uniphore

Information Security Assertion

DOCUMENT CLASSIFICATION	Public
DOCUMENT DATE	15- June- 2021

Table of Contents

General

Uniphore maintains a comprehensive written Information Security Program to establish effective administrative, technical, and physical safeguards for Customer and employee data, and to identify, detect, protect against, respond to, and recover from security incidents. Uniphore's Information Security Program complies with applicable Data Protection Law and is aligned with the NIST. Additionally, Uniphore is certified against ISO 27001:2013, SOC 2 Type II, and Payment Card Industry Data Security Standard v.3.2.1. Uniphore has also undergone a HIPAA/GDPR assessments validated by a qualified third-party assessor.

Maintenance and Compliance

Uniphore's Information Security Program is maintained by a dedicated security team, led by our Chief Information Security Officer. Uniphore monitors compliance with its Information Security Program and conducts ongoing education and training of personnel to ensure compliance. The Information Security Program is reviewed and updated annually to reflect changes to our organization, business practices, technology, services, and applicable laws and regulations. We will not alter or modify the Information Security Program in a way that materially weakens or compromises the effectiveness of its security controls.

Human Resources Security

Policies as part of information security address:

Background Checks

Background verification checks on all candidates for employment are carried out in accordance with relevant laws, business requirements, information to be accessed and perceived risks.

Non-Disclosure Agreement

All Uniphore personnel are bound by Nondisclosure/Confidentiality Agreement that protect Uniphore and its customers' and partners' Confidential Information.

Communication

Uniphore communicates its information security policy to its employees periodicallyor after significant changes.

Security Awareness Training

Prior to receiving access to Uniphore Confidential Information, all personnel receive security awareness training appropriate to their job function, delivered at planned intervals and as required to mitigate significant changes to information security risk.

Training

Uniphore monitors training and job competence using a formal performance and appraisal process.

Removal of Access Rights

The access rights of all employees with access to information processing system(s) or media containing Uniphore Confidential Information is removed immediately upon termination of their employment, contract, or agreement, or adjusted upon change of job function.

Asset Management

Uniphore maintains an inventory of critical assets and establishes ownership of all critical assets, classification of critical assets based on business impact, including privacy implications, labeling of critical assets, and handling standards for introduction, transfer, removal, and disposal of all assets based on asset classification.

Logical Access Control Policy

Uniphore has a documented logical access control policy that includes: the (a) request, approval and access provisioning process (for applications, databases, remote users), (b) user access (local or remote) based on job function (role/profile based, least privilege), (c) user access reconciliation performed periodically, (d) procedures for onboarding and offboarding users, (e) procedures for user inactivity threshold leading to account suspension and removal, and (f) have a clear definition of who is permitted to access, process or store data.

Role-based access control

Uniphore administrators set user roles according to the principle of least privilege. Users only see what they need to perform their job responsibilities.

Authentication and Authorization

User credentials are stored using industry standard and audited one-way hashes. Uniphore supports two-factor authentication (2FA), as well as federated authentication functionality for Single Sign-On (SSO) utilizing Security Assertion Markup Language (SAML).

Password Policy

A documented password policy which includes: (a) that the password must not be shared, (b) the password must be communicated separately from the User ID, (c) the initial password generated is random, (d) a forced initial password change, (e) a minimum password length, (f) password complexity, (g) password history, (h) passwords lock when the threshold for allowable attempts is reached, (i) a secure process is documented for password resets, (j) passwords to be saved only as one-way hash/encrypted files and, (k) service account credentials not to be stored in clear text in any application.

Data Centers and Physical Storage:

Uniphore's deployment model includes on-premises or Cloud (AWS). The Cloud Provider's data centers are compliant with a number of physical security and information security standards, which are detailed at the Cloud Provider's respective websites:

- https://aws.amazon.com/security/

Customers control the region where your data is hosted. This gives you the flexibility to decide where your Data is physically stored, and you may choose to host your Data in a specific geographic region (for example, only within the European Union or only within the United States).

