[****](https://actzero.ai/)

**Acceptable Usage Policy**

**[Template]**

**ActZero challenges cybersecurity coverage for SMB and mid-market companies. Our intelligent MDR provides 24/7 monitoring, protection and response support that goes well beyond other third-party software solutions. Our teams of data scientists leverage cutting edge technologies like AI and ML to scale resources, identify vulnerabilities and eliminate more threats in less time. We actively partner with our customers to drive security engineering, increase internal efficiencies and effectiveness and, ultimately, build a mature cybersecurity posture. Whether shoring up an existing security strategy or serving as the primary line of defense, ActZero enables business growth by empowering customers to cover more ground.**

***This template is for educational purposes. You should consult with your leadership, IT, and legal teams to ensure the contents of your Acceptable Usage or Information Security Policy is right for your business. We provide no warranty and accept no responsibility or liability for the accuracy or completeness of the information contained in this template.***

Acceptable Usage Policy [Template]

[SUBTITLE OR DESCRIPTION]

[MM/YYYY]

# 

ISSUED BY

[COMPANY]

## 

REPRESENTATIVE  
[NAME]

[EMAIL]

[PHONE]

# Table of Contents

[**Table of Contents**](#_56im3jxyxaax) **1**

[**Revision History**](#_wfp53cxv4wn) **3**

[**Introduction & Background**](#_pdc6jw7zlqdr) **4**

[**Security training policy**](#_9bauu0o871o4) **4**

[**Acceptable usage**](#_59geihfkj3ls) **5**

[Data Classification and User Access Rights](#_rk5o1vmhoopc) 6

[Account/Credential management](#_65pva44j83vq) 8

[Accounts](#_v60sztkuxp8o) 8

[Password usage](#_1pxezwc) 8

[Vendor access policy](#_uorzhwewmbjq) 9

[Devices](#_e9jfjtnerrod) 9

[Company-issued devices](#_fs6pnxlm6v1f) 9

[Bring your own device](#_kcq4hhl581uh) 10

[Removable media](#_u33anlupkhgu) 11

[Changes to devices – Hardware](#_147n2zr) 11

[Changes to devices – Software](#_418al1sdtdpd) 11

[Software usage and licensing](#_yqjyzkrumzp1) 12

[Cloud services](#_z1lvojr0qhg7) 12

[Data security services & policies](#_4dl3u2k51p83) 12

[Anti-virus and Anti-malware](#_wnk3sl5o1ods) 12

[Destruction policy: electronic equipment, data and media](#_fd196c5hv9yd) 13

[Encryption](#_kjiva9wmmaif) 13

[Record retention](#_c8vpexi6gm6b) 14

[Email](#_j1wsntkf9yng) 15

[Guidelines for use](#_ivtsjljh26zk) 15

[Procedures for securing email communication](#_sum489epal41) 16

[Receiving email](#_oscxfsldr40x) 16

[Sending email](#_thz4qi1ik9ag) 17

[Etiquette and professionalism](#_vk3iwovfnx0x) 17

[Examples of inappropriate email content](#_okmmvnemgggq) 18

[Canadian Anti-SPAM Legislation (CASL)](#_15lzxnds3nu5) 18

[CAN-SPAM (United States)](#_f9mtgq3japcj) 20

[Instant messaging](#_xgqejzqgjz8x) 20

[Social media](#_kxvedghvxhnm) 20

[Document management](#_2xcytpi) 22

[Destruction procedure](#_aspgtrf0eeqv) 22

[Scanning procedure](#_f1b2fu1cm5q3) 23

[Document naming](#_gbx1qxp1likj) 23

[Storage](#_49z49ij4ie6q) 24

[Network access](#_3as4poj) 24

[Corporate networking](#_ppqstiqzgc0d) 24

[Wireless networking](#_wcpj3hbxm5) 24

[Remote access policy](#_ao7vkkwh9btp) 25

[Physical security](#_814m8ywe1mjd) 25

[Employee access policy](#_mnax7tqzwrkx) 25

[Visitor access policy](#_bk9qjfyiwdrn) 25

[Workstation security](#_1ktbjar44zgy) 26

[Monitoring](#_e82se6tvuok8) 27

[Activities to be logged](#_ytljg5821ht0) 27

[Elements of the log](#_ycz94yx5mms9) 28

[Formatting, transmission, and storage](#_p0wb0mtyp6ny) 29

[Confidentiality](#_csl4p2qfj32m) 29

[Integrity](#_57cf8gftk8be) 29

[Log retention](#_i4nar39okeq0) 29

[Alerting](#_yyru0wjpxwni) 30

[Reporting](#_kbdk3mqty7ip) 30

[Incident response / security events](#_2x2j0wrbeob) 31

[Reporting violations](#_g6im2ac4ykm7) 31

# 

# 

# Revision History

Ensure that any modifications to this document are versioned and annotated here to provide evidence of regular review and updates to the policy.

## 

| Initial Creation | 02/02/2021 |
| --- | --- |
| Addition of Policy for Privacy Regulators in EU/Canada. | 02/04/2021 |

# 

# Introduction & Background

# 

[COMPANY] has produced a consolidated Information Security Policy to provide all personnel including employees either full time or temporary, consultants, contractors, and third party vendors guidance regarding operational aspects of Information Technology, including and especially the Confidentiality, Availability, and Integrity of corporate assets, systems, and data information within the firm. This document also serves as evidence to auditors and security personnel of the guidelines and standards adopted by the organization to enhance Cybersecurity.

**Objectives**

1. Demonstrate to all personnel understand their responsibilities regarding information security prior to being granted access.
2. Demonstrate security controls set forth by the firm for compliance.
3. Simplify the process of documenting for outside stakeholders such as auditors and privacy offices the communication regarding controls in place.

To simplify the process of onboarding and communicating with personnel the remainder of the document is organized as sub-policies, listed in alphabetical order, and a signature page at the end of the document.

**These guidelines are reviewed and amended on an annual basis, as applicable, taking into account new legislation and business changes.**

## 

# Security training policy

Given information security training (including email advisories, computer-based training, and/or information seminars), personnel must remain vigilant and on-guard against common cybercrime and information security risks, including social engineering, online fraud, phishing and web browsing risks – for both business and personal usage.

