Information Security and Privacy Policy

Purpose

The purpose of this document is to specify what procedures and controls are to be in place to protect the *confidentiality*, *integrity* and *availability* of all information stored and processed within the Tricefy service along with any systems involved in this processing.

These terms are defined as follows:

- **Confidentiality** means preserving authorized restrictions on access and disclosure, including means for protecting personal data
    - **Personal Data** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, by reference to an identifier (such as a name, an identification number, location data, an online identifier) or factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
- **Integrity** means guarding against improper information modification or destruction, and includes ensuring information accuracy and authenticity
- **Availability** means ensuring timely and reliable access to and use of said information

Scope

This document will address all information, systems, data, networks and users of technology.

This policy applies to all personnel including management, system development and operations personnel, contractors and third parties.

Per ISO 27001, this policy follows the layered policy/standard format:

1. Policies: to include high level goals, scope, roles and responsibilities
2. Standards: to include minimum requirements for each topic, but in a generic way
3. Procedures and guidelines: specific requirements and details for a given topic

Trice Imaging 18583441531
1343 Stratford Ct info@triceimaging.com
Del Mar, CA 92014 USA http:// www.triceimaging.com

Roles and Responsibilities

- Security Officers
    - Senior Technology Management responsible for:
        - Specifying and documenting the security architecture to include:
            - Ensuring that sensitive information is protected from unauthorized access in all forms at rest and in transit
            - Continuous monitoring strategy
        - Scheduling and coordinating all security review and audit processes
        - Reporting security status and issues to the senior management team and board members in a timely fashion.
    - Data-Protection Officer responsible for:
        - Informing and advising employees who carry out processing of their obligations pursuant to data-privacy laws and regulations, such as GDPR
        - Monitoring compliance with applicable regulations, internal policies, and with policies of the controller in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits
        - Providing advice where requested regarding data protection impact assessment and monitoring its performance
        - Working with the Supervisory Authority on issues relating to processing
        - Being available for inquiries from data subjects relating to data protection practices, withdrawal of consent, right to be forgotten and other rights
    - Compliance Management responsible for:
        - Ensuring mandatory security education and awareness is undertaken by all personnel
        - Ensuring employee and contractor compliance to all security policies and procedures.
        - Specifying the Risk Management framework
    - Quality Assurance Management responsible for:
        - Validation of Security architecture
        - Managing an inventory of systems, devices and peripherals including cloud assets
        - Executing the Risk Management framework
        - Establishing, implementing, and enforcing an incident response program (including any integrity or personal data breaches)
- Software Developers
    - Implementation of security architecture
        - This applies to all systems, projects, and software modules from inception to completion
    - Designing and developing tests for security

Trice Imaging 18583441531
1343 Stratford Ct info@triceimaging.com
Del Mar, CA 92014 USA http:// www.triceimaging.com

    - Analyzing system performance for potential security problems, and providing direction to correct any security problems identified during testing
    - Leading the design, development, and modification of safeguards to correct vulnerabilities identified during system development and test
    - Supporting all security activities including audits of the system
- Customer and Technical support personnel
    - Notifying Senior technical management of any actual or suspected computer-security incidents, including personal data breaches

Violations

Any violations of these Policies or Standards may result in disciplinary action, up to and including termination of employment or contract (see Sanctions Policy below).

Included Policies

Access Management Policy Statement

It is the policy of the company to ensure that information shall be protected against unauthorized access.

Account Access Policies for Employees & Contractors

- System or application accounts created for employees or contractors should follow the Principle of Least Privilege
    - Accounts should only exist for the time period needed (for completion of a project), or removed promptly upon employee departure.
    - Application and system accounts should have the least amount of access required to complete necessary tasks

Related Standards, Procedures and Guidelines

- Security White Paper (http://security.triceimaging.co) includes sections detailing controls for:
    - Server access
    - Account Access
    - User authentication (ID, password)
    - Account creation and termination
    - Auto logoff
    - Break glass procedure

Trice Imaging 18583441531
1343 Stratford Ct info@triceimaging.com
Del Mar, CA 92014 USA http:// www.triceimaging.com

Encryption Policy Statement

It is the policy of the company that all data containing Protected Health Information be encrypted in transit and at rest.

- All encryption algorithms used will be based on the Advanced Encryption Standard (AES)
- All servers used for authentication and/or using certificate based TLS must have installed a valid certificate signed by a known trusted provider
- Cryptographic keys must be generated and stored in a secure manner that prevents loss, theft, or compromise

Related Standards, Procedures and Guidelines

- The Security Whitepaper (http://security.triceimaging.co) includes sections detailing:
    - Data Security
    - Network Security

Systems Security Policy Statement

This policy has two aspects:

1. Local Systems: To establish standards for the security of host equipment that is owned by Trice Imaging and/or operated by Trice Imaging employees and/or contractors. This includes:
    a. Malware protection: Anti-virus and anti-spyware are installed, operating and updated on all devices; periodic scans are conducted to identify and remove unauthorized software.
    b. Laptop security: Employees are responsible for the security of their laptops:
        i. all passwords should be kept secret
        ii. laptop should not be be left unattended or exposed
        iii. Full-disk storage encryption must be enabled (e.g. FileVault for Mac)
2. Cloud Systems: To establish standards for the security of cloud instances that are part of the Tricefy service. This includes:
    a. Software security patching: all systems should have up-to-date software security patches installed.
    b. System hardening: Including locking down ports to prevent unauthorized access, and always using ssh through a bastion host transparently.
    c. Multi-tenancy issues: any systems that access personal data should run on dedicated (single-tenant) servers.

