Operations Security Policy

Policy Owner: Leonard Henriquez

Effective Date: December 22, 2022

Purpose

To ensure the correct and secure operation of information processing systems and facilities.

Scope

All Capsule SAS information systems that are business critical and/or process, store, or transmit company data. This Policy applies to all employees of Capsule SAS and other third-party entities with access to Capsule SAS networks and system resources.

Operations Security

Documented Operating Procedures

Both technical and administrative operating procedures shall be documented as needed and made available to all users who need them.

Change Management

Changes to the organization, business processes, information processing facilities, production software and infrastructure, and systems that affect information security in the production environment and financial systems shall be tested, reviewed, and approved prior to production deployment. All significant changes to in-scope systems and networks must be documented.

Change management processes shall include:

- Processes for planning and testing of changes, including remediation measures
- Documented managerial approval and authorization before proceeding with changes that may have a significant impact on information security, operations, or the production platform
- Advance communication/warning of changes, including schedules and a description of reasonably anticipated effects, provided to all relevant internal and external stakeholders
- Documentation of all emergency changes and subsequent review
- A process for remediating unsuccessful changes

Capacity Management

The use of processing resources and system storage shall be monitored and adjusted to ensure that system availability and performance meets Capsule SAS requirements.

Human resource skills, availability, and capacity shall be reviewed and considered as a component of capacity planning and as part of the annual risk assessment process.

Scaling resources for additional processing or storage capacity, without changes to the system, can be done outside of the standard change management and code deployment process.

Separation of Development, Staging and Production

Environments

Development and staging environments shall be strictly segregated from production SaaS environments to reduce the risks of unauthorized access or changes to the operational environment. Confidential production customer data must not be used in development or test environments without the express approval of the COO.

Refer to the Data Management Policy for a description of Confidential data. If production customer data is approved for use in the course of development or testing, it shall be scrubbed of any such sensitive information whenever feasible.

Systems and Network Configuration, Hardening, and Review

Systems and networks shall be provisioned and maintained in accordance with the configuration and hardening standards described in Appendix A to this policy.

Firewalls and/or appropriate network access controls and configurations shall be used to control network traffic to and from the production environment in accordance with this policy.

Production network access configuration rules shall be reviewed at least annually. Tickets shall be created to obtain approvals for any needed changes.

Protection from Malware

In order to protect the company's infrastructure against the introduction of malicious software, detection, prevention, and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.

Anti-malware protections shall be utilized on all company-issued endpoints except for those running operating systems not normally prone to malicious software. Additionally, threat detection and response software shall be utilized for company email. The anti-malware protections utilized shall be capable of detecting all common forms of malicious threats and performing the appropriate mitigation activity (such as removing, blocking or quarantining).

Capsule SAS should scan all files upon their introduction to systems, and continually scan files upon access, modification, or download. Anti-malware definition and engine updates should be configured to be downloaded and installed automatically whenever new updates are available. Known or suspected malware incidents must be reported as a security incident.

It is a violation of company policy to disable or alter the configuration of anti-malware protections without authorization.

Information Backup

The need for backups of systems, databases, information and data shall be considered and appropriate backup processes shall be designed, planned and implemented. Backup procedures must include procedures for maintaining and recovering customer data in accordance with documented SLAs. Security measures to protect backups shall be designed and applied in accordance with the confidentiality or sensitivity of the data. Backup copies of information, software and system images shall be taken regularly to protect against loss of data. Backups and restore capabilities shall be periodically tested, not less than annually.

Backups must be stored separately from the production data location. Backups must not be editable. Backups must not be removable within the retention policy timeframe. The retention policy is:

- Keep at least one backup per day over the last month

- Keep at least one backup per week over the last year
- Keep at least one backup per month over the last 10 years

Capsule SAS does not regularly backup user devices like laptops. Users are expected to store critical files and information in company-sanctioned file storage repositories.

Backups are configured to run daily on in-scope systems. The backup schedules are maintained within the backup application software.

A backup restore test should be performed at least annually to validate the backup data and backup process.