From this training, users are trained to report any anomalies in system performance as it could indicate malicious activity that requires further investigation. Phishing exercises (and other social engineering engagements) may be used to benchmark adherence and/or effectiveness of this training.

# Acceptable usage

The primary purpose of [COMPANY] information assets (including but not limited to computer systems;software applications including cloud and 3rd party; storage media; communications systems; and, accounts providing email and Internet access) is to support the ongoing operation of the firm. Under no circumstances are personnel authorized or permitted to engage in any activity considered illegal (under local, provincial, state, federal, or international law) while using firm information assets.

Personnel must adhere to all practices in this policy and accompanying human resources documentation.

All data stored on [COMPANY] systems is the property of [COMPANY]. Users should be aware that the company cannot guarantee the confidentiality of information stored on any [COMPANY] system except where required to do so by law. Systems are monitored for security purposes and information including but not limited to system activity, emails, browsing history and files used on [COMPANY] systems may be partially or completely logged or copied by the Information Technology (IT)department while screening for software threats such as viruses, misuse or network attacks.

Personal use is to be kept to a minimum and must not be in any way detrimental to users own or their colleagues’ productivity and nor should it result in any direct costs being borne by [COMPANY] other than for trivial amounts (e.g., an occasional short telephone call).

[COMPANY] trusts employees to be fair and sensible when judging what constitutes an acceptable level of personal use of the company’s IT systems. If employees are uncertain, they should consult their manager.

Examples of Unacceptable Use:

| Categories | Examples |
| --- | --- |
| Activities for personal benefit that have a negative impact on the day-to-day functioning of the business | * Streaming video * Playing networked video games |
| Activities that are inappropriate for [COMPANY] to be associated with and/or are detrimental to the company’s reputation | * pornography * gambling * inciting hate * bullying / harassment * expressing personal views on politics, religion, or any controversial issue |
| Attempting to disable and/or circumvent the IT security controls which [CUSTOMER NAME] Products has put in place | * vulnerability scanning * network sniffing (wired or wireless) * attempting to flood, or otherwise disrupt access to, company services or resources * password guessing/cracking * attempting to gain unauthorized access to resources via either social or technological methods * modifying the network topology (e.g. by adding a modem, hub, switch, router, or wireless access point) |

## Data Classification and User Access Rights

Data Classification helps users identify acceptable methods of storage and transmission of files. The data classifications being defined as such:

**Critical**

Data of a highly sensitive nature, where its loss, destruction, or disclosure would severely impact the firm’s operation due to a violation of federal or state law, violation of contract, a violation of privacy. This would include personally-identifiable information (PII).

**Confidential**

Data of a sensitive nature, where its loss, destruction, or disclosure would impact the firm’s operation through a loss of reputation/credibility.

**Nonpublic information [financials]**

Nonpublic information is information that is not generally known or available to the public. Information is considered to be available to the public only when it has been released to the public through appropriate channels, e.g., by means of a press release or a public statement from one of the company’s senior officers, and enough time has elapsed to permit the investment market to absorb and evaluate the information. As a general rule, information is not considered “public” until the first business day after public disclosure.

**Personally Identifiable Information**

The firm, in the operation of regular business, may collect personally-identifiable information (PII). This collection will be limited to the amount and type required specifically for an identified purpose. This will include data regarding both clients and personnel.

Information gathered (including PII) will be subject to an identified local Data Owner responsible for the data and who can act as a point of contact during security events that affect it. The Data Owner bears responsibility for data loss, appropriate access measures and audience, to ensure that use is appropriate to the purpose for which it was collected, and that appropriate consent has been obtained.

PII must not be stored on portable memory media, including CD’s, DVD’s, or USB drives. Hardcopy PII must be kept in locked file cabinets when not in use. When in use, only employees that have a business-specific need will be given access and must not be removed from the office. If no longer needed, hardcopy PII must be shredded onsite.

Regulations defining PII breach notification laws may be summarized federally in Canada here:

<https://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf11177.html>

Or, in the U.S. by state, here:

<http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>

**Proprietary/Internal Use**

Data of a sensitive nature, where its loss, destruction or disclosure would result in minimal impact to the firm but is not intended for public consumption.

**Public**

Data generally available to the public, where its loss would not impact the firm.

**Personnel**

Personnel, according to their position and need, will require access to various data sources. It is critical that depending on the classification of the data of which access is needed, users understand the serious nature of the data and its impact on the firm if loss, destruction, or disclosure would occur. When personnel leave the firm, an exit checklist is followed to ensure that data access has been fully revoked.

**Expectation of Privacy**

Users should expect no privacy when using [COMPANY] resources. Such use may include but is not limited to: transmission and storage of files, data, and messages. The company reserves the right to monitor any and all use of the computer network. To ensure compliance with or investigate a breach of company policies or the law, [COMPANY] may access records, communications and data, monitor use, intercept and review any communications sent or received using company resources, inspect data, including but not limited to data stored on personal file directories, hard disks, and removable media. Files, data and messages sent from, received by, or stored in or on the company’s resources are the sole property of the company, regardless of the form or content of such files, data and messages.

## Account/Credential management

### Accounts

Accounts give personnel access to systems and data otherwise not available. There are different categories of accounts, including “regular” user accounts, administration accounts, and service accounts. Each category will have specific requirements regarding usage. However, for each of these types of users, it is critical that account management (establishment, suspension, termination, and removal of user accounts) be carefully monitored and documented. Each account must be assigned the minimum required privilege level for business operation. If unauthorized access is detected, it must be investigated. Users should not be granted permissions for convenience or self-service of applications. Accounts are to be issued by the IT department unless otherwise specified. Users should not share or provide information about their account to anyone.

### Password usage

Passwords act as an access control measure against inappropriate activity. Passwords are established by the account owner and must comply with the standards as described below. Passwords are set to expire on predefined intervals and should be changed on a regular basis as follows:

* Retries on locked accounts should be set to [NUMBER] minutes or more
* Passwords are encouraged but not required to be changed every [NUMBER] days or less
* Passwords used should include at least [NUMBER] special characters
* Passwords used should include at least [NUMBER] number
* Passwords used should include upper and lowercase characters

Use the following password safe program to assist where a complex password is for a cloud application or administrators: [PASSWORD MANAGER NAME]. For end-user security, we do not offer or issue password management but recommend [PASSWORD MANAGER NAME].