Trice Imaging 18583441531
1343 Stratford Ct info@triceimaging.com
Del Mar, CA 92014 USA http:// www.triceimaging.com

Related Standards, Procedures and Guidelines

Application Security Policy Statement

Software development or implementation life cycle for all developed applications must include appropriate security controls and audit capabilities to prevent the loss, modification, corruption or misuse of functionality and data.

Related Standards, Procedures and Guidelines

Trice Imaging 18583441531
1343 Stratford Ct info@triceimaging.com
Del Mar, CA 92014 USA http:// www.triceimaging.com

Sanctions Policy Statement

The purpose of this policy is to apply appropriate sanctions against workforce members who fail to comply with the security policies or procedures of Trice Imaging.

This policy applies to all Trice Imaging workforce members including, but not limited to full-time employees, part-time employees, trainees, volunteers, contractors, temporary workers.

Trice Imaging will ensure all members of its workforce comply with the security policies of the organization (including GDPR and HIPAA) by applying appropriate sanction and disciplinary actions as follows:

1. Trice Imaging will appropriately discipline employees and other workforce members for any violation of security policy or procedure to a degree appropriate for the gravity of the violation. These sanctions include, but are not limited to, re-training, verbal and written warnings and immediate dismissal from employment.
2. Employees or workforce members who knowingly and willfully violate state or federal law for improper use or disclosure of a patient's information are subject to criminal investigation and prosecution or civil monetary penalties.

Trice Imaging will record all disciplinary actions taken in the employment records of the employee. Trice Imaging will investigate any security incidents or violations and mitigate to the extent possible any negative effects of the incident a timely manner. Trice Imaging and its workforce members will not intimidate or retaliate against any workforce member or patient that reports the incident.

Related Standards, Procedures and Guidelines

Employee Termination Policy Statement

Terminating employees are required to return any/all property, equipment, and materials which were issued to them during the course of their employment with Trice Imaging. This includes, but is not limited computers, supplies, equipment. These items shall be returned on or before the last day of the individual's employment.

Management shall determine a date to revoke access rights to Trice Imaging related accounts and information, including any 3d party systems where accounts were created as part of the onboarding process. All information access privileges will be revoked and accounts terminated on or before the date of termination with Trice Imaging.

Related Standards, Procedures and Guidelines

Trice Imaging 18583441531
1343 Stratford Ct info@triceimaging.com
Del Mar, CA 92014 USA http:// www.triceimaging.com

Data Security Policy Statement

The confidentiality, integrity and availability of Information assets must be protected using appropriate technical and organizational measures according to data classification and applicable law when being handled and/or transmitted.

Additionally, confidential information should be removed when it's use is no longer legally required.

Related Standards, Procedures and Guidelines

- The Security Whitepaper (http://security.triceimaging.co) includes specific safeguards regarding Personal Health Information (see section on Data Security)

Security Incident Handling Policy Statement

All users are responsible for reporting any security related incidents they may become aware of by utilizing the company's incident response process, described below.

Trice Imaging follows a five-step incident response process when managing both security and availability incidents. The goal is to restore normal service security and operations as quickly as possible after an issue is detected and an investigation is started

1. Detect: The detection processes are designed to discover events that risk the confidentiality, integrity, and availability of data and services. Several events can trigger an investigation, such as:
    a. Customer complaints or customer support tickets
    b. Triggered alarms or alerts (every service has associated monitoring and alerting capabilities)
    c. Ongoing security and penetration testing
2. Assess: The Assess stage of an incident response is a triage effort that includes the following activities:
    a. Escalation as appropriate
    b. Assigning the investigation appropriate priority and severity levels
    c. Assigning a Security Incident Manager who will be responsible for ensuring that the incident response process is managed throughout all stages of the investigation
3. Diagnose: The goals of the Diagnose stage is to examine the collected information to gain a better technical understanding of the events
4. Stabilize and Recover: The Stabilize and Recover processes are to correct and repair any services affected by the incident. The goals of this stage are:
    a. If necessary, take emergency mitigation steps to resolve any immediate security risks

Trice Imaging 18583441531
1343 Stratford Ct info@triceimaging.com
Del Mar, CA 92014 USA http:// www.triceimaging.com

b. Verify that customer and business risk has been successfully contained, and that corrective measures are being implemented.

5. Close and Post Mortem: Processes are refined, documentation is completed

If during the investigation of a security incident, Trice Imaging becomes aware that customer data has been accessed by an unlawful or unauthorized party, the Data Protection Officer (DPO) shall notify the controller without undue delay. If it is not possible to provide all information immediately, the information may be provided in phases without undue further delay.

The Data Protection Officer (DPO) will also immediately begin execution of the Customer Security Incident Notification Process. The goal of the customer security incident notification process is to provide impacted customers with accurate, actionable, and timely notice when their customer data has been breached. Such notices may also be required to meet specific legal requirements.

Trice Imaging 18583441531
1343 Stratford Ct info@triceimaging.com
Del Mar, CA 92014 USA http:// www.triceimaging.com