Information Security and Privacy Awareness

For Third Parties

The Guiding Info Security and Privacy Principles

- Protect Frost and customer information
- About the virtual private network (VPN)
- Use **secure email** when sending sensitive customer or proprietary information and validate the recipient name(s)
- Avoid social engineering scams and think before clicking on links or attachments in emails or texts
- **Dispose** of customer information in the locked shred bins daily and follow the **clean desk** rules
- Only discuss transactions and information with those that have a business need to know
- Report any concerns relating to information security or privacy to your Frost sponsor

❖ Protecting Information

It's your responsibility to protect the confidentiality and security of Frost customer and proprietary information, whether paper or electronic form.

- Always keep devices and documents with you at all times
- Don't leave items in cars or unprotected in your home or hotel
- When traveling, use the hotel safe if available if you can't take the item with you
- Don't forget to collect your briefcases and other devices when going through airport security

Immediately report any loss or concern to your Frost sponsor.

❖ Virtual Private Network (VPN)

Frost utilizes a virtual private network (VPN) to permit certain users to connect to Frost using their PC or mobile device. This mirrors the experience of working in a Frost facility.

What you need to know

While using VPN, you must go through Frost if you connect to another internet source. Because of this internal security protection, you may:

- Experience slightly slower internet speed
- Find that your home or local connection printers may not work during the VPN session

Frost monitors and logs traffic, and enforces web filtering policies. You benefit from Frost intrusion protection and antivirus capabilities to help protect both the network and your device.

Why is this important?

A simultaneous internet connection outside the Frost VPN could allow malicious software access to Frost information or resources without an opportunity to detect or block the attack, causing potential damage to information and systems.

❖ Secure Email

Always use the **Send SECURE** function in Outlook mail when sending any sensitive customer information outside the Frost network. Be sure that:

- You are sending it to the correct recipient(s)
- The "To" name(s) is added after the message is written
- You double check that the name is the correct one

Emails are monitored to validate that sensitive data is sent via this secure method.

❖ Phishing, Malware, and Social Engineering

Cyber criminals have become increasingly sophisticated in their attempts to take over and use personal information for their own gain. They try to manipulate you to perform actions or give up confidential information that can harm you or Frost.

What can the cyber criminals do?

- Hack into your email address and steal information from your device
- Send fraudulent links or websites that install malware - harmful software that can cause damage / disruption to your device or Frost systems
- Ask outright for your personal information saying there is a problem with your account

What should YOU do, whether at the office or at home?

- Only click on links from known sources and from whom you are expecting something
- If you receive something you are unsure of, **DELETE** it

❖ Secure Disposal of Customer Information

Protect customer and Frost information at the office as well as away from the office:

- Empty the desk-side shred box daily into a secure, locked shred bin
- Lock sensitive information in a drawer or cabinet when you step away from your desk and leave for the day
- Ctrl-Alt-Del to lock your computer when you step away from your area

Know that people can access some of our buildings or offices and look for and steal sensitive customer or Frost information.

❖ Sharing Information

The confidentiality of customer information is central to protecting Frost and its customers.

You may **not disclose** customer or Frost information with anyone who doesn't have a business need to know.

❖ Your Frost Sponsor

Your Frost sponsor is the first call you should make if you have a potential privacy, information security or physical concern, or any other issue while working at Frost. What's an issue?

- Lost laptop, thumb drive, mobile device even if no customer information is stored on it
- Lost or misplaced customer or Frost information (paper or electronic) such as names with account numbers, social security numbers, health information, date of birth, balances
- You clicked on a link, attachment or website that you think has compromised your work-related computer or device
- Any other issue affecting your work environment

Signature:_____

Name:_____

Company:_____

Company Email:_____

Date:_____