PRIVACY POLICY

There are several laws in Canada that relate to privacy rights and the protection of personal information. Privacy laws give Canadians control over how their personal information is handled in the private sector and promotes respect for and protection of Canadians' privacy rights and personal information.

Canada has two federal privacy laws that are enforced by the Office of the Privacy Commissioner of Canada (the "Commissioner"):

- The Privacy Act, which covers how the federal government handles personal information; and
- The Personal Information Protection and Electronic Documents Act (PIPEDA), which covers how businesses handle personal information in the course of their commercial activities.

PIPEDA sets out the ground rules for how businesses subject to the law must handle personal information in the course of commercial activities.

The Commissioner oversees compliance with PIPEDA, which includes investigating privacy complaints, and helping businesses improve their personal information handling practices.

Under PIPEDA, the definition of organization (or business) includes an association, a partnership, a person or a trade union.

In addition to federal laws, there are various acts and legislation in Canada that relate to privacy rights, including:

- Provincial laws in:
  - Alberta, https://www.alberta.ca/personal-information-protection-act.aspx;
  - British Columbia, https://www.bclaws.ca/civix/document/id/complete/statreg/00_03063_01; and
  - Quebec, http://legisquebec.gouv.qc.ca/en/ShowDoc/cs/P-39.1.

These provincial privacy laws have been deemed substantially similar to PIPEDA.

- Canada's Anti-Spam Legislation (CASL), which is the federal law dealing with spam and other electronic threats to help protect Canadians while ensuring that businesses remain competitive in the global marketplace; and
- The Digital Privacy Act, which amends PIPEDA to include, among other things, mandatory breach notification requirements.

Under PIPEDA, an independent life and health insurance advisor/entity (the "Business Practice") contracted with one or more insurers are required to develop their own privacy compliance program and meet their legal obligations under PIPEDA and any other applicable privacy legislation.

This privacy compliance program (the "Program") sets out the requirements related to personal information protection (PIP) that apply to the Business Practice and its personnel.

It is the responsibility of advisors to review and understand their obligations under PIPEDA and any other applicable privacy legislation, as outlined by the Office of the Privacy Commissioner of Canada: https://www.priv.gc.ca/en, including compliance program requirements.

Our Commitment

At Aaxel Financial Services Ltd. our advisors and our clients are our business. As a financial services company, we are trusted with some of our clients' most sensitive personal information. We must respect that trust and need our clients to be aware of our commitment to protect the information they provide in the course of doing business with us.

As November 1, 2018, changes to the Personal Information Protection and Electronic Documents Act (PIPEDA) and regulations will come into force.

The main changes that affect those in the life insurance industry are:

- Requirement to notify individuals about security breaches which pose a real risk of significant harm except where prohibited by law
- Requirements to report breaches of security safeguards to the federal Office of the Privacy Commissioner involving personal information that pose a real risk of significant harm
- Requirement to notify other organizations or governments institutions that may be able to mitigate that harm
- Requirement to keep records of all privacy breaches for 24 months.

What is a security breach?

A security breach is a loss of, the unauthorized access to, or disclosure of, personal information. Breaches can happen when personal information is stolen, lost or mistakenly shared.

What is personal information?

Personal information is information in any form about an identifiable individual.

Significant Harm

Significant harm includes identify theft, financial loss, negative effects to credit score or credit record, loss of employment, loss of business or professional opportunities, damage to reputation or relationships, humiliation, loss or damage to property, and bodily harm.

You are expected to make an assessment to determine if there is a real risk of significant harm based on the sensitivity of the personal information involved in the breach and the probability that the information will be misused.

Principles of PIPEDA

There are 10 principles that we must follow to be in compliance with PIPEDA.

1. **Accountability**
   An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

2. **Identifying Purposes**
   The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

3. **Consent**
   The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except when inappropriate.

4. **Limiting Collection**
   The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

5. **Limiting Use, Disclosure, and Retention**
   Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by the law. Personal information shall be retained only as long as necessary for fulfillment of those purposes.

6. **Accuracy**
   Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

7. **Safeguards**
   Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

8. **Openness**
   An organization shall make readily available to individuals' specific information about its policies and practices relating to the management of personal information.

