Azure Environment Acceptable Use Policy (AUP)

Policy Number: IT-AUP-001
Date Adopted: September 17, 2025
Last Revision: September 17, 2025
Last Review: September 17, 2025

1. Purpose
To establish acceptable use guidelines for all Azure resources, ensuring the security, integrity, and compliance of organizational data and systems.

2. Applicability
This policy applies to:
- All employees, contractors, and third-party users with access to the organization's Azure environment.
- All Azure resources, including subscriptions, virtual machines, storage accounts, applications, and services.

3. Accountability
- **Employees and Contractors:** Must comply with this policy and report violations.
- **IT / Security Team:** Responsible for monitoring, enforcing, and reviewing adherence to this policy.
- **Managers:** Ensure their teams understand and comply with acceptable use guidelines.

4. Definitions
- **Azure Resources:** Any compute, storage, network, or application service provisioned within the organization's Azure subscriptions.
- **User:** Any individual authorized to access the organization's Azure environment.
- **Privileged Access:** Elevated permissions that allow changes to security, configuration, or administrative settings in Azure.

5. Policy
- Azure resources must be used for legitimate business purposes only.
- Sharing of credentials or accounts is prohibited.
- Users must not attempt to bypass security controls or access resources beyond their assigned permissions.

- Personal use of resources is permitted only when explicitly authorized and must not interfere with business operations.
- All use of resources is subject to monitoring and auditing in accordance with the Monitoring & Audit Policy.

6. Non-Compliance and Sanctions
Violations may result in:
- Verbal or written warnings.
- Suspension or termination of access privileges.
- Escalation to HR or management for further action.
- Reporting to legal or regulatory authorities if required.