Access Management Procedure

Document ID	**AMP V1.0.1**
Effective Date	**2023-04-01**

Table of Contents

1 Purpose and Applicability

1.1 The Access Management Procedure (AMP) outlines the essential requirements in access management-related processes within the institution.

1.2 The standards and best practices defined within this AMP apply to all units of the institution and are not intended to replace or override any regulatory requirements.

1.3 This AMP will be reviewed on an annual basis or when significant changes occur in regulations, business models, or technologies.

2 Related Policies, Guidelines, Procedures, and Applicable Laws

2.1 This AMP should be reviewed in conjunction with policies and procedures issued by both the organization and the relevant regulatory bodies, which include, but are not limited to, the following:

a. Bank Negara Malaysia (BNM) Policy Document on Risk Management in Technology (RMiT)
b. Circulations, notices, and memos issued by BNM
c. Information Risk Management Policy
d. Information Operations Management Procedure
e. Information Security Management Procedure
f. Payments Network Malaysia Sdn Bhd. (“PayNet”) Guidelines on Cyber Resilience for Participants of PayNet’s Services
g. BNM Guidelines on Cyber Resilience for Participants of RENTAS and FAST
h. BNM Policy Document on Business Continuity Management
i. BNM Notification on Disaster Recovery Readiness for Critical Systems and Services.

3 Glossary of Key Terms

The following are the definition of key terms in this AMP:

Resource Access Management (RAM) is a service that enables systematic management of user authentication and authorisation within an organization. RAM helps streamlining the management of resources within the institution, enabling centralised management of access while maintaining account-level autonomy

Privileged access refers to the elevated or special permissions granted to specific users or systems that allow them to perform actions or access sensitive resources beyond what standard users can. This often includes administrative capabilities such as managing systems, networks, and security settings, as well as accessing confidential information or performing tasks critical to the infrastructure.

Privileged Access Management (PAM) is a security system that controls and monitors access to sensitive systems and data by users with special, high-level permissions (like administrators). PAM ensures that only authorized users can access critical resources, limits what they can do, and tracks their actions to prevent misuse and protect against security threats.

4 Roles and Responsibilities

Role	Responsibilities
Workspace Technology Engineer; RAM Administrator	• Manage and administrate user access throughout the entire user access lifecycle
PAM Administrator	• Manage and administrate privileged user access throughout the entire user access lifecycle
Functional Unit Head	• Review the completeness of each non-privileged user access requests initiated by its unit • Approve non-privileged user access requests
Department Head	• Review the completeness of each privileged user access requested by its department • Approve privileged user access requests • Review and assess the completeness and appropriate of the user access matrices from each system owner • Review and approve user access review reports
Human Resource	• Prepare and submit user access requests for each staff onboarding and offboarding
System Owner	• Prepare and maintain user access matrix for the respective system • Conduct periodic review of user access on the respective system
Cybersecurity Engineering	• Review and assess the completeness and appropriate of the user access matrices from each system owner
Chief Technology Officer	• Review and approve user access review reports

5 Access Management Overview

5.1 The AMP provides guidelines on the access management process and life cycle: from access provisioning, access maintenance, access deactivation, reactivation, and access deletion within the institution's environment.

5.2 All access within the institution will be evaluated based on the need-to-know principle

5.3 All requests for new access or modification to existing access must be explicitly authorised by the designated authority as illustrated by the diagram below.

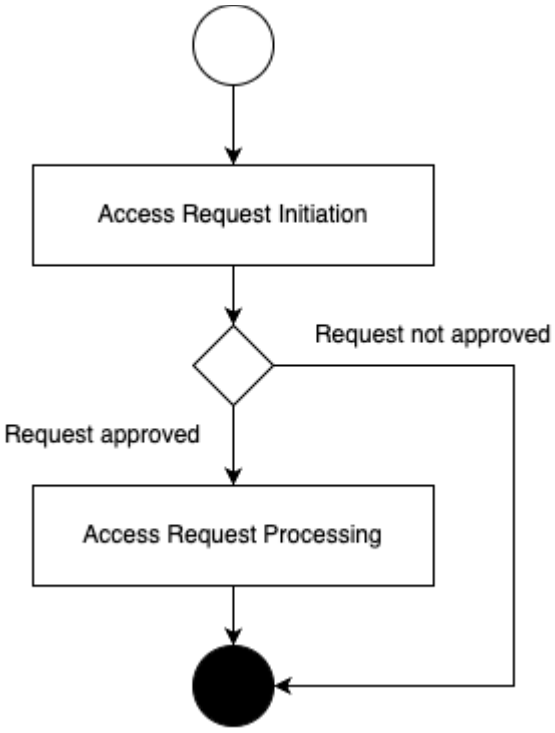

Diagram 1: Access Management Process

6 Mandatory User Access Review

6.1 At least once every 12 months, all system owners are required to conduct a user access review on the respective systems under their ownership. The user access review should cover the following scope:

a. Review the user access matrix and ensure the information is accurate and up-to-date

b. Review the current user access against the user access matrix and ensure the user access is still relevant and accurate for every user

   i. Identify and document all new users that have been added to the system since the last review

   ii. Identify and document all users to be removed from the system

   iii. Identify system configurations and ensure access settings are in accordance with the user access matrix

   iv. Identify and document all access violations along with the recommended remediations

6.2 A user access review report should be prepared and submitted to both the Department Head(s) and the Chief Technology Officer for approval

6.3 Disciplinary actions may be taken for system owners who fail to conduct and submit a proper user access review according to the requirements of this document

7 Access Provisioning Workflow

7.1 Non-privileged User Account

The process for provisioning a non-privileged user account is described below:

1. **Access Request Initiation**
    a. Preparation and submission of the onboarding form by HR, which serves as the request for new user access initiation
    b. New user access request must capture, at minimum, the following information:
        1. Employee ID
        2. Employee Email
        3. Employee Name
        4. Employee Designation
        5. Department
        6. Start Date
        7. Reporting Manager
2. Access Request Approval
    a. New user access request submitted by HR to be approved by the HR functional unit head
    b. The approver to review and ensure both completeness and accurateness of the information captured within the user access request
3. Account Provisioning
    a. Once approved, a non-privileged user account will be created with the following details:
        1. A unique user ID following the adopted naming convention.
        2. Temporary password following the organization's password policy
        3. Access grants according to the user access matrix
4. Account Handover
    a. The new account details will be communicated to the requester through a secure channel
    b. The receiver must provide an acknowledgement on the information received
    c. Upon first login:
        1. User is required to change password and set a new password according to the organization's password policy
        2. User is required to enable and configure multi-factor authentication (MFA)
5. Continuous Monitoring
    a. All user accounts and access will be regularly monitored and reviewed
    b. A user access review, as described in Section 6, must be conducted by the respective system owners

7.2 Privileged User Account

The process for provisioning a privileged user account is described below:

1. Access Request Initiation
    a. A privileged user access must be requested through the service desk
    b. New privileged user access request must capture, at minimum, the following information
        i. Employee ID
        ii. Employee Email
        iii. Target System
        iv. Access Time Range
        v. Justification
2. Access Request Approval
    a. New privileged user access request must be approved by both the functional and department heads
    b. The approver to review and ensure both completeness and accurateness of the information captured within the privileged user access request
3. Account Provisioning
    a. Once approved, a privileged user account will be created with the following details:
        i. A unique user ID following the adopted naming convention
        ii. Temporary password following the organization's password policy
        iii. Access grants according to the user access matrix
        iv. Time-bound access
4. Account Handover
    a. The new account details will be communicated to the requester through a secure channel
    b. The receiver must provide an acknowledgement on the information received
    c. Upon first login:
        i. User is required to change password and set a new password according to the organization's password policy
        ii. User is required to enable and configure multi-factor authentication (MFA)
5. Continuous Monitoring
    a. All user accounts and access will be regularly monitored and reviewed
    b. A user access review, as described in Section 6, must be conducted by the respective system owners

7.3 Access Modification

a. All modifications to existing user access must be requested through the service desk
b. Access modification requests must be approved by the functional unit head of the requester's unit
c. Once approved, the user access will be modified according to the approved access modification request
d. Requester will be notified through a secure channel when the access modification is completed
e. The modified user access will remain to be subjected to the continuous monitoring described in Section 7.1.5

7.4 Access Termination

a. All access termination must be requested through the service desk
b. Access termination requests must be approved by the functional unit head of the requester's unit
c. Once approved, the user access will be removed on the effective date specified in the approved access termination request
d. Requester will be notified through a secure channel when the access termination is completed