9. **Individual Access**
   Upon request, an individual shall be informed of the existence, use and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

10. Challenging Compliance

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals for the organization's compliance.

In addition to these principles, PIPEDA states that any collection, use or disclosure of personal information must only be for purposes that a reasonable person would consider appropriate in the circumstances.

Aaxel Financial Services Ltd. is responsible for the protection of personal information and the fair handling of it at all times, throughout the business practices and in dealings with third parties. Additionally, care in collecting, using and disclosing personal information is essential to continued consumer confidence and good will.

Applicability

The Act is applicable to personal information only. However, it has been suggested that in keeping with the spirit of the law, PIPEDA should also be applied to information obtained on closely-held corporations which would be most, if not, all of our corporate clients. This policy applies to all employees of Aaxel Financial Services Ltd. This policy also applies to all consultants and third parties contracted by Aaxel Financial Services Ltd.

The Privacy Officer

The designated compliance officer is both responsible and accountable for effectively implementing the privacy compliance program.

As at the last review date of this Policies and Procedures Manual the designated Policy Officer of Aaxel Financial Services Ltd. is _____Kuldip Chahal_____ and all inquiries/complaints shall be directed to this individual.

Information Collection and Use

We collect the information required for us to complete the task for which we are engaged, whether that is insurance, money products or financial plans.

This information may include, but are not limited to:

Name
Date of Birth/Date of Death
Social Insurance Number
Home Address(s)
Work Address(s)
Telephone Number(s), Fax Number(s)
Email Address(s)
Marital Status
Financial Income/Expense Info
Lawyer(s)
Banker(s)
Bank information
Investment advisor and account information Financial Statements
Medical Information

Aaxel Financial Services Ltd. must inform clients if the personal information in the clients' file will be accessed by suppliers or other persons in the course of their duties. In the information is used for purposes other than those for which it was collected, Aaxel Financial Services Ltd. must obtain the clients' consent, unless such use or disclosure is required or permitted by law. The authorized persons with whom Aaxel Financial Services Ltd. shares or exchanges personal information must have signed a confidentiality agreement. There must exist effective access management for authorized personnel; clients' personal information must only be accessible to Aaxel Financial Services Ltd. and its personnel if the information is required to conduct business.

Consent

The consent for us to establish a file and collect and maintain personal information is done using the Privacy Protection Notice which is to be signed by the client and placed in their file.

Disclosure

There must exist a limit to the disclosure of the information that is necessary for operations. Aaxel Financial Services Ltd. must exercise caution when discussing a file in public or while travelling and take reasonable measures to prevent the theft or loss of documents. Aaxel Financial Services Ltd. must not leave voice messages containing personal information unless its clients have given their prior consent. If Aaxel Financial Services Ltd. is sold, clients must be informed, and their written consent must be obtained to transfer their files.

Protection of Personal Information

As the principals, management and employees of Aaxel Financial Services Ltd. we are granted access to client information and must understand the need to keep the information protected and confidential. Our training procedures clearly communicate that we are to use the information only for the intended purpose(s).

Staff will be required to sign a Confidentiality Agreement upon commencement of employment.

Personal information is information about an individual (natural person) that, alone or in combination with other data, allows the individual to be identified. The following is a non-exhaustive list of examples of personal information:

- ✓ The person's name, when it is mentioned with other personal information about the person or where disclosure of the name itself would reveal information about the individual
- ✓ Address
- ✓ Email address
- ✓ Age
- ✓ Social Insurance Number (SIN)
- ✓ National or ethnic origin
- ✓ Religion
- ✓ Family situation
- ✓ Level of education
- ✓ Medical Records
- ✓ Criminal record
- ✓ Work history
- ✓ Financial transactions a person has made
- ✓ Cheques or transactions from a person's account

- ✓ Numbers or symbols or any other personal identifier

Retention of Personal Information

We will retain our completed client files for a minimum period of seven years. Any files where there were complaints or legal issues will be kept indefinitely. A secure method must be used for physical storage (such as a locked filing cabinet). Each client file must be stored individually unless written authorization has been obtained for spousal files. For electronic files, a secure method must also be used by implementing reasonable measures such as the use of passwords, firewalls, anti-virus programs and back-ups. This list is not exhaustive. Aaxel Financial Services Ltd. inform its clients of their rights to access their information and rectify any errors or incomplete information in their file. Any client requests for access or rectification must be acknowledged within 5 business days and must be processed within 30 days of the acknowledgement of receipt. Written confirmation must be then sent to the client once the request has been processed or completed.

