Handling a privacy incident

Source: Commission d'accès à l'information (CAI) (S2) https://www.cai.gouv.qc.ca/protection-renseignements-personnels/information-entreprises-privees/incidents-confidentialite-mesures-securite-entreprises ; notice form (S3) https://www.cai.gouv.qc.ca/uploads/pdfs/CAI_FO_Incident_Conf.pdf (CAI documents are in French.)

1. Take reasonable measures to reduce the risk of injury.
2. Assess the risk of serious injury: sensitivity of the information, anticipated consequences, likelihood of injurious use.
3. If the risk is serious: notify the CAI (form S3) and the persons concerned.
4. Record every incident in the register, kept for at least 5 years. Register template: date, description, information involved, number of persons, risk assessment, notices sent (yes/no, date), measures taken. Microsoft 365 side: the audit log helps reconstruct the incident, https://learn.microsoft.com/en-us/purview/audit-log-enable-disable . NIST CSF 2.0: RS and RC functions. To be validated: the 6 mandatory elements of the notice and the exact register fields, to be copied from S2 (CAI website access was limited at the time of writing).