Vulnerability Management Policy

Non-Disclosure Statement:

HealthEdge Software, Inc.
30 Corporate Drive
Burlington, MA 01803

Table of Contents

1 Objective

1.1 Purpose

The purpose of this policy is to establish the requirements for mitigating and/or remediation of known vulnerabilities for Information Assets as well as managing risk and performing penetration testing. Failure to abide by this policy may result in monetary loss, criminal or civil penalties, failure to meet compliance requirements, or impact to market perception and loss of brand value.

1.2 Scope

This Policy applies to all global HealthEdge Information Users who are authorized to access HealthEdge information systems that are owned or controlled by HealthEdge and used to support its business processes.

1.3 Management Commitment

The management of HealthEdge is committed to providing a safe and secure service to our customers. We understand the importance of protecting our customers' covered information and company assets from cybersecurity attacks. We have implemented cybersecurity measures and continuously assess and update them to align with industry standards and best practices. Our HealthEdge Users are trained and held accountable for adhering to our cybersecurity policies and complying with the industry standards and regulations.

1.4 Roles & Responsibilities

Role/Title	Responsibility
Chief Information Security Officer (CISO)	• Develop and maintain the Vulnerability Management Policy.
Information Security Team	• Implement and maintain vulnerability management tools. • Work closely with Information Technology Teams to address vulnerabilities found within the defined timeline.
Information Technology (IT) Teams	• Address vulnerabilities captured in the vulnerability management tools. • Work with Information Security Team on any vulnerabilities that cannot be remediated timely.

1.5 Applicable Law, Standards, and Regulator Requirements

This document has been implemented as mandated by and/or in support of the following applicable law(s), standard(s) or regulatory requirement(s):

- HITRUST Cybersecurity Framework (CSF) v11.3.0
- HIPAA Security Rule
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, rev 5, Security and Privacy Controls for Information Systems and Organizations
- NIST SP 800-66, rev 2, Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide

2 Policy

- Review and update the Vulnerability Management Policy at least every year and following any HealthEdge-defined events (e.g., assessment or audit findings or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines).

2.1 Inventory of Assets

- Identify and inventory all assets including information (e.g., PII), encrypted or unencrypted, wherever it is created, received, maintained, or transmitted (including organizational and third-party sites).
- Document the importance of these inventoried assets. The asset inventory includes:
    - All systems connected to the network.
    - The network devices themselves.
    - Desktops.
    - Servers.
    - Network equipment (routers, switches, firewalls, etc.).
    - Printers.
    - Storage area networks.
    - Voice Over-IP telephones.
    - Multi-homed addresses.
    - Virtual addresses.
    - Mobile phones, regardless of whether they are attached to HealthEdge's network.
    - Tablets, regardless of whether they are attached to HealthEdge's network.
    - Laptops, regardless of whether they are attached to HealthEdge's network.

    - Other portable electronic devices (i.e., other than mobile phones, tablets, and laptops) that store or process data, regardless of whether they are attached to HealthEdge's network.
    - Approved bring your own device (BYOD) equipment.
- Organizational inventories of IT assets are periodically (annually at minimum) reviewed to ensure completeness and accuracy. The asset inventories include:
    - Type or classification of the asset.
    - Format of the asset.
    - Location of the asset.
    - Backup information of the asset.
    - License information of the asset.
    - A business value of the asset.
    - Data on whether the device is a portable and/or personal device.
- The asset inventory record is used to document and ensure that all property is returned to HealthEdge upon employee termination or transfer out of the organization or department. The asset inventory records:
    - The network addresses.
    - The machine name(s).
    - The purpose of each system.
    - An asset owner responsible for each device.
    - The department associated with each device.
- The inventory does not duplicate other inventories unnecessarily, but it will ensure that the content is aligned.
- Records of property assigned to employees is reviewed and updated annually.
- Create, document, and maintain a process and procedure to physically inventory capital assets (at least annually), physically inventory non-capital assets, reconcile IT asset inventory information on hand for capital assets, and reconcile IT asset inventory information on hand for non-capital assets.
- Organizational inventories of IT assets are updated during installations, equipment removals, system changes. The asset inventory includes the:
    - Unique identifier and/or serial number of the IT asset.
    - Information system of which the component is a part.
    - Type of information system component (e.g., server, desktop, application).
    - Manufacturer/model information of the IT asset.
    - Operating system type and version/service pack level of the IT asset.
    - Presence of virtual machines.
    - Application software version/license information.
    - Physical location (e.g., building/room number) of the IT asset.
    - Logical location (e.g., IP address, position with the IS architecture) of the IT asset.
    - Media access control (MAC) address of the IT asset.