Account owners are responsible for securing passwords. They must not be revealed, shared, posted, or stored in a manner that makes them easily available by others (including being sent in cleartext). If a password is demanded, they should be referred to this document and the IT Department should be contacted. At no time the password must be stored or posted complete with the owner’s user account.

Password usage policy will be implemented through a centralized authentication policy. At times, the IT Department may perform tests to confirm adherence to password rigor.

Firm systems attached to the network must be regularly patched to maintain the firm’s security stance and provide ongoing protection. Critical security patches must be installed (after appropriate testing) within [NUMBER] days after being released by the vendor. Other patches (not designated as critical by the vendor) may be applied as it is seen fit. A patch management system is used to deploy software updates in a consistent manner throughout the environment.

A vulnerability scanning system is employed to analyze the security stance of the computing environment, and to act as an adjunct to the patch management system.

### Vendor access policy

All external vendors must comply with the appropriate firm policies as would other personnel, with additional components, which may include contract language that specifies:

* A recent SSAE18(SOC2) report be provided if applicable and available
* Appropriate methods to access the firm’s environment
* Resources to which the vendor has access
* How information stored within the vendor’s sphere of control is to be protected
* Breach notification guidelines and how security breaches will be handled

## Devices

### Company-issued devices

Company-issued devices will have a standard set of products installed for the purpose of its use to support the business. Users shall not alter the devices, add software, or otherwise change the approved configuration of the devices in any manner without the express written consent of the IT team.

Personnel must safeguard their devices from theft by keeping them in a secure place at all times and must report lost, stolen, or damaged devices to the IT Department immediately. As well, the device should “lock out” or “reset” if an incorrect password is entered more than [NUMBER] times in a row.

### Bring your own device

All mobile devices issued by the firm are for the primary purpose of conducting business. For the purposes of this policy, these devices are subject to at least the criteria of laptop computers (especially when regarding possible loss vectors). All electronic communications and records processed on these devices should be secured and retained per this policy. There must be no expectation of privacy from the firm. Certain mobile devices owned by personnel (e.g. BYOD) are granted access to the firm’s computer systems and networks. Although the firm does not own these devices, users must nevertheless strictly adhere to all criteria of this policy.

Personal devices shall be pre-approved by the IT department before connecting physically or wirelessly to the corporate network. Approval by the IT department is conditional on adherence to the other sections of this policy and all other relevant policies.

Approval is rendered null and void in the circumstance where a device’s operating system or software components become End of Support Life (EOSL). In this circumstance, patches for the software are unlikely to be released and the device would otherwise pose a security risk to the company network and all other devices on it. As a result, these devices shall be upgraded or replaced prior to being reconnected to the company network.

The owner of said device further understands those by connecting an employee-owned device to computer systems through a network that they are agreeing to allow the firm to access, monitor, and, as necessary, erase information from these devices without notification or prior written consent of the employee.

Personnel must safeguard their devices from theft by keeping them in a secure place at all times and must report lost, stolen, or damaged devices to the IT Department immediately. As well, the device should “lock out” or “reset” if an incorrect password is entered more than [NUMBER] times in a row.

The firm strongly discourages the use of mobile devices while driving. Personnel must abide by laws pertaining to the use of mobile devices while driving and take appropriate safety precautions while utilizing these devices.

In keeping with the Instant Messaging and Email Policies detailed within this document, mobile phone text (e.g. SMS/iChat) messaging capabilities may not be used for business unless the ability to monitor them is enabled. Messages (e.g. communications that are made directly between mobile devices that bypass the user’s email account) are only to be used to conduct firm’s business in the event of irregular operations (e.g. when the firm’s email system is unavailable).

### Removable media

Removable media (including but not exclusive to recordable media and USB-attached drives) may not be connected to or used in computers that are not owned or leased by the firm without explicit written permission of the firm. This policy is established to reduce the risk of viral/malware infection spread through this vector and to minimize the risk of loss or exposure of sensitive or personally identifiable information.

### Changes to devices – Hardware

Company-issued devices must not have any hardware changes made to them, except by a member of the IT department. This includes adding any hardware, replacing or upgrading hardware, and removing hardware. Hardware includes any device or component that was not provided with the system and includes memory, internal or external storage, network interface cards, video adapters, cameras, microphones, etc.

A personal device that has been approved for connecting to the company network must remain configured as it was at the time of its approval. Any changes, replacements, or upgrades made after its approval will require that it be recertified by the IT department prior to its connection to the company network.

### Changes to devices – Software

Company-issued devices will have a standard set of products installed for the purpose of its use to support the business. Adding, removing, or changing the set of software products on these devices is forbidden, with the sole exception that upgrading an existing, installed software product to the most recent licensed version is both allowed and encouraged.

A personal device that has been approved for connecting to the company network will have a documented set of installed software products. The set of installed software products shall remain unchanged unless prior approval is received by the IT department, with the sole exception that upgrading an existing, installed software product to the most recent licensed version is both allowed and encouraged.

## 

## Software usage and licensing

The use of software not authorized by the firm (including improperly-licensed software) places the company at undue business, legal, and technological risk. Users must not download and/or install any software whatsoever without written advance permission from the IT Department. The IT Department reserves the right to periodically scan the contents of computers and mobile devices for non-standard software that may pose a risk to the network or violate certain laws or regulations and if discovered, disable or remove such software without warning.

The firm has licensed copies of software from a variety of publishers to meet legitimate business needs with copies made in accordance with the licensing agreements (which may, for example, permit an additional copy placed on a home computer for business purposes). No other copies of software or associated documentation can be made without the advance written approval by the IT Department.

## Cloud services

In order to maintain rigor regarding data privacy and access standards within the firm, cloud services (including online backup) may only be used with explicit written permission from the IT Department. Cloud services permitted within the organization are: [CLOUD SERVICE NAME]. Additional security controls may be required when using these services (including additional encryption and/or tokenization methods). As well, information classified as critical or confidential, especially Personally Identifiable Information must not be stored within Cloud Services.

