Information Security Program

(March 2021)

Epicor maintains an information security program (the "**Program**") designed to: (i) protect against threats or hazards to the security, availability or integrity of Customer Data; and (ii) safeguard and prevent unauthorized access to Customer Data. This Program is subject to and governed by the terms of your customer agreement or similar agreement you have with Epicor. Capitalized terms not defined in this document are defined in the customer agreement with Epicor. The Program is comprised of the following:

1. **Definitions**

   1. **"Customer Data"** means all electronic information submitted by Customer to Epicor and stored as part of those Software as a Service (**SaaS**), hosting, application management, and/or other managed services performed by Epicor or its suppliers to process such information or otherwise accessed or processed by Epicor as a result of a professional services and/or support engagement. Customer data excludes statistical information that is anonymized and aggregated with like information, provided the information cannot be attributed to a customer or end user and always excludes Personally Identifiable Information.

   2. "**Incident**" means any actual or reasonably suspected compromise to the security of Customer Data.

   3. **"Personally Identifiable Information"** means Customer Data that may be used to readily identify, locate, or contact an individual.

2. **Customer Data Use.** Epicor may not use or disclose Customer Data other than for purposes of meeting its obligations under the applicable agreement or as required by law or a governmental authority. Epicor will require that any subcontractor who processes Customer Data on Epicor's behalf agrees to abide by the information security measures in this Program (or other applicable measures that are at least as protective of the Customer Data).

3. **Confidentiality.** Epicor and its approved subcontractors keep Customer Data strictly confidential and do not disclose Customer Data to third parties without Customer's consent. Epicor requires personnel and subcontractors to maintain confidentiality of Customer Data through use of non-disclosure or comparable confidentiality agreements.

4. **Epicor Affiliates and Personnel.** Epicor maintains reasonable measures to ensure that affiliates and personnel comply with this Program as if they were a party to it.

5. **Epicor Point of Contact.** Epicor has appointed an appropriate security point of contact ("**POC**") with responsibility for implementing the Program and answering questions regarding the Program. Epicor's POC can assist in relation to all requests Customer may have relating to information security or any requests to investigate Incidents.

6. **Incidents.** Epicor will promptly notify Customer in writing upon becoming aware of any Incident involving Customer Data that is in Epicor's possession, custody, or control after due inquiry. Epicor will reasonably investigate such Incident and cooperate with Customer's efforts to determine the nature and extent of the Incident.

7. **Revisions.** Epicor reserves the right to make amendments to the Program. Customers may access details of the current Program at:

   https://www.epicor.com/company/compliance/default.aspx

Information Security Program Controls

1. **Applicability.** The described hereunder apply to the following products when hosted (via SaaS or otherwise) by Epicor (the "Covered Products"):

    - Epicor ERP (Public and Private Cloud)
    - Epicor Bistrack/LumberTrack
    - Epicor Prophet21 (Public and Private Cloud)
    - Epicor ECM (formerly DocStar)
    - Epicor Eagle
    - Epicor HCM
    - Epicor 1EDI (Public and Private Cloud)
    - Epicor EPN
    - Epicor IDA
    - Epicor Vision

2. **Organizational Security.** Epicor maintains a dedicated and independent security team reporting to its Chief Information Security Officer (CISO). The organizational structure is comprised of two distinct groups:
    a. IT Security, which is responsible for monitoring and incident response, vulnerability assessment and remediation, security design and engineering, and security consulting
    b. Governance, Risk and Compliance, which is responsible for regulatory compliance, IT internal audit and external audit support, risk assessments, and IT policies

3. **Compliance Certifications.** Epicor conducts annual independent assessments for hosted Epicor products. SSAE-18 SOC1 reports for Epicor's organizational and admin / shared IT infrastructure and SSAE-18 SOC2 reports are available to hosted customers via the EpicCare support portal. In addition, Epicor conducts an annual PCI assessment for products that store, process or transmit credit card data.

4. **Audit Findings**. Any audit findings will be made available in the annual SSAE-18 reports. Upon request, Epicor will assist customers on inquiries into any findings.

5. **Background Checks.** Where allowed by applicable regional laws, Epicor conducts background checks prior to onboarding new employees. This process is audited annually as part of our SSAE-18 SOC1 assessment.

6. **Employee Onboarding and Access Assignment.** Epicor's onboarding and termination process is audited as part of an annual SSAE-18 SOC1 process. All privileged access accounts (with access to hosted Customer Data) undergo an approval process and are documented in Epicor's ticketing system. All employee terminations follow a ticketed workflow, with a periodic termination review conducted as a secondary check. Accounts of terminated employees are disabled the day of departure.

