Acceptable Use Policy

IT and Operations – Section 100

Policy # 100.110

Organizational Functional Area:	**IT and Operations**
Policy For:	**Acceptable Use Policy**
Date Originated:	**Prior to 2008**
Date Revised:	**05/29/2018**
Date Board Approved:	**07/23/2019**
Department/Individual Responsible for Maintaining Policy:	**Chief Technology Officer**
Topic: Acceptable Use	**Section 100.110**

OVERVIEW

This policy is applicable to Ameris Bank and all officers and employees thereof. Employees who violate any of the guidelines set in the policy may be subject to disciplinary action including written warnings, revocation of access privileges, and termination. Ameris Bank also retains the right to report any illegal violations to the appropriate authorities.

SCOPE

This policy addresses the acceptable use of computer systems, networks, internet, voice systems and email communications.

RESPONSIBILITY

The Chief Technology Officer or his designee will have the primary responsibility for overseeing compliance with all provisions of this Policy. All employees of Ameris Bank have the responsibility of complying with this Policy. Additionally, all employees will be required to review this policy annually. Unauthorized activities are prohibited and will be brought to the attention of Bank management and could result in disciplinary actions for those in violation of this Policy.

GENERAL PRINCIPLES

- Systems provided for employee use are considered company resources and are intended to be used for business purposes. Limited personal use is permitted; however, usage may be monitored for unusual or unacceptable activity and logged.
- Employees are responsible for any violation of policy or malfeasance committed under their user name.

COMPUTER ACCESS

Ameris Bank employees depend on the proper operation of the bank's computer systems to do their job. Insuring the reliability of these machines and thereby your ability to execute your job duties is dependent upon your cooperation. All employees must agree to, and abide by, the conditions and requirements of this policy.

User Responsibility

All users of Ameris Bank systems will:

- Lock their computers when leaving their terminal unattended. Users should not depend upon the system configured time out feature to secure their session.
- Log off their computers when leaving the bank.
- Save word processing, spreadsheet, database or any other data files to the appropriate file store assigned to them. It is the user's responsibility to back up files to a network server on a regular basis if stored in a location other than a network server (i.e., local hard drive).
- Comply with the Mobile Computer Policy if assigned an applicable device.
- Comply with the Removable Media Acceptable Use Policy.
- Comply with the Email Acceptable Use Policy.
- Report to the Help Desk as soon as possible if any device is lost or stolen.
- Not engage in online gaming during working hours or install any gaming software on company devices.
- Not access non-job related streaming media on company devices.
- Not use company equipment or other resources for any purpose other than that authorized by the Chief Innovation Officer or his designee.

- Not make any changes or modifications to the bank's devices or software without the approval of the Chief Innovation Officer or his designee. Requests for changes should be directed to the Help Desk.

NETWORK ACCESS

You, as an employee of Ameris Bank, are given access to private customer data and proprietary company information through the bank's network. It is your duty under law to safeguard this information, to insure its accuracy and protect its privacy. It is likewise the bank's duty under law to insure that its employees honor their legal obligations. One way Ameris Bank accomplishes this is by monitoring and logging all transactions and requests for information over the network.

Before you can access the network, you are required to enter your user name and password. Since you are the only person who knows the password for your user name, only you can log in using it. And since you are the only person who can log in under your user name, the bank holds you responsible for transactions and/or requests logged using that user name.

User Responsibility

All users accessing company network will:

- Change their password whenever they know or suspect that it is no longer secure and not known to any other person.
- Use passwords that meet or exceed the network requirements for passwords as established by each system.
- Change their passwords when required by each systems established parameters for password age.
- Not divulge their passwords to anyone including support personnel.
- Not use easily guessed passwords such as their first or last name, the word "PASSWORD", their birth date, phone number, etc.
- Not examine, change, or use another person's files, output, or user name for which they do not have explicit authorization.
- Not reveal or publicize confidential or proprietary information which includes, but is not limited to: financial information, confidential client information, marketing strategies and plans, databases and any information contained therein, client lists, computer software source codes, computer/network access codes, and business relationships.
- Not use company equipment or other resources for any purpose other than that authorized by the Chief Innovation Officer or his designee.
- Not disable or remove security software from company devices.

NETWORK ATTACHED DEVICES

- Connecting non-approved computing or computing devices to the Ameris network is prohibited unless specifically authorized by the Information Technology Department. Devices include but are not limited to portable drives, data keys/USB keys/thumb drives, portable music devices, smart phones, tablet computers, notebook computers, desktop computers, or any mass storage device not specifically listed in this policy. A network connection is defined as any connection either wired or wireless that enables the transportation of data between two or more network connected devices. Examples of network connections include, but are not limited to, serial, parallel, USB, patch cable, Bluetooth, wireless or any other communication means not specifically defined by this policy. Only approved devices which are issued and documented by the Information Technology Department may be used to connect to the Ameris Bank network.