    - Data ownership and custodian by position and role.
    - Operational status of the IT asset.
    - Primary and secondary administrators of the IT asset.
    - Primary user of the IT asset.
- The ownership, custodianship, and information classification is agreed upon and documented for each of the assets.
- The ownership, custodianship, and information classification is based on the identified importance of the asset, the business value of the asset, security classification of the asset, levels of protection of the asset, and sustainment commensurate with the importance of the assets.
- The inventory of assets identifies protection and sustainment requirements commensurate with the asset's categorization.
- The information lifecycle manages the secure use, transfer, exchange, and disposal of IT-related assets.
- Maintain an inventory of authorized wireless access points (WAPs). The inventory of WAPs includes a documented business justification and supports unauthorized WAP identification and response.
- If HealthEdge assigns organization-owned property to contractors, the procedures for assigning and monitoring the use of the property are included in the contract.
- If HealthEdge-owned property is assigned to volunteer workers, there is a written agreement specifying:
    - How the property will be inventoried.
    - When the property will be inventoried.
    - How it is returned upon completion of the volunteer assignment.
- Create and document the process/procedure HealthEdge intends to use for deleting data from hard-drives prior to property transfer, exchange, or disposal/surplus.
- The IT asset lifecycle program is monitored to ensure it effectively addresses all six stages of the lifecycle:
    - **Planning** - defining supporting processes, setting standards for configuration and retention, aligning purchase plans to business goals, collecting aggregate information on intended purchases, and negotiating volume discounts.
    - **Procurement** - requisitioning, approving requisitions, ordering, receiving, and validating orders.
    - **Deployment** - tagging assets, entering asset information in a repository, configuring and installing assets including: disabling unnecessary or insecure services or protocols, limiting servers to one primary function, and defining system security parameters to prevent misuse.
    - **Management** - inventory/counting, monitoring usage (some software), managing contracts for maintenance and support, and monitoring age and configuration.

    - **Support** - adding and changing configurations, repairing devices, and relocating equipment and software.
    - **Disposition** - removing assets from service, deleting storage contents, disassembling components for reuse, surplussing equipment, terminating contracts, disposing of equipment, and removing assets from active inventory.
- Employ automated mechanisms to scan the network no less than weekly to detect the presence of unauthorized components/devices (including hardware, firmware, and software) into the information system.
- Disable network access by such components/devices and notify designated HealthEdge officials of such unauthorized components/devices.
- Provide each update of the inventory identifying assets with Private or Confidetial information (e.g., PII) to the CISO or information security official, and the senior privacy official on a HealthEdge-defined basis, but no less than annually, to support the establishment of information security requirements for all new or modified information systems containing this information.

2.2 Security of System Documentation

- The access list for system documentation is kept to a minimum and is authorized by the application owner.

2.3 Input Data Validation

- Develop applications based on secure coding guidelines to prevent:
    - Common coding vulnerabilities in software development processes.
    - Injection flaws, particularly SQL injection (Validate input to verify user data cannot modify meaning of commands and queries, utilize parameterized queries, etc.).
    - Buffer overflow (Validate buffer boundaries and truncate input strings).
    - Insecure cryptographic storage (Prevent cryptographic flaws).
    - Insecure communications (Properly encrypt all authenticated and sensitive communications).
    - Improper error handling (Do not leak information via error messages).
    - Broken authentication/sessions (Prevent unauthorized individuals from compromising legitimate account credentials, keys or session tokens that would otherwise enable an intruder to assume the identity of an authorized user).
    - Cross-site scripting (XSS), e.g., validate all parameters before inclusion, utilize context-sensitive escaping, etc.).

