Privacy & Data Security Seminar: How Are You Managing Your Risk?

Wednesday, November 6, 2019 | The Fairmont Hotel Vancouver

- ☐ Organizational Risk Analysis Checklist
- ☐ Model Incident Response Plan
- ☐ Model Acceptable Use Policy

LAWSON LUNDELL LLP

Model Cyber Incident Response Plan

Overview:

This draft model cyber incident response plan (IRP) outlines how organizations can prepare for and respond to cyber attacks, data breaches, and other information security incidents. This is intended to provide guidance for developing an IRP but is not a comprehensive guide. Every organization will have different risks and unique issues which should be considered when developing an IRP,

Each incident presents unique facts and circumstances, making it difficult for organizations to prepare for every type of event that may arise. An incident response plan (IRP) provides a standard framework that helps organizations prepare for and effectively handle cyber attacks, data breaches, and other information security incidents.

This model IRP:

- Provides guidance for developing an IRP as applicable Canadian laws, regulations, and best practices may require for various organization types, including those mandated to maintain a comprehensive written information security program (WISP).
- Provides an outline of how organizations can prepare for and address information security incidents.
- Outlines the key elements that organizations should consider in developing an IRP.

Legal basis:

Some Canadian jurisdictions have enacted legislation requiring mandatory notification of breaches of security and/or unauthorized access, use or disclosure of personal information. These require timely notification to regulators and individuals of breaches which may give rise to a real risk of harm. It may be difficult for an organization to effectively comply with these requirements without an effective IRP.

Organizations also have obligations to mitigate privacy breaches in accordance with common law principles and may face liability for failing to do so. An IRP can help address responsible and timely mitigation.

An IRP will also help the organization demonstrate that it takes reasonable steps to protect personal information and other sensitive or confidential information, especially if an information security incident gives rise to potential civil claims or regulatory enforcement.

Overall, an established and practiced IRP will help an organization respond more rapidly and effectively to information security incidents.

"Incident" vs. "Breach"

We have intentionally used the term "incident" rather than "breach" or "data breach" in this draft. Organizations should be careful when using the term "breach" as it may have unintended legal implications. In some circumstances, "breach" alone or in conjunction with "privacy" or "security safeguards" have a legal meaning.

Not all, in fact many, incidents do not have legal implications. Some may be appropriately addressed through implementation of the IRP and some do not rise to the level necessary for IRP implementation.

Record keeping

Some legislation (PIPEDA as an example) requires organizations to keep records of all breaches of security safeguards of personal information under its control – whether there is a real risk of significant harm or not.

The following outline should be used to consider further the issues that require completion for the IRP.

1. **Purpose.** The purpose of this cyber incident response plan ("IRP") is to provide a structured and systematic incident response process for all information security incidents (as defined in Section 4, Definitions) that affect any of [ORGANIZATION]'s information technology ("IT") systems, network, or data, including [ORGANIZATION]'s data held or IT services provided by third-party vendors or other service providers.

1.1 Specifically, [ORGANIZATION] intends for this IRP to:

(a) Define [ORGANIZATION]'s cyber incident response process and provide step-by-step guidelines for establishing a timely, consistent, and repeatable incident response process.

(b) Assist [ORGANIZATION] and any applicable third parties in quickly and efficiently responding to and recovering from different levels of information security incidents.

(c) Mitigate or minimize the effects of any information security incident on [ORGANIZATION], its [customers/clients], employees, and others.

(d) Help [ORGANIZATION] consistently document the actions it takes in response to information security incidents.

(e) Reduce overall risk exposure for [ORGANIZATION].

(f) Engage stakeholders and drive appropriate participation in resolving information security incidents while fostering continuous improvement in [ORGANIZATION]'s information security program and incident response process.

1.2 [[ORGANIZATION] developed and maintains this IRP as may be required by applicable laws and regulations [, including [APPLICABLE LAWS AND REGULATIONS]].]

