Aberrant Open-ISM™

INFORMATION SECURITY POLICY

Property	Description
Document Version	1.0
Status	DRAFT
Last Update	2022-03-25
Document Owner	Risk Management
Next Scheduled Review	

PROPRIETARY

Document Approvals		
Approver Name	**Title**	**Date**
???	???	???

Revision History			
Version	**Date**	**Description of Changes**	**Revised by**
1.0	2022-03-25	DRAFT	Aberrant

TABLE OF CONTENTS

1 Overview 8

2 Purpose 8

3 Scope 9

4 Executive Management 9

5 Information Security Reviews 10

5.1 ISMS Review 10

5.2 ISMS Availability 10

5.3 Independent Review of Information Security 10

5.4 Technical Compliance Review 10

5.5 Strategic Review 11

5.6 Privacy Requirements Review 11

6 Operational Security 11

6.1 Responsibility for Policy Maintenance 11

7 Compliance with Legal and Contractual Requirements 12

7.1 Identification of applicable legislation and contractual requirements 12

7.2 Contact with Authorities 12

7.3 Intellectual Property Rights 12

7.4 Protection of records 12

8 Patch Policy and Procedure 12

8.1 Trends and Zero-Day Attacks 12

8.2 Patch Management Guidelines 13

8.2.1 Operating System Patch Review 13

8.2.2 Client Machine Patch Review 13

8.2.3 Mobile Patch Review 13

8.2.4 Firmware Patch Review 13

8.2.5 Application Patch Review 13

9 Management of Technical Vulnerabilities 14

9.1 Security Awareness in the Organization 14

9.2 Information security in project management 14

9.3 Outside Expertise and External Guidance 14
10 Information Systems Audit Considerations 15
11 Audit Log Management 15
11.1 Collect Audit Logs 15
11.1.1 Collect Service Provider Logs 15
11.1.2 Administrator and Operator Logs 16
11.2 Audit Log Access 16
11.3 Audit Log Storage 16
11.4 Audit Log Types 16
11.4.1 SIEM 16
11.4.2 Database 16
11.4.3 Operating Systems for Workstations and Servers 17
11.4.4 Vulnerability Scans 17
11.4.5 Static Analysis Scans (SAST) 17
11.4.6 Dynamic Application Security Testing Results (DAST) 17
11.4.7 Web Logs 17
11.4.8 Application Uptime Logs 17
11.5 Log Reviews 17
11.5.1 SIEM Log Review 17
11.5.2 Application Log Review 18
11.5.3 Database Access Log Review 18
11.5.4 Operating System Log Review 18
11.5.5 Vulnerability Scans 19
11.5.6 SAST Scan Review 19
11.5.7 DAST Scan Review 19
12 Machine Clock Synchronization 20
13 Scheduled Maintenance 20
14 Principle of Zero Trust 20
14.1 Single Source of Identity 20
14.2 Principle of Minimalism 20
15 Network Security 21

15.1 Systems and Configuration 21
15.1.1 Network Topology and Documentation 21
15.1.2 Modifications 21
15.1.3 Secure Traffic 21
15.1.4 Security of Network Services Provisions 22
15.1.5 Network Segregation and Segmentation 22
15.1.6 Least Privilege 22
15.1.7 Network Access 23
15.1.8 Centralize Network Authentication, Authorization, and Auditing (AAA) 23
15.1.9 Firewall 23
15.1.10 Contemporary and Up-to-Date Network Infrastructure 23
15.1.11 Remote Connections to End User Devices 23
15.1.12 Remote Connections to External Networks 24
15.1.13 Dedicated Computing Resources 24
15.1.14 Container Security 24
15.2 Monitoring and Alerts 24
15.2.1 Dataflow Thresholds 24
15.2.2 Firewall Configuration File(s) Monitoring 25
15.2.3 Centralize Security Event Alerting 25
15.2.4 Network Traffic Flow Logs 25
15.2.5 Network Capacity Monitoring 25
15.2.6 Access Control for Remote Assets 25
15.2.7 Security Event Alerting Thresholds 25
15.3 Deploy A Host-Based Intrusion Prevention Solution 25
15.3.1 Network Intrusion Prevention Solution (IPS) 25
15.4 Deploy a Host-Based Intrusion Detection Solution 26
15.4.1 Network Intrusion Detection Solution (IDS) 26
15.5 Establish and Maintain a Secure Network Architecture 26
15.6 Establish and Maintain Architecture Diagram(s) 26
15.7 Centralize Network Authentication, Authorization, and Auditing (AAA) 26
15.8 Use of Secure Network Management and Communication Protocols 26

16 Application Layer 27
16.1 Security 27
16.1.1 DNS Management 27
16.1.2 Web Access Firewall 27
16.1.3 Cloud Access Security Broker (CASB) 27
16.1.4 Content Delivery Network (CDN) 27
16.1.5 API Security 27
16.2 Monitoring and Alerts 28
16.2.1 Performance Monitoring 28
16.2.2 Application Exception Logs 28
16.2.3 Alerting 28
17 Host Based Security 29
17.1 Minimalism 29
17.2 Host-Based Firewalls 29
17.3 Host-Based Intrusion Detection Solution (IDS) 29
17.4 Malware protection 29
17.5 Removable Media 29
17.6 Default Accounts 29
17.7 DNS Configuration 29
17.8 Host-Based Intrusion Prevention Solution 30
18 Capacity Management 30
18.1 Processing 30
18.2 Read / Write Operations 30
18.3 Storage 30
19 Separation of Environments 30
20 Information Transfer 31
20.1 Information Transfer Policies and Procedures 31
20.2 Agreements on Information Transfer 31
20.3 Electronic Messaging 31
20.4 Confidentiality and Nondisclosure Agreements 32
21 Information Backup 32