Destruction of Personal Information

As an organization that has client personal information in its control, Aaxel Financial Services Ltd. does not simply throw it away in the trash. Aaxel Financial Services Ltd. securely disposes of it.

Aaxel Financial Services Ltd.'s goal is to irreversibly destroy the media which stores client personal information so that personal information cannot be reconstructed or recovered in any way. When going through the process of disposal, Aaxel Financial Services Ltd. also destroys all associated copies and backup files.

Privacy Choices

Clients may request copies of our privacy policies and procedures at any time.

Clients may request access to their information. We must respond to this request as quickly as possible, but no later than 30 days after the receipt of the request.

Clients may withdraw their consent at any time by contacting our Privacy Officer. However, they will be made aware that failure to provide adequate information may prevent us from completing the task for which we were engaged.

Clients may file complaints about our privacy procedures as well as a breach in our privacy policy. Complaints should be received in writing and forwarded to the Privacy Officer. The Privacy Officer will contact the client and obtain all details. The Privacy Officer will then review the circumstances of the complaint and determine if there is reason to alter the existing privacy policy. Insurance carriers should be notified of any complaint involving their clients/products.

Exception to Client Access

Organizations must refuse an individual access to personal information:

- If it would reveal personal information about another individual unless there is consent or a life-threatening situation
- If the organization has disclosed information to a government institution for law enforcement or national security reasons. Upon request, the government institution may instruct the organization to refuse access or not to reveal that the information has been released. The organization must refuse the request

and notify the Privacy Commissioner. The organization cannot inform the individual of the disclosure to the government institution, or that the institution was notified of the request, or that the Privacy Commissioner was notified of the refusal.

Organizations may refuse access to personal information if the information falls under one of the following:

- Solicitor-client privilege
- Confidential commercial information
- Disclosure could harm an individual's life or security
- It was collected without the individual's knowledge or consent to ensure its availability and accuracy, and the collection was required to investigate a breach of an agreement or contravention of a federal or provincial law (the Privacy Commissioner must be notified)
- It was generated in the course of a formal dispute resolution process.

Privacy Breach

A privacy breach involves improper or unauthorized collection, use, disclosure, retention or disposal of personal information. A privacy breach may occur within an institution of off-site and may be the result of inadvertent errors or malicious actions by employees, third parties, partners in information-sharing agreements or intruders.

Where a privacy breach occurs, Aaxel Financial Services Ltd. is required to:

Step 1: Contain the breach

Take immediate steps common sense steps to limit the breach with actions such as stopping the unauthorized practice, recovering records, shutting down the system that was breached, correcting obvious weaknesses in physical security, alerting the privacy officer or others responsible for security in your organization and notifying the police if the breach involves theft or other criminal activity.

Step 2: Evaluate the risks associated with the breach

Consider whether personal information was involved. Generally, the more sensitive the data, the higher the risk. Consider what possible uses there are for the personal information. Can it be used for fraudulent or otherwise harmful purposes?

Determine the cause of the breach and whether there is a risk for ongoing or further exposure of the information. Is the information encrypted or otherwise not readily accessible?

Determine what individuals are affected by the breach, how many and what harm may result from the breach. Determine real risk of significant harm based on an assessment of the sensitivity of the personal information involved in the breach and the probability the personal information has been/is/will be misused.

Once you have evaluated the risks, you can determine what other steps you need to immediately take.

Step 3: Notification

Notification of affected individuals and others may be necessary in order to avoid or mitigate harm to an individual whose personal information has been inappropriately collected, used or disclosed.

If there is a real risk of significant harm, you are required to notify affected individuals, the privacy commissioner, any other government institutions or organizations that could mitigate or reduce the risk of harm (for example, law enforcement) and those to whom you have a contractual obligation (for example, insurance carriers).

