[Introduction 2](#_Toc4931157)

[SECURITY policies 3](#_Toc4931158)

[Acceptable Use Policy 3](#_Toc4931159)

[Application Security 4](#_Toc4931160)

[Clean Desk Policy 5](#_Toc4931161)

[Data Breach Response Policy 5](#_Toc4931162)

[Email Policy 6](#_Toc4931163)

[Encryption Policy 6](#_Toc4931164)

[Network Security – Third Party Network Provider 8](#_Toc4931165)

[Network Security – Remote Access 8](#_Toc4931166)

[Network Security – Wireless Communication Policy 8](#_Toc4931167)

[Wireless Communication Standard 9](#_Toc4931168)

[Password Protection Policy 10](#_Toc4931169)

[Technology Equipment Disposal 10](#_Toc4931170)

# Introduction

Sales Optimizer recognizes that in order to be a successful and valued partner to its customers, its business must be conducted in a secure manner. It is Sales Optimizer’s policy to protect its own and its client’s people, property, technical integrity, information and reputation against security threats and risks arising from its operations.

All employees, agents, contractors and vendors of Sales Optimizer are expected to comply with this policy. The consequences of breaching the information security policy may lead to disciplinary action up to and including termination of employment.

**Policy Objectives**

Several organizational objectives are fulfilled by a well-rounded set of Information Security policies including:

* **Maintain Regulatory Compliance:** While risk is a choice, compliance is mandatory and non-negotiable.
* **Manage Risk:**Match business risk with attendant controls to protect the brand and ensure shareholder value preservation.
* **Establish Code of Conduct:** Set the business integrity standard for the organization.
* **Address Threats:** Set the tone of prevention vs. reaction.

**Goals**

Information security measures try to address at least one of three goals (CIA):

* Protect the **confidentiality** of data
* Preserve the **integrity** of data
* Promote the **availability** of data for authorized use

# SECURITY policies

## Acceptable Use Policy

### Overview

This policy applies to the acceptable use of information, electronic and computing devices, and network resources to conduct Sales Optimizer business or interact with internal networks and business systems, whether owned or leased by Sales Optimizer, the employee, or a third party.

### Policy

#### General Use and Ownership

* Sales Optimizer proprietary information stored on electronic and computing devices whether owned or leased by Sales Optimizer, the employee or a third party, remains the sole property of Sales Optimizer.
* You have a responsibility to promptly report the theft, loss or unauthorized disclosure of Sales Optimizer proprietary information.
* You may access, use or share Sales Optimizer proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.
* For security and network maintenance and purposes, authorized individuals within Sales Optimizer may monitor equipment, systems and network traffic at any time.

#### Security and Proprietary Information

* Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.
* Computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 15 minutes or less. You should lock the screen or log off when the device is unattended.
* Postings by employees from a Sales Optimizer email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Sales Optimizer, unless posting is in the course of business duties.
* Employees should use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

#### Unacceptable Use

The following activities are, in general, prohibited. The lists below are by no means exhaustive but attempt to provide a framework for activities which fall into the category of unacceptable use.

*Unacceptable System and Network Activities*

* Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Sales Optimizer.
* Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws
* Introduction of malicious programs into the network or server
* Revealing your account password to others or allowing use of your account by others.
* Using a Sales Optimizer computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
* Making fraudulent offers of products, items, or services originating from any Sales Optimizer account.
* Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
* Effecting security breaches or disruptions of network communication
* Port scanning or security scanning
* Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty
* Circumventing user authentication or security of any host, network or account
* Interfering with or denying service to any user other than the employee's host
* Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session
* Providing information about Sales Optimizer employees to parties outside Sales Optimizer

*Unacceptable Email and Communication Activities*

* Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam)
* Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages
* Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes

*Unacceptable Blogging and Social Media*

* Employees and agents will not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of Sales Optimizer and/or any of its employees. Limited and occasional use of Sales Optimizer’s systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner.
* Employees and agents may not attribute personal statements, opinions or beliefs to Sales Optimizer when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of Sales Optimizer.
* Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, Sales Optimizer’s trademarks, logos and any other Sales Optimizer intellectual property may also not be used in connection with any blogging activity.