Logging & Monitoring

Production infrastructure shall be configured to produce detailed logs appropriate to the function served by the system or device. Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and reviewed through manual or automated processes as needed. Appropriate alerts shall be configured for events that represent a significant threat to the confidentiality, availability or integrity of production systems or Confidential data.

Logging should meet the following criteria for production applications and supporting infrastructure:

- Log user log-in and log-out
- Log CRUD (create, read, update, delete) operations on application and system users and objects
- Log security settings changes (including disabling or modifying of logging)
- Log application owner or administrator access to customer data (i.e. Access Transparency)
- Logs must include user ID, IP address, valid timestamp, type of action performed, and object of this action.
- Logs must be stored for at least 30 days, and should not contain sensitive data or payloads

Protection of Log Information

Logging facilities and log information shall be protected against tampering and unauthorized access.

Administrator & Operator Logs

System administrator and system operator activities shall be logged and reviewed and/or alerted in accordance with the system classification and criticality.

Data Restore Logs

In the event the company needs to restore production data containing PII from backups, either for the purposes of providing services or for testing purposes, shall be logged or tracked in auditable tickets.

Clock Synchronization

The clocks of all relevant information processing systems within an organization or security domain shall be synchronized to network time servers using reputable time sources.

File Integrity Monitoring and Intrusion Detection

Capsule SAS production systems shall be configured to monitor, log, and self-repair and/or alert on suspicious changes to critical system files where feasible.

Alerts shall be configured for suspicious conditions and engineers shall review logs on a regular basis.

Unauthorized intrusions and access attempts or changes to Capsule SAS systems shall be investigated and remediated in accordance with the Incident Response Plan.

Control of Operational Software

The installation of software on production systems shall follow the change management requirements defined in this policy.

Technical Vulnerability Management

Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities shall be evaluated, and appropriate measures taken to address the associated risk. A variety of methods shall be used to obtain information about technical vulnerabilities, including vulnerability scanning, penetration tests, review of external vendor alerts, and the bug bounty program.

Vulnerability scans shall be performed on public-facing systems in the production environment at least quarterly.

Penetration tests of the applications and production network shall be performed at least annually, and additional scanning and testing shall be performed following major changes to production systems and software.

The Engineering departments shall evaluate the severity of vulnerabilities identified from any source, and if it is determined to be a risk-relevant critical or high-risk vulnerability, a service ticket will be created. The Capsule SAS assessed severity level may differ from the level automatically generated by scanning software or determined by external researchers based on Capsule SAS's internal knowledge and understanding of technical architecture and real-world impact/exploitability. Tickets are assigned to the system, application, or platform owners for further investigation and/or remediation.

Vulnerabilities assessed by Capsule SAS shall be patched or remediated in the following timeframes:

Determined Severity	Remediation Time
Critical	30 Days
High	30 Days
Medium	60 Day
Low	90 Days
Informational	As needed

Service tickets for any vulnerability which cannot be remediated within the standard timeline must show a risk treatment plan and planned remediation timeline.

Restrictions on Software Installation

Rules governing the installation of software by users shall be established and implemented in accordance with the Capsule SAS Information Security Policy.

Information Systems Audit Considerations

Audit requirements and activities involving verification of operational systems shall be carefully

planned and agreed to minimize disruptions to business processes.

Systems Security Assessment & Requirements

Risks shall be considered prior to the acquisition of, or significant changes to, systems, technologies, or facilities. Where requirements are formally identified, any relevant security requirements shall be included. The acquisition of new suppliers and services shall be made in accordance with the Third-Party Management Policy.

The company shall perform an annual network security assessment that includes a review of major changes to the environment such as new system components and network topology.

Exceptions

Requests for an exception to this policy must be submitted to the CTO for approval.

Violations & Enforcement

Any known violations of this policy should be reported to the CTO. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.

