CAL Business Solutions, Inc.
Written Information Security Policy

OBJECTIVE:

Our objective, in the development and implementation of this written information security plan, is to create effective administrative, technical and physical safeguards in order to protect our customers' non-public personal information. The plan will evaluate our electronic and physical methods of accessing, collecting, storing, using, transmitting, protecting, and disposing of our customers' non-public personal information.

PURPOSES:

- Ensure the security and confidentiality of our customers' information;
- Protect against any anticipated threats or hazards to the security or integrity of our customers' information;
- Protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any of our customers.

ACTION PLANS:

- Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or information systems;
- Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information;
- Evaluate the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risks.

ACTION STEPS:

- Initial implementation of the plan
- Training of employees (CAL Team Meeting)
- Regular testing of the controls and safeguards established by the plan
- Evaluating the ability of prospective service providers to maintain appropriate information security practices, ensuring that such providers are required to comply with this information security plan, and monitoring such providers for compliance herewith
- Periodically evaluating and adjusting the plan, as necessary, in light of relevant changes in technology, sensitivity of customer information, reasonably foreseeable internal or external threats to customer information, changes to our own business (such as mergers or acquisitions or outsourcing), and/or changes to customer information systems

We ***determine*** reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or information systems, ***assess*** the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information, and ***evaluate*** the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risks.

INTERNAL THREATS

How CAL Prevents:

*Intentional or inadvertent misuse of customer information by **current** employees*

- Dissemination of, and annual training, on privacy laws and firm privacy policy
- Incorporation of privacy policy guidelines into employee handbook
- Employment agreements amended to require compliance with privacy policy and to prohibit any nonconforming use of customer information during or after employment
- Employees are encouraged to report any suspicious or unauthorized use of customer information.

*Intentional or inadvertent misuse of customer information by **former** employees*

- Require return of all customer information in the former employee's possession -Policy requires return of all firm property, including laptop computers and other devices in which records may be stored, files, records, work papers, etc…
- Eliminate access to customer information- Policy requires surrender of keys, business cards; disable remote electronic access; invalidate voicemail, e-mail, internet, passwords, etc…, and maintain a highly secured master list of all lock combinations, passwords, and keys.
- Change passwords for current employees periodically.
- Amend employment agreements during employment to require compliance with privacy policy and to prohibit any nonconforming use of customer information during or after employment.
- Send notification to clients informing them that the employee has left the firm.

*Inadvertent disclosure of customer information to the **general public** or **guests** in the office*

- Prohibit employees from keeping open files on their desks when stepping away.
- Require all files and other records containing customer records to be secured at day's end.
- Change passwords for current employees periodically
- Restrict guests to one entrance point; restrict areas within the office in which guests may travel unescorted.
- Use shredding machines on unused photocopies or other records being discarded before depositing in trash or recycling containers
- Ensure secure destruction of obsolete equipment, including computer hardware and software systems.
- Encourage employees to report any suspicious or unauthorized use of customer information.

NOTE: Periodic testing to ensure all these safeguards are implemented uniformly.

EXTERNAL THREATS

How CAL Prevents:

Inappropriate access to, or acquisition of, customer information by third parties:

- The internal calszone.net domain is protected from attacks from both inside and outside through the use of Antivirus protection, SSL-VPN, and 3rd-party email filtering.

- Incoming attacks are blocked with a SonicWALL TZ500 firewall with only essential ports open. Ping response from outside is blocked to deter robotic detection. Antivirus protection is provided by the latest Avast Business Premium software which is automatically updated daily. Both incoming and outgoing email is filtered externally by Proofpoint SaaS for incoming viruses and malware as well as a guard against any mass-mailing worms which may have escaped detection. There are no servers or workstations with outward-facing IP addresses, and any internet-facing services running at CAL require the use of a DMZ.
- Servers are all Windows 2012 or 2016 and all are members of the internal domain. File structure on all servers is NTFS which is encryption-capable. All customer data which is entrusted to CAL will be stored on these NTFS partitions and encrypted with at least 128-bit algorithm. Workstations and notebook computers on which data may be stored are Windows 10 whose NTFS partitions which are encryption-capable.