When accessing cloud systems without a corporate-issued assets users are encouraged not to locally copy files and applications to non-corporate assets, or to fully remove information copied for work temporarily when this is untenable.

## Data security services & policies

### Anti-virus and Anti-malware

All systems, where possible (including servers, workstations, laptops and tablets), whether connected to the network or standalone, must only use firm-approved anti-virus and anti-malware software. The anti-virus and anti-malware software standardized within the firm is [ANTIVIRUS PRODUCT NAME].

Anti-virus updates are to be pushed automatically to all non-server systems (including workstations, tablets, and laptops). A manual check may be performed regularly. If malicious code is detected, it must be reported to the IT Department as soon as possible so that further investigation may be performed (if deemed necessary) as part of the Security Event/Incident Management program.

Anti-virus updates to servers are to be pushed manually on a defined regular basis (daily).

Devices must also include a running firewall and/or host-based intrusion detection system (HIDS).

Anti-malware detection may include collection of raw data periodically from the operating system for inspection of malicious files, system changes and network activity. This process uses the artificial intelligence capabilities of the products in some cases to determine if software or activity is malicious.

Temporarily, or permanently, disabling any of the security software or modifying the firewall configuration shall render the approval for that device null and void.

Subsequently, the device shall be inspected, audited, and – if deemed necessary – wiped and given a clean installation by the IT Department before being reapproved for connection to the company network.

### Destruction policy: electronic equipment, data and media

At all equipment’s end-of-life, sensitive data must be properly erased, destroyed, or as otherwise made unreadable. Doing so ensures that all appropriate legal measures are taken to comply with software license agreements, non-disclosure agreements, to keep critical and/or confidential information (including personally-identifiable information) safeguarded. Repurposed equipment must have hard drives removed and destroyed before reuse. Physical media disposal performed by an external party must have appropriate attestation subject to audit.

The company will utilize 3rd party recycling services from [DATA DISPOSAL COMPANY]. Efforts must be taken to wipe or re-image systems or hard drives. If this cannot be done physical destruction by shredding or drilling hard-drives is recommended.

### Encryption

Encryption technology is used within the firm to keep data secure both in motion and at rest. As appropriate to the data and access being protected, strong encryption technology must be used on all laptops, portable computing devices and removable media.

The email servers are configured to use TLS (Transport Layer Security) to provide a transparent encryption process when email is exchanged between servers configured appropriately. Internet-facing systems that require credentials for access are configured to use HTTPS. Where possible and appropriate (as per legislation and regulation), HTTPS (supported by strong encryption ciphersuites) must be used when accessing critical or sensitive data.

### Record retention

Policy represents the Company’s formal policy regarding the retention and disposal of documents and official records related to or generated in connection with the Company’s operations.

This Policy applies to all recorded information in any form or medium that is related to or generated in connection with the Company’s business activities, financial affairs or client transactions, or that demonstrates the Company’s compliance with applicable laws (“**Records**”).

Records may include but are not limited to:

* hardcopy (e.g., paper) documents and records;
* electronic documents and records (e.g., email, web files, text files, PDF files);
* records of correspondence (e.g., inquiries, complaints)
* recorded audio material (e.g., voicemail)
* video, digital images or graphic representations;
* archived web content; and
* documents derived from Records which cannot be re-created in an identical form at a later date.

**Excluded Records**

This Policy does not apply to, and Records do not include, personal documents which do not record the Company’s business activities, financial affairs or client transactions nor demonstrate the Company’s compliance with applicable laws, even if they form a foundation on which Records are based (e.g., working papers which are reflected in a recommendation).

The general rule is that a Record must be kept for **seven (7) years following its creation or receipt**, unless it is subject to a different retention period set out in Section 2 hereof.

**Exceptions**

The following types of Records must be retained for the following periods:

| **RECORD TYPE** | **EXAMPLES** | **RETENTION PERIOD** |
| --- | --- | --- |
| **Accounting Information** | * Financial Records * Account operating agreements * Account application forms * Records setting out the intended use of the account | 7 years from the creation of the Records **or** 5 years from the day of closing of the account to which they relate, whichever period is longer |

## Email

### Guidelines for use

* Emails are the property of [CUSTOMER NAME] and management reserves the right to audit all company emails as needed
* Broadcast messages to all employees or customers cannot be sent except to inform employees of an interruption of data, electrical services or emergency situations. Broadcast messages are reserved for situations where 85% of the target user group MUST need to know the content of the message being sent. Examples of broadcast messages that ARE NOT PERMITTED include:
  + Solicitation such as selling of concert or sport tickets
  + Vacation alert messages (use email response settings rather than non-targeted emails)
  + Announcing farewell parties
  + Seeking information about a topic
  + Holiday greetings
* All personal email communications must be kept to a minimum
* All email messages sent or received externally are recorded and can be reviewed regularly by the IT department
* Do not attach images or embedded video in email messages. Retrieving these types of messages is not only time consuming but costly for employees connecting remotely for their email messages and consumes valuable network data storage
* When responding to a received email message with more than one addressee, use discrimination when replying to all

### Procedures for securing email communication

* Sensitive information shall be carefully controlled so that its confidentiality, integrity, and availability are not negatively impacted. The following are some general examples of sensitive information:
  + PII (personally identifiable information) about any employee, customer, or vendor
  + Confidential or proprietary business information
* All email from unknown senders shall be regarded as suspicious
* Email from known senders with unusual or unexpected content shall be regarded with suspicion for the following reasons:
  + The email could have been forged to appear to have come from someone other than the real sender
  + The sender’s email account might have been hacked
  + The sender’s computer may have become infected with malware
* Users shall be suspicious of phrases like “Open Immediately”, “Invoice Past Due”, or “P&L Report.” These phrases are common tricks to lure unsuspecting recipients into opening attachments that have malware attached to them
* Users shall familiarize themselves with all other red flags that might indicate an illegitimate Email message (c.f. Social Engineering Red Flags)
* Users shall disable and keep disabled any features of their mail program that are designed to do any automatic processing of attachments, except for any that automatically scan for malware

Antivirus software is not infallible. Users should follow the above procedures to reduce risk, where possible, and use good judgment for anything not specifically covered.

