1 Introduction

The creation of new user accounts and the ongoing management of system access are fundamental to the provision of effective information security. This process describes how user accounts and access rights should be requested, approved, created, amended, reviewed and removed in a secure way which complies with [Organization Name] policies.

This control applies to all systems, people and processes that constitute the organisation's information systems, including board members, directors, employees, suppliers and other third parties who have access to [Organization Name] systems.

The following policies and procedures are relevant to this document:

- *Access Control Policy*
- *Mobile Device Policy*
- *Password Policy*

User Access Management Process

2 User registration

2.1 Registration process

The process of user registration is shown in the diagram below:

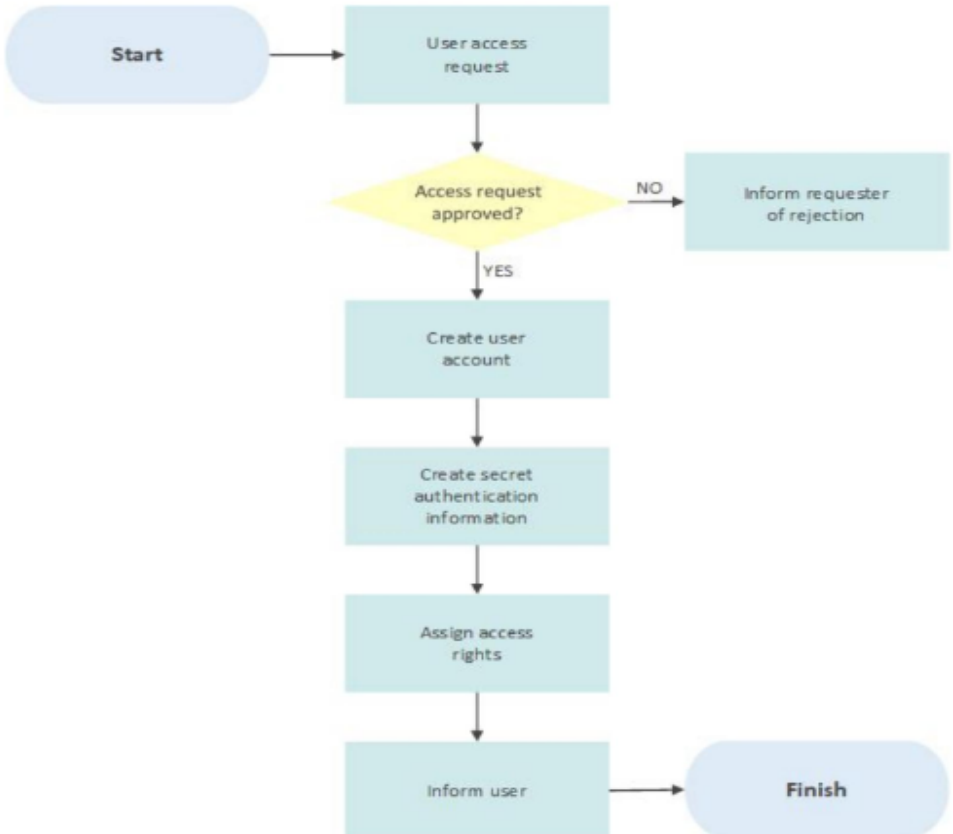

Figure 1: User registration process

This process is described in more detail in the remainder of this section.

[Organization Name] maintains and supports a wide variety of IT systems, and the level of access required by individuals to these systems in order to perform their job role will vary widely across the organisation. Although the specifics of how user accounts are created will also vary across systems, the following basic process should always be followed.

2.2 Requesting access

Access to IT systems should be requested via the [IT Service Desk]. Where online or electronic forms are available for specific systems, these should be used. In addition to system-specific details, the following should always be given:

- Name
- Role
- Department
- Contact Details
- Name of line manager
- Start date (and end date if applicable)

For each system to which access is requested, further information may be required, such as:

- Name of an existing user whose access should be duplicated (if new user is performing the same or similar role)
- Modules required
- Payroll or employee number

Where possible, requests for access should be pre-approved by the system owner or line manager before being submitted to the [IT Service Desk] via the approver's email address.

2.3 Access approval or rejection

All requests for access to a specific system must be approved by the system owner. This will normally be a manager within the organisation with specific responsibility for the security and use of that system. In some circumstances, the system owner may delegate authority to approve requests to the employee's line manager, but this fact must be recorded and verified on a regular basis.

No user accounts should be created without the required approval having been given. In the event that approval is refused, the [IT Service Desk] will inform the submitter of the request, together with any reason given. It is up to the requester to discuss the rejection directly with the system owner if required.

2.4 User account creation

Once an approved request with sufficient details has been received, the [IT Service Desk] will manage the creation of the user account. User accounts should be created in line with the standards established and documented for that specific system. These will detail parameters such as account name format, initial program calls, assigned printers etc.