2. **Scope.** This IRP applies to [all [ORGANIZATION] business groups, divisions, and subsidiaries; their employees, contractors, officers, and directors; and [ORGANIZATION]'s IT systems, network, data, and any computer systems or networks connected to [ORGANIZATION]'s network /[DEFINE SCOPE]].

2.1 [Other Plans and Policies. [ORGANIZATION] may, from time to time, approve and make available more detailed or location or work group-specific plans, policies, procedures, standards, or processes to address specific information security issues or incident response procedures. Those additional plans, policies, procedures, standards, and processes are extensions to this IRP. [You may find approved information security policies and other resources at [RESOURCE LISTING].]]

3. **Accountability.** [ORGANIZATION] has designated [TITLE/PERSON] to implement and maintain this IRP (the "information security coordinator").

3.1 Information Security Coordinator Duties. [Among other information security duties [, as defined in [ORGANIZATION]'s written information security program ("WISP") available at [WISP REFERENCE],] the information security coordinator/The information security coordinator] shall be responsible for:

(a) Implementing this IRP.

(b) Identifying the incident response team ("IRT") and any appropriate sub-teams to address specific information security incidents, or categories of information security incidents (see Section 5, Incident Response Team).

(c) Coordinating IRT activities, including developing, maintaining, and following appropriate procedures to respond to and document identified information security incidents.

(d) Conducting post-incident reviews to gather feedback on information security incident response procedures and address any identified gaps in security measures (see Section 11, Post-Incident Review).

(e) Providing training and conducting periodic exercises to promote employee and stakeholder preparedness and awareness of this IRP (see Section 12, Plan Training and Testing).

(f) Reviewing this IRP at least annually, or whenever there is a material change in [ORGANIZATION]'s business practices that may reasonably affect its cyber incident response procedures (see Section 13, Plan Review).

3.2 Enforcement. Violations of or actions contrary to this IRP may result in disciplinary action, in accordance with [ORGANIZATION]'s information security policies and procedures and human resources policies. Please see [HR POLICIES REFERENCE] for details regarding [ORGANIZATION]'s disciplinary process.

4. **Definitions.** The terms defined below apply throughout this IRP:

4.1 "Confidential Information.". Confidential information means information [as defined in [ORGANIZATION]'s [WISP/information security policy] available at [WISP OR POLICY REFERENCE]/that may cause harm to [ORGANIZATION] or its [customers/clients], employees, or other entities or individuals if improperly disclosed, or that is not otherwise publicly available].

4.2 "Personal Information". Personal information means information about an identifiable individual. [as defined in [ORGANIZATION]'s [WISP/information security policy] available at [WISP OR POLICY REFERENCE]/that [ORGANIZATION] owns, licenses, or maintains and that is from or about an individual including, but not limited to (a) first and last name; (b) home or other physical address, including street name and name of city or town; (c) email address or other online information, such as a user name and password; (d) telephone number; (e) government-issued identification or other number; (f) financial or payment card account number; (g) date of birth; (h) health information, including information [regarding the individual's medical history or mental or physical condition, or medical treatment or diagnosis by a health care professional/created or received by [ORGANIZATION]]; and (i) any information that is combined with any of (a) through (h) above].

4.3 "Information Security Incident.". Information security incident means an actual or reasonably suspected (a) loss or theft of confidential or personal information; (b) unauthorized use, disclosure, acquisition of or access to, or other unauthorized processing of confidential or personal information that reasonably may compromise the privacy or confidentiality, integrity, or availability of confidential or personal information; or (c) unauthorized access to or use of, inability to access, loss or theft of, or malicious infection of [ORGANIZATION]'s IT systems or third party systems that reasonably may compromise the privacy or confidentiality, integrity, or availability of confidential or personal information or [ORGANIZATION]'s operating environment or services.

4.4 [[ADDITIONAL TERM(S)]. [DEFINITION.]]