### Receiving email

* Before opening links, users should hover over links to ensure that:
  + The item being linked to matches the text of the link
  + The link is to a well-known site, paying extra attention to the last two components of the URL (for example, “td.com.ru”, “www.td.net”, and “www.td-deposits.com” are not the same as “td.com” and would almost certainly not be legitimate, but “email.td.com” would probably be safe)
  + The link is not a misspelling or unusual spelling of a well-known site (examples: “amazom.com”, “td-banque.com”)
* Users should not click or follow suspicious links, even if the message appears to be from a trusted source
* Users should not open suspicious attachments, even if the message appears to be from a trusted source
* No type of attachment shall be considered “safe”; any file (document, image, spreadsheet, etc.) could potentially harbor some form of malware
* Users should not reply to a suspicious email or forward it to another party
* If in doubt, users should call the sender and verify whether the content of the message is legitimate
* Users should not click on “unsubscribe” links embedded in spam; unless they had previously subscribed to the mailing list and the link passes the tests mentioned earlier. Unsubscribe links are equally likely to be harmful as any other type of link
* If the sender, the message, and the attachment all appear to be legitimate, the attachment shall be scanned for malware prior to being opened. The reasons for this are two-fold:
  + Email communication is not, by nature, secure and the message could have been modified in transit
  + The attachment may have been unknowingly infected by malware on the sender’s computer system

### Sending email

* When sending mail that contains sensitive information (see the Policy section of this document), the body of the message must be encrypted to prevent interception by unauthorized parties.
* When sending messages with attachments that contain sensitive information, then the attachment must be encrypted in accordance with the corporate [Encryption Policies and Procedures](#_kjiva9wmmaif). Note that the decryption key (a.k.a. “password”) must not be sent in the same message as the encrypted data; that is analogous to locking a door and leaving the key in the lock. Where possible, use a communication channel other than email to transmit the key to the recipient.
* When replying to email, note the recipient list and be aware of the audience. Don’t include confidential information if any of the recipients aren’t authorized to know. If the information is vital to the thread or a response to a direct question, remove the individuals from the copy list, or reply privately.
* When forwarding email, be aware of the information not only being sent, but also any information that might be in attachments or buried in the previous messages in the thread. Don’t inadvertently forward sensitive information to unauthorized parties.
* Users should never send login or password information via email.

### Etiquette and professionalism

* Provide a subject line that is meaningful and to the point. Don’t send a carbon copy of a message to the rest of the company. Be judicious with respect to the people who gets a copy of a message
* Sometimes it is difficult to convey "tone" in an electronic format. What is said in a joking or sarcastic manner may be misinterpreted. Be careful.
* Don’t use all capitals in messages
* Use appropriate punctuation
* Summarize what is being responded to. Remove unnecessary text and send only the information important to the message. Be concise.
* Compose memos directly in email rather than creating a word document and attaching it to an empty email file
* Be aware when sending email to customers that the Internet has no controls for guaranteeing end-to-end message delivery within a specific timeframe, or at all. Nor does it guarantee the confidentiality, or the integrity of messages transmitted
* To share jokes, make announcements, or any other personal activity prohibited by this document, please use social media instead of corporate email

### Examples of inappropriate email content

* Gossip, such as personal information about the user or others
* Emotional responses
* Inappropriate language
* Derogatory, offensive or insulting remarks
* Harassment of others, including sending or soliciting sexual oriented messages or images, harassment or any remarks that may be interpreted as such
* Operating a business for personal gain, searching for jobs outside [CUSTOMER NAME], sending chain letters or soliciting money for religious or political causes
* Offensive or harassing statements, including disparagement of others based on their race, national origin, sex, sexual orientation, age, disability, religious or political beliefs
* Dissemination or printing copyrighted materials (including articles and software) in violation of copyright laws

### Canadian Anti-SPAM Legislation (CASL)

All electronic communications that are intended to encourage participation in a commercial activity are considered commercial electronic messages (‘’CEMS’’). The Company may engage in electronic communication activities with the goal to raise awareness. Email marketing is currently the only form of electronic communication that the Company utilizes for marketing purposes.

The following procedures and applicable exemptions (as described) apply to all CEMs that are sent by the Company:

* The Company does NOT send CEMs unless these messages comply with both the Consent and Content Requirements as described below
  + Generally, a commercial electronic message is compliant with the Consent requirement if the recipient has provided express or implied consent
    - Express consent is when an individual provided the Company and its employees permission to send them any type of message, including CEMs, by either:
      * Signing up and checking a box to receive email communications from the Company
      * Providing an email address, if it is clear that the Company (represented by its employees) intends to send CEMs
      * Oral or written requests to receive messages
    - Implied consent is where there is an ‘’existing business relationship’’ between the Company and the recipient. An ‘’existing business relationship’’ applies to, for example, mutual fund dealers and their financial advisors with whom the Company has a Dealer Agreement or to recipients with whom the sender has a contract that is ongoing or has expired within the past 2 years.
  + The Company will ensure compliance with the Content Requirement by including the following identity and contact information in each CEM:

[CUSTOMER NAME]; [CUSTOMER ADDRESS]

* All CEMs will include a mechanism to allow the recipient to unsubscribe from receiving CEMs from the Company
* All unsubscribe requests will be made effective within 10 business days
* All emails that are sent should include the following disclosure:   
    
  *“The content of this email is confidential and intended for the recipient specified within the message only. It is strictly forbidden to share any part of this message with any third party, without a written consent of the sender. If receiving this message by mistake, please reply to this message and follow with its deletion, so that we can ensure such a mistake does not occur in the future.”*

The Compliance team, or responsible entity, is responsible for the ongoing review and monitoring of compliance with CASL.

The Compliance team reviews proofs of all mass email communications that are sent by the Company. The Compliance team has access to email marketing tools and will monitor and review on a periodic basis samples of marketing emails that are sent.