Notification should be done as soon as feasible following the breach as time is of the essence. You can file the breach report immediately and further information can be added as it becomes available.

The preferred method of notification is direct to affected individuals by letter, email, phone call or in person. The notification should include the following information:

- Date(s) of the breach or time period over which it occurred
- Description of the breach
- Description of the personal information that is subject of the breach
- Description of the steps taken to reduce the risk of harm that could result from this breach
- Description of the things affected individuals could do to reduce the risk of harm that could result from the breach or to mitigate the harm
- Contact information that the affected individuals can use to obtain further information about the breach.
- That individuals have a right to complain to the Office of the Information and Privacy Commissioner. Provide contact information.

Step 4: Prevention

Once the immediate steps are taken to mitigate the risks associated with the breach, you need to take the time to thoroughly investigate the cause of the breach. As a result of this investigation, you should develop or improve as necessary adequate long term safeguards against further breaches.

Examples of situations that could result in the disclosure of, or access to, personal information by unauthorized parties are:

- The theft, loss or disappearance of equipment or devices containing personal information;
- The sale or disposal of equipment or devices containing personal information without purging prior to sale or disposal;
- The transfer of equipment or devices without adequate security measures;

- The use of equipment or devices to transport or store personal information outside the office for telework or off-site work arrangements without adequate security measures;
- The inappropriate use of electronic devices to transmit personal information, including telecommunication devices;
- Intrusions that result in unauthorized access to personal information held in office buildings, file storage containers, computer applications, systems, or other equipment and devices;
- Low level of privacy awareness among employees, contractors or other third parties that handle personal information;
- Inadequate security and access controls for information in print or electronic format, on site or off-site;
- The absence of provisions or inadequate provisions to protect privacy in contracts or in information-sharing agreements involving personal information;
- Insufficient measures to control access and editing rights to personal information, which may result in wrongful access to, and the possible tampering with, records containing personal information;
- Phishing or the use of deceptive tactics to trick an individual into providing their personal information either directly or by going to a fake web site. For example, an individual pretending to perform system maintenance calls an employee to obtain his or her security password; and
- Pharming or the use of a fake copy of an official Aaxel Financial Services Ltd. web site to redirect to a malicious web site in order to steal information without the user's knowledge. This method takes advantage of the weaknesses in the Data Network System (DNS). For example, an individual access what he or she believes is an official Aaxel Financial Services Ltd. web site and submits personal information as requested by the site. The individual is unaware that he or she has been redirected to a fake copy of the official web site.

Containment of Privacy Breach

If a privacy breach occurs, Aaxel Financial Services Ltd. will take the following steps within 48 hours to manage and contain the situation as best it can:

1. **Freeze Everything**

   Take affected devices offline but do not shut them down or make any changes just yet. The goal here is to stop any ongoing activity by limiting communication to and from the impacted systems but not commit any action which might erase clues, contaminate evidence or otherwise inadvertently aid the attacker. In the case of virtual machines or other systems you can snapshot, it is recommend doing so now so that you will have a recorded version of the system at the time the breach was occurring. You can analyze the snapshot later in an offline state.

2. **Ensure auditing and logging is ongoing**

   Ensuring that existing system auditing remains intact and has been operational will be one of the most useful steps you can take to determine the scope of the breach and devise remediation methods. If auditing has been disabled (to cover someone's trail for instance), restore it before proceeding; it will also assist in establishing whether breach activity is ongoing and when the breach can be safely determined to have concluded.

3. **Change passwords or lock credentials**

Changing passwords or locking credentials is a common tactic in preparing to investigate a data breach since it will help ensure the cessation of said breach if it is ongoing, and data breaches commonly rely on compromised passwords and credentials. Make sure to apply this step to all involved accounts, whether confirmed or suspected.

4. **Determine the impact**

Now the investigation starts. Figure out what happened here; what information was accessed, what systems were compromised, and which accounts may have been utilized. You'll need the logs referenced in the prior step, as well as the tools discussed in step number two. Determine and establish the scope of the breach to formulate how to solve it.