Version	Date	Description	Author	Approved by
1.0	22-dec-2022	First Version	Léonard Henriquez	Dan Elkaïm

APPENDIX A - Configuration and Hardening Standards

Configuration and hardening standards shall be maintained on the internal documentation portal.

https://www.notion.so/capsulespace/

Include links to external sources, or internally created samples:

https://aws.amazon.com/compliance/resources/

Address baseline config management and deployment per control 3.4, 7.1

Servers and Virtual Machines

This is the standard for system-level server and virtual server (VM) configuration hardening. Some customization to these settings may be required to configure the system for its specific target environment, such as setting the proper names, groups, authentication settings, and other personalization options.

In addition to the requirements to secure systems to the baseline outlined above, all physical and virtual systems must adhere to the following technical requirements:

- All vendor defaults (including default passwords on operating systems, software providing

security services, application and system accounts, Simple Network Management Protocol (SNMP) community strings, etc.) must be changed before a system is installed on the network.
- Unnecessary default accounts (including accounts used by operating systems, security software, applications, systems, SNMP, etc.) must be removed or disabled before a system is installed on the network.
- Only one primary function may be implemented per server or virtual machine to prevent functions that require different security levels from coexisting on the same system.
- Only necessary services, protocols, daemons, etc., may be enabled, and only as required for the function of the system. All unnecessary functionality (such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers) must be disabled
- Additional security features for any required services, protocols or daemons that are considered to be insecure must be documented in Appendix B of this document, justified, and tested to ensure that they do not introduce unnecessary risk or vulnerabilities.
- All security patches identified as critical must be applied to systems within SLAs established in this policy.

Network Standards

- Management of network rules and settings may only be performed by authorized members of Engineering team and all changes must comply with change Management procedures defined in the Operations Security Policy.
- Network diagrams must be created and kept current. Significant changes (additions or deletions to VPCs and subnets, new external connections, etc.) must be documented in the diagrams; even if no changes occurred, the diagrams will be reviewed at least annually for completeness and accuracy, and approved/acknowledged (in version number/date field etc.) by authorized members of Engineering team.
- Supported network controls for production networks are AWS NACLs. Management of production network systems is accomplished through the use of the AWS console.
- In the production environment, defined rules and configurations must be enforced to control traffic from untrusted networks (e.g. publicly available services) to internal production networks; additionally, rules must be in place to restrict traffic to and from production networks to untrusted networks, and all inbound and outbound traffic must be evaluated by the the traffic management configuration.
- Network control systems must be configured to use default Network Address Translation to prevent the disclosure of internal IP addresses to the Internet. If private IP addresses are used, any disclosure to external parties must be appropriately authorized, documented, and periodically reviewed for business necessity.
- Mobile devices connecting to production networks must employ the use of a personal firewall or equivalent (such as endpoint protection with network restrictions enabled). Disabling or bypassing personal firewalls while connected to Capsule SAS systems is prohibited. Personal firewalls must be configured to specific standards, including: disabling the use of split tunneling, configurations to block known malicious sites, blocking of insecure protocols.
- All network control systems must be configured with default antispoofing rules to block or deny inbound internal addresses originating from the Internet
- Network control systems may only allow established connections into the internal network and must deny any inbound connections not associated with a previously established session.
- External configurations must limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.
- Port and IP ranges are prohibited unless specifically reviewed and justified; all available services must be justified, and support secure configurations, all other ports, services, and network traffic must be specifically denied.
- Use of insecure services and protocols without justification and documentation of additional security features implemented to mitigate risk is prohibited.
- Remote access sessions must be configured to enforce timeout after a specified period of (X hours).

- Remote-access technologies for vendors and business partners used to access production systems must be enabled only when needed for business purposes and immediately deactivated after use.
- Any hybrid networks with both cloud and on-premise access shall be scanned and tested at least annually to ensure that security requirements are maintained

Specific NACLs, ports, zones, and services allowed in and out of the production environment are defined below: Rules and allowed traffic must be evaluated at least annually and formally approved by the Tech Team:

Source Zone	Dest. Zone	Service	Action	Purpose
Trusted zone (VPN protected)	Internal resources	SSH HTTPS	Permit	Allow management host access
Any	External facing resources	HTTP HTTPS	Permit	Allow inbound web services from the Internet
Any	Internal resources	Any	Deny	Default deny all