21.1 File Shares and Images 32

21.2 Database Backups 32

21.3 Cloud Backups 32

22 Data Loss Prevention 33

22.1 Peripheral Control Policy 33

22.2 Data Loss Prevention Policy 33

23 Email Gateway Security 33

23.1 Email Server Configuration 33

23.2 DMARC 33

24 Security Requirements of Information Systems 34

24.1 Information security requirements analysis and specification 34

24.2 Securing application services on public networks 34

24.3 Protecting application services transactions 34

25 Penetration Testing 35

25.1 Penetration Testing Program 35

25.2 External Penetration Tests 35

25.3 Penetration Test Findings 35

25.4 Validate Security Measures 35

25.5 Internal Penetration Tests 36

26 Contact Information 37

27 Document RACI 37

28 License Information 38

Appendix A: Executive Meeting Minutes Template 39

1 OVERVIEW

Our objective, in the development and implementation of this comprehensive information security policy (“Policy”), is to create effective administrative, technical and physical safeguards for the protection of personal information of <<Company Name>> customers, and to comply with regulatory standards. The Policy sets forth our procedure for evaluating our electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting personal information of <<Company Name>> members.

For purposes of this Policy, “personal information” (personally identifiable information (PII)) means a <<Company Name>> member’s first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to the named member:

1. Social Security number;
2. Driver's license number or state-issued identification card number;
3. financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "Personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

The ‘definition’ for personal information used by this Policy was derived from Massachusetts legislation 201 CMR 17.00; and California data breach notification law, SB1386.

2 PURPOSE

The purpose of the Information Security Policy is to set forth the underlying tenets, framework, and reasoning for the <<Company Name>> Information Security Management System (ISMS) in accordance with the requirements of ISO standard ISO/IEC 27001:2013. More specifically:

1. Establish a framework for the monitoring and maintenance of controls for business and operational processes—e.g. manual, automated, preventive, detective, and corrective controls.
2. Ensure the security and confidentiality of personal information.
3. Protect against the risk of any anticipated threats or hazards to the security or integrity of such information.
4. Protect against unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft or fraud.

3 SCOPE

In formulating and implementing the Information Security Policy, <<Company Name>> will:

1. Identify reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information;
2. Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the personal information;
3. Evaluate the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risks;
4. Design and implement a policy that puts safeguards in place to minimize those risks; and
5. Regularly monitor the effectiveness of those safeguards.
6. Continuous improvement of the company's security program over time.

4 EXECUTIVE MANAGEMENT

Executive Management is charged with protecting the confidentiality, integrity, and availability (CIA) of the information held by <<Company Name>>. Toward this end, management must ensure that employees adhere to the policies, procedures, and standards that make up the company's Information Security Program.

Executive management shall demonstrate leadership and commitment with respect to the ISMS by supporting the following objectives:

- Demonstrate management commitment to, and support for, information security;
- Establish directives and principles for action with regards to information security based on internal controls;
- Ensure alignment with the company's mission continuity requirements;
- Ensure alignment with client requirements and contractual security obligations;
- Ensure alignment with applicable legal and regulatory requirements;
- Ensure alignment with applicable privacy requirements;
- Account for risk to the enterprise;
- Ensure that strategic objectives are used to determine entity structure and performance metrics; and,
- Support and foster a culture that leverages the ISMS as a mechanism to drive continuous improvement.

5 INFORMATION SECURITY REVIEWS

5.1 ISMS REVIEW

The program should be reviewed annually by the ISMS Committee. The objectives of the review should be:

1. Review of policies, procedures and other control documents for accuracy, applicability, and identify opportunities to improve existing security and operational controls. Reviews should be conducted on at least an annual basis.
2. Assessment as to whether the detection and handling of incidents are operating properly, and identifies the need for system changes and implementation of additional controls based on incident patterns and root causes.
3. Ensure alignment with the company's Information Security objectives.
4. The company's internal controls environment takes into consideration affecting laws, regulations, standards, and legislation.
5. Defining, coordinating, and monitoring compliance and audit activities in order to ascertain program effectiveness.
6. Review of internal audits enterprise compliance assessment of the ISMS program.
7. Review activities and corrections shall be submitted for approval to the ISMS Governance Committee.

5.2 ISMS AVAILABILITY

The information security policy must be communicated to employees and made available as documented information, to interested parties, as appropriate.

5.3 INDEPENDENT REVIEW OF INFORMATION SECURITY

The organization's approach to managing information security and the program implementation shall be independently audited by a third-party at regular intervals or when a significant change occurs. It is the responsibility of the compliance manager to coordinate independent third-party reviews of the program.

5.4 TECHNICAL COMPLIANCE REVIEW

1. Operational systems and controls shall be reviewed and tested periodically for technical compliance with information security requirements—e.g. logical access reviews, backup restoration tests, etc. Testing should be performed on at least an annual basis.
2. Testing shall be conducted by competent, authorized individuals with the advice and cooperation of Internal Audit.

3. Test results shall not be distributed to any person without a valid “need to know”.

5.5 STRATEGIC REVIEW

Operational Management and Executive Management should meet at least annually to review:

- results of assessments performed by third parties;
- business plans;
- strategic objectives;
- budgets; and
- roles and responsibilities. (This should be a recurring action.)

5.6 PRIVACY REQUIREMENTS REVIEW

Privacy requirements will be reviewed by <<Company Name>>’s General Counsel, Chief Privacy Officer (CPO) and ISMS Manager at least annually.

6 OPERATIONAL SECURITY

The systematic and proven process by which potential adversaries can be denied information about capabilities and intentions by identifying, controlling and protecting generally unclassified evidence of the planning and execution of sensitive activities. The process involves five steps:

1. identification of critical information;
2. analysis of threats;
3. analysis of vulnerabilities;
4. assessment of risks, and;
5. application of appropriate countermeasures.

The Information Security Policy incorporates monitoring processes and software to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs, and unusual system activity. Operating procedures incorporate overlapping controls to create a defense-in-depth that prevents the failure of one control from compromising the program. It’s important that managers who oversee the implementation of the program should have total visibility into daily operations in order to ensure that documented operating procedures are being adhered to operational staff.