5. **Determine how it happened**

It's not enough to remediate a data breach based on impact alone; you have to determine root cause or you may simply be slapping a temporary band-aid on the situation. Did someone erroneously give out their password? Was a system not patched for a particular vulnerability? Did someone plug an unauthorized laptop into the company network which then subjected the organization to malware? Or did an employee simply leave their unencrypted mobile device in a taxi cab and was then subjected to blackmail?

6. **Determine what needs to be done**

Now comes the step where you build out your remedy to seal the hull of the ship from the iceberg damage, so to speak. Establish whether you need to remotely wipe a stolen mobile device, update software, change network firewall rules, segregate subnets, run antimalware scans, increase logging and alerting or some other technical steps, get these planned out. Then enact them immediately.

7. **Communicate the details to the appropriate internal personnel**

It's not just technical steps you need to worry about. There's also the communication and notification process. Who do you have to involve to let them know the breach occurred, how it occurred, what details were involved, and what has to be done?

8. **Make public announcements and prepare for responses**

This is never going to be the most fun of these steps, but quite likely it will be up to someone to make a public announcement, perhaps in the form of a press conference, series of emails, social media announcements, website announcements or any other form of communication which exists between the company and the outside world.

Make sure to describe what the organization has done to remedy the breach, what it intends to do in the future, and what (if any) steps customers should take to protect themselves, such as by changing passwords, contacting credit card companies or placing fraud alerts.

If possible, establish a hotline or name specific group/contact information to address customer concerns regarding this breach so they can answer questions and provide guidance.

Evaluate Risks Associated with Privacy Breach

Personal data passes through many areas of a business, and it needs to be kept secure at all times, whether it's saved on a database, in hard-copy form and stored in an office, or being transferred to or from third parties. Each area has its own risk and below is a list of some of the most prominent risks:

1. **Web application vulnerabilities**, including injection flaws (which allow attackers to copy or manipulate data) and sensitive data exposure (which allows attackers to gather sensitive information).
2. **Operator-sided data leakage**, which consists of any failure to prevent the leakage of information containing or related to user data.
3. **Insufficient data breach response**, such as failing to inform affected data subjects about a possible breach or data leak.
4. **Insufficient deletion of personal data**, i.e. not deleting data subjects' information after a set period of time or when it is no longer necessary.
5. **Non-transparent policies, terms and conditions**, such as failing to provide sufficient information on how data is collected, stored and processed.
6. **Collection of inessential data**, including descriptive or demographic information that's not needed for the purposes of the system.
7. **Sharing data with a third party** without obtaining the data subject's consent.
8. **Outdated personal data**, including incorrect or bogus data, or the failure to update data when it's no longer correct.
9. **Missing or insufficient session expiration**, i.e. failing to effectively enforce session termination. This might result in an organisation collecting additional data without the user's consent.
10. **Insecure data transfer**, i.e. failing to provide data transfers over secure channels or to put in place mechanisms limiting the leak surface.

Prevention of Privacy Breach

To prevent a privacy breach, Aaxel Financial Services Ltd. should:

- Take privacy into account before making contracting decisions or entering into information-sharing agreements. Aaxel Financial Services Ltd. should include adequate privacy protection provisions, such as a requirement to immediately notify the proper authorities of a privacy breach;
- Provide regular and ongoing training to employees, managers and executives to ensure that they are aware of the requirements of these policies and procedures;
- Ensure that personnel working off-site are aware of their privacy and security responsibilities. This means ensuring that appropriate measures are taken to safeguard the personal information they handle off-site;