Encryption Policy

A documented data security policy that dictates encryption technical architecture and use, and the encryption method and strength used to protect Confidential information is defined. Confidential Information (including authentication credentials) is encrypted while intransit over any shared network, non-wired network, and at rest. Key management procedure is employed assuring the confidentiality, integrity, and availability of cryptographickey material. VPN transmissions are over an encrypted tunnel and encryption automation details of storage and transmission between Uniphore, and relevant stakeholders is documented.

Encryption at rest

All stored data, session cookies, backups, and other sensitive data, is encrypted at rest. Database fields storing credentials are also encrypted for additional security. Account passwords are salted and hashed using the latest strong algorithms and approaches, which are routinely audited. No humans, our staff included, can ever view passwords.

Encryption in transit

All communication between customer systems and Uniphore is performed using high levelsof encryption (HTTPS)

Process Integrity

Uniphore ensures that any data stored, received, controlled, or otherwise accessed isaccurate and reliable. Inspection procedures are in place to validate data integrity.

Physical and Environmental Security

Uniphore has documented physical security policy to protect against unauthorized physical penetration, damage from environmental contaminants, and electronic penetration through active or passive electronic emissions.

- Access control procedures that restrict physical access (e.g., badge access, turnstile entry doors, and security guards). A record of all accesses will be securely maintained for a minimum of ninety (90)-days and physical access periodically recertified.
- Intrusion detection alarms at egress/ingress points and monitored when triggered.
- Monitoring external doors to Uniphore's facility
- Monitoring cameras to cover sensitive areas in the facility.
- Monitoring equipment (CCTV) feed either internally or externally by a qualified team
- Requirement that all Personnel wear some form of visible identification to identify them as employees, contractors, visitors, et cetera.
- Visitor management: visitors to secure areas are supervised. Date and time of entry and departure will be recorded and kept for a minimum of ninety (90) days.

Environmental Controls

Uniphore has documented Environmental Security Controls that include server(s) and computer equipment be located in an environmentally appropriate area with the following controls: (a) climate control (temperature and humidity), (b) system thermostat sensor, (c) raised floor, (d) smoke detector, (e) heat detector, (f) fluid or water sensors, (g) CCTV installation points, (h) fire suppression system, (i) Uninterruptable Power Supply (UPS), (j) power generators, and (k) fire extinguisher equipment. The controls are tested periodically.

Operations

Uniphore has documented Information Technology operations procedures to ensure secure operations of its Information Technology assets.

Operational Procedures and Responsibilities

Uniphore has documented operational procedures that include: (a) scheduling requirements, (b) error handling, (c) generating and handling special output, (d) maintenance and troubleshooting of systems, (e) procedures to manage SLAs/KPIs and (f) the reporting structure for escalations. A minimum-security baseline has been established for the operating systems and versions. Uniphore's information systems is deployed with appropriate security configurations and reviewed periodically to ensure compliance with Uniphore's security policies and standards.

Change Management

Uniphore ensures that changes to the system, network, applications, and data file structures, other system components and physical/environmental changes are monitored and controlled through a formal change control process. Changes are reviewed, approved, and monitored during postimplementation to ensure the desired result is achieved.

Change Policy and Procedure

The change policy includes (a) application changes, (b) operating system changes, (c) network infrastructure changes, (d) firewall changes, (e) clearly defined roles and responsibilities (including separation of duties), (f) impact or risk analysis of the change request, (g) testing prior to implementation, (h) security implications review, (i) authorization and approval, (j) post-installation validation, (k) back-out or recovery plans, (l) management signoffs, (m) post-change review.

Anti-Virus and Malicious Code

Servers, workstations, and internet gateway devices are monitored through Endpoint Detection and Remediation (EDR). Uniphore has documented procedures in place to detect and remove any unauthorized or unsupported application. Endpoint devices are secured with hard drive encryption, endpoint detection and remediation (EDR) and advanced malware detection with central management and control.

Back-up and Off-site Storage

Uniphore has a defined back-up policy and associated procedures for performing back-up of data in a scheduled and timely manner. Procedures encompass the ability to fully restore applications and operating systems. Periodic testing of successful restoration from back-up media is demonstrated. Backup are taken based on customer requirements, encrypted in transit and at rest, and are tested regularly.