The following CEMs are exempt from CASL:

1. Emails sent internally
2. Personal emails to friends and family
3. Communications with vendors and suppliers
4. Emails sent in response to a client or potential client email (therefore solicited by the person to whom the message is sent).

### CAN-SPAM (United States)

The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003(“CAN-SPAM”) is a federal law regulating the transmission of commercial email messages and Internet-to-phone SMS commercial messages to addresses that reference Internet domains.

The full text of this law can be found here: <http://www.gpo.gov/fdsys/pkg/PLAW-108publ187/pdf/PLAW-108publ187.pdf>

**Approval from a member of the Compliance Team is required prior to engaging in practices that are not specifically mentioned in this Acceptable Use Policy.**

## Instant messaging

Instant messaging is archived on an ongoing basis and is subject to review as is all communication. Users may not, under any circumstances, use instant messaging software that has not been approved and installed by the IT Department to send or receive correspondence directly or indirectly related to the firm and its business (this includes subcomponents within websites – e.g. Facebook Chat or Skype Chat). The approved company messaging application is [INSTANT MESSAGING APP NAME].

## Social media

[CUSTOMER NAME] Products uses social media as a marketing tool, primarily as a complementary method of sharing content posted on the Company’s website in order to raise awareness of the [CUSTOMER NAME] brand and to share relevant topics or third party content relating to it’s activities.

[CUSTOMER NAME] currently uses the following social media channels: LinkedIn, Facebook, Twitter and YouTube or any other additional channels that may be used at a later time upon approval from Compliance (the “Platforms”).

Most of the content posted on social networking sites is typically static content with minimal or no interactive (real-time) postings. All static content is considered a sales communication and must comply with the applicable regulations.

The following guidelines apply to content published on any of the Platforms and must be adhered to by all applicable Marketing employees (the “Employees”) when using social media for business and marketing purposes.

1. All posts (static and non-static content), including responses to comments must be pre-approved by the Compliance Department.

The Marketing department is responsible for ensuring that only compliance approved content is posted on the Platforms; [CUSTOMER NAME] Compliance may conduct sample reviews of social media postings from time to time at its discretion and disciplinary action may be taken against Employees if the firm’s guidelines are violated.

1. Employees should not generally delete any communications made through social media sites.  If a circumstance arises and a post must be deleted, it must be approved by the Compliance Department.
2. Posts to Platforms should not be viewed as advice to clients or recommend a security or or any product offered by [CUSTOMER NAME]
3. All posts should be consistent with [CUSTOMER NAME]‘s commitment to act honestly, in good faith and in the best interests of the clients.
4. When responding to users’ comments or questions on the Platforms, [CUSTOMER NAME] Products may redirect users to other [CUSTOMER NAME] channels, such as phone, which may offer opportunities for more detailed and effective communication.
5. Third-party content shall not be posted in a manner that may be perceived as an endorsement by [CUSTOMER NAME] of the originator.
6. Participation in interactive electronic forums (interactive real-time communications) is currently prohibited. Should [CUSTOMER NAME] consider enhancing the firm’s online presence, the Compliance department must be approached to ensure that appropriate technology and supervisory procedures are in place.
7. All social media pages shall include the following disclaimer (or direct the users to read it on [CUSTOMER NAME] website) , as applicable:
8. The employee’s primary email address associated with the login is their firm-registered email address;
9. The username is not a pseudonym;
10. The password used on the Twitter account differs completely from the user’s account password.

[CUSTOMER NAME]’s LinkedIn and Facebook profiles, Twitter account and YouTube channel information and updates are for Canadian residents only.

[CUSTOMER NAME] endeavors to ensure that the contents have been compiled or derived from sources that we believe are reliable and contain information that is accurate and complete. However, [CUSTOMER NAME] makes no representation or warranty, express or implied, in respect thereof, takes no responsibility for any errors and omissions contained herein.

While all social media channels encourage information sharing and conversation, users should not disclose personal information\* for security and privacy reasons. Users should not post inappropriate, disrespectful, inaccurate or unrelated content. [CUSTOMER NAME] reserves the right to delete inappropriate, disrespectful, inaccurate or unrelated content posted on its social media channels at any time at its discretion.

[CUSTOMER NAME] is not affiliated with any social media website and cannot control how they or other parties will use the information shared on it. Users are encouraged to read and understand the privacy policies and terms of service for each social media platform and should have no expectation of privacy for information posted in public forums.

***For more information about our products and services, please visit [COMPANY WEBSITE].***

## Document management

This Hardcopy (Paper) Document Management Procedure (the “Procedure”) shall apply only to hardcopy (e.g., paper) Records created or received by the Company and which may be scanned or converted into a Portable Document Format (“PDF”) file (the “Documents”).

The Company employee who creates or receives a Document (the “Responsible Employee”) shall be responsible for following this Procedure with respect to that particular Document.

### Destruction procedure

After record retention periods have elapsed and if record administrators have not extended retention documents are to be destroyed by shredding hard copies on company premises if in hard copy or use the digital media destruction guidelines in this document.

The Company may recycles the information produced as part of our corporate policy:

### Scanning procedure

* The Responsible Employee shall scan or convert all Documents into PDF files.
* The Responsible Employee shall review the PDF file in order to confirm that the Document was clearly, accurately and completely scanned or converted into the PDF file.
* The Responsible Employee should also apply optical character recognition (“OCR”) to the PDF file.

### Document naming

The Responsible Employee shall name each PDF file using the following standard format:

*Date\_DocumentType\_DocumentDescription\_AnyAdditionalInformation*

*E.g., 2016-02-20\_invoice\_for\_telephone\_service.pdf*

Files names shall contain the following elements (as applicable):

* Date of the document: using the YYYY-MM-DD format – e.g., 2016-02-26
* Type of document: e.g., invoice
* Description of the Document: e.g., for\_telephone\_service
* Any additional information: e.g., V\_2 for the second version of a document

In addition, file names shall:

* only use alphanumeric characters
* use underscores ( \_ ) to represent spaces, and
* be short, simple and easy to understand

### Storage

The Responsible Employee shall upload the PDF file to the applicable network drive of the Company or the Company’s electronic document storage system, if any.