6.1 RESPONSIBILITY FOR POLICY MAINTENANCE

The CISO is responsible for ensuring that the Information Security Policy is kept current as needed for purposes of compliance with regulations. The CISO will utilize designated employees to complete the previously mentioned tasks as members of the <<Company Name>> Information Technology and Development teams have an understanding of the subject matter mentioned above and are familiar with <<Company Name>>'s infrastructure. This will allow the CISO to fully utilize all employees who will assist and report on completed work and any findings.

7 COMPLIANCE WITH LEGAL AND CONTRACTUAL REQUIREMENTS

7.1 IDENTIFICATION OF APPLICABLE LEGISLATION AND CONTRACTUAL REQUIREMENTS

All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.

7.2 CONTACT WITH AUTHORITIES

Appropriate contacts with relevant legal and regulatory authorities should be maintained.

7.3 INTELLECTUAL PROPERTY RIGHTS

Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.

7.4 PROTECTION OF RECORDS

Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with applicable legislation, regulations, and contractual requirements.

8 PATCH POLICY AND PROCEDURE

8.1 TRENDS AND ZERO-DAY ATTACKS

In the event of a zero-day vulnerability with no existing patch where <<Company Name>> deems that there is a high risk of exposure, InfoSec personnel will take steps to mitigate the issue via alternate means—e.g. changes to configuration. If a hot fix is available InfoSec will research, test and deploy the hot fix prior to deployment. For known zero-day exploits that are high risk to the company <<Company Name>> targets remediation within 24 hours.

8.2 PATCH MANAGEMENT GUIDELINES

Good patch policy is one of the most important elements in a good defense in-depth security program. It’s the job of everyone in security to:

- Review vendor alerts to determine if patches are required for any systems or software.
- Maintain awareness of vulnerability listings, or alerts of any software utilized in the <<Company Name>>’s environment.
- Stay alert to announcements regarding faulty updates and regression issues that could manifest in the environment.
- Ensure that software / firmware updates are consistently applied to all hardware and software in the <<Company Name>>’s inventory.

Patch Policy should conform the following criteria:

1. All software patches should be reviewed and applied on at least a monthly basis. In the event of an urgent patch a change control request should be generated.
2. Patches should be downloaded only from a trusted confirmed source. For software updates patch integrity should be verified before patches are applied.
3. Patches and updates shall include measures to rollback / restore the last known good system state in the event of an installation failure.

8.2.1 OPERATING SYSTEM PATCH REVIEW

Ensure that severs operating systems and containers are patched at least monthly.

8.2.2 CLIENT MACHINE PATCH REVIEW

Ensure that client machines, e.g. laptops, are patched on at least a monthly basis.

8.2.3 MOBILE PATCH REVIEW

Ensure registered mobile devices, e.g. devices with an MDM, are up to date on patches on at least a monthly basis.

8.2.4 FIRMWARE PATCH REVIEW

Ensure that firmware on system peripherals such as web access points and firewalls are patched on at least a monthly basis.

8.2.5 APPLICATION PATCH REVIEW

Ensure that third party applications that require patching are update to date with their latest patches on at least a monthly basis.

9 MANAGEMENT OF TECHNICAL VULNERABILITIES

9.1 SECURITY AWARENESS IN THE ORGANIZATION

All employees should be aware of common security threats and computer incidents that may potentially compromise the organization’s network infrastructure, cause harm to other related systems or pose a significant financial, operational or business threat to the organization as a whole. There are numerous security threats and computer incidents that are potentially detrimental to any organization, such as the following:

- Malicious or careless employees;
- Malware (computer viruses, worms, Trojan horses, most root kits, spyware and other malicious and unwanted software);
- Social engineering;
- Spam;
- Spoofing and phishing;
- Denial of service;
- Distributed denial of service;
- Man-in-the-middle attacks;
- Additional network attacks, including hacking and other common attack vectors;
- Physical and environmental conditions resulting in threats to the organization’s system resources.

Adequately preparing for an incident requires security personnel to be aware of common threats to systems and to implement safeguards and control mechanisms that protect system resources within the organization.

9.2 INFORMATION SECURITY IN PROJECT MANAGEMENT

Information security should leverage the same project management paradigm as other projects in order to maintain visibility to management. This approach enables reuse of KPIs and other indicators to ensure that projects related to security are given adequate prioriortiy relative to other projects.

9.3 OUTSIDE EXPERTISE AND EXTERNAL GUIDANCE

A vital component of preparing for an incident is ensuring that all personnel have relevant security training pertinent to their roles and responsibilities within the organization. Additionally, all system components and other I.T. resources deemed critical by the organization must be securely hardened with best of breed hardening and configurations standards at all times. Sources used may include, but are not limited to the following:

- NIST (http://www.nist.gov/index.html);
- CIS (https://www.cisecurity.org/);
- SANS (http://www.sans.org/);
- CERT (http://www.cisecurity.org/), (http://www.kb.cert.org/vuls/);
- ISACA (http://www.isaca.org/);
- BITS & Shared Assessments (http://www.sharedassessments.org/);
- BugTraq (http://www.securityfocus.com/archive/1);
- CVE (http://cve.mitre.org/);
- Exploit DB (http://www.exploit-db.com/);
- NVD (http://invd.nist.gov/);
- OSVDB (http://www.osvdb.org/);
- Secunia (http://secunia.com/community/advisories/).

10 INFORMATION SYSTEMS AUDIT CONSIDERATIONS

<<Company Name>>'s internal audit function is responsible for coordinating testing and review of business processes, procedures, and system to ensure that <<Company Name>> is operating in a way that is consistent with our ISMS. When planning an audit the internal auditor should account for the following:

1. Audit requirements and activities involving checks on operational systems shall be carefully planned and must minimize the risk of disruptions to business processes.
2. The scope of testing shall be limited to those systems and resources specified in the audit plan and agreed to by the resource owner(s).
3. Persons performing audit services must document their activities, procedures, findings and recommendations. Audit documentation and evidence should be stored in a secure location consistent with <<Company Name>>'s data retention policies.

