# SALEM TRUST COMPANY
# INFORMATION TECHNOLOGY SECURITY

## OVERVIEW

The release of specific procedures and practices would compromise the integrity of the Company's data security processes. However, we can provide general information on our approach to cyber security and, more generally, to ensure the security of our systems.

Salem Trust Company employs many components to properly secure its data. It follows the guidelines established by the Federal Financial Institutions Examination Council ("FFIEC") and has a framework to provide security at all levels of critical infrastructure. Salem's Information Security Policy and Procedures Manual was developed to govern all aspects of our Information Services usage and has been reviewed by the Company's Board of Directors. Our Technology Risk Management Framework is implemented through our Technology Steering Committee and the Information Technology Director.

The security methods used by the Company include, but are not restricted to:

- Performing scheduled risk assessments of critical systems and vendors
- Enforcing proper account administration and reviews to protect data
- Employing independent agents to audit systems and perform random tests of security procedures
- Maintaining hardware and software inventory
- Utilizing aggressive vulnerability remediation
- Using encrypted email transmission of confidential client information
- Deploying Anti-Virus solutions
- Employing backup and disaster contingency planning
- Deploying Firewall and Intrusion Detection programs to protect against internet threats
- Training employees to recognize threats to the organization
- Maintaining appropriate levels of insurance

Additionally, the company protects its data against threats by preparing its Business Continuity Plan (BCP). This document establishes several key components of the company's disaster readiness. It consists of:

- Risk Assessments
- Business recovery objectives
- Recovery instructions
- Methods of protecting against numerous threats to business continuity
- Backup and Recovery step
- Testing requirements

Through a proper Information Systems Policy and a Business Continuity Plan, the company provides data security to its clients and vendors.

11-26-2017