Pinpoint Global
Privacy and Information Sensitivity Policy

v6.3
Version

September 7, 2023
Date of Version

Karen Dapkus, CFO
Created By:

Malcolm Brown, CTO
Approved By:

Change History

Date	Version	Created By	Description of Change
10/01/14	v1.0	Karen Dapkus	
11/12/19	v2.0	Karen Dapkus	Include Change History
11/12/20	v3.0	Karen Dapkus	Include Change History
3/19/2021	v4.0	Karen Dapkus	Include Highly Confidential Category
5/9/2022	v5.0	Karen Dapkus	Process Updates added to Section 4.0
7/25/2022	v6.0	Karen Dapkus	Added Third Party privacy obligations
10/28/2022	v6.1	Karen Dapkus	Added responsible party to Section 4.0
12/24/2022	v6.2	Karen Dapkus	Add roles/responsibilities of CTO/CISO; new employee access;
9/7/2023	v6.3	Karen Dapkus	Add Digital Marketing Service Providers privacy information to Section 4.0

1.0 Purpose

The Information Sensitivity Policy is intended to help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of Pinpoint Global Communications without proper authorization.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

All employees should familiarize themselves with the information labeling and handling guidelines that follow this introduction. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that you can take to protect Pinpoint Global Communications Confidential information (e.g., Pinpoint Global Communications. confidential information should not be left unattended in conference rooms).

Please Note: The impact of these guidelines on daily activity should be minimal.

Questions about the proper classification of a specific piece of information should be addressed to your manager. Questions about these guidelines should be addressed to IT.

2.0 Scope

All Pinpoint Global Communications information is categorized into three main classifications:

- Pinpoint Global Communications Public
- Pinpoint Global Communications Confidential
- Pinpoint Global Communications Highly Confidential

Pinpoint Global Communications Public information is information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to Pinpoint Global Communications Systems, Inc.

Pinpoint Global Communications Highly Confidential information contains information that is more sensitive than other information and should be protected in a more secure manner. Included is information that should be protected very closely, such as trade secrets, client data, development programs, potential acquisition targets, and other information integral to the success of our company.

Pinpoint Global Communications Confidential information contains all other information. Included in Pinpoint Global Communications Confidential is information that is less critical, such as telephone directories, general corporate information, personnel information, etc., which does not require as stringent a degree of protection as Highly Confidential Information

A subset of Pinpoint Global Communications Highly Confidential information is "Pinpoint Global Communications Third Party Confidential" information. This is confidential information belonging to or pertaining to another corporation which has been entrusted to Pinpoint Global Communications by that company under non-disclosure agreements and other contracts. Examples of this type of information include everything from joint development efforts to vendor lists, customer orders, and supplier information. Information in this category ranges from extremely sensitive to information about the fact that we've connected a supplier / vendor into Pinpoint Global Communications' network to support our operations.

Pinpoint Global Communications personnel are encouraged to use common sense judgment in securing Pinpoint Global Communications Confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their manager.

3.0 Policy

The Sensitivity Guidelines below provide details on how to protect information at varying sensitivity levels. Use these guidelines as a reference only, as Pinpoint Global Communications. Confidential information in each column may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of the Pinpoint Global Communications Confidential information in question.

3.1 **Minimal Sensitivity:** General corporate information; some personnel and technical information

Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential".

Marking is at the discretion of the owner or custodian of the information. If marking is desired, the words "Pinpoint Global Communications Confidential" may be written or designated in a conspicuous place on or in the information in question. Other labels that may be used include "Pinpoint Global Communications Proprietary" or similar labels at the discretion of your individual business unit or department. Even if no marking is present, Pinpoint Global Communications information is presumed to be "Pinpoint Global Communications Confidential" unless expressly determined to be Pinpoint Global Communications Public information by a Pinpoint Global Communications employee with authority to do so.

