Management Team Security Policy

Purpose:
This policy outlines the specific security measures the management team must follow to safeguard sensitive company data and oversee compliance with security standards.

Key Areas:

1. Password Security:
- All management accounts must use strong, unique passwords, adhering to company password policies.
- Multi-factor authentication (MFA) is mandatory for accessing critical systems and sensitive data.

2. Risk Management:
- Regularly assess potential security risks and ensure proper risk mitigation strategies are in place.
- Engage in security risk assessments quarterly and update risk mitigation plans accordingly.

3. Incident Response:
- Management must lead in coordinating incident response activities, ensuring swift resolution of security incidents.
- All incidents must be documented for review and post-incident analysis to prevent future occurrences.

4. Data Access Control:
- Ensure role-based access control (RBAC) is applied across the organization, limiting access to sensitive data based on user roles.
- Management must review and approve all access control changes.

5. Security Awareness:
- Management is responsible for ensuring that all employees complete mandatory security awareness training.
- Regularly communicate security policies and updates to the team.

6. Reporting:
- All security incidents, suspicious activities, and policy breaches must be reported to the IT security team immediately for investigation.