.

8.9. Personal equipment used to connect to our networks must be approved, meeting the same requirements of the organisation's owned equipment for remote access.

8.10. Staff shall contact the IT Support Team for approved methods and software to remotely connect to the organisation's IT resources

- Staff accessing systems remotely using a personal device are responsible for ensuring their mobile device is compliant with this and other applicable organisation policies.
- Staff must make the organisation devices assigned to them available for periodic inspection when asked, to ensure the device is up to date with all applicable security patches and virus / malware protection software.
- Members of staff with remote access privileges shall ensure that their remote access connection is used explicitly for work business and used in a manner consistent with their on-site connection to the organisation's network.
- The IT Support Team will determine the appropriate access methodology and hardening technologies, including two factor password authentication, smart card, or PKI technology with strong passphrases.
- All user passwords shall be strong and follow guidelines and procedures in the *Passwords and Work Station Security* section of the Staff Handbook
- Staff shall ensure that devices used for work purposes are not shared in a multi-user capacity, violate the organisation conditions, or used in any inappropriate activity.
- Staff shall bear full responsibility for any access misuse.
- Staff with remote access privileges shall ensure their remotely connected workstation, does not bridge or share another private or public internet connection.
- Personal equipment shall not be used to connect to the organisation IT resources using remote connection software and exceptions require **written approval from the Head Office Manager**

9. Addition and removal of approved applications

9.1. the organisation provides the following Core Microsoft Apps as standard:

- Edge
- Excel
- Microsoft Office
- Outlook
- PowerPoint

- Word

and the following for specific job roles:

- Microsoft 365
- Microsoft Access
- SharePoint

9.2. In addition, the organisation agrees to certain staff having access to a number of other applications to support its work.

9.3. While making sure that staff can be productive, it is essential that the organisation is protected against data loss, intentional and unintentional. In addition, it is important to protect the organisation's data that is accessed from sites that are not managed by the organisation as staff can use their mobile devices for both personal and work tasks (e.g. logging onto Twitter or Instagram to promote the work of the organisation).

9.4. Where an application requires IT Support to reconfigure the organisation device to allow access, the IT Permissions Form must be used to request agreement. Similarly, if the application is no longer required (change in job role or responsibilities), the Form must be used for it to be removed and the central record updated.

10. Actions to be taken in the event of systems (password) compromise

Individuals

10.1. All new members of staff, Bank Workers and volunteers who are given permission to access the organisation's IT resources are issued with a centrally-set password on joining the organisation. They are then forced to create a new password at first login.

10.2. ***This must be changed when / if prompted and also upon known or suspected compromise***.

Administrators

10.3. The account password related to:

- Individual user accounts

- Administrators (for cloud services, firewall and any other IT service)

must be changed upon known or suspected compromise. This could be as a result of employee movers and leavers; employees advising that they think their password has been guessed or their account hacked; malware infection or if advised to do so by the manufacturer, or the IT Support Team.

10.4. In every case, the individual should change their password immediately, in line with the Passwords and Work Station Security section of the organisation's Staff Handbook, and the IT Support Team contacted immediately, if relevant.

Firewall

10.5. The IT support team will change the default password on any new firewall device and once it is put into service they will update the records it holds about the firewall device configuration and send an email to the senior manager to confirm that the work is complete.

Applications

10.6. Any member of staff who is advised that the password used to access any external application has been or is suspected of compromise, must change it immediately and contact all other staff who are known to use the application for work purposes.

11. Monitoring user access

11.1. Systems will be capable of logging events that have a relevance to potential breaches of security.

11.2. User access may be subject to checks by Head Office Manager and the IT Support Team.

12. Related Policy and Procedure

12.1. Due to the number of areas covered and impacted by IT, staff are also directed to read the following policy and procedure;

- ICT Policy
- Staff Mobile Devices - Acceptable Use and Protection
- Introduction to GDPR

- Data Protection Access Policy
- Data Protection Impact Assessment Procedure

……