  - Improper access control, such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access functions (e.g., properly authenticate users and sanitize input, and do not expose internal object references to users).
  - Cross-site request forgery (CSRF), e.g., do not reply on authorization credentials and tokens automatically submitted by browsers.
  - Any other input-validation vulnerability listed in the OWASP Top 10.
- Applications which store, process or transmit Private or Confidential information undergo automated (non-manual) application vulnerability testing with an emphasis on input validation controls at least annually by a qualified party.
- The information system checks the validity of organization-defined information inputs for accuracy, completeness, validity, and authenticity as close to the point of origin as possible.
- For in-house developed software, ensure that explicit error checking is:
  - Performed and documented for all input.
  - Performed which includes checking the input size.
  - Performed which includes checking the input data type.
  - Performed which includes checking the input acceptable ranges or formats.
- Procedures, guidelines, and standards for the development of applications are periodically reviewed, assessed, and updated as necessary by the appointed senior-level information security official of HealthEdge.

2.4 Control of Technical Vulnerabilities

- Once a potential technical vulnerability has been identified, HealthEdge identifies the associated risks and the actions to be taken. Further, HealthEdge performs the necessary actions to correct identified technical vulnerabilities in a timely manner.
- Deploy automated software update tools in order to ensure that systems are running the most recent security updates provided by the software vendor, and install software updates manually for systems that do not support automated software updates.
- Information Assets are periodically scanned to proactively (annually at minimum) identify technical vulnerabilities.
- Only necessary and secure services, protocols, daemons, etc., required for the function of the system are enabled.
- Security features are implemented for any required services, protocols or daemons that are considered to be insecure (e.g., use secured technologies such as SSH, S-FTP, TLS v1.2 or later, or IPsec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, FTP, etc.).
- Regularly compare the results from consecutive vulnerability scans to verify that vulnerabilities have been remediated in a timely manner.

- The configuration standard for all system components (workstations, databases, servers, applications, routers, switches, wireless access points) are hardened to address, to the extent practical, all known security vulnerabilities.
- Laptops, workstations, and servers are configured so they will not auto-run content from removable media (e.g., USB tokens–thumb drives, USB hard drives, CDs/DVDs, FireWire devices, external serial advanced technology attachment devices, and mounted network shares).
- Configuration standards are consistent with industry-accepted system hardening standards (e.g., CIS, ISO, NIST, SANS).
- A prioritization process is required to determine which patches must be applied across HealthEdge's systems.
- Require patches installed in the production environment to also be installed in HealthEdge's disaster recovery environment in a timely manner, as defined by HealthEdge.
- Define and establish the roles and responsibilities associated with technical vulnerability management, including vulnerability monitoring, vulnerability risk assessment, patching, asset tracking, and any coordination responsibilities required.
- Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities which considers the CVSS score, classification of the vendor supplied patch, and/or the classification and criticality of the affected system.
- Ensure internal and external vulnerability assessments of sensitive information systems, virtualized, and networked environments, including both network- and application-layer tests, are performed by a qualified individual on a quarterly basis and after any significant change in the network.
- Security vulnerability assessment tools or services accommodate the virtualization technologies used by HealthEdge (e.g., virtualization aware).
- Patches are tested and evaluated before they are installed to ensure they are effective and do not result in side effects that cannot be tolerated.
- The technical vulnerability management process is evaluated on a quarterly basis in order to ensure its effectiveness and efficiency.
- Information resources (including tools and vulnerability mailing lists/other information sources), that will be used to identify relevant technical vulnerabilities and/or to maintain awareness about them, are identified for software and other technology (based on the asset inventory list) and are updated based on changes in the inventory, or when other new or useful resources are found.
- Conduct an enterprise security posture review as needed, but no less than once within every 365 days, in accordance with HealthEdge information security procedures.
- Vulnerability scanning tools are regularly updated with all relevant information system vulnerabilities or it updates its list of vulnerabilities based on a subscription

to one or more vulnerability intelligence services to stay aware of emerging exposures.