11 AUDIT LOG MANAGEMENT

Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.

11.1 COLLECT AUDIT LOGS

As a design principle, log data should be stored in a centralized location.

11.1.1 COLLECT SERVICE PROVIDER LOGS

If a service provider makes log data available it should be collected for forensic troubleshooting. The decision to do this is the purview of the CISO, or an employee delegated by the CISO.

11.1.2 ADMINISTRATOR AND OPERATOR LOGS

System administrator and system operator activities should be handled in the same way as other data that is logged and reviewed.

11.2 AUDIT LOG ACCESS

Logs have the potential to contain sensitive information such as PII. Access to audit logs should be limited to employees based on their job function.

11.3 AUDIT LOG STORAGE

The following practices should be adhered to when setting up log storage:

- When possible, configure audit logs to ‘autogrow’ when they reach a certain capacity or threshold.
- When possible, configure logs to temporally rotate logs—rotation must respect the Data Retention Policy.
- Log growth should be reviewed periodically as part of capacity planning. See the Capacity Planning section of this document for more detail.

11.4 AUDIT LOG TYPES

Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, UTC timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.
Collect audit logs for:

11.4.1 SIEM

The SIEM must be configured to ingest data from traffic sources: syslog, IDS/IPS, firewall, WAF, VPN, iislogs, CLI, and eventlog. The company should also deploy an endpoint detection & response (EDR) system to identify threats quickly and remediate them.

11.4.2 DATABASE

11.4.2.1 DATA ACCESS LOGS

Database access reviews are completed by management on a monthly basis.

11.4.2.2 SENSITIVE DATA ACCESS LOGS

Sensitive data access is logged, this includes modification and disposal of data. Sensitive data access logs are reviewed on a monthly basis.

11.4.3 OPERATING SYSTEMS FOR WORKSTATIONS AND SERVERS

Store event log security and events on the hosts.

11.4.4 VULNERABILITY SCANS

Vulnerability scans are stored via a SaaS provider system. Logs are stored for one year.

11.4.5 STATIC ANALYSIS SCANS (SAST)

SAST scans are stored via a SaaS provider system. Logs are stored for one year.

11.4.6 DYNAMIC APPLICATION SECURITY TESTING RESULTS (DAST)

DAST scans are stored in the SaaS provider system. Logs are stored for one year.

11.4.7 WEB LOGS

Collect centralized HTTP requests for analytics and forensic troubleshooting.

11.4.8 APPLICATION UPTIME LOGS

Application Uptime requests made to a health-check end-point are stored via a SaaS provider. Logs are stored for one year or more.

11.5 LOG REVIEWS

Audit logs are critical for forensic reviews and resolving anomalies. Logs should be collected, stored, and reviewed on a regular cadence.

11.5.1 SIEM LOG REVIEW

The SIEM should be configured to capture log events from syslog, IDS/IPS, firewall, WAF, VPN, iislogs, CLI, and eventlog.

11.5.1.1 DAILY REVIEW

Logs should be reviewed daily for anomalous incidents. If suspicious log data is detected the operations security team is notified.

11.5.1.2 MONTHLY REVIEW

Logs should be reviewed at least monthly to evaluate the following:

- Abnormal activity which could be the result of malware or an unauthorized user.

- Account logon events.
- Account management.
- Firewall and other traffic management device log analysis.
- Logon events.
- Mobile devices that have connected to the organization’s wireless services.
- Policy changes.
- Unauthorized or authorized use of or access to personal information and sensitive systems.
- Use of privileged escalation by unauthorized users or service accounts.
- System events.
- VPN access from employees and vendors.

Activity that is deemed to be suspicious or abnormal should utilize a heuristic like the Mitre ATT&CK® Framework to assess the validity of the threat.

11.5.2 APPLICATION LOG REVIEW

Application logs should be reviewed at least monthly. Application should publish events to the eventlog:

- Account logon events.
- System events.

11.5.3 DATABASE ACCESS LOG REVIEW

Database logs should be reviewed at least monthly.

- Failed login attempts.
- Successful login attempts.
- Suspicious service account activity.

11.5.4 OPERATING SYSTEM LOG REVIEW

Operating system logs should be reviewed at least monthly.

- Abnormal activity which could be the result of malware or an unauthorized user.
- Account logon events.
- Account management.
- Logon events.
- Policy changes.
- System events.
- Violations of acceptable use policy.

11.5.5 VULNERABILITY SCANS

Once a scan is performed, <<Company Name>> will perform a risk assessment of identified vulnerabilities within a week of performing the scan. The scan should utilize both authenticated scans & unauthenticated scans, using a SCAP, or something similar to SCAP. Vulnerabilities that require remediation should adhere to Corrective Actions guidance in the Enterprise Risk Policy.

11.5.5.1 INTERNAL

An automated vulnerability scan of the network layer and operating system layer are performed monthly.

- Anti-virus is confirmed to be running on all systems and the dashboard is checked daily.
- Updates are completed if not set to automatic.

11.5.5.2 EXTERNAL

An automated vulnerability scan of the application layer is performed quarterly.

- Any automated vulnerability scan of the application layer is performed by an external agent.
- A port scan is completed, the security analyst should confirm that only authorized ports and protocols are open to data ingress.

11.5.6 SAST SCAN REVIEW

SAST scans are done nightly, but only require remediation at the conclusion of a sprint. Please see the SDLC for more detail.

11.5.7 DAST SCAN REVIEW

Any automated DAST scan of application layer is reviewed at least quarterly. <<Company Name>> will perform an internal risk assessment of identified vulnerabilities within a week of performing a scan. Please see the SDLC for more detail on how DAST is incorporated into application testing.