2.5 Allocation of secret authentication information

If passwordless authentication is not being used, the [IT Service Desk] will set an initial password. This will be a strong password according to published guidelines. A random password generation tool may be used if available. The password will be set to expire upon first logon, at which point the user will define a new one which is known only to them.

If additional authentication tools are to be used (such as a multi-factor authentication method) or passwordless authentication is available, the appropriate procedure for the setup of these items should be followed.

2.6 User access rights assignment

Once the user account has been created, access rights may be assigned to the account. For most systems, this will be achieved by placing the user account in a specific group or role that is specified on the approved request.

2.7 Informing the user

Upon successful completion of account setup the [IT Service Desk] will inform the user of the account name via email along with instructions regarding how to set a strong password when changing the initial one set by the [IT Service Desk] (if appropriate). The initial password should be communicated by telephone (or other secure method) directly to the user after verifying the user's identity. If the user is not available, a message should be left for them to contact the [IT Service Desk]. The password should not be left as a message.

If a physical method of multi-factor (passwordless) authentication is also required (as opposed to using an app), this will be sent to the user by internal or external post. For external mail, a recorded delivery service should be used. Correct receipt of the token should be confirmed with the user by the [IT Service Desk] before communicating the initial password (unless passwordless authentication is to be used).

3 User access adjustment

From time to time, there is a need to amend user access rights, often as a result of role changes or promotions. This adjustment must be carried out in a secure manner to ensure that the principles set out in the *Access Control Policy* are maintained.

3.1 Access adjustment process

The process for user access adjustment is shown below:

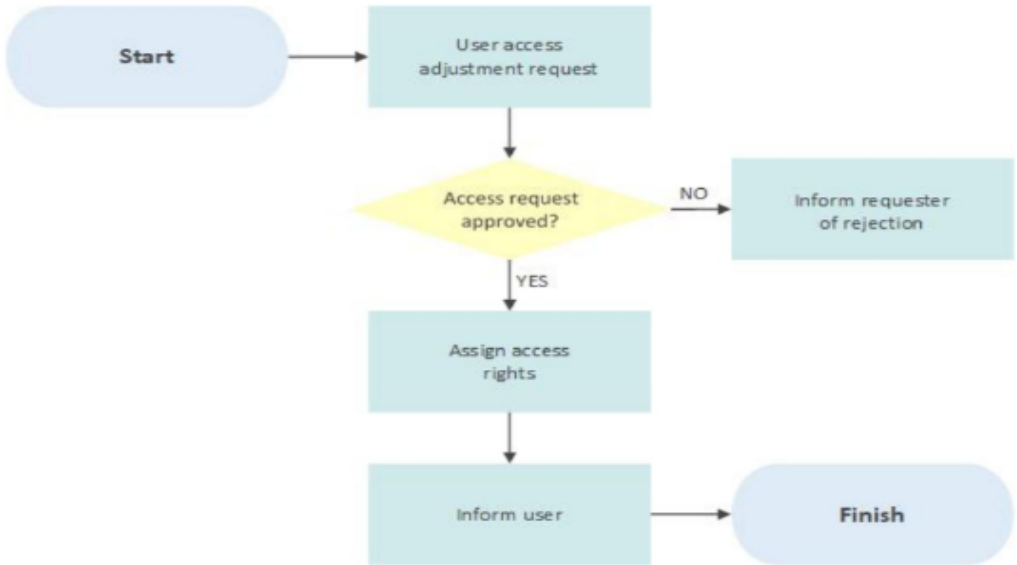

Figure 2: Access adjustment process

3.2 User access adjustment request

Requests for adjustments to user access to IT systems should be sent to the [IT Service Desk]. Where online or electronic forms are available for specific systems, these should be used. In addition to system-specific details, the following should always be given:

- Name
- Role
- Department
- Contact details
- Name of line manager
- Date adjustment required from

If any of the above items of information are changing (such as a move of role or department) then both old and new details should be given.

For each system to which access is requested to be amended, further information may be required, such as:

- Name of an existing user whose access should be duplicated (if amended user will be performing the same or similar role)
- Modules required
- Payroll or employee number

Where possible, requests for adjustments to access rights should be pre-approved by the system owner or line manager before being submitted to the [IT Service Desk] from the approver's email address.

3.3 Access approval or rejection

All requests for adjustments to access rights to a specific system must be approved by the system owner. This will normally be a manager within the organisation with specific responsibility for the security and use of that system. In some circumstances the system owner may delegate authority to approve requests to the employee's line manager, but this fact must be recorded and verified on a regular basis.

No access rights should be amended without the required approval having been given. In the event that approval is refused, the [IT Service Desk] will inform the submitter of the request, together with any reason given. It is up to the requester to discuss the rejection directly with the system owner if required.

