Information Security Program Overview
Subscription and Support Services

(Effective May 2018)

1. **Security Program**. Epicor maintains an information security program (the "**Program**") for handling and processing Customer Data that is designed to reasonably: (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. The Program is designed to include:

    a. physical security of all premises in which Customer Data will be processed or stored;

    b. reasonable precautions taken with respect to the employment of and access to Customer Data by Epicor's employees and staff ("**Personnel**") who will be instructed and required to act honestly and ethically in the operation of Epicor's business;

    c. a network security program that includes:

        (i) a written information security policy that is designed to reflect generally accepted data security standards;

        (ii) access and data integrity controls; and

        (iii) reasonable and appropriate standards for safeguarding of sensitive data, including Customer Data; and

    d. security standards for any outsourced providers that have access to Customer Data, including, as a minimum, a requirement that each such provider has a written agreement committing to confidential treatment of Customer Data.

2. **Security Framework.** Epicor uses the ISO (International Organization for Standardization) and IEC (International Electrotechnical) 27002 Standard (Information technology — Security techniques — Code of practice for information security controls) as a reference for our information security controls and practices. The domains included in the Standard are:

    a. Information Security Policies
    b. Organization of Information Security
    c. Human Resource Security
    d. Asset Management
    e. Access Control
    f. Cryptography
    g. Physical and Environmental Security
    h. Operations Security
    i. Communications Security
    j. System Acquisition Development and Maintenance
    k. Supplier Relationships
    l. Information Security Incident Management
    m. Information Security Aspects of Business Continuity Management
    n. Compliance

3. **Security Organization.** Epicor's security organization consists of a team of information security professionals who report to the Vice President of Global Information Security/CISO.

4. **Security Training.** Upon hire, and annually thereafter, employees are required to complete information security training.

5. **Security Reviews and Testing.**

   a. Epicor's operating environment and associated processes pertaining to the security of Customer Data (collectively, the "**Systems**") are the subject of periodic (no less than annually) industry standard information security reviews and audits conducted by internal and/or third party resources as appropriate.

   b. Epicor engages an external auditor to conduct annual AICPA Auditing Standards Board Service Organization Control Report 1, Type II or industry standard successor audits (SOC 1 Type II) audits for certain hosted products. Upon request, Epicor will furnish a copy of its current SOC 1 Type II annual audit report (individually, a "**SOC Report**") to Customers that have Customer Data processed by Epicor. Epicor will use commercially reasonable efforts to promptly remediate any material weaknesses or significant control deficiencies identified in any SOC Report.

6. **Background Checks.** Epicor conducts, in line with applicable local customs and laws, criminal background checks and/or seeks references on proposed Personnel (and, where appropriate, requires its subcontractors or other service providers) to conduct a background check on their own personnel prior to their engagement who are expected to have access to Customer facilities or have access (remotely or otherwise) to Customer Data as part of the performance of their duties in relation to Epicor.

7. **Disaster Recovery**. In accordance with Epicor's current disaster recovery and service level agreements, Epicor offers its Customers a subscription based, disaster recovery plan (the "**DR Plan**"). The DR Plan is designed to ensure that Customer Data in Epicor's possession or control, at any given time, is capable of being recovered; that the integrity of all such recovered Customer Data is retained; and that Epicor will be able to recommence performance of the Services within the defined service level targets (SLTs) in the event that any portion of the Systems experiences (i) a declared disaster; or (ii) any significant interruption or impairment of operation or any loss, deletion, corruption or alteration of data. Epicor performs selected sample tests to validate its DR Plan from time to time in accordance with commercially reasonable standards.

8. **Customer Inquiry**. Epicor agrees to reasonably cooperate with Customer requests for additional information regarding the Program.

9. **Revisions.** Epicor reserves the right to make amendments to the Program from time to time. Customers may access details of the then current Program at:

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