QUICK REFERENCE

SHARING CONFIDENTIAL INFORMATION

Objective

Provide advice and tools to securely share confidential information.

Sharing information is one of the most common things we do at work. However, there is a high risk that confidential information may be disclosed or modified. Therefore, it's important that we adapt the way information is exchanged to the method used.

Target recipient: Everyone

Last update: 2017-06

Recommendations

General recommendations to follow, regardless of the method used:

- Confirm the recipient's identity.
- Follow the "need-to-know" principle and don't disclose confidential information to unauthorized persons.

Specific recommendations for each method:

In person	• Find a room or an office where you can close the door. • Try not to specify names, places, facts or any other information that could identify someone.
Phone	• If you're leaving a message, don't include any confidential information. Ask the person to call you back. • Find a room or an office where you can close the door. • Try not to specify names, places, facts or any other information that could identify someone.
Email	• Don't write confidential information in the body of an email. • Put confidential information in a file and encrypt it with an approved encryption tool. • Add a confidentiality notice at the bottom of emails. • Double check the recipient's email address before you send the email. • Send the file password by another means of communication other than email (e.g., phone, fax, text message).

	• Don’t ask clients for confidential information if they did not solicit and expect the communication. If not, only first and last names, addresses (mailing and email), age and phone number in the file may be requested (e.g., in the case of contests, promotions, etc.).
 **Removable media**	• Put confidential information in a file and encrypt it with an approved encryption tool. • Send the flash drive or file password by email, telephone, in person, etc. • Once the transfer is complete, delete the information on the flash drive. • Don’t insert USB flash drives from unknown sources on your workstations to avoid malware.
 **Mail**	• Make sure that the recipient’s contact details are up to date. • Don’t ask clients for confidential information unless the communication was solicited and expected. If not, only first and last names, age, addresses (mailing and email) and phone number in the file may be requested (e.g., in the case of contests, promotions, etc.). • Put the documents or material in an envelope or parcel that ensures privacy and conceals the contents (e.g., no address window, not identifiable by touch) • Use a reliable service to send the envelope or parcel by registered mail (e.g., Canada Post – Xpresspost, UPS, FedEx, Dicom Express, Purolator, etc.). • Keep the tracking number. • Ask for a signature of receipt.
 **SMS**	• Don’t exchange confidential information.
 **Cloud**	• Only use cloud file-sharing services approved by the company. • Encrypt confidential information shared through the cloud. • Only give authorized individuals access to files and documents. • Remove access to a file or document once the individual no longer needs it. • If you share your computer, log out from the cloud file-sharing service when you’re finished.
 **Videoconference**	• Find a room or an office where you can close the door. • Try not to specify names, places, facts or any other information that could identify someone.