NetGain systems	No of Pages	**1** of **7**
	Document Classification:	Internal
	Effective Date	1 Aug 2025
ACCESS CONTROL	Doc No	ISMS-ORG-07
	Revision	1.0

AMENDMENTS LOG

Revision History

Version	Revision Author	Reviewer / Approver	Date	Summary of Changes
1.0	Nor Asfiah Binte Jamalludin (ISMS MR)	James Chia (CEO)	1 Aug 2025	Initial Release

TABLE OF CONTENTS

PURPOSE

The creation of user accounts and the on-going management of system access are fundamental to the provision of effective information security controls. This process describes how accounts and access rights are requested, approved, created, amended, reviewed and removed in a secure way which complies with the organisation's *Access Control Policy*.

SCOPE

This control applies to all systems and processes that constitute the organization's information assets, including the people who have access to the information.

REFERENCE

ISO/IEC 27001 Standard	Annex A 5.15 Access control Annex A 5.16 Identity management Annex A 5.17 Authentication information Annex A 5.18 Access rights

RESPONSIBILITIES & AUTHORITIES

Top Management has the prime responsibility and approval authority for this control.

Asset owners shall ensure segregation of duties in account creation and access rights assignment and make sure that regular checks are carried out to identify any areas for further investigation.

PROCEDURE

1 User Registration

This process must be followed for all user creations. The organisation maintains a variety of systems, and the level of access required by individuals to these systems in order to perform their job role will vary widely across the organization. Although the specifics of how users are created will also vary across systems, the following over-arching principles will be followed:

- Need-to-know: a user is only given access to the information which is required in order to perform his/her tasks
- Need-to-use: a user is only assigned access to information technology infrastructure where a clear need is present

1.1 Requesting Access

User registration and role-based access to will be requested from the designated System Admin upon joining date as per the notification from HR. No user accounts should be created without notification from HR of any new joiner or with no documented request with approval from designated Department Head.

Once joining date has been notified or approved request with sufficient details has been received, the respective System Admin will manage the creation of the user account. Account creation details and the System Admin creating the user account must be traceable in the log.

1.2 Identity Management

In the context of identity management, the creation of a user account should ensure that:

- For identities assigned to persons, a specific identity (User ID) is only linked to a single person to be able to hold the person accountable for actions performed with this specific identity.
- Identities assigned to multiple persons (shared identities) are only permitted where they are necessary for business or operational reasons and are subject to dedicated top management approval.
- Identities assigned to non-human entities (if applicable) are subject to appropriately segregated approval and independent ongoing oversight.
- Identities are disabled or removed in a timely fashion if they are no longer required.
- Records of all significant events concerning the use and management of user identities and of authentication information are kept.

1.3 User Access Rights Assignment

Once the user account has been created, the access rights shall be assigned by the System Admin to the account according to the role and in line with the approval given by the authorized approver.

For file-level access to department folders, it is the department head responsibility to assign the specific rights (“Read”, “Write”, “Read/Write”).

1.4 Allocation of Secret Authentication Information

An initial password will be given for a new user account by the System Admin, and the new user shall be prompt of the steps to set up a new password. The password will be set to expire upon first logon at which point, the user will define a new password which is known only to them and which meets the parameters defined for that system in line with the organisation’s *Password Policy.*

Additional authentication tools are to be set-up such as a two-factor authentication (2FA) by the user as enabled in the system. Users shall be responsible to keep their authentication information safe and confidential in line with the organisation’s *Password Policy.*

Records of significant events concerning the allocation and management of authentication information are kept.

2 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.

2.1 User Access Adjustment Request

Requests for adjustments to user access should be sent to the System Admin via email upon approval of the designated Department Head or the System Owner.

No access rights should be amended without the required approval having been given.

2.2 Adjust Access Rights

Once the request has been approved, the System Admin shall assign the amended access rights to the account and inform the requestor once done.

3 User Deregistration

When a user leaves the organization or there is a need to disable a user account, it is vital that access controls are updated promptly to avoid a situation where an unauthorised person retains access to our systems.

3.1 Deregistration Request

It is the responsibility of HR to inform the System Admin in a timely manner when an employee is about to leave the organization and so no longer need access to systems after their last day. As much advance notice as possible should be given preferably not later than 1 week. In those circumstances where an employee has been involuntarily terminated at short notice, the System Admin must be informed immediately of the decision within the day.

3.2 Disable and Delete User Account

For most systems, the System Admin will take the initial step of disabling the user account rather than deleting it within 1 working day from the last day of the resigning employee. For unfriendly terminations, the user account will be disabled on the same day the System Admin has been informed. Disabling the user account will prevent access by the user but will retain all of the information associated with the account and its data.

One (1) month after disabling the account, the System Admin shall delete the account. The department head may request to extend this date for any outstanding issues that have yet to be resolved with confirmation on the date it can be deleted by the System Admin.

4 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?
- How long are the rights needed for?
- Is a documented agreement such as a Non-Disclosure Agreement required (e.g., for third parties)?

A separate user account may be considered for a user who requires privileged access rights such as domain admin. Under no circumstances should the password for the default admin user account be issued. If the need for access is temporary then an expiry date should be set on the user account when it is created.

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

Similarly, the use of utility programs that can be capable of overriding system and application controls (e.g., diagnostics, patching, antivirus, backup, network tools) should be restricted and tightly controlled. The following guidelines will be considered:

- Removing or disabling all unnecessary utility programs
- Limitation of the use of the utility programs to the minimum practical number of trusted, authorised users
- Authorisation for ad hoc use of utility programs
- Limitation of the availability of utility programs (e.g., for the duration of an authorised use)
- Logging of all use of utility programs

5 Access Reviews

In order to ensure that access is only available to authorised personnel, user access privileges shall be reviewed every six months and if there are significant changes in the organisation’s structure or workforce.

The review will aim to identify:

- People who should not have access (e.g., 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 e.g., generic or shared accounts
- User accounts that are inactive for 60 days or more
- Any other issues that do not comply with the organisation's *Access Control Policy*

A list of issues should be compiled by the responsible teams. Any issues that appear to be urgent should be flagged to the System Owner and System Admin without delay so that prompt action may be taken.

Actions identified from the review should be prioritised and carried out according to their urgency. Non urgent issues may be added to the continual improvement plan as part of a wider programme of improvement. Proof of review and record of all actions taken shall be maintained.

6 Systems and Services that Process Personal Data

The following shall be ensured for systems and services that process personal data:

- Any de-activated or expired user IDs for systems and services that process personal data cannot be re-issued to another user.
- An accurate, up-to-date record of the user profiles created for users who have been authorized access to the information system and the personal data contained therein shall be maintained. This profile comprises the set of data about that user, including user ID, necessary to implement the identified technical controls providing authorized access.
- Systems shall be configured to identify who accessed personal data and what additions, deletions or changes they made.

7 Incident Management

Where user access control is found to be compromised, such as corruption or compromise of passwords or other user registration data (as a result of inadvertent disclosure), this shall be investigated as an incident in line with *ISMS-ORG-10 Information Security Event & Incident Management.*

FORM

ISMS-ORG-07-F1	Access List & Rights Review