- Establish clear administrative controls that restrict access and editing rights to records containing personal information to only those employees who have a legitimate need to know, and for Aaxel Financial Services Ltd. to put in place appropriate audit trails to ensure that these administrative controls are functioning as intended;
- Use cryptography (encryption) to protect sensitive personal information stored in a computer or a portable storage device or being transmitted through email, on a company network, a wireless network, or across the Internet;
- Establish clear procedures for the use of wireless devices;
- As a general rule, do not send personal information by facsimile unless absolutely necessary. If you must fax personal information, consider the safeguards recommended by the Office of the Privacy Commissioner of Canada for faxing personal information;
- Purge all equipment and other electronic devices containing personal information before selling, disposing of, or transferring such equipment or devices;
- Empty security containers such as file cabinets, safes or mobile shelving units and ensure that no classified or protected material is left inside before selling or transferring them;
- Take precautions against "phishing" and "pharming":
    - Ensure that requests for personal information are valid and that individuals asking for personal information are who they claim to be;
    - Refuse to provide personal information in response to an unsolicited telephone call, fax, letter, email attachment or Internet advertisement;
    - Be on the lookout for clues indicating that a website may be fraudulent (i.e., spelling errors, unusual advertisements, or portions of the site that do not work properly);
    - Check the lock icon at the bottom of your browser to ensure that you are sending personal information over a secure connection; and
    - Verify the phone number and call the individual to determine validity if you have any concerns.
- Notify the Privacy Officer immediately of situations where personal data is at risk of being compromised and a potential privacy breach may occur.

Examples of best practices in managing privacy breaches include:

- Preliminary assessment and containment;
- Full assessment;
- Notification (to affected individuals and internal management where required);
- Mitigation and prevention;
- Notification to the Privacy Officer; and
- Sharing of lessons learned.

Should Aaxel Financial Services Ltd. become aware of a privacy breach, we will review our privacy policy and amend as required, as well as maintain a record of all privacy breaches.

- The record should include information as to the nature and extent of the breach, the type of personal information involved, the parties' involved, anticipated risks, steps taken or to be taken to notify individuals, any remedial action taken and whether the investigation determined it to be a material privacy breach.
- Records documenting privacy breaches should not contain personal information.

Notification of Privacy Breach

Aaxel Financial Services Ltd. will notify individuals whose personal information has been wrongfully disclosed, stolen or lost. Where necessary, Aaxel Financial Services Ltd. will also notify the insurance carrier, if affected, and may notify its E&O provider if the case warrants such notification.

- Aaxel Financial Services Ltd. will notify all affected individuals whose personal information has been, or may have been, compromised through theft, loss or unauthorized disclosure, especially if the breach:
    - Involves sensitive personal data such as financial or medical information, or personal identifiers such as the Social Insurance Number;
    - Can result in identity theft or some other related fraud; or
    - Can otherwise cause harm or embarrassment detrimental to the individual's career, reputation, financial position, safety, health or well-being.
- Notification should occur as soon as possible following the breach to allow individuals to take actions to protect themselves against, or mitigate the damage from, identity theft or other possible harm.
- Consult with the Privacy Officer and with law enforcement authorities to determine whether notification should be delayed to ensure that any possible investigation is not compromised.
- Care should be exercised in the notification process to not unduly alarm individuals, especially where the institution only suspects but cannot confirm that certain individuals have been affected by the breach.
- It is always preferable to notify affected individuals by letter (first class recommended), by telephone or in person, unless the individuals cannot be located or the number of individuals is so large that the task would become too onerous.

In such cases, Aaxel Financial Services Ltd. could post a conspicuous notice on its web site or on log-in screens used to access departmental data and/or use major local or national media (television, radio, newspapers and magazines). Aaxel Financial Services Ltd. should use electronic mail only when the individual has previously consented to the receipt of electronic notices.

Notification of affected individuals should include:

- A general description of the incident, including date and time;
- The source of the breach (an institution, a contracted party, or a party to a sharing agreement);
- A list of the personal information that has been or may have been compromised;
- A description of the measures taken or to be taken to retrieve the personal information, contain the breach and prevent reoccurrence;
- Advice to the individual to mitigate risks of identity theft or to deal with compromised personal information (e.g., Social Insurance Number);
- The name and contact information of the Privacy Officer at Aaxel Financial Services Ltd. with whom individuals can discuss the matter further or obtain assistance;
- A reference to the effect that the Privacy Officer has been notified of the nature of the breach and that the individual has a right of complaint, when applicable; and
- Aaxel Financial Services Ltd. should also inform affected individuals of developments as the matter is further investigated and outstanding issues are resolved.

