Operations Security Policy

Policy Owner: CareValidate, Inc.

Effective Date: 8/1/2022

Purpose

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

CareValidate Key Personnel Hierarchy

Chief Executive Officer

Chief Operating Officer

Chief Technology Officer – pending

Chief Information Officer – pending

Senior VP of Engineering – the person in this position is the default IT Manager unless otherwise designated by any of the above officers

Legal Lead

Scope

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

Operations Security

Documented Operating Procedures

Operating procedures shall be documented and made available to all users who need them.

Change Management

Changes to the organization, business processes, information processing facilities, and systems that affect information security in the production environment and financial systems shall be controlled. All significant changes to in-scope systems 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 CareValidate 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 and/or CIO/CTO.

For a full description, see 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 Configuration, Hardening, and Review

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

Firewalls shall be used to control traffic to and from the production environment in accordance with this policy.

Production firewall 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 employee issued laptops 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.

CareValidate should scan all files upon their introduction to systems, and continually scan files upon access, modification, or download. Anti-malware definition 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. 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.

CareValidate 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, GCP.

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.

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.

File Integrity Monitoring and Intrusion Detection

CareValidate 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 CareValidate 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, and the bug bounty program.

External vulnerability scans shall be run on the production environment at least quarterly. Interior vulnerability scans shall be run against test environments which mirror production configurations.

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

The Engineering department shall evaluate the severity of vulnerabilities, and if it is determined to be a critical or high-risk vulnerability, a service ticket will be created. The CareValidate assessed severity level may differ from the level automatically generated by scanning software or determined by external researchers based on CareValidate’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 CareValidate shall be 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 CareValidate 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.

Exceptions

Requests for an exception to this policy must be submitted to the IT Manager and/or COO for approval.

Violations & Enforcement

Any known violations of this policy should be reported to the IT Manager and/or COO. 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	8-1-2022	v.1	JMB-Legal DT-Engineering	JC-COO

APPENDIX A - Configuration and Hardening Standards

The company operates in the GCP environment.

Configuration and hardening standards shall be maintained as follows:

Network Hardening

- Firewall configuration
- Limit users and secure access points
- Block unnecessary network ports
- Disallow anonymous access

Application Hardening

- Application access control
- Remove default passwords
- Implement password best practices
- Configure account lockout policy

Database Hardening

- Implement admin restrictions on access
- Encrypt data entering and leaving the database
- Remove unused accounts

Operating System Hardening

- Apply necessary updates and patches automatically
- Remove unnecessary files, libraries, drivers and functionality
- Log all activity, errors and warnings
- Limit sharing and system permissions
- Configure file system and registry permissions