12 MACHINE CLOCK SYNCHRONIZATION

<<Company Name>>'s domain controllers run on Microsoft Azure use Active Directory in the root domain. Active Directory uses the "W32Time" service to synchronize machines joined to the network with NIST using Network Time Protocol (NTP). The W32Time service is used by the Kerberos authentication protocol used by Active Directory. Kerberos authentication requires correct time on all clients participating in authentication. If the clocks on two machines trying to authenticate to each other are more than five (5) minutes apart, Kerberos authentication will fail. <<Company Name>>'s domain controllers are configured to use two of four NIST internet time servers. Machines joined to the domain have their clocks synchronized with the domain controller at startup. There should be a minimum to two machines configured to be time servers.

13 SCHEDULED MAINTENANCE

If downtime is required we maintain an optional 2-hour maintenance window on Monday from midnight to 2:00 AM ET. In the event of a major system changes that falls outside of <<Company Name>>'s planned maintenance window we will provide customers with 45 days prior notification. <<Company Name>>'s maintenance schedule is available on a dedicated web page that customers can view at any time. The page can be viewed at https://company.status.io/.

14 PRINCIPLE OF ZERO TRUST

The main concept behind zero trust is that devices should not be trusted by default, even if they are connected to a managed corporate network such as the corporate LAN and even if they were previously verified. The zero trust approach advocates for mutual authentication, including checking the identity and integrity of devices without respect to location, and providing access to applications and services based on the confidence of device identity and device health in combination with user authentication. This principle is inspired by the "NIST Special Publication (SP) 800-207, ZERO TRUST ARCHITECTURE."

14.1 SINGLE SOURCE OF IDENTITY

A domain controller should be used to authorize and authenticate users and machines on the network.

14.2 PRINCIPLE OF MINIMALISM

Assets should only have what they need.

15 NETWORK SECURITY

Network security utilizes a multi-layered defense approach that multiple overlapping controls.

15.1 SYSTEMS AND CONFIGURATION

Network security addresses vulnerabilities regarding network services and access points, and provides guidance on preventing an attacker from exploiting weaknesses.

15.1.1 NETWORK TOPOLOGY AND DOCUMENTATION

Network diagrams and documentation must accurately reflect the composition and configuration of the network and associated assets. Use of digital active / passive discovery tools is required to:

- Discover and scan Windows, Linux, and macOS assets in your enterprise.
- Perform network scans to discover IP devices: e.g. printers, routers, switches, and access points.

15.1.2 MODIFICATIONS

It is strongly preferred that network modifications should be performed using an infrastructure-as-code (IAC) methodology that conforms to the company’s SDLC. Deployments should leverage an immutable image and incorporate a container security system.
At minimum, modifications or additive changes to the network must adhere to the company’s Change Control Policy.

15.1.3 SECURE TRAFFIC

Internal and external data-in-transit should be encrypted in accordance with the company’s Encryption Policy. DNS should be configured to use enterprise-controlled DNS servers and/or reputable externally accessible DNS servers.

15.1.3.1 APPROVED PROTOCOLS

Approved protocols should utilize only white-lists, and not black-lists.

15.1.4 SECURITY OF NETWORK SERVICES PROVISIONS

Network services agreements, whether in-house or outsourced, shall include the following provisions:

1. Security features and requirements.
2. Service level agreements.
3. Specified responsibility for managing security requirements on both sides of the service delivery process.

15.1.5 NETWORK SEGREGATION AND SEGMENTATION

Networks should be segregated and segmented to enable compartmentalization in the event of a breach incident.

- Network segregation involves developing and enforcing a ruleset for controlling the communications between specific hosts and services. *
- Network segmentation involves partitioning which reduces the attack surface of the network, a blocks lateral movement by an attacker to other segments of the network.

The following actions must be performed:

- Assets that a directly exposed to external requests such as web servers, web services, etc. should be located within a DMZ.
- Traffic between segments should be limited to only the ports and protocols absolutely required based on operational requirements. Any traffic not explicitly permitted must be implicitly denied.
- Traffic between network segments should be controlled via access control lists (ACLs).
- Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.
- Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.

15.1.6 LEAST PRIVILEGE

If a host, service or network doesn't need to communicate with another host, service or network, it should not be allowed to. If a host, service or network only needs to talk to another host, service or network on a specific port or protocol, and nothing else, it should be restricted to this.

15.1.7 NETWORK ACCESS

Deploy port-level access control. Port-level access control should utilizes 802.1x, or similar network access control protocols, such as certificates, and should incorporate user and/or device authentication.

15.1.8 CENTRALIZE NETWORK AUTHENTICATION, AUTHORIZATION, AND AUDITING (AAA)

Centralize network AAA via a domain controller.

15.1.8.1 GROUP POLICY OBJECT (GPO) REVIEW

- GPOs should be reviewed on a quarterly basis.
- GPOs should be tested to ensure that they are working as designed.

15.1.9 FIREWALL

- All production web traffic should be routed through a web application firewall in order to access <<Company Name>>'s network environment.
- The firewall is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.
- Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists.
- Shutdown/disable Tor exit nodes
- Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone.
- Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network.
- Remote access requires two factor authentication.
- Internal addresses of externally available devices should be hidden or protected using network address translation (NAT).

15.1.10 CONTEMPORARY AND UP-TO-DATE NETWORK INFRASTRUCTURE

As a guideline, network-as-a-service (NaaS) offerings are preferred to dedicated network appliances. Dedicated network infrastructure should patched to stay current with the latest stable release of software / firmware. Patches should applied based on the company's patch policies and procedures.

15.1.11 REMOTE CONNECTIONS TO END USER DEVICES

Users must authenticate to enterprise-managed VPN and authentication services prior to accessing enterprise resources on end-user devices. DNS should be configured to utilize two-factor authentication.

15.1.12 REMOTE CONNECTIONS TO EXTERNAL NETWORKS

Remote connections to external networks require an IPsec Tunnel or dedicated ICMP circuit. Traffic transmitted or received via remote connections must be sent via a secure protocol that complies with the company's Encryption Policy. Remote connections should be specific protocols and ports.

15.1.13 DEDICATED COMPUTING RESOURCES

Applications and systems should be segregated on the network in order to isolate workloads and minimize resource contention. Access control policies should be enforced to ensure that only appropriate personnel are allowed access to resources.