5. **Incident Response Team.** The incident response team ("IRT") is a predetermined group of [ORGANIZATION] employees and resources responsible for responding to information security incidents.

5.1 Role. The IRT provides timely, organized, informed, and effective response to information security incidents to (a) avoid loss of or damage to [ORGANIZATION]'s IT systems, network, and data; (b) minimize economic, reputational, or other harms to [ORGANIZATION] and its [customers/ clients], employees, and partners; and (c) manage litigation, enforcement, and other risks.

5.2 Authority. Through this IRP, [ORGANIZATION] authorizes the IRT to take reasonable and appropriate steps necessary to mitigate and resolve information security incidents, in accordance with the escalation and notification procedures defined in this IRP.

5.3 Responsibilities. The IRT is responsible for:

(a) Addressing information security incidents in a timely manner, according to this IRP.

(b) Managing internal and external communications regarding information security incidents.

(c) Reporting its findings to management and to applicable authorities, as appropriate.

(d) Reprioritizing other work responsibilities to permit a timely response to information security incidents on notification.

5.4 IRT Roster. The IRT consists of a core team, led by the information security coordinator, with representatives from key [ORGANIZATION] groups and stakeholders. The current IRT roster [is available at [IRT ROSTER LOCATION]/includes the following individuals:

[FUNCTION], [NAME], [CONTACT INFORMATION], [ALTERNATE/DESIGNATE CONTACT INFORMATION]]

[Drafting note: Organizations should establish an incident response team (IRT) as part of their incident response planning and preparation activities. The IRT:

- *Coordinates the organization's response to information security incidents.*
- *Controls internal and external communications regarding information security incidents.*
- *Manages risks to the organization and its employees, partners, and customers or clients.*

Organizations should tailor IRT membership to their unique activities, structure, and culture. However, information security coordinators typically enlist IRT members from:

- *Potentially affected departments or business units.*
- *Support functions, such as:*
  - *IT;*
  - *information security;*

- *legal;*
- *privacy;*
- *communications or public relations;*
- *human resources;*
- *risk management;*
- *ethics and compliance; and*
- *business continuity and disaster recovery (disaster preparedness).*

(a) Sub-Teams and Additional Resources. The information security coordinator assigns and coordinates the IRT for any specific information security incident according to incident characteristics and [ORGANIZATION] needs. The information security coordinator may:

(i) Identify and maintain IRT sub-teams to address specific information security incidents, or categories of information security incidents.

[SUB-TEAMS LISTING]

(ii) Call on external individuals, including vendor, service provider, or other resources, to participate on specific-event IRTs, as necessary.

[EXTERNAL RESOURCES LISTING]

Include contact information and engagement protocols for key external resources, such as:

- *vendor or service provider representatives;*
- *outside counsel;*
- *cyber forensics investigators or other technical experts;*
- *crisis communications specialists; and*
- *breach notification and identity theft prevention and mitigation service providers*

6. **Detection and Discovery.** [ORGANIZATION] shall develop, implement, and maintain procedures to detect, discover, and assess potential information security incidents through automated means and individual reports.

(a) Automated Detection. [ORGANIZATION] shall develop, implement, and maintain automated detection means and other technical safeguards [as described in [ORGANIZATION]'s [[WISP]/information security policy] available at [WISP OR POLICY REFERENCE]/including [AUTOMATED DETECTION MEANS DESCRIPTION]].

(b) Reports from Employees or Other Internal Sources. Employees, or others authorized to access [ORGANIZATION]'s IT systems, network, or data, shall immediately report any actual or suspected information security incident to [INTERNAL INCIDENT REPORTING CONTACT]. Individuals should

report any information security incident they discover or suspect immediately and must not engage in their own investigation or other activities unless authorized.

