Standard Operating Procedure (SOP)

Computer Network and Sensitive Data Security Measures

1. Purpose

This SOP outlines **computer network and sensitive data security measures**, including network access control, data encryption protocols, user authentication procedures, regular security audits, malware detection and prevention strategies, secure data storage practices, incident response plans, employee training on cybersecurity best practices, and compliance with data protection regulations. The objective is to safeguard the integrity, confidentiality, and availability of computer networks and sensitive information against unauthorized access, cyber threats, and data breaches.

2. Scope

This SOP applies to all employees, contractors, and third-party users who access the organization's computer networks and handle sensitive information.

3. Responsibilities

- IT Department: Implementation, monitoring, and maintenance of security measures.
- All Users: Adherence to security protocols and reporting incidents.
- Management: Enforcement and regular review of this SOP.

4. Procedure

1. **Network Access Control**
   - Restrict network access to authorized personnel only.
   - Implement network segmentation and firewalls.
   - Regularly review and update access permissions.
2. **Data Encryption Protocols**
   - Encrypt sensitive data at rest and in transit using industry-standard algorithms (e.g., AES-256, SSL/TLS).
   - Ensure encryption keys are securely stored and managed.
3. **User Authentication Procedures**
   - Enforce strong password policies and multifactor authentication (MFA).
   - Deactivate inactive accounts in a timely manner.
4. **Regular Security Audits**
   - Conduct periodic vulnerability assessments and penetration tests.
   - Document findings and remediate vulnerabilities promptly.
5. **Malware Detection and Prevention**
   - Deploy up-to-date anti-malware software on all endpoints and servers.
   - Perform regular system scans and monitor for suspicious activity.
6. **Secure Data Storage Practices**
   - Store sensitive data in secure, access-controlled environments (e.g., encrypted drives, secure cloud storage).

    - Limit data retention to only what is necessary for business operations.

7. **Incident Response Plan**
    - Establish procedures for reporting, responding to, and documenting security incidents and data breaches.
    - Communicate breaches to affected parties and authorities as required by law.
8. **Employee Training**
    - Conduct regular cybersecurity awareness training for all staff.
    - Provide up-to-date resources and simulate phishing attacks to reinforce best practices.
9. **Compliance with Data Protection Regulations**
    - Remain informed of and comply with relevant data protection laws (e.g., GDPR, HIPAA).
    - Implement procedures for data subject requests and privacy impact assessments where applicable.

5. Records and Documentation

- Maintain logs of network access, security audits, incidents, and training programs.
- Retain documentation as required by regulatory authorities and internal policy.

6. Review and Update

This SOP must be reviewed and updated at least annually or upon significant changes in technology, business operations, or regulatory requirements.

7. Approval

Approved by: ________________________
Date: ________________