15.1.14 CONTAINER SECURITY

Adopt immutable infrastructure practices with no human access to better meet your audit and compliance needs such as a lightweight secure image with a minimal set of dependencies necessary to satisfy your requirements. Installation of additional software that is not needed for the operation of the container should be prohibited. Container images should never be modified during runtime. Containers should use an Infrastructure as Code (IaC) methodology that leverages the SDLC.

Leverage a container security solution to maintain configuration consistency and perform scans. Reference "NIST Special Publication 800-190: Application Container Security Guide" for more information.

15.2 MONITORING AND ALERTS

Network monitoring enables visibility into activities occurring on the network and enables administration to manage network traffic. Network alerts call attention to aberrant activity or behaviors and help administrators to more quickly identify malicious activity.

15.2.1 DATAFLOW THRESHOLDS

The requisite Service Level Indicators and internal Service Level Objectives should be determined with stakeholders by consensus. This document is not proscriptive about what metrics are used to ensure that Support Level is maintained. At minimum, however, dataflow thresholds should be established, documented, and monitored at both the traffic layer and the solution layer. IT personnel should be alerted when thresholds have been exceeded.

15.2.2 FIREWALL CONFIGURATION FILE(S) MONITORING

Changes to <<Company Name>>'s firewall configuration generate alert notifications. Firewall rules are periodically certified by InfoSec on a quarterly basis.

15.2.3 CENTRALIZE SECURITY EVENT ALERTING

Use of a SIEM is required. See section on Audit Log Management for more detail.

15.2.4 NETWORK TRAFFIC FLOW LOGS

All network devices should be configured to publish Flow Logs to a SIEM, or other centralized log store for analysis / review.

15.2.5 NETWORK CAPACITY MONITORING

Network Administrators should monitor network capacity and ensure that traffic doesn't exceed capacity thresholds by configuring alerts.

15.2.6 ACCESS CONTROL FOR REMOTE ASSETS

Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.

15.2.7 SECURITY EVENT ALERTING THRESHOLDS

Security event alerting thresholds are tuned at least monthly by operations staff.

15.3 DEPLOY A HOST-BASED INTRUSION PREVENTION SOLUTION

Deploy a host-based intrusion prevention solution on enterprise assets, where appropriate and/or supported. Example implementations include use of an Endpoint Detection and Response (EDR) client or host-based IPS agent.

15.3.1 NETWORK INTRUSION PREVENTION SOLUTION (IPS)

A network intrusion prevention solution is deployed for defense-in-depth. Example implementations include the use of a Network Intrusion Prevention System (NIPS) or equivalent CSP service.

15.4 DEPLOY A HOST-BASED INTRUSION DETECTION SOLUTION

Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.

15.4.1 NETWORK INTRUSION DETECTION SOLUTION (IDS)

A network intrusion detection solution on enterprise assets is deployed for defense-in-depth. Example implementations include the use of a Network Intrusion Detection System (NIDS) or equivalent cloud service provider (CSP) service. The IDS is configured to notify personnel upon intrusion detection.

15.5 ESTABLISH AND MAINTAIN A SECURE NETWORK ARCHITECTURE

Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.

15.6 ESTABLISH AND MAINTAIN ARCHITECTURE DIAGRAM(S)

Establish and maintain architecture diagram(s) and/or other network system documentation. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

15.7 CENTRALIZE NETWORK AUTHENTICATION, AUTHORIZATION, AND AUDITING (AAA)

Centralize network AAA.

15.8 USE OF SECURE NETWORK MANAGEMENT AND COMMUNICATION PROTOCOLS

Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater).

16 APPLICATION LAYER

The ‘Application Layer’ refers to Layer 7 of the OSI model.

16.1 SECURITY

16.1.1 DNS MANAGEMENT

Manage DNS through a centralized application.

- DNS infrastructure must be secure, e.g. point origin attack, configure apex zone mapping if using a CDN.
- Configure DNS filtering services on all enterprise assets to block access to known malicious domains.
- Deny Traffic to/from OFAC entries.
- Kerberos should be configured to use NIST Time Servers via NTP from the root domain.
- Ensure enterprise assets are configured to use only enterprise-controlled DNS servers and/or reputable externally accessible DNS servers.
- Collect DNS query audit logs on enterprise assets, where appropriate and supported.

16.1.2 WEB ACCESS FIREWALL

Use a WAF or Firewall as a Service (FWaaS) to provide additional protection against malicious traffic: e.g. block Tor exist nodes, configure content filtering to prevent code injection, DDOS protection, etc.

16.1.3 CLOUD ACCESS SECURITY BROKER (CASB)

Outbound request from the production system should be routed through a CASB.

16.1.4 CONTENT DELIVERY NETWORK (CDN)

Inbound requests should be cached at the BGP layer via reverse proxy to mitigate DDOS.

16.1.5 API SECURITY

16.1.5.1 API GATEWAY

Incorporate an API Gateway as an abstraction in front of your APIs. API Gateway provides including traffic management, CORS support, authorization and access control, throttling, monitoring, and API version management.

16.1.5.2 OPENID CONNECT (OIDC)

Leverage OIDC for authentication.

16.2 MONITORING AND ALERTS

16.2.1 PERFORMANCE MONITORING

Application performance is monitored via software telemetry systems. The following information is used to evaluate system performance.

- HTTP Request and Response times are evaluated to ensure that the system is performing within acceptable tolerance limits.
- Unplanned outages are recorded and used to establish an SLA.
- CPU utilization, thread pool utilization, etc. is monitored to ensure that the application is utilizing machine resources efficiently.

16.2.2 APPLICATION EXCEPTION LOGS

Each application server is configured to log event messages via NLog depending on the event category. Log events are sent to one or more of four channels: UDP broadcast, the server's event log, a database log table, and Sentry—sentry.io is a logging cloud provider. Log data is stored for 180 days.

16.2.3 ALERTING

<<Company Name>> monitors and receives alerts from the following different systems.