(c) Reports from External Sources. External sources who claim to have information regarding an actual or alleged information security incident should be directed to [EXTERNAL INCIDENT REPORTING CONTACT]. Employees who receive emails or other communications from external sources regarding information security incidents that may affect [ORGANIZATION] or others, security vulnerabilities, or related issues shall immediately report those communications to [INTERNAL INCIDENT REPORTING CONTACT] and shall not interact with the source unless authorized.

(d) Assessing Potential Incidents. [ORGANIZATION] shall assign resources and adopt procedures to timely assess automated detection results, screen internal and external reports, and identify actual information security events. [ORGANIZATION] shall document each identified information security incident, with initial details, using [INCIDENT DOCUMENTATION TOOL OR PROCESS].

[Drafting note: Consider adding the following for an effective IRP:

- *Establish a formal reporting process to timely collect key incident information whether detected using automated means or discovered by individuals.*
- *Identify how internal employees and contractors should report actual or suspected information security incidents, preferably on a 24-hour, 365-day basis. IRP training should focus on when and how to report incidents and encourage individuals to err on the side of caution if they are not certain.*
- *Provide multiple contact methods to report incidents, such as phone, email, and other online mechanisms in case one or more is affected or unavailable.*
- *Explain how to handle incident reports from external sources, including any vendors or other parties that may be obligated to notify the organization of certain events and channels those reports to a standard process for timely and consistent response.*
- *Define tools or processes for the organization's information security, IT, or other initial contact group to use in screening potential incident reports and documenting key details.*

7. **Escalation.** Following identification of an information security incident, the information security coordinator, or a designate, shall perform an initial risk-based assessment and determine the level of response required based on the incident's characteristics, including affected systems and data, and potential risks and impact to [ORGANIZATION] and its [customers/clients], employees, or others.

7.1 Based on the initial assessment, the information security coordinator, or a designate, shall:

(a) IRT Activation. Notify and activate the IRT, or a sub-team, including any necessary external resources (see Section 5.4, IRT Roster).

[ACTIVATION CRITERIA AND ACTION DETAILS]

[Drafting note: The information security coordinator or a designate on detection or discovery of an information security incident to:

- *Perform an initial assessment to determine the level of response and resources required.*

- *Based on the initial assessment results:*
    - *activate the IRT or an appropriate sub- team, including any external resources needed;*
    - *set expectations for how and when IRT members should engage in incident response activities; and*
    - *if necessary and applicable, make initial notifications of an incident in progress to the organization's insurer and law enforcement authorities.*

(b) IRT Expectations. Set expectations for IRT member replay and engagement. [REPLY AND ENGAGEMENT EXPECTATION DETAILS]

[Drafting note: specify that on activation for a particular information security incident, the IRT must collaborate to:

- *Investigate the incident.*
- *Analyze its effects.*
- *Formulate a response plan to contain, remediate, and recover from the incident.*

[Note: This should be done in collaboration with legal counsel to protect the organization's interest, including legal privilege, if applicable]

(c) Initial Notifications. Notify (if necessary) organizational leadership and any applicable business partners or service providers [, [ORGANIZATION]'s cyber insurance carrier,] [and law enforcement or other authorities] (see Section 10, Communications and Notifications).

8. **Containment, Remediation, and Recovery**. Next, the IRT shall direct execution of the response plan it formulates according to its incident investigation and analysis to contain, remediate, and recover from each identified information security incident, using appropriate internal and external resources.

8.1 The IRT shall document its response plans and the activities completed for each identified information security incident using [INCIDENT DOCUMENTATION TOOL OR PROCESS]

9. **Evidence Preservation**. The IRT shall direct appropriate internal or external resources to capture and preserve evidence related to each identified information security incident during investigation, analysis, and response activities (see Section 8, Containment, Remediation, and Recovery). The IRT shall seek counsel's advice as needed, to establish appropriate evidence handling and preservation procedures and reasonably identify and protect evidence for specific information security incidents.