Both original paper and electronic documents should NOT to be destroyed

The original Documents shall not be destroyed and shall be kept in their original form and stored in the traditional manner (in addition to being uploaded to the applicable network drive of the Company or the Company’s electronic document storage system, if any).

## Network access

### Corporate networking

The firm’s network provides access to the company’s confidential and business-critical information and assets. Only computer equipment with express authorization to be connected to the firm’s network may be given access. All other equipment must require advance written approval by the IT Department before installed or connected. In many cases, installation by an appropriate member of the IT Department will be required. When personnel leave the firm, an exit checklist is followed to ensure that network access has been fully revoked.

### Wireless networking

Prior to connecting to any network outside the office please ensure that all applications such as Microsoft Office (Outlook, Word, Excel Files), Browsers and Remote Drives.

Personal devices can be connected to the corporate guest network when using a Virtual Private Network (VPN) immediately upon connection.

We use a always on VPN connection implying that the filtering for (Firewall/URL/Gateway) are maintained when on Guest or 3rd Party Wireless.

All traffic that originates on the guest network is required to be separate from the corporate network. If the guest network is used to access the internal network (e.g. through a VPN), it is subject to the same policies regarding authorization, authentication, and logging as found within the Network Access Policy.

In-office wireless network access is subject to the same policies regarding authorization, authentication, and logging as found within the Network Access Policy.

Outside the office, the use of public Wi-Fi without the use of a VPN is actively discouraged.

### Remote access policy

It is the responsibility of all personnel with remote access privileges to the firm’s network to ensure that the remote access connection is given at least the same consideration as the user’s onsite connection. Additional rigor may be needed to effect remote access (including approval for remote access and/or two-factor authentication measures). Personnel must use only the remote access methods offered by the firm and not substitute others they may consider “easier” (e.g. ThinClient Virtual Desktop/VPNClient or Ad-Hoc installation of a remote support application like Gotomeeting, Teamviewer) that might produce an unwanted access vector into the firm.

If personnel connect from a public system (e.g. Internet kiosk) with two-factor authentication they must recognize that this cannot defend against software or hardware that enables screen-scraping or key-logging behavior. As such, it is highly recommended that the corporate environment be accessed only through hardware that is specifically permitted for corporate use.

## Physical security

The office is securely locked by default (24 hours a day, 7 days a week).

### Employee access policy

Building security requires all employees use a passcard for access to the building/suite. Employees’ access to specific areas will be assigned as privilege requires.

### Visitor access policy

Building security requires the check-in of visitors at reception and a temporary access pass be granted. Upon leaving, personnel responsible for the visitors must retrieve the temporary access pass and accompany the visitors through the exit.

Personnel are issued a building pass to gain access at the lobby and the office upstairs. Upon termination, an employee is required to turn over their building pass. Periodic reviews of the physical access list are performed.

Access to the data centers and equipment rooms requires two-factor authentication for entry. Visitors must be signed-in, and accompanied at all times by authorized personnel who are responsible for them.

## Workstation security

The purpose for this policy is to establish the minimum requirements for maintaining a secure workstation or “clean desk” – where sensitive/critical information about employees, intellectual property, customers and vendors is secure in locked areas and out of site. A Clean Desk policy is not only ISO 27001/17799 compliant, but it is also part of standard basic privacy controls.

Personnel computers must be protected from unauthorized access during any temporary absence or breaks. The following protocol must be followed if not physically present at the computer:

1. Workstations must be locked immediately when leaving the workspace, regardless of how long the intent to be away, or how far away.
2. All users will be cognizant of the sensitivity of the information with which they are working and lock their screen, if needed, to prevent accidentally disclosing information to unauthorized individuals
3. If a workstation has been idle for more than [IDLE TIME], the workstation must be automatically locked, and the user must reauthenticate to unlock the workstation
4. All users must log out of all workstations before leaving at the end of the work day
5. When possible, workstations should be shut down and powered off at the end of the work day
6. Any media containing sensitive information must be removed from the desk top and locked in a drawer or filing cabinet when the desk is unoccupied and at the end of the work day. This includes hard copy paper and digital media devices (CD-ROM, USB drive, etc.)
7. File cabinets containing sensitive information must be kept closed and locked when not in use or when not attended
8. Keys used for access to sensitive information must not be left at an unattended desk
9. Mobile devices such as laptops and tablets must be either locked with a locking cable or locked away in a drawer if left at the end of the work day
10. Passwords may not be written down. See the Password Protection Policy for additional password handling requirements
11. Printouts containing sensitive information should be immediately removed from the printer or fax machine to prevent them from being picked up by unauthorized individuals
12. Upon disposal, sensitive documents should be immediately shredded using either a cross-cut or diamond method. If an onsite shredder is not available, the documents must be placed in locked confidential disposal bins designated for off site or mobile shredding services
13. Whiteboards containing sensitive information should be erased

## Monitoring

The firm reserves the right to monitor and ensure the appropriate use of company computing resources in a manner consistent with all applicable laws (including national, state, and local jurisdictions). These actions may include periodic assessments of software use, unannounced inspections of the firm’s computers, email stores, workstation hard drives, mobile devices, monitoring of website visits and network traffic, and the removal of any software found on the firm’s property for which a valid license or proof of purchase cannot be located or is determined to be inappropriate.

Logs are monitored 24/7 by security partner, [ActZero](https://actzero.ai/). This provides a continuous, centralized log management system and provides regular reporting and review.

### Activities to be logged

* A create, delete, or modify operation on any data
* A read operation on confidential information (see Data Classification Policy)
* Initiation of a network connection
* Acceptance of a network connection
* User authentication and authorization, such as user login and logout
* Grant, modify, or revoke access rights or other user attributes, including but not limited to:
  + adding or deleting a user or group
  + changing a user’s role, privilege level, group membership, or organizational unit
  + changing a group’s privileges
  + changing file permissions or ownership
  + changing database object permissions .changing firewall rules .
  + user password changes
* System, network, or services configuration changes, including installation of software patches and updates, or other installed software changes
* Application process start, stop, or restart
* Application process abort, failure, or abnormal end, especially due to insufficient permission to access an object or resource, resource exhaustion, reaching a resource threshold, the failure of network services such as LDAP or DNS, memory corruption, or a hardware fault
* Detection of suspicious/malicious activity such as from an Intrusion Detection or Prevention System (IDS/IPS), anti-virus system, or anti-spyware system
* Environmental monitors exceed documented thresholds (temperature, humidity, power, etc.)