3.4 Adjust access rights

Once the request has been approved, the request should be allocated to a member of the [IT Service Desk] team to assign the amended access rights to the account. For most systems, this will be achieved by placing the user account in a different group or role as specified on the approved request.

3.5 Informing the user

Upon successful completion of the adjustment request the [IT Service Desk] will inform the user via email.

If a physical method of multi-factor (or passwordless) authentication is also required (as opposed to using an app), this will be sent to the user by internal or external post. For external mail, a recorded delivery service should be used. Correct receipt of the token should be confirmed with the user by the [IT Service Desk] before communicating the initial password (unless passwordless authentication is to be used).

4 User deregistration

When an employee or contractor leaves the organisation, it is vital that access controls are updated promptly to avoid a situation where an unauthorised person retains access to our systems.

4.1 Deregistration process

This will be achieved using the process below:

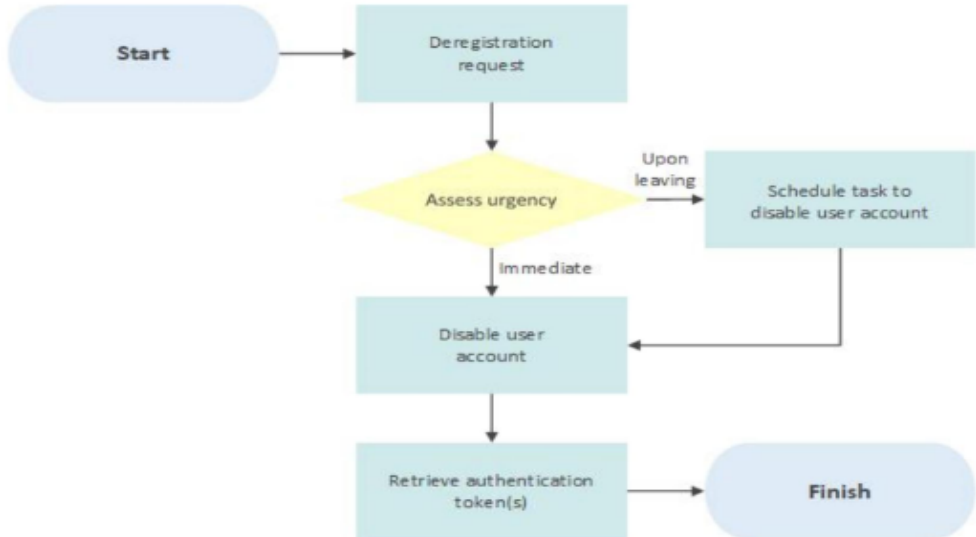

Figure 3: User deregistration process

4.2 Deregistration request

It is the responsibility of users and their managers to inform the [IT Service Desk] in a timely manner when employees leave the organisation and so no longer need access to IT systems. As much advance notice as possible should be given. In those circumstances where an employee has been involuntarily terminated at short notice, the [IT Service Desk] must be informed by telephone immediately.

4.3 Assess urgency

The [IT Service Desk] will assess the urgency of the deregistration request based on the information provided and will decide whether to disable the user account straight away or to wait until the user leaves the organisation. In general, for unfriendly terminations, deregistration will be completed immediately whereas, for voluntary resignations, it will be done on the day the person leaves.

4.4 Disable user account

For most systems, the [IT Service Desk] will take the initial step of disabling the user account rather than deleting it. This will prevent access by the user but will retain all information associated with the account and its data.

At a later date and with the system owner's permission, the account may be deleted once any outstanding issues have been resolved.

All user accounts associated with the user in question should be disabled even if Single Sign On (SSO) is in place, for example if the user is in Finance, access to Entra ID and the Finance system (and any other systems the user has an account on) should be disabled. This is necessary to prevent the account being used by someone who still has access to the network in future. Accounts should be disabled in order of importance, such as the Finance system account before an email account.

4.5 Retrieve authentication token

If the deregistered user has any access-related hardware, such as an authentication token, this should be retrieved as part of the termination process and returned to the [IT Service Desk].

5 Management of privileged access rights

Privileged access rights are those that involve a higher level of system access than a typical user. This includes "root" or "domain administrator" access and various types of supervisory access within application systems and databases.

The process for managing privileged access rights is basically the same as for other types of users but the approval and review aspects should be treated much more rigorously. The number of people with such rights should be carefully controlled, and rights should be removed as soon as they are no longer required.

The following factors should be considered by the system owner as part of the approval criteria for such requests:

- Why does the user need privileged access rights?
- Is there an alternative way to achieve the desired end result without granting privileged access rights?
- Does the user have the necessary training and expertise to avoid mistakes when using the privileged access rights?
- For how long are the rights needed?

A user who requires privileged access rights such as domain admin should request that a separate user account be created with these rights (for example "John Smith Admin"). Under no circumstances should the password for the default admin user account be issued. If the need for access is temporary, an expiry date should be set on the user account when it is created.