[EVIDENCE PRESERVATION PROCESS AND TOOLS DETAILS]

10. **Communications and Notifications**. For each identified information security incident, the IRT shall determine and direct appropriate internal and external communications and any required notifications. Only the IRT may authorize information security incident-related communications or notifications. The IRT shall seek counsel's advice [, as needed,] to review communications and notifications targets, content, and protocols.

(a) Internal Communications. [Working with [INTERNAL COMMUNICATIONS GROUP], the/The] IRT shall prepare and distribute any internal communications it deems appropriate to the characteristics and

circumstances of each identified information security incident.

(i) Organizational Leadership. The IRT shall alert organizational leadership to the incident and explain its potential impact on [ORGANIZATION], its [customers/clients], employees, and others as details become available.

(ii) General Awareness and Resources. As appropriate, the IRT shall explain the incident to [ORGANIZATION]'s employees and other stakeholders, and provide them with resources to appropriately direct questions from [customers/clients], media, or others.

(b) External = Communications. [Working with [PUBLIC RELATIONS GROUP], the/The] IRT shall prepare and distribute any external communications it deems appropriate to the characteristics and circumstances of each identified information security incident.

(i) Public Statements. If [ORGANIZATION] determines that external statements are necessary, the IRT shall provide consistent, reliable information to the media and public regarding the incident using [ORGANIZATION]'s website, press releases, or other means.

[PLANNED RECIPIENTS CONTACT INFORMATION]

[LOCATION FOR PREPARED FORMS, TEMPLATES, OR OTHER EXTERNAL COMMUNICATION EXAMPLES]

(ii) Law Enforcement. The IRT shall report criminal activity or threats to applicable authorities, as [ORGANIZATION] deems appropriate.

[LAW ENFORCEMENT CONTACT LIST]

(c) Notifications. While the IRT may choose to authorize discretionary communications, certain laws, regulations, and contractual commitments may require [ORGANIZATION] to notify various parties of some information security incidents. If applicable to a specific information security incident, as required, the IRT shall:

(i) Authorities. Notify applicable regulators, law enforcement, or other authorities. [APPLICABLE AUTHORITIES AND NOTIFICATION PROCESS DETAILS]

(ii) Affected Individuals. If an applicable breach of personal information occurs, prepare and distribute notifications to affected individuals.

[PROCESS DETAILS TO IDENTIFY AFFECTED INDIVIDUALS AND PREPARE AND DISTRIBUTE NOTIFICATIONS]

[LOCATION FOR NOTIFICATION LETTER TEMPLATES]

(iii) [Cyber Insurance Carrier. Notify [ORGANIZATION]'s cyber insurance carrier according to the terms and conditions of its current policy, including filing a claim, if appropriate.

[CYBER INSURANCE CONTACT INFORMATION AND PROCESS DETAILS]]

(iv) [Others. Notify [customers/clients] or business partners according to current agreements.

[CONTACT INFORMATION AND PROCESS DETAILS REGARDING OTHER REQUIRED NOTIFICATIONS]]

11 **Post-Incident Review**. [At a time reasonably following/Within [DAYS] of] each identified information security incident, the information security coordinator, or a designate, shall reconvene the IRT, others who participated in response to the incident, and affected work group representatives, as appropriate, as a post-incident review team to assess the incident and [ORGANIZATION]'s response.

(a) Review Considerations. The post-incident review team shall consider [ORGANIZATION]'s effectiveness in detecting and responding to the incident and identify any gaps or opportunities for improvement. The post-incident review team shall also seek to identify one or more root causes for the incident and, according to risk, shall recommend appropriate actions to minimize the risks of recurrence.

(b) Report. The post-incident review team shall document its findings using [INCIDENT DOCUMENTATION TOOL OR PROCESS].

(c) Follow-Up Actions. The information security coordinator shall monitor and coordinate completion of any follow-up actions identified by the post-incident review team, including communicating its recommendations to and seeking necessary authorization or support from [ORGANIZATION] leadership.