- Require secure authentication for internet and/or intranet and extranet users.
- Require encryption and authentication for all infrared, radio, or other wireless links.
- Train employees to protect and secure laptops, handheld computers, or other devices used outside the office that contain customer information.
- Establish uniform procedures for installation of updated software. Security patches are installed automatically on both workstations and servers.
- Establish systems and procedures for secure back-up, storage and retrieval of computerized and paper records.
- Establish procedures to ensure external physical points of entry to the office are closed, locked and accessible to unauthorized persons when the office is closed.
- Install burglar alarm or other security systems, with training for authorized persons on activation, and deactivation.
- Use shredding machines on unused photocopies or other records being discarded before depositing in trash or recycling containers.
- Ensure secure destruction of obsolete equipment, including computer hardware and software systems.
- Encourage employees to report any suspicious or unauthorized use of customer information.

Third-Party Access (Cleaning Company, etc…)

- Evaluate the ability of all prospective third-party service providers to maintain appropriate information security practices.
- Provide all third-party service providers who have access to the premises with a copy of the Privacy Policy.
- Require all such third-parties—by written contract—to adhere to the Privacy Policy, agree to make no use of any nonpublic personal information on your customers that would be prohibited thereby, or otherwise by law or contract, and agree to hold harmless and indemnify the firm for any inappropriate use of customer non-public personal information.
- Require all such third-parties—by written contract—to return all keys and all other property at the completion or termination, for whatever reason, of the agreement between the firm and the third-party.

Building Security (to protect physical access to data)

- **Keys-** Any key given to an employee must be returned when requested by Management, or when terminated. In the event of a termination, clients must be notified that employee has left and key was returned. Alarm code will be removed so no longer active.

- **Employee Responsibilities**- Whomever is the last to leave the building, that employee is responsible to set alarm and lock all doors.

- **Lost or Stolen Key**- management must be notified immediately

Electronic Mail Acceptable Use Policy

Our User Responsibilities

We provide electronic mail to our staff to enable them to communicate effectively and efficiently with other members of staff, other companies and partner organizations.

We comply with the following guidelines.

DO

- Do check our electronic mail daily to see if we have any messages.
- Do include a meaningful subject line in our message.
- Do check the address line before sending a message and check we are sending it to the right person.
- Do delete electronic mail messages when they are no longer required. Note that all incoming email is archived for legal purposes with access on a need-to-know basis only.
- Do respect the legal protections to data and software provided by copyright and licenses.

DO NOT

- Do not print electronic mail messages unless absolutely necessary.
- Do not expect an immediate reply, the recipient might not be at their computer or could be too busy to reply straight away.
- Do not forward electronic mail messages sent to us personally to others, particularly newsgroups or mailing lists, without the permission of the originator.
- Do not use electronic mail for personal reasons.
- Do not send excessively large electronic mail messages or attachments, unless necessary
- Do not participate in chain or pyramid messages or similar schemes.
- Do not represent ourselves as another person.
- Do not use electronic mail to send or forward material that could be construed as confidential, obscene, threatening, offensive or libelous.

I.T. Security Policy

Our User Responsibilities

We comply with the following Guidelines:

- Every individual is responsible for protecting the data and information in your hands. Security is everyone's responsibility.
- Recognize which data is sensitive. If you do not know or are not sure, ask.
- Even though you cannot touch it, information is an asset, sometimes a priceless asset.
- Use the resources at your disposal only for the benefit of the Organization.
- Understand that you are accountable for what you do on the system.
- If you observe anything unusual, tell management

When using the CAL Business Solutions' computer system we comply with the following guidelines:

- Choose a password that would be hard to guess
- Log off or lock your PC before you leave your workstation. This is important if you are working on sensitive information or leaving your workstation for any length of time.
- Protect equipment from theft and keep it away from food and drinks.
- Ensure that all important data is backed up regularly.
- Make sure that on every occasion floppy disks, CD's, DVD's and USB sticks are brought in to the Office that they are checked for viruses before use.
- Inform the I.T. Department immediately if you think that your workstation may have a virus.