Clean Desk Policy

Employees are responsible for clearing their desks when they leave the office at the end of the business day and Aaxel Financial Services Ltd. is responsible for providing access to a paper shredder and storage space. The office manager or the employee's supervisor must check the office at the end of the business day and confiscate or destroy any folders, papers or portable storage media an employee might have left out on their desk. Consequences for policy non-compliance are a verbal warning and termination if continual breach of policy after already having received a verbal warning.

E-mail Privacy Disclosure Sample

All Senior Management, employees and advisors of Aaxel Financial Services Ltd. using an Aaxel domain e-mail address are required to include the following privacy disclosure in their e-mail signature:

This message contains confidential information and is intended only for the individual named. If you are not the named addressee, you should not disseminate, distribute or copy this email. Please notify the sender immediately by email if you have received this email by mistake and delete this email from your system. Email transmission cannot be guaranteed to be secure or error-free, as information could be intercepted, corrupted, lost, destroyed, arrive late or incomplete, or contain viruses. The sender, therefore, does not accept liability for any errors or omissions in the contents of this message which arise as a result of email transmission. If verification is required, please request a hard-copy version.

Office Safeguards

In an effort to ensure the privacy of our client information Aaxel Financial Services Ltd. has implemented the following safeguards:

- Disclaimer on all e-mails, faxes etc.
- Clean desk policy
- All confidential materials to be removed from view at end of day, lunch, break time, etc.
- No information in view of public, on desks
- No discussion of client files outside the office
- Empty shredding file daily
- Lock shredding bin
- Password protected screensavers on all computers
- Any inquiry should be directed to the Privacy Officer
- All filing cabinets to be locked
- All waste paper containing personal information to be shredded
- Any person, client or broker, must identify themselves by a broker code, Social Insurance Number, Date of Birth, etc. in order to confirm identity
- Employees must be furnished with a copy of the privacy policy and sign off acknowledging that they have read it
- Staff are required to sign a Confidentiality Agreement
- Office is locked and alarmed and professionally monitored
- Complaint logs are maintained
- Certificates of Destruction are received for shredded material.

Ensuring Effectiveness of Privacy Procedures

In order to ensure the effectiveness of these privacy procedures, Aaxel Financial Services Ltd.:

1. **Monitors and tracks network access**
   Controls and systems are in place that allow for early detection of network intrusions and the ability to identify the intruders. This is critical to mitigating breaches or other types of security incidents. Network access is adequately monitored such that suspicious activity on our network can be detected prior to breach.
2. **Provides effective employee Policies and Procedures**
   Employees can be a common cause of data breaches, data loss and data misappropriation if appropriate safeguards are not instituted and enforced. To mitigate these risks, these policies and procedures dictate which employees have access to particular data, how confidential and proprietary information must be handled, instructions on reporting impermissible uses or violations of policies related to confidentiality and security and onboarding and exit procedures to protect against information misappropriation upon termination of employment. Employee awareness of these policies and procedures is provided through regular training and discussed expectations within the organization that privacy and data security are taken seriously.
3. **Has a Breach Response Plan.** A critical part of Aaxel Financial Services Ltd.'s data security plan is the breach response plan, which governs how to respond to a suspected or actual breach. The response plan identifies the leaders of the response team, is easy to follow and is scenario-based. It includes checklist that ensure proper procedures are followed to collect pertinent information related to the breach and promptly secure the premises and systems where the breach occurred in order to prevent additional data loss. Legal counsel is involved in all aspects of an investigation – including communications about the potential breach, remediation efforts and disclosure and reporting.
4. **Conducts regular audits**
   Aaxel Financial Services Ltd. regularly measures the effectiveness of these policies and procedures by conducting regular audits to evaluate information-security practices and whether the company is effectively following these practices, including conducting tests to ensure that employees are properly and consistently implementing the policies and procedures.

Aaxel Financial Services Ltd. ensures the effectiveness of its privacy policies and procedures on an annual basis, at minimum. In accordance, Aaxel Financial Services Ltd. has appointed a Chief Privacy Officer, has documented data process flows, continually defines and communicates privacy policies, monitors and controls the use of personal information, establishes incident response procedures, governs third-party relationships and ensures its privacy policies and procedures are kept current.