## Application Security

Sales Optimizer’s applications are located in Salesforce and therefore we adhere to their security guidelines. Salesforce security information can be found:

* General security information: <https://trust.salesforce.com/en/>
* Application Security Review: <https://developer.salesforce.com/docs/atlas.en-us.packagingGuide.meta/packagingGuide/security_review_about.htm>
* Salesforce compliance certifications: <https://trust.salesforce.com/en/>

## Clean Desk Policy

### Overview

A clean desk policy can be an important tool to ensure that sensitive/confidential materials about our employees, our intellectual property, our customers and our vendors are removed from an end user workspace and locked away when the items are not in use or you leave your workstation.

A Clean Desk policy is not only ISO 27001/17799 compliant, but it is also part of standard basic privacy controls.

### Policy

* + Secure restricted/sensitive/confidential information in hardcopy or electronic form when workstation is unoccupied and at the end of the day.
  + Lock computers/laptops and mass storage devices such as CDROM, DVD or USB drives when workspace is unoccupied.
  + File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.
  + Passwords may not be written down in an accessible location.
  + Restricted/sensitive printouts should be immediately removed from the printer.
  + Disposal of restricted/confidential documents should be shredded.
  + Whiteboards containing restricted/sensitive/confidential information should be erased.

## Data Breach Response Policy

### Overview

Sales Optimizer Information Security's intentions for publishing a Data Breach Response Policy are to focus attention on data security and data security breaches and how Sales Optimizer’s established culture of openness, trust and integrity should respond to such activity.

### Policy

Any individual who suspects that a theft, breach or exposure of Sales Optimizer Protected data or Sales Optimizer Sensitive data has occurred must immediately provide a description of what occurred via e-mail by calling the CEO or COO. Then the following will occur:

* As soon as a theft, data breach or exposure containing Sales Optimizer Protected data or Sales Optimizer Sensitive data is identified, the process of removing access to that resource will begin.
* Confirm theft, breach or exposure of data
* Determine the root cause: Analyze how the breach or exposure occurred; the types of data involved; the number of internal/external individuals and/or organizations impacted.
* Management to decide how to communicate the breach to: a) internal employees, b) the public, and c) those directly affected.

## Email Policy

### Overview

The purpose of this email policy is to ensure the proper use of Sales Optimizer email system and make users aware of what Sales Optimizer deems as acceptable and unacceptable use of its email system.

### Policy

* Use of email must be consistent with Sales Optimizer policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.
* Sales Optimizer email account should be used primarily for Sales Optimizer business-related purposes; personal communication is permitted on a limited basis, but non-Sales Optimizer related commercial uses are prohibited.
* Email should be retained only if it qualifies as a Sales Optimizer business record. Email is a Sales Optimizer business record if there exists a legitimate and ongoing business reason to preserve the information contained in the email.
* Email that is identified as a Sales Optimizer business record shall be retained according to the Internal Revenue Service record retention guidelines ([IRS Record Retention Guidelines from BBB](https://www.bbb.org/storage/0/Shared%20Documents/secure%20your%20id%20day/bbb%20records%20retention%20schedule.pdf)).
* Users are prohibited from automatically forwarding Sales Optimizer email to a third-party email system.
* Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, etc. to conduct Sales Optimizer business, to create or memorialize any binding transactions, or to store or retain email on behalf of Sales Optimizer.  Such communications and transactions should be conducted through proper channels using Sales Optimizer-approved documentation.
* Sales Optimizer employees should have no expectation of privacy in anything they store, send or receive on the company’s email system.
* Sales Optimizer may monitor messages without prior notice. Sales Optimizer is not obliged to monitor email messages.

