Least Privilege Access Control SOP

Purpose

To ensure users, administrators, devices, and applications are granted only the minimum permissions necessary. This SOP leverages Microsoft Intune Role-Based Access Control (RBAC), Entra ID built-in and custom roles, Conditional Access, and access governance to reduce risk and adhere to internal policies.

1. Entra ID Role Assignments
2. Use the least-privileged built-in roles, aligned to common tasks:

* Create/reset users 🡪 User Administrator
* Assign licenses 🡪 License Administrator
* Manage device enrollment/status 🡪 Cloud Device Administrator
* Manage enterprise apps/consent 🡪 Cloud Application Administrator or Application Administrator
* Audit logs/configuration review 🡪 Reports Reader or Security Reader

1. If built-in roles grant excessive privileges, create custom roles limited to only required permissions.
   1. Go to **Microsoft Intune admin Center > Tenant administration > Roles > All roles > Create**.
   2. On the Permissions page, expand each category and choose specific actions as needed.
   3. Optionally assign Scope Tags to limit what objects the role can manage (see below on creating and assigning scope tags). Only objects sharing the same scope tag will be visible or manageable by users assigned this role.
   4. Navigate back to All roles, locate the custom role and go to **Assignments > Assign** to apply the custom role assignment.
2. Always assign roles with limited scope (e.g., particular groups, specific devices, or boundaries), never tenant-wide.
   1. Go to **Microsoft Intune admin center > Tenant administration > Roles > Scope tags > Create** to create a new scope tag.
   2. Go to **Tenant administration > Roles > All roles** and edit roles to assign specific scope tags for them.
   3. Use **Tenant administration > Monitor** to verify what users can do and see.
3. Intune RBAC Configuration
4. Navigate to **Intune Admin Center > Tenant administration > Roles**.
5. Assign built-in roles with permissions tailored to tasks.
   1. Create custom Intune roles when built-ins are too broad, limiting permissions strictly to required action sets and management categories.
6. Implement Scope Tags to restrict admin visibility and management to specific device and user subsets.
7. Assign roles only to specific Entra ID or Intune groups, never blanket assignments.
8. Device Enrollment and Access Controls
9. Permit only authorized device types and OS versions, blocking personal devices when appropriate.
   1. Navigate to **Microsoft Intune admin center > Devices > Enrollment > Device platform restriction > Create restriction** to create new device restrictions.
   2. Add Scope Tags to control which Intune administrators can see or manage this restriction.

NOTE: Enrollment restrictions affect only new enrollments, not already enrolled devices.

1. Set up conditional access policies with conditions (e.g., requiring compliant device, trusted network zones, or blocking legacy authorizations).
   1. Define policy objectives and device on target user groups, target applications, required conditions, and/or access controls.
   2. Navigate to **Microsoft Intune admin center > Endpoint security > Conditional access > Create policy** to create a new policy.
   3. Under Enable policy, toggle to Report-Only first for safe testing. Once tested, switch to On to enforce the policy.
2. Enable application protection policies to prevent data leakage on personal, BYOD devices (e.g., controlling copy/paste or storage permissions).
   1. Navigate to **Microsoft Intune admin center > Apps > Protection > Create policy** to create a new app protection policy.
   2. To enforce usage of protected apps, combine the app protection policy with a Conditional Access policy that requires approved apps and requires app protection policy before access to organization services.
3. Review and Audits
4. Conduct quarterly reviews of Entra ID role assignments and Intune RBAC assignments, removing stale or unnecessary permissions promptly.
5. Use Entra Access Reviews to revalidate continued access in groups or roles and automatically remove expired assignments.
   1. Navigate to **Microsoft Entra admin center > ID Governance > Access Reviews > New access review** to create access review.
   2. Specify scope to select specific groups/apps or optionally limiting to inactive users only.
6. Enable unified audit logs in Microsoft 365 and Intune.
7. Incident Response
8. Immediately log incidents of over-permissioning or misuse in the ticketing system.
9. Revoke access or scopes, adjust roles assignments, and/or escalate to IT Lead.
10. For suspected negligence, follow Misuse of Device or Termination of Employee SOPs.

This SOP must be reviewed annually or when Microsoft access management features changes, new regulatory requirements emerge, or major organizational role changes occur.