Handling sensitive information: do’s and don’ts

Here are some measures to take and things to avoid when handling sensitive information.

✓ Do

- Make sensitive information inaccessible when you are not using it:
  - ~ Use digital safeguards like passwords and multifactor authentication for accessing your sensitive digital information.
  - ~ Use physical safeguards for sensitive information on paper, which could include locked filing cabinets or locked desk drawers.
- Comply with role-based access controls, which determine the permissions that individual employees are granted based on their role.
- Visit only legitimate and trusted websites.
- When getting rid of physical media like a CD, external hard drive, or outdated computer, make sure to destroy it. Some forms of media storage, such as CDs, can be put through a paper shredder.
- Use only high-quality shredders that crosscut paper into small pieces. If you do not have access to a high-quality shredder, seek guidance from your manager or IT team.
- Be aware of the legal and regulatory requirements for data and record retention and routinely destroy archived data and records that no longer need to be retained.

! Don’t

- Don’t share access or login credentials with anyone else. It’s important that you are aware of and follow all cybersecurity policies regarding the use and sharing of credentials.
- Don’t remove or disable safeguards like firewalls or anti-virus software on your personal or work devices. Doing so could endanger the sensitive information stored on your system.
- Don’t provide sensitive information to anyone before verifying they are who they say they are. Always call them using a known phone number that you already have on record.
- Don’t assume that data not labeled as private does not still include sensitive business information.
- Don’t forget the business’s data classification levels and appropriate measures for handling data. If you’re unsure, seek guidance from your manager or IT governance team to determine the classification level and handling protocols.
- Don’t assume that deleted data has been completely erased from your media drives. The data remains on the drive until it is written over with new files. Clearing and purging media drives is highly recommended.

Scotiabank®