Policy Statement

This policy establishes guidelines for the professional, ethical, lawful, and productive use of Cullen/Frost Bankers, Inc. and its affiliates ("Frost") information systems, equipment, and resources by employees and applicable third parties, and establishes safeguards for sensitive and confidential information.

It is the policy of Frost to protect customer, prospective customer, consumer, and employee information in compliance with any and all applicable federal and state laws.

Employees and applicable third parties who have access to the Frost network are responsible for the proper use and safeguarding of such information, as well as Frost proprietary information, whether in paper or electronic form.

This policy is intended to supplement the provisions of the Frost Standards of Conduct and any other Frost policies regarding confidential information and record retention.

Further, this policy applies to information which is obtained, created, or maintained by employees and/or third parties of Frost. Information, data, and communications created or stored on Frost systems, or on Frost service providers' systems, is the property of Frost.

Frost has an information security program to manage and continually improve security. This program is maintained by the Enterprise Information Security department and enforced through Human Resources.

Employees may find this policy and other IT-related standards, practices, and policies in the Information Security and HR manuals in Gateway.

Policy Enforcement

Violations of this policy can lead to the compromise of data security, unauthorized disclosure of confidential information, system or equipment damage or destruction, potential monetary loss, or damage to Frost's reputation.

- A violation by an employee or applicable third party is subject to disciplinary action, up to and including termination
- Managers are responsible for notifying Human Resources of any violation of which they have knowledge. Human Resources conducts all investigations related to this policy.
- If a violation involves a data or privacy incident, employees must report the incident to the Help Desk first at x55100 (210-220-5100), **24/7**

Monitoring

For security, privacy, and compliance purposes, authorized individuals monitor Frost's equipment, systems, network traffic, and access and review any email, electronic communications, or Internet usage on such equipment and systems.

Frost reserves the right to review, audit, intercept, access, and disclose all messages created, received, or sent over the Frost email system or any other electronic communication network provided by Frost.
Employee email, Internet use, and other forms of electronic communications are for business purposes and are not to be misused.

Employees should have no expectation of privacy regarding any use of Frost's information systems, devices, and resources.

I. *Creating an Anonymous Compliant*

Email, electronic communications, and Internet usage are not anonymous. Your name and location are automatically attached to every message sent.

Under the provisions of the Sarbanes-Oxley Act, you may submit an anonymous complaint or other information about accounting or auditing matters without fear that you will be dismissed or suffer retaliation. To ensure anonymity, sender information is electronically removed from all email sent to **auditcommittee@frostbank.com**.

II. *Subpoenas*

Electronic messages can be subpoenaed as they are legally considered documents.

Access and Usage

- The Frost information technology department (IT) is responsible for the acquisition, installation, and technical support of information technology products
- The IT department establishes the technical architecture under which all client/server and other end-user computing devices or programs are deployed throughout the network
- Your computer (software and hardware) has been configured by Frost IT for use on the Frost network
- Email, Internet, removable storage media, or any other media may not be used to bring unauthorized or illegal software into the Frost network
- If there is a business reason to bring software into the network, contact the Help Desk at x55100 for assistance

I. *Login Credentials*

- Do not share login IDs and passwords or allow anyone to use them
- Secure your IDs and passwords. Don't leave them in obvious places that can be accessed by unauthorized persons.
- If you suspect that someone knows your password, change it immediately

II. *Cloud Storage Services*

- Internet-based (Cloud) storage services such as, but not limited to, Dropbox, iCloud, and Skydrive are not accessible from the Frost network and are not be used to store Frost data
- Frost data may only be stored in an authorized Frost provisioned cloud service

If a legitimate business reason exists to access these services, a Service Catalog request may be submitted for evaluation and temporary access may be granted to use ShareFile to fulfill the business need.

III. Removable Media

The use of removable media is restricted for business purposes only and must be approved by IT management.

For assistance in acquiring a Frost approved encrypted USB drive, contact the Help Desk at x55100

IV. Remote Access

Remote access to connect to the Frost network using a personal PC or a Frost mobile device may be permitted with management approval.

Email and Internet Usage

I. Email and Internet

Email, internet, or any electronic communications usage that is discriminatory, harassing, threatening, vulgar, or hostile in any way is not permitted.

- Frost cannot ensure the confidentiality of e-mail leaving the network to its final destination, nor can it ensure that email generated within the organization is not copied or forwarded
- Access to certain web sites and personal email accounts may be blocked. If a legitimate business need arises for a blocked site, contact the Help Desk at x55100 for assistance.

II. Secure Email

Any sensitive, confidential, or Frost proprietary information transmitted outside of Frost must be for company and business purposes only, approved for sharing by management, and must utilize a secure method of transmission.

Frost-Issued Mobile Devices

Data contained on a Frost-issued mobile device is subject to the same policies and rules as a company-provided workstation/laptop. You are responsible for securing any Frost-issued device.

Immediately contact the Help Desk at x55100 (210-220-5100), **24/7**, if your Frost issued mobile device has been lost or stolen.

Protecting Information

Non-Frost individuals have access to some Frost buildings and could look for and steal customer or company information.

- You are responsible for the security of work station devices and customer and Frost information whether in paper or electronic form
- Use the locked shred bins for sensitive information
- Don’t leave any information or devices covered by this policy in vehicles or unprotected in your home, a hotel, or other locations

Immediately report any loss or similar concern to the **Help Desk** at x55100 (210-220-5100) **24/7**.

3rd Party Acknowledgement

Signature:___________________________
Name:______________________________
Company:___________________________
Company Email:_____________________
Date:_______________________________