## Encryption Policy

### Overview

The purpose of this policy is to define the acceptable use and management of encryption software and hardware.

### Policy

*Laptop, Mobile Computer & Smart Devices*

* Sales Optimizer laptop computer devices should have Sales Optimizer approved encryption software installed. In addition to encryption software, the laptop must be password protected and strongly recommends having up to date anti-virus software installed.
* Sales Optimizer mobile computer devices/smart devices should have device encryption enabled.
* The preferred method of encryption for laptop computers, mobile computer devices and smart devices is whole disk encryption. Mobile computer devices and smart devices which are not capable of whole disk encryption should use file/folder level encryption to encrypt confidential and restricted information stored on the device.
* Laptop, mobile computer devices and smart devices must not be used for the long-term storage of confidential/restricted information.

*Removable Storage* *Devices*

* Confidential/ restricted information stored on removable storage devices must be encrypted. In addition to being encrypted, removable storage devices must be stored in a locked cabinet or drawer when not in use.
* Removable storage devices except those used for backup purposes must not be used for the long-term storage of confidential and restricted information.
* The preferred method of encryption for removable storage devices is whole disk/device encryption. Where whole disk encryption is not possible, then file/folder level encryption must be used to encrypt confidential and restricted information stored on the removal storage device.

*USB Memory Sticks*

* Confidential and restricted information may only be stored on Sales Optimizer approved encrypted USB memory sticks.
* Sales Optimizer approved USB memory sticks must only be used on an exceptional basis where it is essential to store or temporarily transfer confidential or restricted information. They must not be used for the long-term storage of confidential or restricted information, which must where possible be stored on a secure Sales Optimizer network server.
* Confidential and restricted information stored on the Sales Optimizer approved USB memory stick must not be transferred to any internal (except a secure Sales Optimizer network server) or external system in an unencrypted form.

*Transmission Security*

* Confidential/restricted information transmitted through email to an email address outside of the Sales Optimizer domain (i.e. one that does not end in “@Sales Optimizer.com”) must be encrypted. The transfer of such information outside of the Sales Optimizer domain must be authorized by the COO.
* Where confidential and restricted information is transmitted through a public network (for example the internet) to an external third party the information must be encrypted first or sent via secure channels (for example: Secure FTP, TLS, VPN etc.). The transfer must be authorized the COO.
* Confidential/restricted information transmitted around existing wireless networks must be encrypted using WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) or better.

## Network Security – Third Party Network Provider

Spectrum (Charter Communications, Inc.) provides Sales Optimizer’s internet services. For information on **their security policies** please go to <https://brighthouse.com/policies/policies/network-management-policy.html>.

## Network Security – Remote Access

### Overview

The purpose of this policy is to define rules and requirements for connecting to Sales Optimizer's network from any host. This policy applies to anyone with a Sales Optimizer-owned or personally-owned computer or workstation used to connect to the Sales Optimizer network. This policy applies to remote access connections used to do work on behalf of Sales Optimizer, including reading or sending email and viewing intranet web resources. This policy covers any and all technical implementations of remote access used to connect to Sales Optimizer networks.

### Policy

When accessing the Sales Optimizer network from a personal computer, Authorized Users (employees, agents, vendors, contractors) are responsible for preventing access to any Sales Optimizer computer resources or data by non-authorized users. Performance of illegal activities through the Sales Optimizer network by any user (authorized or otherwise) is prohibited. Authorized users will not use Sales Optimizer networks to access the Internet for outside business interests.

*Requirements*

* Authorized users will protect their login and password.
* While using a Sales Optimizer-owned computer to remotely connect to Sales Optimizer's corporate network, authorized users will ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an authorized user or third party.
* All hosts that are connected to Sales Optimizer internal networks via remote access technologies must use the most up-to-date anti-virus software.

## Network Security – Wireless Communication Policy

### Overview

This policy applies to wireless infrastructure devices that connect to a Sales Optimizer network or reside on a Sales Optimizer site that provide wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular phones, and tablets. This includes any form of wireless communication device capable of transmitting packet data.