When creating such accounts, it should be emphasised to the user that they are only for use when a higher level of permissions is needed. Their normal, lower access level, account should be used most of the time.

The need for accounts to hold privileged access rights will be reviewed according to the standard review process but may be performed on a more frequent basis depending on the sensitivity of the system(s) involved.

6 Access reviews

To ensure that access to IT systems is only available to authorised personnel, the [IT Department] will carry out a user access review every six months.

6.1 Access review process

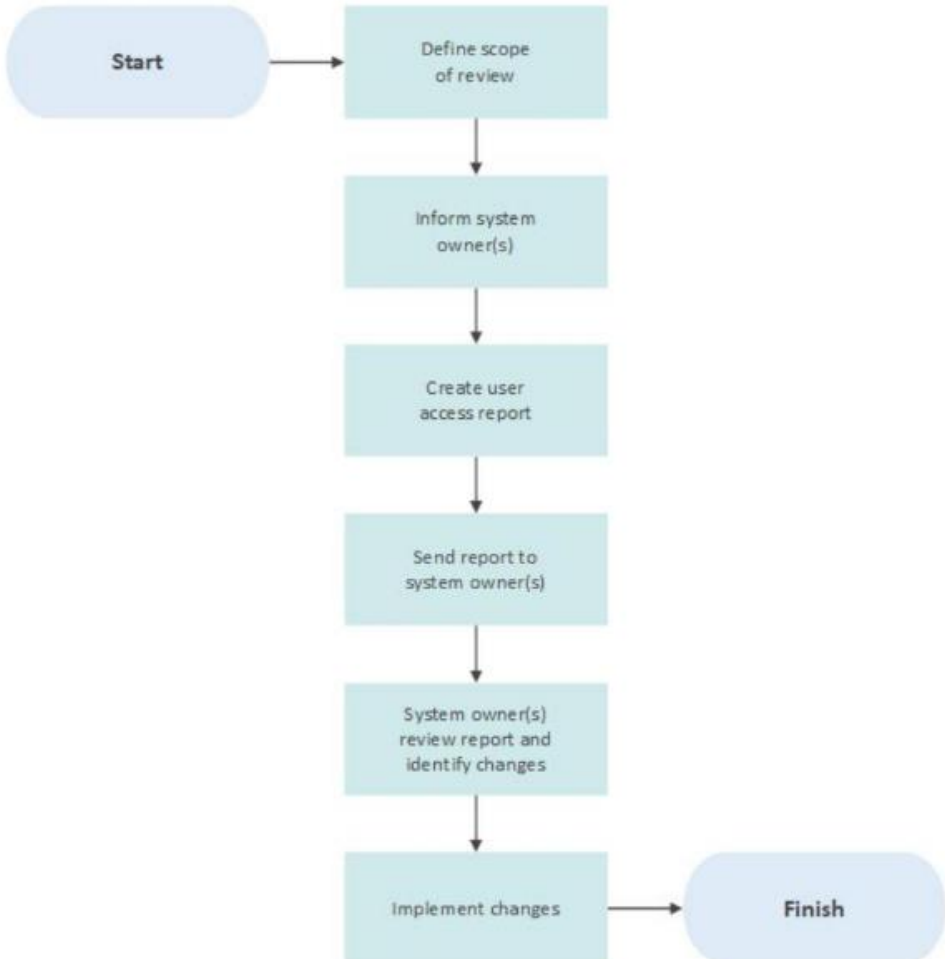

Figure 4: Access review process

The scope of the review should be defined in terms of the systems and networks that will be covered.

The owners of the systems and networks to be reviewed should be informed of the intention to carry out a review so that adequate time can be allocated to complete it within the target timescale.

The [IT Department] will create a listing all authorised users of each system together with their current level of access. This should, as a minimum, state the following information:

- Name of system
- Username
- User role title
- User department
- User account name
- Date of user account creation
- User role(s) assigned
- Additional access rights assigned
- Are privileged access rights assigned to this account?

Where appropriate, supporting information such as the specific permissions associated with each role defined in the system should also be provided.

The report should be produced in electronic form (either spreadsheet or text document) and securely emailed to the system owner.

The list will be reviewed by the system owner, and any accounts that should not be maintained will be identified.

System owners will look to identify:

- People who should not have access (for example leavers)
- User accounts with more access than required by the role
- User accounts with incorrect role allocations
- User accounts that do not provide adequate identification, such as generic or shared accounts
- Any other issues that do not comply with the organisation's access control policy

A list of issues identified should be compiled by the system owner and sent to the [Information Security Manager]. Any issues that appear to be urgent should be flagged as such without delay so that prompt action may be taken.

Actions identified from the review should be prioritised and carried out according to their urgency.