Access: Pinpoint Global Communications employees, contractors, people with a business need to know.
Distribution within Pinpoint Global Communications: Standard interoffice mail, approved electronic mail and electronic file transmission methods.
Distribution outside of Pinpoint Global Communications internal mail: U.S. mail and other public or private carriers, approved electronic mail and electronic file transmission methods.
Electronic distribution: No restrictions except that it be sent to only approved recipients.
Storage: Keep from view of unauthorized people; erase whiteboards, do not leave in view on tabletop. Machines should be administered with security in mind. Protect from loss; electronic information should have individual access controls where possible and appropriate.
Disposal/Destruction: Deposit outdated paper information in specially marked disposal bins on Pinpoint Global Communications premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.
Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

3.2 **More Sensitive:** Business, financial, technical, and most personnel information.

Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential". As the sensitivity level of the information increases, you may, in addition or instead of marking the information "Pinpoint Global Communications Confidential" or "Pinpoint Global Communications Proprietary", wish to label the information "Pinpoint Global Communications Internal Use Only" or other similar labels at the discretion of your individual business unit or department to denote a more sensitive level of information. However, marking is discretionary at all times.

Access: Pinpoint Global Communications employees and non-employees with signed non-disclosure agreements who have a business need to know.
Distribution within Pinpoint Global Communications: Standard interoffice mail, approved electronic mail and electronic file transmission methods.
Distribution outside of Pinpoint Global Communications internal mail: Sent via U.S. mail or approved private carriers.
Electronic distribution: No restrictions to approved recipients within Pinpoint Global Communications but should be encrypted or sent via a private link to approved recipients outside of Pinpoint Global Communications premises.
Storage: Individual access controls are highly recommended for electronic information.
Disposal/Destruction: In specially marked disposal bins on Pinpoint Global Communications premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.
Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

3.3 **Most Sensitive:** Trade secrets & marketing, operational, personnel, financial, source code, & technical information integral to the success of our company.

Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential". To indicate that Pinpoint Global Communications Confidential information is very sensitive, you may should label the information "Pinpoint Global Communications Internal: Registered and Restricted", "Pinpoint Global Communications Eyes Only", "Pinpoint Global Communications Confidential" or similar labels at the discretion of your individual business unit or department. Once again, this type of Pinpoint Global Communications Confidential information need not be marked, but users should be aware that this information is very sensitive and be protected as such.

Access: Only those individuals (Pinpoint Global Communications employees and non-employees) designated with approved access and signed non-disclosure agreements.
Distribution within Pinpoint Global Communications: Delivered direct - signature required, envelopes stamped confidential, or approved electronic file transmission methods.
Distribution outside of Pinpoint Global Communications internal mail: Delivered direct; signature required; approved private carriers.
Electronic distribution: No restrictions to approved recipients within Pinpoint Global Communications, but it is highly recommended that all information be strongly encrypted.
Storage: Individual access controls are very highly recommended for electronic information. Physical security is generally used, and information should be stored in a physically secured computer.
Disposal/Destruction: Strongly Encouraged: In specially marked disposal bins on Pinpoint Global Communications premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.
Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

3.4 Third Party Controls

Client data is not available to any Third Parties. Pinpoint Global takes all appropriate measures to ensure that all client data is appropriately safeguarded. All client data is treated with the highest level of confidentiality and is not shared with any Third Parties. Pinpoint Global has implemented appropriate technical, physician and organization measures to protect client data against accidental or unlawful destruction or accidental loss, damage, alteration, unauthorized disclosure or access as well as all other forms of unlawful processing. We use

the industry-standard security protocol Secure Sockets Layer (SSL) to encrypt all sensitive information, and we employ the latest 256-bit encryption technology.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

A process is in place to monitor changes to applicable privacy laws and regulations. This Privacy Program is reviewed on an annual basis.

- As an Arctic Wolf customer, Arctic Wolf drives information security initiatives for Pinpoint Global. Pinpoint Global's CTO is responsible to oversee, implement, and enforce the security program. The Chief Technology Officer (CTO) is a highly skilled technologist. In addition to making executive technology decisions on behalf of the company, this person is a strategic thinker, effective communicator and an expert in technological development. The CTO position at Pinpoint Global includes Chief Information Security Officer (CISO) experience. The CTO oversees the development and dissemination of technology for external customers, vendors and other clients to help improve and increase business. The CTO also deals with internal IT operations. This position reports directly to the CEO.