Employees should understand the following:

- All network attached devices and any associated peripheral devices are monitored by the Information Technology Department. The Information Technology Department asserts and maintains authority over all network attached devices and peripherals and reserves the right to confiscate any device not approved for use on the Ameris Bank network.
- The Information Technology Department will maintain an inventory of all approved devices by type and serial number. Any device that is used to connect to the Ameris Bank network to transfer or transport data must use 256-bit Advanced Encryption Standard (AES) hardware-based encryption. Encrypted information must be accessible using passwords that comply with the standard for complex passwords.
- Unless specifically authorized, employees are prohibited from changing the network settings, security settings, passwords, port settings, BIOS instructions, or attempting in any other way to circumvent security restrictions on the Ameris Bank network or attached devices.
- Connecting an unauthorized device to the Ameris Bank network and/or transferring data using an unauthorized device is considered a potentially serious security breach and a cause for disciplinary action up to and including termination.

INTERNET ACCESS

Internet access is deemed to be a business tool providing a source of information with the potential for benefiting all areas of Ameris Bank and enhancing customer service, customer retention, and growth. Therefore, it is the policy of Ameris Bank that management will approve Internet access as deemed appropriate and will determine what components of the Internet will be available (email, World Wide Web, newsgroups, list-servers, social media sites, etc.). All employees accessing the Internet on company equipment or on a company Internet access account should become proficient in its capabilities, practice proper network etiquette, and agree to the conditions and requirements of this policy.

User Responsibility

All Internet users will:

- Not knowingly visit prohibited Internet sites including those that contain obscene, hateful or other objectionable materials;
- Not send or receive any material, whether by email, voice mail, memoranda or oral conversation, that is obscene, defamatory, harassing, intimidating, offensive, discriminatory, or which is intended to annoy, harass, or intimidate another person.
- Not solicit non-company business for personal gain or profit.
- Not use the Internet or email for any illegal purpose.
- Not use the Internet or email for offensive or vulgar messages such as messages that contain sexual or racial comments or for any messages that do not conform to Ameris Bank's policies against harassment and discrimination.
- Not attempt to download or install any software or electronic files without the express consent of the Chief Innovation Officer or his designee.
- Not represent personal opinions as those of Ameris Bank or purport to represent Ameris Bank when not authorized to do so.
- Not make or post indecent remarks, proposals, or materials.
- Not upload, download, or otherwise transmit commercial software or any copyrighted materials.
- Not intentionally interfere with the normal operation of the network in a manner which substantially hinders others in their use of the network.
- Not reveal or publicize confidential or proprietary information which includes, but is not limited to: financial information, confidential client information, marketing strategies and plans, databases and any information

contained therein, client lists, computer software source codes, computer/network access codes, and business relationships.
- Not perform any other uses identified by Ameris Bank as inappropriate.
- Not share passwords with any other user.
- Not identify themselves in any way other than honestly, accurately, and completely while participating in chats or newsgroups, or when setting up accounts on outside computer systems.

Telephony and Instant Messaging Systems

Ameris Bank provides its employees with access to a number of devices and services to facilitate business communications. Similar to Internet and email access, telephone, voicemail, fax, instant messaging and cell phone services are available for business purposes with the intent of facilitating customer service and general operating efficiency. Limited personal use of these services is generally permitted provided that it is not disruptive, is conducted during appropriate times, and does not present material costs to the bank.

User Responsibility

- Limit personal telephone calls during work hours.
- Use voicemail professionally. Greetings should be courteous, but not provide unnecessary details that could be used to facilitate a fraud or security breach.
- Password-protect voicemail boxes according to the bank's password standards. Messages should be returned promptly and voicemail boxes should be purged of old messages regularly.
- Not leave faxes unattended on machines in public or unsecured areas as they may contain confidential information.
- Not make or attempt international calls without express consent of executive management.
- Not accept or facilitate any collect charges from a third party or accept or make calls which will result in reverse charges to Ameris Bank.
- Understand that there is no expectation of privacy when using Ameris Bank voice systems. All data and voice traffic is monitored and can be recorded if deemed necessary and approved by executive management.
- Internal instant messaging is monitored and archived for retention purposes.
- Text messaging causes drivers to take their eyes off the road and at least one hand off the steering wheel, endangering both themselves and others. Texting while driving on official business or while using Ameris Bank owned equipment is strongly discouraged and prohibited in circumstances where it is against state law.

ELECTRONIC COMMUNICATION (Email, Instant Messaging and Texting)

Personal Use

Personal use of the bank's email system should be kept to a minimum. As previously stated, the bank may monitor email both incoming and outgoing on a regular basis. Accessing personal email or alternate email accounts, such as Gmail, Hotmail, Yahoo, etc., is prohibited.

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 Chief Innovation Officer to take appropriate action to correct any exceptions found as a result of the audit.

Acceptable Use Policy

EMPLOYEE CONSENT AND ACKNOWLEDGMENT FORM

I, (print name) _____, have read the Ameris Bank Acceptable Use Policy. I recognize that these systems are the property of the bank and that Ameris Bank reserves the right to monitor usage for any reason at any time. My signature on this document means I have consented to this monitoring. I understand that should I become aware of any misuse of Ameris Bank's systems, I am obligated to inform a member of management of such misuse immediately. I understand that the failure to abide by any of the provisions of this policy may result in disciplinary action up to and including immediate termination, without prior warning or notice.

Acknowledged and agreed to by:

Signature: _____ Date: _____

Employee's Signature