# Information Security Policy

Revision 4
*Effective date: January 29, 2021*

## Policy Statement

Forte's Senior Leadership Team have made it the policy of Forte to:

> Ensure the confidentiality, integrity and availability of information and data, systems, applications and networks under Forte's control through use of industry best practices and a consistent approach to security in the development and delivery of high-quality products and services.

## Information Security Principles

Advarra, Inc. acquired Forte Research and maintains an overall ***Corporate Information Security Policy (CP-806).*** This document provides the details Forte adopted. These high-level information security principles form a foundation for all Forte information security policies, procedures and practices. These principles are:

- Information in any form is fundamental to Forte's success, and Forte must manage information security in a framework based on ISO 27001:2013 and all applicable laws.
- Data and information is classified as open information or sensitive information and as Forte's, Forte's customer's, or third party information in accordance with ***QSP – 234 Information and Data Classification***.
- Information security risks must be managed in the context of Forte's business needs, strategies, and objectives. A risk management approach is used to identify, evaluate, and mitigate risks for Forte's systems and information assets. This is supported by ***QSP - 160 Risk Assessment and Management*** and related policies and procedures.
- Active support by Forte management through clear direction, education, explicit assignment, delegation, and acknowledgement of information security responsibilities.

This policy is based on the following three tenets of information security, outlined in ISO 27001:2013:

- **Confidentiality**: ensuring information is accessible only to those authorized to access the information
- **Integrity**: safeguarding the accuracy and completeness of information and processing methods, and
- **Availability**: ensuring that authorized users will have access to information and assets when required.

**WHAT IS THIS?**
This sidebar is a brief, plain-language explanation of the content to the left. You can use this to guide your review of our Information Security Policy.

**Why are we doing this?**
Forte is committed to managing information security in accordance with Forte policies, and all relevant laws and regulations

This policy is intended to set out information security principles to guide customers, vendors, suppliers and team members.

**Why information security?**
Forte's customers entrust their Sensitive Information to us. As such, in order to continue providing valuable products and services, we must ensure that we're properly handling, managing and securing that information.

**What information security factors?**
It is not enough to just maintain customer data as confidential. We also need to ensure it's available to our customers and stored and presented accurately.

## Information Security Controls

Under this policy, Forte has implemented procedures and controls intended to reduce the information security risks related to data, information, and systems under Forte's control.

### Training and personnel

Forte trains team members regarding processes and responsibilities relating to information security during onboarding, through the duration of employment, and upon separation. Background checks are conducted prior to employment, and all team members receive security awareness training and HIPAA training upon hire, and at least annually thereafter. See ***QSP – 200 Competency Training and Awareness Process.***

**What are these references?**
This policy is a high-level summary of *some* of the relevant information security controls. Forte has formal, documented procedures that layout with specificity how we can achieve these objectives.

### Data handling and protection.

Forte takes reasonable steps to monitor, review and audit information security effectiveness. Forte also uses encryption methods and controls to ensure data is secure during transmission and storage. See ***QSP - 220 Information Security***, ***QSP - 230 Customer Data and PHI Handling***, ***QSP - 232 Secure Communication***, ***QSP - 238 Release of Sensitive Information***, and ***QSP - 236 Data Encryption Standards***.

**Customer Data**
Forte has special procedures for working with and securing customer data, regardless of its data classification. These procedures are intended to meet or exceed legal and regulatory requirements regarding the treatment of Protected Health Information, Personally-Identifiable Information, and commercially sensitive information.

### Access Controls

Methods and controls to manage access to Sensitive Information to protect the confidentiality, integrity, and availability of information. Access to Forte information and systems must be attributable to an individual, permissions must be based on the requirements of the individual's role and managed by passwords. See ***QSP - 220 Information Security***.

### Physical security

Forte uses appropriate physical controls to protect information assets against loss, physical destruction, unauthorized physical access, and natural disasters. See ***QSP - 240 Physical Security Process - Madison***, and ***QSP - 241 Physical Security Process – India***.

