Compliance Documentation

1. Purpose:

   The purpose of this Standard Operating Procedure (SOP) is to outline the policies, procedures, and guidelines for ensuring the effective implementation of cybersecurity measures at Cyber Guardian. This SOP aims to protect our clients' valuable data and maintain the confidentiality, integrity, and availability of their information systems.

2. Scope:

   This SOP applies to all employees, contractors, and stakeholders of Cyber Guardian who are involved in handling, processing, or managing sensitive information and IT infrastructure.

3. Roles and Responsibilities

   3.1 Management
   - Ensure the establishment and maintenance of the cybersecurity program.
   - Allocate necessary resources to support cybersecurity initiatives.
   - Foster a culture of cybersecurity awareness and compliance.

   3.2 IT Department
   - Implement and maintain cybersecurity measures and tools.
   - Monitor and analyze network traffic and system logs.
   - Respond to security incidents and conduct investigations.

   3.3 Employees
   - Adhere to the guidelines set forth in this SOP.
   - Report any suspicious activity or potential security threats to the IT department.
   - Participate in cybersecurity training and awareness programs.

4. Procedures

   4.1 Access Control
   - Implement role-based access control (RBAC) to limit access to sensitive data and systems.
   - Enforce strong password policies and require regular password updates.
   - Set up multi-factor authentication (MFA) for all critical systems.

   4.2 Network Security
   - Deploy firewalls, intrusion detection/prevention systems (IDS/IPS), and virtual private networks (VPNs) to protect the network perimeter.
   - Encrypt all sensitive data transmitted over the network.

- Regularly patch and update software and firmware on all devices.

4.3 Endpoint Security

- Install and update antivirus and anti-malware software on all endpoints.
- Enable full-disk encryption (FDE) on all company devices.
- Restrict the installation of unauthorized software and use of removable media.

4.4 Incident Response

- Develop and maintain an incident response plan (IRP) to guide the handling of cybersecurity incidents.
- Regularly conduct IRP drills and exercises.
- Notify appropriate stakeholders and authorities in the event of a breach or incident.

4.5 Backup and Recovery

- Perform regular data backups and store them securely, both on-site and off-site.
- Implement a disaster recovery plan (DRP) to ensure business continuity in the event of a cyber incident.
- Test backup and recovery processes periodically to verify their effectiveness.

5. Training and Awareness
    - Provide mandatory cybersecurity training for all employees during onboarding and at regular intervals.
    - Conduct ongoing awareness campaigns, including email updates, posters, and workshops.
    - Regularly test employee awareness through simulated phishing exercises and other security assessments.
6. Auditing and Monitoring
    - Regularly audit and review cybersecurity policies and practices.
    - Monitor and log all network activity, including access attempts and data transfers.
    - Conduct vulnerability assessments and penetration tests to identify and remediate security weaknesses.
7. Continuous Improvement
    - Review and update this SOP periodically to address new threats, emerging technologies, and changes in industry best practices.
    - Encourage feedback from employees and stakeholders to improve cybersecurity measures.
    - Stay up-to-date with the latest cybersecurity trends and threat intelligence.
8. Non-Compliance
    - Document and report instances of non-compliance with this SOP.

- Investigate non-compliance incidents and take corrective actions as necessary.
- Implement disciplinary measures for repeat offenders or severe violations of this SOP.

Authored by Dylan Dempsey/ Alexander Echols
Document Version: 1.0 Last Updated: May 12, 2023
Next Review: May 12, 2024