Checklist for Protecting Sensitive Information

This checklist was developed as a guideline to ensure the protection of sensitive information. Information security is a business need that, in addition to providing security technologies, must extend to what people do and how they do it. Using this checklist will assist in protecting the Confidentiality, Integrity, and Availability (CIA) of information systems and assets.

Take Action

- ☐ Participate in Information Security Awareness & Training
- ☐ Work in sensitive areas should be communicated with discretion.
- ☐ The location of sensitive office(s) should be communicated with discretion.
- ☐ Question unfamiliar individuals entering restricted areas.
- ☐ Watch for individuals 'tailgating' into restricted areas.
- ☐ Ensure all individuals are wearing/displaying their issued ID.
- ☐ A clean desk policy should be followed at all times.
- ☐ Report all security incidents (real or suspected) to the Support Desk and security officer.
    - Physical security: theft, break-in, physical threats: report
    - Information security: hacking, phishing, viruses, compromised accounts or systems: report
    - OH&S: hazard, near miss: report
    - Privacy: breach of PII: report

Oral Communication

- ☐ Use discretion when discussing sensitive information.
- ☐ Be aware of the potential for others to overhear communications about sensitive information in offices, on telephones, or in public places like elevators, restaurants, and sidewalks.

Paper Documents

- ☐ Consider secure briefcases or folders for documents being physically transported.
- ☐ Establish a chain-of-custody for the receipt and forwarding of sensitive documents being physically transported.
- ☐ Do not leave sensitive documents unattended; protect them from the view of all non-authorised persons.
- ☐ Store sensitive documents in locked cabinets.
- ☐ Ensure all keys to cabinets are secured, and are part of a key control system.
- ☐ Store documents that contain sensitive information and identified as critical to the conduct of business in fireproof file cabinets. Keep copies in an alternate secure location.
- ☐ Disposal of documents is to follow policy.
- ☐ Immediately retrieve or secure sensitive documents that are printed on copy machines, fax machines, and printers.
- ☐ When printing, ensure the printer location before clicking 'print.'
- ☐ When faxing, recheck the recipient's fax number before pressing 'start.'

- ☐ When faxing, ensure an authorized recipient is present at the receiving location prior to sending.
- ☐ When receiving faxes, ensure that an authorized person is present to receive the fax. Identify to business partners that faxes are not to be sent after business hours unless an authorized person is present.

Protecting Email

- ☐ Understand that email can be forged; it is possible to impersonate someone else in an email.
- ☐ Do not open unexpected email attachments, and do not download documents or software from unknown parties; they may contain viruses or other malware.
- ☐ Use discretion when sending information by email. Recipients can potentially distribute information to unauthorized recipients or store it on unsecured devices.
- ☐ Encrypt (password protect) any sensitive documents.
- ☐ Do not send emails that contain confidential mailing lists.
- ☐ Verify all recipients' email addresses before clicking 'send.'
- ☐ Do not use personal email to send/receive business information.

Restricting Access To Information On Your Computer (Desktop or Laptop) or Mobile Device

- ☐ Orient computer and mobile device screens away from the view of people passing by.
- ☐ Turn off computers at the end of the workday, unless otherwise directed.
- ☐ Lock computers or mobile devices when not in use.
- ☐ Use security devices to lock down laptop computers.
- ☐ Do not allow non-authorized persons to have access to computers or mobile devices.

Protecting Passwords & Access

- ☐ Employ passwords that are easy to remember but impossible for someone else to guess. (10 characters, mix of upper & lower case letters, numbers, and special characters)
- ☐ Secure passwords and restrict access to them. Passwords written on a post-it in a work area, placed under a keyboard, or stored in an unlocked desk drawer are not safe from unauthorized access.
- ☐ Never share passwords or accounts; this includes with assistants who should not have access to some sensitive information.
- ☐ Be mindful of surroundings when entering login credentials; there may be the opportunity for others to 'shoulder surf'.
- ☐ Be aware of social engineering, such as phishing, which may try to get you to divulge your login credentials.
- ☐ Use 2-factor authentication when possible.

Alberta

Checklist for Protecting Sensitive Information

Safeguarding the Integrity of Information

- ☐ Follow all usage policies for the information systems to which you have been given access.
- ☐ Store all information on a centrally managed server and not on individual computers or mobile devices.
- ☐ Try to minimize the number of devices that may have access to sensitive information.
- ☐ Do not place any information in an unsecured online location (such as Dropbox).
- ☐ Do not use instant messaging or social media services to send information.
- ☐ When transporting or storing information, use encrypted storage devices. This includes laptop hard drives, USB thumb drives, external hard drives, and mobile devices.
- ☐ Lock up any encrypted storage devices; do not leave visible in vehicle or other location.
- ☐ Revoke or suitably adjust (physical, network, system and application) access and change shared passwords as soon as staff leave or change responsibilities.
- ☐ Maintain an inventory of all issued encrypted storage devices. Staff must return all devices containing sensitive information as they leave or change responsibilities.
- ☐ When possible, only access sensitive information from approved devices.

Information in Meeting Rooms

- ☐ Remember to clean whiteboards and remove flipcharts, papers and notes when they contain information.
- ☐ Use meeting rooms where sensitive information cannot be observed by outside parties.

Completed by: _____

Signature: _____

Verified by: _____

Signature: _____

Date: _____