- Require regular penetration testing, no less than every 365 days, on defined information systems or system components to identify vulnerabilities and attack vectors that can be used to successfully exploit enterprise systems.
- Require penetration testing from outside the network perimeter (i.e., the Internet or wireless frequencies around HealthEdge) as well as from within its boundaries (i.e., on the internal network) to simulate both outsider and insider attacks. This includes tests for the presence of unprotected system information and artifacts that would be useful to attackers, including network diagrams, configuration files, older penetration test reports, emails or documents containing passwords or other information critical to system operation.
- Require use of an independent penetration agent or penetration team to perform penetration testing on the Information Assets and system components.
- Employ vulnerability scanning procedures that can identify the breadth and depth of coverage (i.e., information system components scanned and vulnerabilities checked).
- Review historic audit logs to determine if high vulnerability scan findings identified in the information system have been previously exploited.
- Scan for vulnerabilities in the information system monthly and when new vulnerabilities potentially affecting the systems and networked environments are identified and reported.
- Scan for vulnerabilities in the hosted applications monthly and when new vulnerabilities potentially affecting the systems and networked environments are identified and reported.
- Employ automated mechanisms monthly to determine the state of information system components with regard to flaw remediation.
- Update the list of information system vulnerabilities scanned within every 30 days or when new vulnerabilities are identified and reported.
- Include privileged access authorization to operating system, telecommunications, and configuration components for selected vulnerability scanning activities to facilitate more thorough scanning.

3 Exceptions

In situations where a vulnerability could be effectively mitigated without applying a patch to the vulnerable software, the mitigation should be documented before the vulnerability is exempted from future tracking. Where vulnerabilities are found to be false positives, the reasoning should be documented to exempt from further action.

Vulnerabilities that will not be fully mitigated within SLA should be tracked via a ticket or Risk and Compliance Governance Committee (RCGC) platform. The reason for the SLA exception or Risk Acceptance should be fully outlined in the ticket and Critical, High, and Medium vulnerabilities must be approved as part of the normal Risk Review process conducted by the RCGC Team.

4 Authority

The designated CISO, Legal Team, and Risk and Compliance Governance Committee (RCGC) have responsibility over the enterprise IT and Information Security policies.

5 Non-Compliance with This Policy

Failure to comply with HealthEdge Policy may result in disciplinary action up to and including termination of employment, services, or relationship with HealthEdge.

6 Terms and Definitions

Chief Information Security Officer – The CISO has authority over the Information Security and Compliance Program with oversight by HealthEdge Legal Team and the Risk and Compliance Governance Committee (RCGC).

Confidential – Data should be classified as Confidential when the unauthorized disclosure, alteration, or destruction of that data could cause significant risk to HealthEdge or its customers. This data should always be secured from unauthorized access. Data falling into this category includes proprietary business information, such as unannounced product specifications, business-related information that is designated for internal use only, any information containing one or more of the Sensitive Data Elements listed in Appendix B, data elements that are subject to regulatory and legal protection, or information that the Data Owner or Data Steward feels requires the consistent use of the extra controls involved with this classification. Confidential data is identified by a required "Confidential" stamp or watermark on the data or information.

Contractor - Throughout Company security policies, the term 'contractor' is defined as temporary workers who undertake a contract to provide materials, labor or services.

Critical Information Assets – Information assets that are required to be operational in support of critical business processes.

Employee - Throughout Company security policies, the term 'employee' is defined as full, part-time and per diem persons, non-contract workers, volunteers, and trainees where the Company has the right to dictate the resource's work duties.

Information Assets - Throughout Company security policies, the term 'information assets' is defined as any data, devices, or other components of the Company environment that have value to the organization and support Company business operations. Company information assets must be protected against unauthorized access, use, disclosure, alteration, destruction, and/or theft, resulting in loss to the Company.

Personally Identifiable Information – Throughout Company security policies, the term 'personally identifiable information' is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual.

Private - Data should be classified as Private when the unauthorized disclosure, alteration, or destruction of that data could result in a moderate risk to HealthEdge or its customers. By default, Private data is any information generally intended for use within HealthEdge by HealthEdge Associates. For HealthEdge projects, it isn't sensitive or subject to regulatory and legal protection requirements. Private Data is identified by a required "Private Data" stamp or watermark on the data or information.

Protected Health Information – Throughout Company security policies, the term 'protected health information' is defined as individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations.

Public - Data should be classified as Public when the unauthorized disclosure, alteration, or destruction of that data would result in little or no risk to HealthEdge or its customers. Unlike the other two classifications, a watermark or a stamp is optional for Public Information. Protecting information that is considered Public is not required; after all, it is meant to be shared.

Workforce Members - Throughout Company security policies, the term 'Workforce Members' is defined as all users, including employees, contractors, consultants, vendors, and temporary employees, who are authorized to access Company information systems that are owned or controlled by the Company and used to support its business processes.

