REFERENCE SHEET

EXCHANGING CONFIDENTIAL INFORMATION

Purpose of the document

Provide advice and tools to safely exchange confidential information.

Exchanging information is a fundamental component of our work. However, disclosing and updating confidential information involves many risks. It is therefore important to adapt how information is exchanged based on the method used.

Recommendations

General recommendations to follow regardless of the method you use:

- Check the recipient's identity
- Follow the "need-to-know" principle and do not disclose confidential information to anyone not authorized.

Specific recommendations for each method used:

 **In person**	• Go to a closed room or office • Avoid mentioning names, places, or any other information that would make it possible to identify someone.
 **By phone**	• Do not leave confidential information on a voicemail box. Ask the person to call you back. • Go to a closed room or office • Avoid mentioning names, places, or any other information that would make it possible to identify someone.
 **By email**	• Do not write any confidential in the body of an email message • Put confidential information instead in a file and encrypt it with an authorized encryption tool • Add a confidentiality notice at the bottom of the email • Check the recipient's email address before sending an email • Use a different communication method to send the password for a file (e.g. phone, fax, SMS) • Do not ask a client for confidential information if they did not contact you or expect you to contact them. Otherwise, you can only ask them for their first and last name, age, phone number and email and postal address on file (e.g. for contests, promotions).

 **Via removable media**	• Save confidential information in a file and encrypt it with an authorized encryption tool • Provide the password for the key or encrypted file by email, phone, in person, etc. • Once the information has been transferred, destroy the information contained on the USB key • To keep malware from spreading, do not insert USB keys on any of your workstations if you do not know where they come from.
 **By mail**	• Check that the person's contact information is up to date before sending them information. • Do not ask a client for confidential information if they did not contact you or expect you to contact them. Otherwise, you can only ask them for their first and last name, age, phone number and email and postal address on file (e.g. for contests, promotions). Do not ask their date of birth. • Insert the document or medium in an opaque envelope or package so that the contents cannot be seen or recognized by touch. • Send the envelope or package via the registered delivery service of a reputable company (e.g. Canada Post's Xpresspost, UPS, FedEx, Dicom Express, Purolator) • Take note of the tracking number. • Ask for a signature upon delivery.
 **By SMS**	• Do not exchange confidential Information.
 **Via cloud computing technology**	• Use only your organization's authorized cloud file sharing service. • Encrypt confidential information exchanged using a cloud file sharing service. • Grant access to a file or document only to authorized individuals. • Remove access to a file or document as soon as the person no longer needs access to it. • Log out of the cloud file sharing service when you finish using it if the computer you are using is shared with other people.
 **By videoconference**	• Go to a closed room or office • Avoid mentioning names, places, or any other information that would make it possible to identify someone.