**PIM model template**

# Purpose

This document provides guidance on managing Microsoft 365 tenants for <company name>. It should be reviewed every 6 months and follows the principle of least privilege to ensure governance.

**Privileged Identity Management (PIM)** helps manage, control, and monitor access to critical resources in Azure AD, Azure, and other Microsoft Online Services like Microsoft Office 365. PIM offers just-in-time (JIT) and just-enough access (JEA) to minimize the number of users with administrative privileges, reducing the risk of:

* Malicious actors gaining access.
* Authorized users inadvertently impacting sensitive resources.

PIM also enables auditing of administrative activities to mitigate risks of excessive, unnecessary, or misused access rights. Each tenant includes an emergency "BreakGlass" account for emergency access only.

**Audience**

This document is intended for System Administrators who need elevated privileges in Microsoft 365 tenants for daily maintenance. Regular users of Microsoft 365 services do not require access to PIM or related information.

# Privileged Identity Management (PIM) Model

Azure PIM in the Azure portal offers time-based and approval-based role activation to minimize privilege exposure and enhance visibility, reducing risks of excessive or misused access. The PIM model allows specific actions within defined scopes.

**Key features of PIM:**

* Just-in-time privileged access to Azure AD and Azure resources.
* Eligibility assignment for privileged access group membership or ownership.
* Time-bound access with start and end dates.
* Approval requirement for activating privileged roles.
* Multi-factor authentication enforcement for role activation.
* Justification for role activation.
* Notifications for privileged role activations.
* Access reviews to confirm ongoing role necessity.
* Audit history downloads for internal or external audits.

**PIM PRINCIPLES**

There are 3 main principles of PIM. These principles are mapped back ISO 27002:2022 controls to demonstrate how the implementation will adhere to Security and Compliance requirements.

|  |  |
| --- | --- |
| Principles | ISO 27002:2022 |
| Controlling Logical Access Privileges and Implementing Least Privilege Access | B.5.15 – Business requirement of access control  B.5.15 – Access to networks and network services  B.5.18 – User access provisioning  B.8.2 – Management of privileged access rights  B.8.3 – Information access restriction |
| Enforcing Separation of Duties | B.5.3 – Segregation of duties |
| Access Logging / Monitoring / Auditing | B.8.15 – Event logging  B.8.15 – Administrator and operator logs |

# Privileged Accounts – Configuration

All accounts created for PIM need to adhere to the following:

* **Admin Accounts:** Must be cloud-only and follow this naming convention
  + Staff: FirstName.LastName.Admin@[tenant].onmicrosoft.com
  + Vendors: Company.FirstName.LastName.Admin@[tenant].onmicrosoft.com
* **Conditional Access Policy:** All admin accounts must be members of the conditional access policy group (e.g., "MFA REQUIRED ADMINS CONDITIONAL").
* **No Shared Accounts:** Each account must be owned by an individual with Multi-Factor Authentication (MFA) enabled and registered before roles are added.
* **Self-Service Password Reset (SSPR):** Must be enabled and registered before roles are added.
* **Service Accounts:** Must never have global administrator rights, with exceptions approved by the <IT Senior Leadership Team/CIO/CISO>. Service accounts must have passwords of at least 30 characters.
* **Auditing:** All administrative actions will be audited with indefinite log retention.
* **Vendor Accounts:** Must have expiry dates and only be granted eligible roles necessary for their tasks. Accounts must be disabled when the vendor's engagement ends, with notice given to the <Security/governance team> by the responsible manager.
* **Manual Audits:** Conducted monthly or quarterly to ensure appropriate access levels and remove stale accounts (inactive after X days). Reports will be presented to PIM managers and the <IT Senior Leadership Team/CIO/CISO>.
* **Automated Auditing:** Requires PIM approvers to review assignments in the Azure portal.
* **Account Removal:** IT Managers must report accounts needing removal to the <Security/governance team> immediately when staff leave their position (movers or leavers).
* **BreakGlass Accounts:** Tested yearly, with updated phone numbers for <IT Senior Leadership Team/CIO/CISO> & <Security/governance team>.

# PIM Roles

Certain roles must be limited to specific teams. For example, the Global Administrator role should be restricted to no more than 5 users, including the BreakGlass account.

In emergencies or MFA failures, the BreakGlass account, owned by the <CIO/CISO>, will be activated and used only in emergencies.

**General Rules**

Not all roles are equal, some higher privileges must be restricted.

* **Global Administrator:** Maximum of 4 eligible users, with the BreakGlass account as the only active user. As recommended by Microsoft (Secure score metric).
* **Privilege Role Administrator:** Limited to the <Security/Governance team>.
* **Security Administrator:** Most security roles, except Security Reader, should be restricted to the <Security/Governance team>.
* **Restricting Role available:** Only commonly used roles can be requested via the <your ticketing system>. Other roles require prior discussion with the <Security/Governance team> manager.
* **Use of Administrative Units:** to restrict access to different types of accounts rather than applying the role to the entire tenant. E.g. Student administration service desk can only change Student passwords by using a “students” unit. This restricts “password admins” to Students and not all accounts in the tenant. Administrative Units use the same filter rules like Dynamic groups, so careful planning is required.