12. **Plan Training and Testing**.

12.1 Training. The information security coordinator shall develop, maintain, and deliver training regarding this IRP that periodically [, but at least annually]:

(a) Informs all employees, and others who have access to [ORGANIZATION]'s IT systems, network, or data, about the IRP and how to recognize and report potential information security incidents.

(b) Educates IRT members on their duties and expectations for responding to information security incidents.

[The information security coordinator may choose to include training on this IRP in other information security training activities as defined in [ORGANIZATION]'s [WISP/information security policy] available at [WISP OR POLICY REFERENCE].] [Training materials and resources are available at [TRAINING REFERENCE].]

12.2 Testing. The information security coordinator shall coordinate exercises to test this IRP periodically [, but at least annually]. The information security coordinator shall document test results, lessons learned, and feedback and address them in plan reviews (see Section 13, Plan Review).

[IRP TESTING DETAILS]

13. **Plan Review**. [ORGANIZATION] will review this IRP at least annually, or whenever there is a material change in [ORGANIZATION]'s business practices that may reasonably affect its cyber incident response procedures. Plan reviews will also include feedback collected from post-incident reviews and training and testing exercises. The information security coordinator must approve any changes to this IRP and is responsible for communicating changes to affected parties.

[Send any suggested changes or other feedback on this IRP to [INFORMATION SECURITY COORDINATOR CONTACT INFORMATION].]

Effective Date: Reviewed: Revision date:

Model Acceptable Use Policy

Sample Employer Policy – Acceptable Use Policy

[This Sample is a draft only and is not intended to be legal advice. Employers must review and consider their legal obligations and appropriate rules. There may be good reason to take a different approach to various aspects of this policy. Further guidance may be appropriate in areas not covered in this sample. Highlights indicate areas which most likely require modification to the particular workplace.]

1. **Purpose**

Company Name (the "**Company**") provides technology for use in the furtherance of its business objectives. The purpose of this Acceptable Use Policy (the "**Policy**") is to outline acceptable use of technology at the Company and to ensure the risks associated with inappropriate or unauthorized use of computer technology are adequately managed to support business objectives.

For the purpose of this Policy, technology includes, but is not limited to, computers, laptops, mobile devices, internet, software, systems, email, telephones, voice mail and related equipment ("**Company Technology**"). Users of Company Technology must respect the rights of other users, respect the integrity of the Company Technology and observe all relevant laws and regulations.

2. **Scope**

This Policy applies to all employees (including temporary employees) who use the Company Technology ("**Users**"). This Policy applies to the Company's unionized and non-unionized workforce. With respect to the Company's unionized workforce, to the extent that there is any inconsistency between the provisions of this Policy and the applicable collective bargaining agreement, the provisions in the collective bargaining agreement will prevail.

3. **Responsibilities**

(a) Acceptable Use

The Company provides Company Technology to Users for legitimate business purposes. Users are expected to exercise good judgment and professionalism in the use of all Company Technology.

Incidental and occasional personal use of Company Technology is permissible as long as it does not interfere with workplace productivity or the Company's systems or business operations, does not pre-empt any business activity, does not consume more than a trivial amount of the Company's resources and is lawful. Users should be aware that all use of Company Technology is subject to monitoring as described in this Policy and as such, Users have no right to, or expectation of, privacy with respect to their use of Company Technology, subject to applicable laws.

Notwithstanding the above, any use of the Company Technology must be in accordance with the provisions set out within this Policy. If a User requires additional clarification about the appropriate use of Company Technology, they should contact their manager.

(b) Unacceptable Use

The relationship between the Company and its Users is based on trust. This trust must be maintained at all times as it is

fundamental to the employment relationship. Users must, at all times, hold themselves to the highest standards of conduct so as to maintain the Company's reputation and the integrity of the Company's business.