Third Party Processors

Our carefully selected partners and service providers may process personal information about you on our behalf as described below:

Digital Marketing Service Providers

Pinpoint Global periodically appoints digital marketing agents to conduct marketing activity on our behalf, such activity may result in the compliant processing of personal information. Our appointed data processors include:
(i)Prospect Global Ltd (trading as Sopro) Reg. UK Co. 09648733. You can contact Sopro and view their privacy policy here: *http://sopro.io*. Sopro are registered with the ICO Reg: ZA346877 their Data Protection Officer can be emailed at: *dpo@sopro.io*. ”

New Employee Access

- The CTO/CISO is responsible for granting new employee access. All employees are granted the lowest access possible to perform their job function. The CTO will identify and manage all access. A quarterly review is performed to ensure that all employee access is updated if necessary

Risk Management

- Arctic Wolf is the lead on risk management for the Company and is overseen by Pinpoint's CTO.

5.0 Definitions

Terms and Definitions

Appropriate measures

To minimize risk to Pinpoint Global Communications from an outside business connection. Pinpoint Global Communications computer use by competitors and unauthorized personnel must be restricted so that, in the event of an attempt to access Pinpoint Global Communications corporate information, the amount of information at risk is minimized.

Configuration of Pinpoint Global Communications-to-other business connections

Connections shall be set up to allow other businesses to see only what they need to see. This involves setting up both applications and network configurations to allow access to only what is necessary.

Delivered Direct; Signature Required
Do not leave in interoffice mail slot, call the mail room for special pick-up of mail.

Approved Electronic File Transmission Methods
Includes supported FTP clients and Web browsers.

Envelopes Stamped Confidential
You are not required to use a special envelope. Put your document(s) into an interoffice envelope, seal it, address it, and stamp it confidential.

Approved Electronic Mail
Includes all mail systems supported by IT. These include, but are not necessarily limited to, Webmail.US, Inc.

Company Information System Resources
Company Information System Resources include, but are not limited to, all computers, their data and programs, as well as all paper information and any information at the Internal Use Only level and above.

Expunge
To reliably erase or expunge data on a PC or Mac you must use a separate program to overwrite data, supplied as a part of Norton Utilities. Otherwise, the PC or Mac's normal erasure routine keeps the data intact until overwritten. The same thing happens on UNIX machines, but data is much more difficult to retrieve on UNIX systems.

Individual Access Controls
Individual Access Controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. On UNIX machines, this is accomplished by careful use of the chmod command (use *man chmod* to find out more about it). On Mac's and PC's, this includes using passwords on screensavers, such as Disklock.

Insecure Internet Links
Insecure Internet Links are all network links that originate from a locale or travel over lines that are not totally under the control of Pinpoint Global Communications.

One Time Password Authentication
One Time Password Authentication on Internet connections is accomplished by using a one-time password token to connect to Pinpoint Global Communications' internal network over the Internet. Contact IT for more information on how to set this up.

Physical Security
Physical security means either having actual possession of a computer at all times or locking the computer in an unusable state to an object that is immovable. Methods of accomplishing this include having a special key to unlock the computer so it can be used, thereby ensuring that the computer cannot be simply rebooted to get around the protection. If it is a laptop or other portable computer, never leave it alone in a conference room, hotel room or on an airplane seat, etc. Make arrangements to lock the device in a hotel safe or take it with you. In the office, always use a lockdown cable. When leaving the office for the day, secure the laptop and any other sensitive material in a locked drawer or cabinet.

Private Link
A Private Link is an electronic communications path that Pinpoint Global Communications has control over its entire distance. For example, all Pinpoint Global Communications networks are connected via a private link. A computer with a modem connected via a standard land line (not cell phone) to another computer has established a private link. An ISDN line to an employee's home is a private link.