Bank Security Policy

IT and Operations – Section 100

Policy # 100.250

Organizational Functional Area: IT and Operations
Policy For: Bank Security
Date Originated: 2009
Date Revised: 05/23/2016
Date Board Approved: 06/21/2016
Department/Individual Responsible for Maintaining Policy: Information Security Officer

Topic: Bank Security

Section 100.250
PURPOSE

The purpose of this policy is to provide Ameris Bancorp and Ameris Bank (the Bank) with a written plan that encompasses prevention, training and instructions for dealing with emergency situations that may occur. This policy is designed to comply with the minimum security procedures found in 12 CFR 326 of the FDIC regulations.

12 CFR 326 requires each bank to adopt appropriate security procedures to discourage robberies, burglaries and larcenies and to assist in identifying and apprehending persons who commit such acts.

OBJECTIVE

The goals of this policy are as follows:

1. Establish authority and responsibility in the development, implementation and maintenance of an emergency and security policy.
2. Provide a reference for emergency prevention measures that have been implemented.
3. Establish requirements for periodic testing of the adequacy of security plan.

RESPONSIBILITY

The Ameris Bank Board of Directors is responsible for ensuring management complies with the regulation; ensuring that a written security program is developed; ensuring that the written security program is implemented; and for designating a security officer to carry out these tasks under its supervision.

AUTHORITY

The Ameris Bancorp/Bank Security Officer will have the authority to develop and administer a written security program for Ameris Bancorp and Ameris Bank. The Security Coordinator for each office will have the authority to add employee names, opening and closing times, emergency telephone numbers, branch names and locations, vendor’s names and phone numbers and other information to customize this policy to fit their needs. The Security Officer shall report to the Board of Directors, on the implementation, the administration, and the effectiveness of the security program at least annually.

The Ameris Bank Board of Directors has appointed the Information Security Officer as the Bank's Security Officer.
Security Coordinator

All Ameris Bank employees are responsible for the Security effort of the entire Company. Each location will have a colleague who is designated as the Security Coordinator. In a branch location the Branch Manager/ABM will be the Security Coordinator. The Security Coordinator is responsible for administering the Ameris Bank Security program for their area (for example a Branch Manager may be the Security Officer for their branch which may include a Market/Regional President, Business Banker and corporate staff). Security Coordinator is a responsibility that is taken on by an existing colleague in addition to their normal job accountabilities.

SECURITY PROGRAM

In order to reasonably ensure that the Bank’s security program is effective and meets current industry standards, and to best ensure that the institution’s security officer is knowledgeable in fulfilling assigned responsibilities under the program, it is the policy of this Board that the security officer receive and document proper periodic training. This will consist of, but need not be limited to the following:

• Meetings with, and instructions or guidance given by the Board, Chief Executive Officer, or other superiors.

• Meetings and discussions with law enforcement officials.

• Meetings and discussions with financial institution security officers in the area.

• Reading security manuals published for the financial community.

It will be the policy of this institution that the security officer will prepare, implement, maintain, and supervise a program for the initial training and periodic training of officers and employees who are assigned responsibilities, for performing duties under this written security program. The training program will also encompass initial training and periodic training of all employees in the proper use of security devices and in their proper conduct during and after a robbery, burglary or larceny.

The security officer is charged with the responsibility to provide for selecting, testing, operating, and maintaining appropriate security devices at each banking facility, as specified in the federal security regulations, and other security devices that are deemed appropriate, upon the concurrence of this Board.

OPENING AND CLOSING PROCEDURES

The Officer of the Day and/or an Officer will be designated to open each subsidiary office.

The Ameris Bank closing procedures will also be established to include the initial closing of the premises, which generally span a period of time immediately prior to and immediately after locking the doors for business; and the final closing, which occurs when the last employees leave for the day. The Officer of the Day, Supervisor or a designated employee will be responsible for inspecting the premises before the last employee leaves for the day.
SAFEKEEPING PROCEDURES

The procedures for safekeeping of all currency, negotiables and similar valuables at all times are as follows:

Cash Limits

The amount of currency maintained at each banking office and within each teller’s station will be kept at a reasonable minimum commensurate with operational needs. The security officer will establish the specific maximums permitted.

Safe Removal of Cash

The movement of cash to and from a banking office and between tellers’ stations and other areas, such as the vault or safe, will be accomplished in the most secure and expeditious manner possible.

Receipt and Shipment of Cash

There will be a receipt system established to ensure that all shipments of cash, either sent or received, are properly accounted for and to provide an audit trail if it becomes necessary to trace a shipment. This system will apply to all shipments, whether handled by bank employees, armored courier, the U.S. Postal Service or some other means.

Identification of Persons Committing Crimes

This institution will maintain procedures that will assist in identifying persons committing crimes against the Bank and will preserve evidence that may aid in the identification, apprehension and prosecution of the perpetrators. Such procedures will include:

• Identification devices, such as prerecorded serial-numbered bills (bait money), cameras in banking offices and cameras in ATM locations where feasible.

• A record of any robbery, burglary or larceny committed against the institution.

SECURITY DEVICES

This Bank will maintain a security system that consists of the following components or devices:

• Vaults and/or safes for protecting cash, negotiables and other liquid assets.
• A lighting system that illuminates the area around the vault or safe during the hours of darkness, if it is visible from outside the banking office.
• Tamper-resistant locks on all exterior doors and windows that can be opened.
• An alarm system that will promptly notify the nearest responsible law enforcement agency of any actual or attempted robbery or burglary.
• Cameras that record activity in the banking office.
• Prerecorded serial numbered bills to be given out in each robbery.
• Time locks on vaults and safes to prevent opening other than at specified times.

Selecting Security Devices

Ensure that all existing security devices, and future acquisitions of devices, meet or exceed industry standards. In determining and recommending the needs for security devices, in addition to those specified in the regulation (e.g., lighting, locks, and alarms), the security officer will take the following into consideration:

• The incidence of crimes against financial institutions in the area.
• The amount of cash and other valuables exposed to robbery, burglary, or larceny.
• The distance of the banking office from the nearest responsible law enforcement office.
• Other security measures in effect at the banking office.
• The physical characteristics of the structure of the banking office and its surroundings.

Furthermore, the security officer is charged with the responsibility to design procedures to ensure that installed security devices are properly tested, operated and maintained.

Testing Security Devices

Develop a schedule (daily, weekly or monthly) for testing all security devices and a means to document that the testing was accomplished.

Operating Security Devices

Ensure that all security systems and devices are turned on and operating during the time they are intended to be operational. This process will include a visual inspection of the control systems of the devices to determine whether the devices are working and functioning properly.

Maintaining Security Devices

Schedule preventive maintenance inspections and maintain a record of same.

INCIDENT REPORTS

The security officer will ensure that a record is retained of any burglary or larceny committed against the institution. The security officer’s annual report to the Board will include a section that contains, at a minimum, the number of such incidents at each banking office, effectiveness of the security devices and procedures, data regarding losses and injuries, as well as information about the identification and prosecution of the perpetrators of the incidents.

AUDIT AND INDEPENDENT REVIEW
The Bank has designated the Internal Audit Department to conduct periodic risk based internal audit reviews of the Bank’s efforts to adhere to the guidelines of this policy. Results of the audit are reported to the Audit Committee. It is the responsibility of the Information Security Officer to take appropriate action to correct any exceptions found as a result of the audit.

Refer to the institution’s security manual for further information.