### Policy

*General Requirements*

Wireless infrastructure devices that reside at a Sales Optimizer site andconnect to a Sales Optimizer network, or provide access to information classified as Sales Optimizer Confidential, or above must:

#### Abide by the standards specified in the Wireless Communication Standard.

#### Use Sales Optimizer approved authentication protocols and infrastructure.

#### Use Sales Optimizer approved encryption protocols.

#### Maintain a hardware address (MAC address) that can be registered and tracked.

*Home Wireless Device Requirements*

* + - Wireless infrastructure devices that provide direct access to the Sales Optimizer network must conform to the Home Wireless Device Requirements as detailed in the *Wireless Communication Standard*.
    - Access to the Sales Optimizer corporate network through this device must use standard remote access authentication.

## Wireless Communication Standard

### Overview

This standard specifies the technical requirements that wireless infrastructure devices must satisfy to connect to a Sales Optimizer network. This standard applies to wireless devices that make a connection the network and wireless infrastructure devices that provide wireless connectivity to the network.

### Standard

*General Requirements*

Wireless infrastructure devices that connect to a Sales Optimizer network or provide access to Sales Optimizer Confidential or Restricted information must:

#### Use Extensible Authentication Protocol-Fast Authentication via Secure Tunneling (EAP-FAST), Protected Extensible Authentication Protocol (PEAP), or Extensible Authentication Protocol-Translation Layer Security (EAP-TLS) as the authentication protocol.

#### Use Temporal Key Integrity Protocol (TKIP) or Advanced Encryption System (AES) protocols with a minimum key length of 128 bits.

#### Bluetooth devices use Secure Simple Pairing with encryption enabled.

*Home Wireless Device Requirements*

Home wireless infrastructure devices that provide direct access to a Sales Optimizer network, such as those behind Enterprise Teleworker (ECT) or hardware VPN, must adhere to the following:

#### Enable WIFI Protected Access Pre-shared Key (WPA-PSK), EAP-FAST, PEAP, or EAP-TLS

## Password Protection Policy

### Overview

Everyone is responsible for taking the appropriate steps to select and secure their passwords.

The purpose of this policy is to establish a standard for creation of strong passwords and the protection of those passwords.

### Policy

#### Password Protection

* + - Passwords must not be shared with anyone, including supervisors and coworkers. All passwords are to be treated as sensitive, confidential Sales Optimizer information.
    - Passwords must not be inserted into email messages or other forms of electronic communication, nor revealed over the phone to anyone.
    - Passwords may be stored only in “password managers” authorized by the organization.
    - Do not use the "Remember Password" feature of applications (for example, web browsers).
    - Any user suspecting that his/her password may have been compromised must report the incident and change passwords.

## Technology Equipment Disposal

### Overview

The purpose of this policy it to define the guidelines for the disposal of technology equipment and components owned by Sales Optimizer. This policy applies to any computer/technology equipment or peripheral devices that are no longer needed within Sales Optimizer (e.g. personal computers, servers, hard drives, laptops, smart phones, handheld computers, keyboards, mice, speakers, printers, scanners, typewriters, compact and floppy discs, portable storage devices, backup tapes, printed materials).

### Policy

*Technology Equipment Disposal*

* Sales Optimizer will securely erase storage mediums in accordance with current industry best practices.
* Data including, files and licensed software will be removed from equipment using disk sanitizing software that cleans the media overwriting each and every disk sector of the machine with zero-filled blocks, meeting Department of Defense standards.
* Electronic drives should be degaussed or overwritten with a commercially available disk cleaning program. Hard drives may also be removed and rendered unreadable (drilling, crushing or other demolition methods).
* Technology equipment with non-functioning memory or storage technology will have the memory or storage device removed and it will be physically destroyed.
* Any equipment not in working order will be donated or disposed.