Users shall not be permitted to use any of the Company Technology to:

- solicit or recruit for any non-job-related commercial ventures, religious or political causes, outside organizations or other non-job-related solicitations;
- store, access, transfer, download, upload, communicate or create any fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, libelous, slanderous, threatening, abusive, defamatory, or otherwise unlawful or inappropriate materials;
- download entertainment software or games, or to play games over the Internet;
- access Internet sites for gambling or any illegal activity;
- embarrass Company executives, or to jeopardize the Company's reputation;
- download, store or transmit material that infringe any copyright, trademark or other proprietary right;
- post or transmit proprietary or confidential information related to clients, suppliers, vendors, allied parties, or other third parties;
- post or store Company business-related information on public storage sites;
- download or distribute pirated software or data;
- deliberately propagate a virus, malware, or any other malicious program code;
- send confidential Company information without prior authorization from the proper authoritative manager. Such confidential information includes, but is not limited to, Company copyrighted materials, trade secrets, intellectual property, proprietary financial information, employee information, customer information, or other similar materials that would be considered confidential in nature ("**Confidential Information**");
- access, use or disclose Confidential Information without authority;
- engage in activities for personal gain or a personal business, or for any commercial or business purposes other than Company purposes;
- perform any scanning or information gathering regarding Company Technology, including the following: port scanning, security scanning, network sniffing, keystroke logging, or other information gathering techniques, when not part of the User's job function;
- violate any applicable laws;
- send unsolicited email;
- install or use peer-to-peer file-sharing programs or access those types of networks; or
- use Company resources in a manner that violates applicable laws, including without limitation, those laws relating to discrimination and harassment, privacy, financial disclosure, intellectual property and proprietary information,

defamation and criminal laws.

Users shall also not be permitted to use the Company Technology to view, access, amend, update, change, collect, use or disclose: (i) any personal information in the Company's possession or control; or (ii) any Confidential Information without proper authorization.

Users should report any suspected unacceptable use of Company Technology to their manager.

Any User who uses Company Technology for any of these unacceptable uses will be subject to discipline in accordance with this Policy.

4. Monitoring

The Company maintains ownership over all Company Technology and all data created, sent, received or stored on or using Company Technology. Users should have no expectation of privacy with respect to their use of Company Technology.

Subject to compliance with applicable laws, the Company reserves the right to and may from time to time inspect, access, audit, monitor and/or record Users' use of and access to Company Technology and any information accessed, created, modified, stored, sent, received, copied, manipulated or otherwise handled in any way, by or through any Company Technology, at any time, in its sole discretion, without notice to any User.

These actions will be performed only as reasonably necessary to ensure compliance with this Policy and other Company policies, to detect and prevent loss or theft of Confidential Information, personal information or other misconduct, to conduct investigations into suspected inappropriate or unlawful activity, to meet legal disclosure and document production requirements, and other compliance requirements.

5. Security and Confidentiality

The Company reserves the right to implement controls in respect of Company Technology at any time in its sole discretion where it is deemed necessary to protect the security of the Company Technology, Confidential Information, personal information or other assets. Users may not block, uninstall or otherwise interfere with such controls.

Users must maintain basic controls to prevent Company Technology assets being lost or stolen, potential security breaches, leaking of Confidential Information or personal information and breaches of software licensing agreements.

Users must maintain confidentiality and exclusive control of authentication credentials (passwords, tokens, certificates) used to access the Company Technology. Credentials must not be shared with others at any time or left in a place where an unauthorized person might find them. If a User has reason to believe that his/her password has been compromised or discovered by another person, the User must immediately inform his/her manager (if an employee) or [IT?] if any other type of User, and change his/her password immediately. Other basic controls include, but are not limited to:

- Ensuring that laptops, mobile devices and desktop computers are protected by lock screen passwords of at least 8 characters in length and that screens are set to lock within 10 minutes of inactivity;
- changing passwords not less than every 30 days. The same password cannot be used more than once every 24 passwords;
- keeping laptops, mobile devices and portable storage devices and media appropriately secured (e.g. not leaving these items unattended in a vehicle or public place);
- preventing unauthorized changes being made to the operating system software or configuration of personal

computers or mobile devices used to access Company Technology; and

- not sharing mobile devices used to access Company Technology, or portable media containing Confidential Information or assets, with third parties (including family members);

Users must exercise caution when opening attachments or selecting links (these can be contained in electronic messages, blogs or social networks) from unknown sources as these may contain malicious software (also known as malware, examples include viruses, worms and trojans).

The Company reserves the right to revoke access to or use of any or all Company Technology any time in its sole discretion. Access to Company Technology will be revoked when a User leaves the Company.

All Company Technology resources must be returned to the Company at the end of a User's employment, or at any time Company deems it necessary.

6. Breaches, Investigations and Discipline

All Users must comply with this Policy at all times and take care to ensure that their use of Company Technology does not jeopardize the interests of the Company, personal information in its custody or control, or its Confidential Information.

Users must immediately notify the Company of any suspected breach of this Policy. The Company will investigate any reasonably suspected breach of this Policy promptly and impartially.

In the course of an investigation, the Company may require a written statement from the User involved in or with knowledge of the suspected breach, as well as an interview of any person with knowledge of the incident, and collect any and all relevant and material documents and other evidence. The Company may involve investigators and experts where appropriate to investigate and report to the Company.

A User may, in the Company's sole discretion, be suspended while an investigation is undertaken and completed.

Confidentiality will be maintained through the investigation process to the extent practicable and appropriate in the circumstances. Information obtained in connection with this Policy, including identifying information about any individuals involved, will not be disclosed unless the disclosure is necessary for the purposes of investigating or taking corrective action with respect to the incident, or as otherwise required by law. However, the Company may disclose certain information to the affected parties to gather pertinent facts or answer allegations.

All Users are expected to cooperate fully in any investigation pursuant to this Policy. If, after investigation, the Company finds that a violation of this Policy has occurred, the Company will determine what remedial action should be taken to avoid future incidents and to ensure compliance with this Policy in the future. Any such remedial action will be undertaken in accordance with this Policy.

Any and all breaches of this Policy will be treated with the utmost seriousness by the Company. Any breach of this Policy will result in discipline, up to and including termination of employment for just cause.

7. Administration

This Policy shall be administered in accordance with all applicable federal, provincial and local laws and regulations.

The Company may amend this Policy from time to time, at its sole discretion. Users are responsible for regularly reviewing this Policy.

8. **Questions**

Any questions regarding this Policy should be directed to a supervisor/[title of appropriate manager].

Acknowledgement and Agreement

I, _____, hereby acknowledge that I have received, read and understand the Company's Acceptable Use Policy and agree to comply with its terms. I understand that a violation of this Policy may subject me to discipline, up to and including termination of my employment for just cause.

Name: _____

Signature: _____

Date: _____

Let us help you.

Vancouver

Suite 1600 Cathedral Place
925 West Georgia Street
Vancouver, British Columbia V6C 3L2
t 604.685.3456
f 604.669.1620

Calgary

Suite 1100, 225 - 6th Avenue S.W.
Brookfield Place
Calgary, Alberta T2P 1N2
t 403.269.6900
f 403.269.9494

Yellowknife

Suite 200, 4915 - 48th Street
P.O. Box 818
Yellowknife, Northwest Territories X1A 2N6
t 867.669.5500
f 867.920.2206

Kelowna

Suite 403 - 460 Doyle Avenue
Kelowna, British Columbia V1Y 0C2
t 778.738.2610

Use your phone camera to scan the QR code
to subscribe to our Privacy & Data Management Blog!

@LawsonLundell

lawsonlundell.com

LAWSON LUNDELL LLP