### HIPAA, HITECH and Protected Health Information

In addition to the robust security processes in place to protect Sensitive Information in Forte's control, we have additional requirements to protect Protected Health Information our customers provide to us, in accordance with all applicable laws, rules, and guidance and to have documented procedures for investigating and reporting security incidents and for releasing PHI. See ***QSP - 230 Customer Data and PHI Handling***, ***QSP - 238 Release of Sensitive Information***, and ***QSP - 250 Security Incident Reporting***.

**Why is HIPAA called out specifically?**
We are a "business associate" to many of our customers. Our ISO 27001:2013 directly incorporates our HIPAA obligations and is fundamental to many of our data security measures.

### Incident Reporting, Audits and Compliance

Forte applies a consistent and effective approach to the detection, investigation, and management of information security incidents. Processes include the maintenance and auditing of policies and processes in practice, as well as reporting and correction of non-compliance. See ***QSP - 250 Security Incident Reporting***, ***QSP - 110 Management Review Process***, ***QSP - 130 Corrections & Corrective Action Process***, and ***QSP – 131 Quality Management System Procedure Deviations.***

### Risk Management and Change Control

Identification and mitigation of risks associated with Forte information and systems is of paramount importance. Risks are to be identified prior to development or procurement of IT systems and software, documented in business requirements, validated and tested prior to implementation, and upon material changes through the lifecycle of the system. See ***QSP - 160***

*Risk Assessment and Management; QSP - 210 Purchasing; QSP - 300 SDLC Process.*

## Disaster Recovery and Business Continuity

Systems are designed to minimize disruption to Forte operations. Procedures define the approach to resilience, disaster recovery, and general contingency controls. See *QSP - 009 Business Continuity and Disaster Recovery Planning Process.*

## Compliance and responsibilities

The SVP Technology, Security Officer and SVP Quality Assurance (Management Representative) are responsible for monitoring, reviewing and ensuring compliance with this policy.

The SVP Technology, Security Officer and SVP Quality Assurance (Management Representative) are responsible for reviewing this policy regularly, but at least on an annual basis, with a goal of continual improvement of the information security management system.

The Chief Compliance Officer (Advarra, Inc.) is the designated Privacy Officer for purposes of HIPAA. The SVP Technology is Advarra Technology Solutions Inc.'s Security Officer.

**Is this forever and always the policy?**
As part of Forte's and Forte's management's ISO 27001:2013 commitment, we are continually reviewing opportunities to improve our information security. The compliance team, together with leadership, will review and update this policy as appropriate.

### Associated DocumentsStatutes

## Revision History:

| Revision | Effective Date | Changes Made | Training Required |
|---|---|---|---|
| 1 | 09/27/2017 | Original Policy Document | Yes |
| 2 | 12/07/2018 | Update made for Chief Compliance Officer and Security Officer designees<br>Minor clarifications/grammatical corrections<br>Updated Related documents<br>Revision History Added<br>Approvals revised to reflect separation of Chief Compliance Officer and Security Officer | No |
| 3 | 09/10/2019 | Rewrite to be a high-level Policy and refer to specific procedural controls (QSP's) in place for Information Security. Adopt the IS Policy statement from the manual. Training will be with reference only to specific procedure changes. | No |
| 4 | 01/29/2021 | Remove references to procedural and work instruction controls<br>Update to reflect the acquisition of Forte by Advarra | No |

## Policy Approval:

Digitally signed by

Beau Grignon
Senior Vice President, Engineering & Infrastructure
Security Officer

Digitally signed by

Doug Fulton
Senior Vice President, Quality Assurance
Management Representative

## REVISION HISTORY

**Version 01 Effective on 29-Jan-2021**
Remove references to procedural and work instruction controls. Update to reflect the acquisition of Forte by Advarra.

## DOCUMENT ELECTRONIC SIGNATURES

### DOCUMENT APPROVAL WORKFLOW

**Author Approval**

Robert Grignon
Sr. VP Technology, Security Officer
beau.grignon@advarra.com

I am the author of this document.
*Signed 9:27:08 PM UTC 28-Jan-2021*

**Required Workflow Steps for this Category**

Douglas Fulton
Sr. VP, Quality Assurance, Process Improvement, & Training
douglas.fulton@advarra.com

*Advarra / Technology Solutions Approver*
I have reviewed and approve this document.
*Signed 10:27:54 PM UTC 28-Jan-2021*