MANDELBULB TECHNOLOGIES

Information Security Policies

Purpose

To establish security controls and responsibilities to protect organizational data in Azure cloud environments.

Scope

Applies to all employees, contractors, and systems that access organizational resources hosted in Azure.

Policy Sections

1. Governance and Responsibilities

- Assign **Azure Security Administrators** and **Data Owners**.
- Establish an **Information Security Committee**.
- Define roles for **Access Control**, **Monitoring**, and **Incident Response**.

2. Data Classification and Handling

- Classify data as **Public, Internal, Confidential, and Restricted**.
- Implement **Azure Information Protection (AIP)** labels for sensitive data.
- Encrypt sensitive data **at rest** (Azure Storage Encryption, SQL TDE) and **in transit** (TLS 1.2+).

3. Identity and Access Management

- Enforce **Entra ID** for all authentication.
- Implement **Multi-Factor Authentication (MFA)** for admin and sensitive accounts.
- Use **Role-Based Access Control (RBAC)** for least privilege.
- Regularly review and revoke inactive accounts.

4. Network Security

- Use **Azure Firewall**, **Network Security Groups (NSGs)**, and **Azure DDoS Protection**.
- Segregate environments using **VNETs** and **subnets**.
- Implement **VPN or Private Endpoint connections** for sensitive data access.

5. Threat Protection and Monitoring

- Enable **Azure Security Center / Defender for Cloud**.
- Enable **Azure Monitor, Log Analytics, and Azure Sentinel** for logging and alerts.
- Regularly review **security alerts and audit logs**.

6. Backup and Disaster Recovery

- Use **Azure Backup** and **Azure Site Recovery** for critical workloads.
- Test **DR plans** periodically.

7. Compliance and Audit

- Align with **ISO 27001, SOC2, GDPR** as applicable.
- Conduct **regular security audits and penetration tests**.

8. Incident Response

- Define **incident reporting procedures**.
- Maintain an **incident response playbook** for Azure resources.
- Perform **post-incident reviews** and remediation.

Privacy Policy

Purpose

To communicate how the organization collects, stores, processes, and protects personal data in Azure services.

Scope

Applies to all personal data processed in Azure by employees, applications, or third-party services.

Policy Sections

1. Data Collection

- Clearly define **types of personal data** collected.
- Specify **purpose of collection**.
- Ensure **data minimization** (only collect what is necessary).

2. Data Storage

- Store personal data in **Azure regions** compliant with legal requirements.
- Encrypt personal data **at rest and in transit**.
- Use **Azure Key Vault** to manage encryption keys securely.

3. Data Access and Sharing

- Limit access using **RBAC** in Entra ID.
- Share data **only with authorized parties** under contractual agreements.
- Log and monitor all access to personal data.

4. Data Retention

- Define retention periods for each data type.
- Implement automated deletion/archival using **Azure Storage Lifecycle Management**.

5. Rights of Data Subjects

- Provide mechanisms for **data access, correction, and deletion**.
- Ensure compliance with **GDPR, CCPA, or local privacy laws**.

6. Third-Party Services

- Conduct due diligence for Azure **Marketplace solutions**.
- Include **data processing agreements** with third-party vendors.

7. Breach Notification

- Follow **Azure incident response protocols**.
- Notify affected individuals and authorities as required by law.

8. Training and Awareness

- Conduct periodic **security and privacy training** for all employees.
- Promote awareness of **Azure security features** and compliance obligations.