To prevent any security issues:

- Do not write down your password.
- Do not share or disclose your password.
- Do not give others the opportunity to look over your shoulder if you are working on something sensitive.
- Do not duplicate or copy software.

Internet Acceptable Use Policy

Our User Responsibilities

CAL Business Solutions provides Internet access to staff to assist them in carrying out their duties for the Company. It is envisaged that it will be used to lookup details about suppliers, products and other information regarding work issues. It should not be used for personal reasons.

- Only access the Internet by using the Organization's content scanning software, firewall and router.

When using CAL's Internet access we comply with the following guidelines:

- Keep your personal use of the Internet to a minimum of no more than 15 minutes per day.
- Check that any information you access on the Internet is accurate, complete and current.
- Check the validity of the information found.
- Respect the legal protections to data and software provided by copyright and licenses.
- Inform the I.T. Department immediately of any unusual occurrence.

Company Policy and to prevent any security Issues:

- Do not download text or images which contain material of a pornographic, racist or extreme political nature, or which incites violence, hatred or any illegal activity.
- Do not download content from Internet sites unless it is work related.
- Do not download software from the Internet and install it upon CAL computer equipment.
- Do not use CAL computers to make unauthorized entry into any other computer or network.
- Do not disrupt or interfere with other computers or network users, services, or equipment.
- Do not represent yourself as another person.
- Do not use Internet access to transmit confidential, political, obscene, threatening, or harassing materials.

Password Security Policy

Our User Responsibilities-Choosing A Secure Password

Ideas in order to secure passwords:

- Don't use dictionary words - All real words are easy to guess. Avoid using any words, words in foreign languages, swear words, slang, names, nicknames, etc.
- The names of family, friends and partners, anniversary dates, car registrations and telephone numbers are the first thing potential crackers will try when guessing your passwords.
- Try to pick acronyms, mnemonics, random letters, etc, or insert non-alphabetic characters in the middle of the word, replace letters with numbers
- Use a mIxTuRe of UPPER and lower case on case sensitive systems
- Include a number (0-9) somewhere in the password. Try to fit this in somewhere inside whatever letters you choose, instead of at the end or beginning of the password.
- If possible include a symbol somewhere in the password.
- When changing passwords, change more than just the number: perhaps move its position within the password, add or subtract letters, change capitalization, etc.
- Never tell anyone else your password or allow them to log in as you. If it is necessary to provide your password to someone else to allow a fault to be fixed, ensure that they are genuine members of Information Technology Department first.

Data Encryption Policy

Purpose

This policy covers all computers, electronic devices, and media capable of storing electronic data. This policy also covers the circumstances under which encryption must be used when data is being transferred. It provides CAL Business Solutions guidance on the use of encryption to protect resources that contain, process, or transmit confidential Client information.

Scope

This policy applies to all CAL Business Solutions, Inc. employees and affiliates. This policy is to establish the types of devices and media that need to be encrypted, and when encryption must be used. It addresses encryption policy and controls for confidential Client data that is at rest (including portable devices and removable media), data in motion (transmission security), and encryption key standards and management.

Policy

Based on the data protection risk assessment described above, CAL Business Solutions, Inc. uses Microsoft BitLocker technology for encrypting confidential Client data on workstations and portable media. BitLocker Encryption is available onWindows 10 Enterprise and Windows 10 Professional. As of the date of this document, all CAL users are running either Windows 10 Enterprise or Windows 10 Professional.

Devices and Media Requiring Encryption

- Encryption is required for all laptops, workstations, and portable drives that may be used to store or access customer data.

Electronic Data Transfers

- Any transfer of unencrypted customer data must take place via an encrypted channel.

Physical Transfer of Electronic Data

- Any time customer data is placed on a medium such as a CD, DVD, or portable drive to facilitate a physical transfer, the data must be encrypted.

NOTE: Any employee's failure to follow this policy can result in disciplinary action as provided in the Employee Handbook. Disciplinary action for not following this policy may include termination.