**Other Roles**

Azure AD Privileged Identity Management (PIM) manages privileged access policies for Azure AD users. PIM assigns users to roles as either Active or Eligible, with roles having permanent or expiry-based assignments. Eligible roles require self-approval or “PIM role approver” action for elevation, with a maximum elevation time of <insert hours here> hours (up to 24 hours).

**Role Assignments:**

1. **Eligible:** Requires actions to use the role. Users can activate the role as needed, with no difference in access between active and eligible roles. Vendors should have eligible roles during their engagement, not active roles.
   * **With Approval:** For roles accessing sensitive information, approved by responsible managers.
   * **Without Approval (Self-approving):** For roles with minimal impact or single-person responsibility.
2. **Active:** Always usable without actions, for required roles.

All roles can have a set duration, either permanent or with an expiry date. Vendors must have expiry dates for role removal. Most IT staff may have permanent roles based on responsibilities, but casual staff or vendors should have expiry dates, typically no longer than 6 months.

# Requesting a Role - Process

Defined Positions:

* **Requestor:** Assigned the role for administrative tasks.
* **Requestor’s Manager:** The requestor's supervisor.
* **PIM Role Manager:** Approves privileged roles, approves elevation.
* **<Security/Governance Team>:** Reviews and assigns roles.

**Role Request Submission:** <your ticketing system>

**Suggested Workflow:**

1. **Submission:** Requestor or Manager submits the request. If the manager's approval is missing, it will be sought.
2. **Review:** <Security/Governance team> ensures:
   * Role suitability for the team/staff member's responsibilities.
   * Appropriate least privilege access with correct expiration.
   * Justification for the role.
3. **Approval:** Sent to the PIM Role Manager for access approval.
4. **Application:** Security/Governance team applies roles after all approvals.

Role requests can be rejected with justification by the manager, security/governance, or role manager.

Roles and responsibilities governed by

| Roles | Responsibilities | who | recommendation |
| --- | --- | --- | --- |
| Approvers | * Responsible for ensuring each person approved to have an administrative role has adequate training to perform their job function. * View pending approvals (requests) within a timely manner * Approve or reject requests for role elevation (single and bulk) * Provide justification for approval or rejection | Business system owners:   * CIO * CISO * Associate directors * National managers | IT is ultimately responsible for the management of the Microsoft 365 tenants. |
| Global administrators | * Eligible accounts for Global Admin (these accounts are eligible to be promoted as Global Admin, every time a global admin task needs to be done, an approver will need to approve). * M365 administrators are responsible for ensuring that tenant wide controls are up to date. This includes ensuring service availability. * M365 administrators only to use Global Admin as and when required – all actions impacting whole tenants are to be approved. * Cyber Security team is responsible for ensuring security controls are not changed and perform audits on the environment. In the event of a security incident, this role should be able to demote a privilege account and remove them from the environment. Security Reports generated will be for upper management consumption. | * Microsoft 365 Administrator/s * Cyber Security Operations Staff * 1 Break Glass account for each tenant | No more than 5 eligible accounts assigned at a time. Guests should/must not be assigned.  Break Glass accounts must have their passwords changed yearly and stored in a secure location i.e. fire proof safe (electronically and paper based) but must be accessible in an emergency. |
| Azure resource | For Azure resource roles in Privileged Identity Management, only a subscription administrator, a resource Owner, or a resource User Access administrator can manage assignments for other administrators.  Users who are Privileged Role Administrators, Security Administrators, or Security Readers manage Azure resource roles in Privileged Identity Management. | e.g. Manager for Infrastructure and Platform Administrator |  |
| PIM administrator  (Privilege Role Administrator) | Administer PIM  Enable approval for specific roles.  Specify approver users or groups to approve requests.  View request and approval history for all privileged roles.  Regular Auditing of roles.  Remove roles when required for password reset or when users change responsibilities. | e.g. Information security team |  |
| Auditing | Ensure controls within M365 meet all IT Security and Compliance requirements. Perform security investigations and compliance reporting.  Manually audit all PIM roles monthly or quarterly | Security team | E-discovery Managers |
| M365 Administrators | M365 administrator is responsible for ensuring that tenant wide controls are up to date. This includes ensuring service availability. (Microsoft 365 Administrator) | EXO, SharePoint, Teams administrators. | Changes done using elevated Global Admin rights on tenants must be recorded and in line with CAB policies. |
| Application Administrators | Manage applications, create app registrations, enterprise apps etc | Security team/Apps team | Changes done using elevated Admin rights on tenants must be recorded and in line with CAB policies.  Applications must have security/privacy reviews before connected to tenant |
| Desktop support | Manage hybrid connected or Intune connected devices | Desktop support teams |  |

**Acknowledgements:**

Several people contributed to this document, and we would like to recognise the work they have done:

* Stephanie Park
* Aloka Gunawardena
* Mark Laffan

This document was rewritten by Mark Laffan for AusCERT 2025 based on the current policy at ACU.