7. **Framework Overview.** Epicor's control objectives are aligned to the industry standard SCF MetaFramework (Secure Controls Framework), which allows us to map and assess against other frameworks such as NIST, ISO and PCI. The framework covers the following security domains:
    - Security & Privacy Governance (GOV)
    - Asset Management (AST)
    - Business Continuity & Disaster Recovery (BCD)
    - Capacity & Performance Planning (CAP)
    - Change Management (CHG)
    - Cloud Security (CLD)
    - Compliance (CPL)
    - Configuration Management (CFG)
    - Continuous Monitoring (MON)
    - Cryptographic Protections (CRY)
    - Data Classification & Handling (DCH)
    - Endpoint Security (END)

- Human Resources Security (HRS)
- Identification & Authentication (IAC)
- Incident Response (IRO)
- Maintenance (MNT)
- Mobile Device Management (MDM)
- Network Security (NET)
- Physical & Environmental Security (PES)
- Privacy (PRI)
- Risk Management (RSK)
- Secure Engineering & Architecture (SEA)
- Security Operations (OPS)
- Security Awareness & Training (SAT)
- Technology Development & Acquisition (TDA)
- Third-Party Management (TPM)
- Threat Management (THR)
- Vulnerability & Patch Management (VPM)
- Web Security (WEB)

8. **Security Awareness Training.** All Epicor employees are required to complete security awareness training during their onboarding process and annually thereafter. This process is audited as part of our annual SSAE-18 assessment.

9. **Physical Security.** Covered Products and associated Customer Data are hosted with reputable and certified cloud and colocation providers. Epicor limits access to colocation centers to only necessary administration staff and reviews such access quarterly. Annually, Epicor reviews each vendor's certifications (SSAE-18, ISO Certificate, etc.) as part of our vendor management process.

10. **Logging and Monitoring.** Epicor monitors production servers and infrastructure for operational and security issues. Logs are centrally stored and retained for at least 30 days (one year for PCI environments). Any operational threshold triggers or identified security issues are ticketed and routed to personnel who can review and remediate.

11. **Vulnerability Management.** Epicor performs vulnerability assessments on the Covered Products at least quarterly. Results are reviewed by hosting and internal security teams for analysis, remediation tracking, and risk trending.

12. **Anti-Malware.** All environments that have risk of malware have anti-malware software installed. Updates are pushed at least daily, and alerts are generated for any issues found.

13. **Data Retention.** The Covered Products allow customers to retain as much history within the application as they require to meet their data retention needs.

14. **Backup / Recovery.** All Covered Products undergo at least daily backups, with the ability to recover data from the preceding 30 days. Data recovery tests are performed at least annually, using a sample subset of data or servers. Any testing issues are documented and remediated.

15. **Uptime**. Epicor's published Service Level Agreement for uptime is 99.5% uptime.

16. **Network.** An Internet connection is required to access hosted products. Epicor maintains redundant Internet paths to reach our environments.

17. **Intrusion Detection.** Intrusion Detection is in place at key network points. Alerts are analyzed by our Security Operations Center (SOC) and escalated to our Cloud Reliability Center (CRC) if needed. Critical issues detected follow Epicor's Incident response process.

18. **Incident Response Plan.** Epicor maintains a documented Incident Response Plan that involves escalations, functional level collaboration, internal and external notifications, and documentation.

19. **Server Patching.** Hosted production servers are subject to regular maintenance and patching at least monthly. All available security patches are prioritized, with high and critical items applied within 30 days.

20. **Change Management.** Application version upgrades follow a change management process which requires authorization (or pre-authorization in the case of standard changes).

21. **System Inventory.** All hosted product groups maintain inventories of the components that make up the solution. These inventories are used in conjunction with security and compliance controls and monitoring.

22. **Endpoint Security.** All corporate-issued workstations have centrally installed and managed antimalware software. In addition, where allowed by regional laws, laptops have full disk encryption and secure web proxy software installed.

23. **Access Control.** Epicor hosted and corporate environments undergo a quarterly privileged access review process. All administrative access requires documented authorization. System administrators utilize multifactor authentication when they remotely access production environments.

24. **Encryption in Transit.** All public and private cloud offerings encrypt sensitive data in transit using TLS 1.2 or later. Some services that do not contain sensitive information may not be encrypted.

25. **Encryption at Rest.** Epicor-hosted applications that reside in the Microsoft Azure environment have encryption at rest using Azure Storage Service Encryption (SSE). Epicor Content Management (ECM – formerly DocStar) uses encryption-at-rest services from AWS.

26. **Data Breaches.** In the event of a confirmed data breach, Epicor will notify impacted customers within 72 hours. Epicor has a documented process that includes internal notifications and coordination, contacting appropriate authorities, and third-party crisis management (on retainer).

27. **Media Destruction.** When physical media is decommissioned or retired, it is erased or destroyed as to no longer allow data retrieval.

28. **Data Privacy**. Epicor maintains up-to-date guidance on data privacy polices (such as GDPR and CCPA) on our website at: **https://www.epicor.com/en-us/company/compliance/.**