Portable Drive Security

Portable devices represent a specific category of devices that contain data-at-rest. Many incidents involving unauthorized exposure of confidential Client data are the result of stolen or lost Portable Computing Devices. The best way to prevent these exposures is to avoid storing confidential data on these devices. As a general practice, confidential Client data should not to be copied to or stored on a portable computing device. However, in situations that require confidential data to be stored on such devices, encryption reduces the risk of unauthorized disclosure in the event that the device becomes lost or stolen.

Guidelines to follow to prevent security Issues:

- Each designated information resource owner will identify information that is confidential.
- All users must obtain specific permission from the data owner before storing confidential data on a portable computing device.
- Confidential information stored on portable devices including laptops and personal digital assistants (PDAs), must be encrypted.
- Portable devices including laptops and personal digital assistants (PDAs), should not be used for the long-term storage of any Confidential information.
- Portable devices including such as laptops and personal digital assistants (PDAs) that store or transmit confidential information must have the proper protection mechanisms installed, including antivirus or firewall software, with unneeded services and ports turned off and subject to needed applications being properly configured.
- Removable media including CD-ROMs, floppy disks, backup tapes, and USB memory drives that contain confidential information must be encrypted and stored in a secure, locked location.
- Removable media including CD-ROMs, floppy disks, backup tapes, USB memory drives, etc. that contain Confidential information must be transported in a secure manner.
- Portable or removable media that contain confidential data must be in the possession of the authorized user at all times (e.g., must not be checked as luggage while in transit).
- The receiver of the removable media must be identified to ensure the person requesting the data is the one claimed.
- Data owners and users of portable computing devices and containing confidential data must acknowledge how they will ensure that data are encrypted and how encrypted data will be accessible by the owner in the event that an encryption key becomes lost or forgotten.

Data Disposal Policy

The purpose of this policy is to establish a standard for the proper disposal of electronic data and physical data records.

- Electronic media containing secure information
- Physical data records

General - All electronic media must be properly sanitized before it is transferred from the custody of its current owner. The proper sanitization method depends on the type of media and the intended disposition of the media.

- Overwriting hard drives for sanitization. Government-approved scrubbing is to be performed before reformatting.
- Destruction of electronic media: Destruction of electronic media is the process of physically damaging medium so that it is not usable by any device that may normally be used to read electronic information on the media such as a computer, tape player, audio or video player.
- Clearing data: Clearing data such as formatting or deleting information removes information from storage media in a manner that renders it unreadable unless special utility software or techniques are used to recover the cleared data. Once data is removed, empty disk space will be scrubbed with government-approved processes.

Manual Records: CAL Business Solutions, Inc. recognizes the importance of destroying all records effectively in order to protect the security our customer's non-public information in its possession. This policies purpose is to ensure a rigorous and consistent approach to the secure destruction and disposal of such records.

It is the individual responsibility of all staff to ensure information they are handling is destroyed effectively, securely and in accordance with this policy. Manual records that have reached the end of their lifecycle are divided into the following two categories, and are destroyed in accordance with the instructions relating to each category.

- **Paper Recycle Bins-** For non-confidential records and/or data, and those containing no personal information, bins are provided for recycling purposes. All recycle bins are emptied whenever necessary by a member of staff. As paper collected in the bins is only ever recycled and never shredded, it is the responsibility of all those placing material in the bins to check that it has been identified correctly for recycling.

- **Confidential Shredding -** A record containing any type of confidential, non-public data or personal information, such as name, address, SSN, contact details, etc., is shredded by a member of staff.

Printers, Fax Machines, Copiers

Many of these devices contain hard drives or other types of media in them. Some can store past data that has been copied or printed and pose a data security risk. It is our responsibility to make sure any confidential information is deleted off these devices when needed.

Delete Files-Recycle Bin- If recycle bin contains customer data, recycle bins will be emptied immediately and cleared areas scrubbed.

Delete Files-Secure Erase- Will be used as requested.

Ensuring That Our Staff Follows our WISP

Our Information Security Team trains every new member of our staff in his or her role in carrying out the Written Information Security Policy (WISP). This training is refreshed annually. New staff members agree to

follow our WISP, and understand that their continued employment in our organization depends on their following the WISP. Employees who fail to follow the WISP are given written warnings, followed, if necessary, by being asked to leave the organization.

01/27/2021