Security Event Monitoring

Security events are logged (log files), monitored (appropriate individuals), addressed and resolved in a timely manner. Actions are taken to resolve security events and such actions are documented. Network components, workstations, applications, and any monitoring tools are enabled to monitor user activity. Organizational responsibility for responding to events are defined. Configuration checking tools or other logs are utilized thatrecord critical system configuration changes. The log permission restricts alteration by administrators or any user. Retention schedule for various logs is defined and followed.

Vulnerability Management

Uniphore continuously gathers and analyzes information regarding new and existing threats and vulnerabilities, actual attacks on the organization or others, and the effectiveness of the existing security controls.

Penetration Tests

Periodically, Uniphore engages a recognized, industry leading third party to conduct or attest to an external penetration test of Uniphore's external-facing and internal environments. Issues rated as critical or high risk are remediated within the timelines consistent with industry standard.

Communications and Connectivity

Uniphore has implemented robust controls over its communication network to safeguard data such as tightly control access to network devices through management approval and subsequent audits, disable remote communication if business need does not exist, log, and monitor remote access, secure remote access devices and use strong authentication and encryption methods for secure communications.

Network controls

Uniphore maintains all production systems in a dedicated Virtual Private Cloud (VPC). Production data never leaves the dedicated VPC, and communication and access to it is restricted by firewalls and access control mechanisms. Intrusion Detection Systems (IDS) monitor and alert our 24/7/365 Security Operations Center (SOC) whenever unusual behavior or traffic is detected.

Cloud Technology

Uniphore safeguards stakeholders' Confidential Information stored, processed, or transmitted using Cloud Technology. Information Security Requirements apply to any use of cloud technology to store, process, or transmit stakeholders Confidential Information. Uniphore shall inform stakeholders of and obtain stakeholders written approval of Cloud Technology before it is used to store, process, or transmit stakeholders Confidential Information.

Remote Access Administration

Uniphore ensures that unauthorized remote connections are disabled as part of the standard configuration. Data flow in the remote connection is encrypted and multifactor authentication is utilized.

Mobile Computing

Uniphore ensures that mobile computing (where permitted) is performed over encrypted channels and that Uniphore seeks stakeholder's prior approval before processing or storing any stakeholders Confidential Information on a mobile device. Wireless access to Uniphore's network is configured to require authentication.

Web Access

Web content filtering and Data Loss Prevention applications are in place to restrict external webmail, instant messaging, file sharing, and other data leak/attack vectors.

E-mail and Instant Messaging

Uniphore has policies and procedures established and adhered to ensure proper control of an electronic mail and/or instant messaging ("IM") system that displays and/or contains stakeholders Confidential Information.

Authorized E-mail Systems

Use of non-corporate/personal e-mail solutions is restricted based on policy. Preventive and detective controls block malicious e-mails/attachments. Policy prohibits auto-forwarding of e-mails.

Separation of Production and Non-Production Environments

Uniphore has strict separation between production and non-production environments. Our production environment, and Customer Data are never utilized for non-production purposes. Our non-production environments are utilized for development, testing, and staging.

Secure System Development

Uniphore shall have an established Software Development Life Cycle ("SDLC") for the purpose of defining, acquiring, developing, enhancing, modifying, testing, or implementing information systems. SDLC Requirements include:

- Version control and release management procedures.
- Security activities that foster development of secure software (e.g., requirements in requirements phase, secure architecture design, static code analysis during development and dynamic scanning or penetration test of code during QA phase with High and above vulnerabilities remediated before moving to the next phase).
- Software security testing occurs based on the Open Web Application Security Project (OWASP) Top 10 and includes: (a) cross site scripting (XSS), (b) injection flaws, (c) malicious file execution, (d) insecure direct object, (e) reference cross site request forgery (CSRF), (f) information leakage and improper error handling, broken authentication, and session management, (g) insecure cryptographic storage, (h) insecure communication, and (i) failure to restrict URL access.
- SDLC methodology include: (a) validation of security requirements (static/dynamic scanning); (b) requirements for documentation; and (c) managed by appropriate access controls.
- Software executables related to client/server architecture that is involved in handling stakeholders Confidential Information is penetration tested.
- Software vulnerability assessments is conducted on an on-going basis internally or using external experts and any gaps identified is remediated in a timely manner.
- The development, test, and production environments are either firewalled and or physically separate from one another.
- Third Party and Open-Source Code used in Uniphore-provided applications is appropriately licensed, inventoried, supported, patches applied timely and evaluated for security defects on an on-going basis.