1. <<Operations Alert System>>: Operational alerts from our production system.
2. Sentry: Application errors from our production system.
3. Amazon Web Services CloudWatch
4. Security alerts from vSOC (Virtual Security Operations Center)

Monitoring and alerting systems should be consistently available 24x7x365. Each sprint a developer is assigned as the sprint's PBM (Problem Management) queue boss. We use <<Incident Management Tool>> to notify our PBM queue boss whenever an exception is thrown by our system, or when a threshold has been exceeded. <<Incident Management Tool>> sends notification alerts via SMS. The job of PBM queue boss is to investigate, triage and remediate the exceptions in our production application. If the PBM queue boss is unable to remediate an issue he / she is supposed to escalate to the team at large. In the event that a PBM queue boss does not receive a message or fails to escalate <<Incident Management Tool>> will escalate the event to the team.

17 HOST BASED SECURITY

Host based security provides defense in-depth for network base security. Host based security applies to servers.

17.1 MINIMALISM

- Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.
- An ideal configuration is headless.
- All unused ports and protocols should be switched off by default.

17.2 HOST-BASED FIREWALLS

Implement and manage a firewall on servers, where supported.

17.3 HOST-BASED INTRUSION DETECTION SOLUTION (IDS)

Deploy a host-based intrusion detection solution on servers, where appropriate and/or supported.

17.4 MALWARE PROTECTION

Anti-malware software must be deployed on all servers. Ensure that automatic updates are configured for anti-malware signature. The antivirus software should be configured to perform scanning of workstations and servers in real time and scheduled scanning on workdays.

17.5 REMOVABLE MEDIA

Disable removable media and configure anti-malware software to automatically scan removable media.

17.6 DEFAULT ACCOUNTS

Disable unnecessary default and pre-configured vendor accounts.

17.7 DNS CONFIGURATION

Configure servers and workstations to use only enterprise-controlled DNS servers and/or reputable externally accessible DNS servers.

17.8 HOST-BASED INTRUSION PREVENTION SOLUTION

Manage servers and workstations via an Endpoint Detection and Response (EDR) or eXtended Detection & Response (XDR) system.

18 CAPACITY MANAGEMENT

<<Company Name>> monitors information processing systems to ensure that servers are tuned and assessed on an ongoing basis to ensure adequate capacity is available to perform required tasks. Monitoring software is configured to alert operations staff when system thresholds are being exceeded, or when performance degradation is occurring.

Periodically, systems are tested to ensure that they have adequate capacity for ten (10) times their normal traffic load. Future processing capacity is forecast at least annually to ensure that <<Company Name>> is able to accommodate anticipated demands on infrastructure. Management reviews annual forecast and incorporates forecasts into financial planning.

18.1 PROCESSING

Ensure that resources available for processing can handle bursts in demand. For systems that are not elastically scalable you should have capacity and budget for peak demand for at least six months at any given point in time.

18.2 READ / WRITE OPERATIONS

Ensure that resources available for read and writing data can handle peak demand. For systems that are not elastically scalable you should have capacity and budget for peak demand for at least six months at any given point in time.

18.3 STORAGE

Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management processes. For systems that are not elastically scalable you should have capacity and budget to account for at least three months of projected storage.

19 SEPARATION OF ENVIRONMENTS

<<Company Name>> maintains clean abstraction between different operating environments. Development, Test and Production maintain no scope overlap. Customer information is confined solely to <<Company Name>>'s production environment. For more information please reference <<Company Name>>'s SDLC document.

As a principle of design all data in Production environments is treated as if it's confidential — This implies that the data is encrypted at rest and in transit. When data is used in lower environments the PII is elided or removed entirely as per the SDLC.

20 INFORMATION TRANSFER

20.1 INFORMATION TRANSFER POLICIES AND PROCEDURES

1. Information should exchanged between parties should adhere to guidance provider in the company's Data Classification Policy.
2. Information stored on company assets must comply with the company's Data Retention Policy.
3. Information exchanged with third parties must adhere to the company's Encryption Policy.
4. Rules of information exchange shall comply with all applicable laws or regulations as determined by the Chief Compliance Officer, or executive management.
5. PII or restricted information should never be shared or migrated to a non-production environment.

20.2 AGREEMENTS ON INFORMATION TRANSFER

1. The exchange of Confidential information between the company and external third parties shall be subject to the formation of an agreement between the parties.
2. The agreement shall address the following:
    1. Security rules and requirements for the exchange
    2. Procedures to ensure traceability and non-repudiation
    3. Technical requirements for information transmission. Procedures for notifying both sender and recipient when a fault occurs. Responsibilities and roles in the event of an information security incident.
3. Exchange agreements may be included in contracts, conditions of employment or service agreements; if so stated, separate formal documentation is not required.
4. No agreement is required in situations where all inbound and outbound traffic is encrypted.

20.3 ELECTRONIC MESSAGING

1. Information involved in electronic messaging shall be appropriately protected as per the company's Encryption Policy.

20.4 CONFIDENTIALITY AND NONDISCLOSURE AGREEMENTS

1. The organization shall identify and regularly review the requirements for confidentiality or nondisclosure agreements on a quarterly basis.
2. All confidentiality and nondisclosure agreements must comply with relevant law and regulation for the jurisdiction where the agreement applies.

21 INFORMATION BACKUP

Information submitted to <<Company Name>> is archived in our system and indexed by its UTC date of insertion. Storing and indexing data in this way allows us to recreate the state of our system for any point in time. Our system uses RAID 1+0 SAN that is encrypted using AES256.

21.1 FILE SHARES AND IMAGES

Backups of file shares and images are completed nightly. Backup retention is set at 30 days and no fewer than 10 versions.

21.2 DATABASE BACKUPS

<<Company Name>> is committed to maintaining data for seven years. We do nightly full backups of our database and 5-minute snapshots of our transaction logs. DB backups are held for 7 days.

In the event that a backup job fails, the backup tool sends an alert to the PBM Queue Boss who investigates and resolves the failure.