### Elements of the log

* Type of action/activity. Examples: authorize, create, read, update, delete, and accept network connection
* Subsystem performing the action. Examples: process or transaction name, process or transaction identifier
* Identifiers (as many as available) for the subject requesting the action. Examples: user name, computer name, IP address, and MAC address. Note that such identifiers should be standardized to facilitate log correlation
* Identifiers (as many as available) for the object the action was performed on. Examples: file names accessed, unique identifiers of records accessed in a database, criteria used to determine records accessed in a database, computer name, IP address, and MAC address. Note that such identifiers should be standardized to facilitate log correlation
* Whether the attempted action was allowed or denied by access-control mechanisms
* Description and/or reason-codes of why the action was denied, if applicable
* Whether the attempted action succeeded or failed
* Description and/or reason-codes of why the action was unsuccessful, if applicable
* Before and/or after values when the action involves updating a data element or configuration item, whenever either or both are available
* Date and time that the action was attempted, including relevant time-zone information if not in Coordinated Universal Time. To maximize the ability to correlate events, all participating systems shall automatically maintain their clocks in sync with a central time server via NTP, SNTP, or similar technology so that the logs from different systems will appear in the correct order when amalgamated

### Formatting, transmission, and storage

The system shall support the formatting and storage of audit logs in such a way as to ensure the integrity of the logs, to control access to the logs, and to support enterprise-level analysis and reporting.

### Confidentiality

Some of the logs will contain sensitive information, and therefore must be protected from access by unauthorized individuals.

* If supported by the system, logs shall be encrypted during transmission to the centralized logging system. Furthermore, the log data shall be stored in an encrypted format. Refer to the Encryption Policy and Procedures document for details regarding acceptable methods of encryption
* Access to the logging server should be tightly controlled due to the sensitive nature of some of the data stored in the logs

### Integrity

Centralized logging has many benefits, including:

* increasing the difficulty for a bad actor to erase or modify the logs by creating a duplicate on a remote system with limited access
* reducing the risk that logs on the systems will be lost or overwritten
* reducing the risk of an outage due to logs growing to fill the available disk space on critical systems
* facilitating log correlation

### Log retention

The logs will need to be persisted for sufficient time to ensure that the data is available if a forensic analysis were required. To that end, the following restrictions shall be observed.

* All security-related events (e.g. authentication, authorization, security configuration changes, access to sensitive data) shall be retained for 12 months
* All logs shall be retained in an easily searchable format for a minimum of 3 months. Logs older than 3 months may be compressed and/or moved to less expensive storage media

Notwithstanding the previous bullet points, and in compliance with the above section on Confidentiality, access to the log data must continue to be tightly controlled and it must remain encrypted; both in transit, and at rest.

### Alerting

Internal IT and security partners report Incidents that represent a potential immediate or imminent threat to the confidentiality, integrity, or availability of the production systems and/or production data in the form of an alert. At a minimum, this alert shall be communicated via email but integration with [INSTANT MESSAGING APP NAME] or other rapid response system (ActZero MDR Platform) is also performed. The alert, if sent over public networks, shall contain minimal information regarding the specific threat to mitigate the risk of the nature of the incident being intercepted by unauthorized individuals.

The following is a list of examples of events that meet the criteria previously outlined and, consequently, for which alerts will be sent. It should not be considered exhaustive. A periodic internal review of the criteria for sending alerts shall be made at least annually to maintain a balance between ensuring adequate protection from significant threats and minimizing the number of false alarms.

* The intrusion detection system detects an attempted or successful intrusion, a denial of service attack, or other highly suspicious behaviour
* The firewall is blocking an unusually high number of connections or packets
* The number of failed login attempts in a recent time interval exceeded a reasonable threshold
* The overall number of file accesses in a recent time interval exceeded a reasonable threshold
* The number of file accesses by any single individual exceeded a reasonable threshold
* The monitors on one or more systems has exceeded a minimum or maximum threshold (unless this overlaps with a centralized monitoring system)

### Reporting

Reports are provided on a monthly basis by security partner ActZero Networks. Reports shall contain:

* a summary of behaviours and incidents from the previous reporting period. Including Network, Endpoint and Servers/Application systems
* A list of all vulnerabilities and security hygiene issues for the organization
* A Security Committee Task list for follow-up items

Monthly reports are reviewed by IT on a regular interval, and actions summarized for continuous improvement.

The firm reserves the right to limit access to any program, service, or capability accessed through the firm’s network or Internet that is deemed to pose a threat to information systems, violates any company policy, or impacts the productivity of the firm’s staff.

## Incident response / security events

Rapid response to security incidents and regular review of security events are vital to determining a cyberattack in progress. If a user sees suspicious activity or loss of information they are required to report the incident.

Example scenarios include:

| **Scenario** | **Detection** | **Alerting** | **Response** | **Time Elapsed** |
| --- | --- | --- | --- | --- |
| I’ve been hacked and I don’t know how they got in | None | User Reports Encrypted Machine | Call 1 888 855 3555 | 2 Hours |
| I’ve been hacked and I know they accessed sensitive data | RDP Logs | Anti-virus | For data on UK citizens call ICO @ … For other sites see this page for contact details... | 3 days |

## Reporting violations

The firm has an “open door” policy regarding the reporting of violations to security policy. All personnel are responsible for ensuring the ongoing confidentiality, integrity, and availability of systems and information within the firm. If a violation of policy is detected, personnel are obliged to report it as soon as possible. Depending on the nature of the violation, a report should be made to an appropriate subset of the following within the firm:

* IT Department
* Human Resources Manager
* Chief Compliance Officer
* Chief Operations Officer
* General Counsel
* Senior Management

As stated earlier, a data security violation in which PII is exposed may require a formal breach notification, appropriate to data and domicile.