Third Party Management

Uniphore has a process to establish appropriate contracts for all dependent third- party providers prior to services being initiated; ensuring appropriate security language is incorporated.

Oversight of Third-Party Relationships

Uniphore has a risk-based process to ensure appropriate monitoring mechanisms for all dependent third-party providers and sub-contractors.

Risk Assessment and Strategic Planning

Uniphore has a process to identify all dependent third-party providers providing services to Uniphore and perform an appropriate risk assessment associated with the services.

Selecting a Dependent Third-Party Provider and Due Diligence

Uniphore has a risk-based process to review all dependent third-party providers to ensure they can provide appropriate control environment associated with the services they provide.

Third Party Relationships

Uniphore adequately identifies, assesses, manages, and monitors all dependent third- party providers to ensure an appropriate control environment. Replacement or risk mitigation strategies is in place for operating systems, software applications, and critical infrastructure nearing the end of life.

Incident Response

Uniphore has a documented plan and associated procedures in case of an information security incident. The plan clearly articulates the responsibilities of personnel and identify relevant notification parties. Incident response personnel is trained, and the plan tested periodically. The Incident Response policy and procedure is documented and include the following: (a) defined organizational structure, (b) identified response team, (c) documented availability of the response team, and (d) documented timelines for incident detection and disclosure.

- The Incident Response process lifecycle includes the following steps (i) identification, (ii) assignment of severity to each incident, (iii) communication, (iv) resolution, (v) training, (vi) testing, and (vii) reporting.
- Incidents are classified and prioritized, and incident response procedures include notification to stakeholders.
- The incident response process is executed as soon as Uniphore is aware of the incident.

Security Breach Reportable Breach

Where required, Uniphore shall notify stakeholders of (i) the theft, loss or unauthorized disclosure, acquisition, access to or misuse of stakeholders Confidential Information in the

possession or control of Uniphore or any third party providing services to Uniphore; or (ii) a compromise of the confidentiality and/or integrity of any hardware, software, network (including any "cloud" network), or telecommunications or information technology systems used by Uniphore to transmit, store, process or otherwise handle stakeholders Confidential Information ("Reportable Breach") as soon as Uniphore knows or reasonably suspects that such Reportable Breach exists or did exist.

Business Continuity, Disaster Recovery

Uniphore has formal documented recovery plans to include annual testing to identify the resources and specify actions required to help minimize losses in the event of a disruption to the business unit, support group unit, application, or infrastructure component.

Business Recovery Plans

Formal business resiliency plans are in place with comprehensive recovery strategies to address business interruptions. The plans have an acceptable alternative work location in place to ensure service level commitments are met.

Information Security Awareness and Training

Uniphore provides ongoing information security and privacy training to all workforce members to ensure a common understanding of applicable data protection laws and regulations, to watch for and report security risks and issues to executive management. This effort is designed to promote a culture of compliance with respect to data protection accountability at all levels of the company.

Data Retention

Retention period indicates the minimum time the data is required to be maintained. The data Retention period shall be decided based on:

- Organization's business requirements
- Legal or regulatory compliance requirements
- Contractual obligations

On completion of retention period, owner can extend the retention period as per valid business or contractual requirements. In such case, records shall be given original level of protection. Additionally, a record shall be maintained about the change of retention period with justification.

Entity will maintain a quarterly review process for data identification and secure deletion of stored information which exceeds defined retention requirements.

Data Disposal

Data shall be securely disposed with secure deletion process after completion of identified retention period. Data to be disposed shall be identified in the course of normal business activity as per organization's procedures.

No disposition action shall take place without the assurance that:

- Record is no longer required and out of retention period.
- No litigation or investigation is current or pending.
- Not required by any law or regulation or contractual obligation which would involve relying on the data as evidence.

Entity will utilize secure data disposition methods based on industry practices such as NIST SP 800-88 Clear/Purge etc.