7 Security Framework Mapping

Framework	Controls
NIST 800-53 rev 5	AC-4(25), AC-4(11), CA-2a, CA-8, CA-8(1), CA-8(2), CM-12a, CM-7a, CM-7b, CM-8(1), CM-8(2), CM-8(3), CM-8(4), CM-8(6), CM-8(7), CM-8(8), CM-8a, CM-8b, IA-3(3), IA-5(17), MA-3(6), PE-20, PE-3f, PM-5, PM-5(1), RA-3a1, RA-5(10), RA-5(11), RA-5(2), RA-5(3), RA-5(4), RA-5(5), RA-5(6), RA-5(8), RA-5a, RA-5b, RA-5c, RA-5d, RA-5e, RA-5f, RA-9, SA-10(6), SA-11(1), SA-11(2)a, SA-11(2)b ,SA-11(2)c, SA-11(2)d, SA-11(5), SA-11(6), SA-11(8), SA-11(9), SA-15(3), SA-15(7)a, SA-15(7)b, SA-15(7)c, SA-15(7)d, SA-15(8), SA-3(3), SA-5c, SA-5d, SC-16(2), SC-3(4), SC-30(4), SC-41, SC-7(10)b, SC-7(14), SC-7(17), SC-7(26), SI-10, SI-10(1)a, SI-10(2), SI-10(3), SI-10(4), SI-10(5), SI-10(6), SI-13(1), SI-13(3), SI-2(2), SI-2(3), SI-2(4), SI-2(5), SI-2(6), SI-2c, SI-2d, SI-3(8), SI-4(11), SI-4(18), SI-4(22), SI-8(2), SR-10, SR-11(3), SR-12, SR-4(2), SR-4(3), SR-6(1)
HITRUST	0701.07a1Organizational.7, 07.07a1Organizational.8, 0701.07a1Organizational.8, 0704.07a1Organizational.8, 0704.07a1Organizational.9, 0703.07a2Organizational.1, 0702.07a2Organizational.2, 0721.07a2Organizational.3, 0722.07a2Organizational.4, 0723.07a2Organizational.5, 0705.07a3Organizational.3, 0724.07a3Organizational.4, 0725.07a3Organizational.5, 0732.09r1Organizational.3, 0706.10b1System.2, 0707.10b2System.1, 0733.10b2System.4, 0791.10b2System.5, 0709.10m1Organizational.1, 07.10m1Organizational.2, 07.10m1Organizational.3, 0715.10m1Organizational.4, 0778.10m1Organizational.5, 0710.10m2Organizational.1, 0786.10m2Organizational.13, 0787.10m2Organizational.14, 0711.10m2Organizational.23, 0712.10m2Organizational.4, 0713.10m2Organizational.5, 0714.10m2Organizational.7, 0737.10m2Organizational.9, 0716.10m3Organizational.1, 0717.10m3Organizational.2, 0788.10m3Organizational.20, 0789.10m3Organizational.21, 0790.10m3Organizational.22, 0718.10m3Organizational.34, 0719.10m3Organizational.5, 0741.10m3Organizational.6
HIPAA	164.308(a)(8), 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.316(a)

APPENDIX A: Vulnerability Remediation Service Level Agreements (SLAS)

HealthEdge maintains basic SLAs for vulnerability remediation or adequate compensating controls depending on vulnerability classification. While triaging vulnerabilities, we may adjust the CVSS or overall Risk score based on existing mitigation that affects the likelihood or impact of an exploit in our environment.

Vulnerability Classification	Scope and Analysis	Total Remediation/Mitigation Window
Critical vulnerabilities with exploits in the wild (CVSS Score 9-10, where applicable)	Commence within 24 hours of discovery. Conclude within 3 days.	Maximum 7 days post discovery for vulnerable and operable systems
Critical (CVSS Score 9-10, where applicable)	Commence within 3 days of discovery. Conclude within 7 days.	Maximum 14 days post discovery for vulnerable and operable systems
High (CVSS Score 7-8.9, where applicable)	No SLA	Maximum 30 days post discovery for vulnerable and operable systems
Medium (CVSS Score 4-6.9, where applicable)	No SLA	Maximum 60 days post discovery for vulnerable and operable systems
Low (CVSS Score 0=3.9, where applicable)	No SLA	Maximum 180 days post discovery for vulnerable and operable systems