21.3 CLOUD BACKUPS

DB backups and file backups are periodically encrypted and stored in S3. Backups are retained for two weeks.

22 DATA LOSS PREVENTION

22.1 PERIPHERAL CONTROL POLICY

Peripheral control allows us to control access to computer peripherals and removable media. As a policy, <<Company Name>> does not permit connecting any type of peripheral to user workstations, with two noted exceptions:

1. Wireless connectivity using 802.11b/a/g/n protocols.
2. MTP/PTP protocol so that users may charge their phones when connected to a USB port on the computer. While this exception allows users to charge their phones, it does not permit them to mount their internal phone disk as a volume.

22.2 DATA LOSS PREVENTION POLICY

Data Loss Prevention (DLP) policies allow <<Company Name>> to prevent accidental data loss. DLP policies include one or more rules that specify conditions and actions to be taken when the rule is matched. <<Company Name>> DLP rules check for the following types of information:

1. Personal Identification Numbers
2. Personal or Banking Identifiers with Contact Details

23 EMAIL GATEWAY SECURITY

23.1 EMAIL SERVER CONFIGURATION

1. Deploy and maintain email server anti-malware protections, such as attachment scanning and/or sandboxing.
2. Block Unnecessary filetypes at the gateway.

23.2 DMARC

To lower the chance of spoofed or modified emails from valid domains, implement DMARC policy and verification, starting with implementing the Sender Policy Framework (SPF) and the DomainKeys Identified Mail (DKIM) standards.

24 SECURITY REQUIREMENTS OF INFORMATION SYSTEMS

24.1 INFORMATION SECURITY REQUIREMENTS ANALYSIS AND SPECIFICATION

1. Security requirements for all new information systems, and all systems which have been significantly modified, shall be established by appropriate analysis and incorporated into the system specifications.
2. The Information Security Program should act as a Subject Matter Expert regarding security requirements, providing consulting services as needed.
3. Security requirements shall reflect the business value of the assets and potential harm if the system were compromised.
4. Purchased information processing products, whether hardware or software, shall be evaluated for security risk and mitigating controls established as needed.

24.2 SECURING APPLICATION SERVICES ON PUBLIC NETWORKS

1. Information published on publicly available systems (e.g., public web sites) shall be protected against unauthorized modification.
2. Publicly available systems shall be tested for vulnerabilities and failures prior to deployment and re-tested on a regular schedule thereafter.
3. Access to publicly available systems shall not allow unintended access to the networks and resources connected to the system.
4. The level of protection assigned to all information exchanged shall maintain the confidentiality and integrity of the subject information, regardless of form.
5. Electronic commerce arrangements between trading partners shall be supported by a documented agreement which commits both parties to the agreed terms of trading, including authorizations. Terms and conditions applicable to electronic commerce services shall comply with applicable law and regulation.
6. Information involved in software development passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.

24.3 PROTECTING APPLICATION SERVICES TRANSACTIONS

1. Information involved in on-line transactions shall be protected in a manner commensurate with the sensitivity of the information.
2. The user credentials of all parties in a transaction shall be validated.
3. Transactions shall protect both confidentiality and privacy of all aspects of the transaction.
4. Communication paths between the parties to the transaction shall be encrypted.

5. Transaction information shall not be stored in a publicly accessible environment (e.g. DMZ or Internet-accessible locations).
6. Transactions shall be conducted in compliance with all applicable law and regulations in the jurisdictions where the transaction originates, is processed, fulfilled and/or stored.

25 PENETRATION TESTING

Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker. Penetration testing should be performed by a third-party service provider.

25.1 PENETRATION TESTING PROGRAM

Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the enterprise. Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements.

25.2 EXTERNAL PENETRATION TESTS

Perform periodic external penetration tests based on program requirements at least annually. External penetration testing must include enterprise and environmental reconnaissance to detect exploitable information. Penetration testing requires specialized skills and experience and must be conducted through a qualified third party. Testing should be performed at least annually. The testing may be clear box or opaque box.

25.3 PENETRATION TEST FINDINGS

Remediate penetration test findings based on the timeframes stipulated for Corrective Actions in the Enterprise Risk Policy.

25.4 VALIDATE SECURITY MEASURES

Validate security measures after each penetration test. If deemed necessary, modify rulesets and capabilities to detect the techniques used during testing. Perform purple testing if necessary.

25.5 INTERNAL PENETRATION TESTS

Perform periodic internal penetration tests based on program requirements, no less than annually. The testing may be clear box or opaque box.

26 CONTACT INFORMATION

Name of Security Program Owner

Title of Security Program Manager

Phone Number

Email

27 DOCUMENT RACI

Responsible	Assigned to do the work	Security Program Manager
Accountable	Final decision, ultimately answerable	ISM Governance Committee
Consulted	Consulted BEFORE an action or decision is taken (proactive)	Executive Management
Informed	Informed AFTER a decision or action has been taken (reactive)	Named Participants in this document Other parties affected by the change

28 LICENSE INFORMATION

APPENDIX A: EXECUTIVE MEETING MINUTES TEMPLATE

<<Company Name>>'s Meeting Minutes

Facilitator:		Date: 20XX-XX-XX

Opening

The regular meeting of the Organization/Committee Name was called to order at time on date in location by Facilitator Name.

Attendance

A list of the members invited and whether or not they’re present. Executive management and operational management should both be present.

Name of Member	Role	Present (Y/N)

Agenda

The agenda should include a review of:

- the ISMS program;
- business plans;
- strategic objectives;
- budgets; and,
- roles and responsibilities.

Item #	Agenda Item	Description (optional)

Review of Minutes

The minutes of the previous meeting should be reviewed.

Open Issues

Summarize the discussion for each existing issue, state the outcome, and assign any action item.

Action Item	Next Steps	Assigned to

Adjournment

Meeting was adjourned at time by Facilitator Name. The next general meeting will be at time on date, in location.

Minutes submitted by:	Approved by:	Date: 20XX-XX-XX

Date of next meeting: **20XX-XX-XX**