Enterprise Information and Technology Security Policy

Enterprise Information Technology Security Policy

Table of Contents

1. Introduction

In the following pages, the terms “Application” and “Platform” will generally be referring to Pinsight®’s Leader Readiness Platform (our core Technology).
This policy handbook has several objectives:

- To outline a basic Pinsight® Enterprise Information Technology (EIT) Security Policy that conforms to ISO 27001 and GDPR regulations.
- To encourage ethical and knowledgeable behavior in all who use or provide information resources;
- To provide a guideline for protecting valuable Pinsight® assets and intellectual property from theft, damage, and unauthorized access or change;
- To raise awareness of confidentiality and possible legal requirements in the use of sensitive PI information, as well as the possible liability for inappropriate uses of information resources.

This document is broken into the following sections:

- The General Policies section is intended to give guidance on protection of information resources applicable to all Pinsight® staff, clients, and participants.
- Access Control provides ways to protect information resources in different environments and requires balancing the degree of risk, the value of the resources and the cost of protection.
- Security and Systems Monitoring provides guidance on accountability over Information Systems, auditing, censorship, capacity planning and privacy rights.
- Software Controls defines Pinsight®'s policies on all aspects of software, including but not limited to: web application programs and data protection, intellectual assets, change control and source library management.
- Hardware Controls outlines measures being taken to ensure that Hardware is appropriately secured and maintained.
- Physical Security Controls addresses some of the very specific aspects of maintaining our facilities, equipment and even forms.
- Business Continuance Controls covers the requirements of routine actions and extraordinary actions.

1.1 Information and Security Policy Statement

Information and information systems are critical and vitally important Pinsight® assets. Pinsight® has a fiduciary duty to preserve, improve, and account for Pinsight® information and information systems.

Individuals employed by Pinsight® have a responsibility to our clients and participants to maintain and safeguard information and information systems and ensure Pinsight® is properly protected from a variety of threats such as error, fraud, sabotage, industrial espionage, privacy violation, service interruption, and natural disaster.

Pinsight® information is to be protected in a manner commensurate with its sensitivity, value, and criticality. Security measures must be employed regardless of the media on which information is stored (paper, electronic, etc.), the systems which process it or the methods by which it is moved (electronic mail, face-to-face conversation, etc.). Such protection includes ***restricting access to information based on the need-to-know***. Management must devote sufficient time and resources to ensure that information is properly protected.

Pinsight® management must additionally make sure that information and information systems are protected in a manner that is at least as secure as other organizations in the same industry handling the same type of information. To achieve this objective, annual reviews of the risks to Pinsight® information and information systems are to be conducted. Similarly, whenever a major security incident indicates that the security of information or information systems is insufficient, management must promptly take remedial action to reduce Pinsight®'s exposure.

This document outlines the commitment of Pinsight® to act in our clients' best interests by ensuring the best possible protection of their information assets. As stewards we ensure that appropriate efforts are expended to maintain the integrity, confidentiality, and availability of these resources by:

- Protecting the assets from destruction, unauthorized use, or unauthorized change

- Ensuring that processes are in place for correcting damaged systems to enable continuation of operations with minimal disruption
- Balancing the need for security with the need for minimizing the complexity of information access

1.2 Record of Changes

The contingency plan should be a living document that is changed as required to reflect system, operational, or organizational changes. Modifications made to the plan should be recorded in the following Record of Changes.

Record of Changes			
Page No.	Change Comment	Date of Change	Signature
All	Initial Draft	9/15/2018	Brad Sather (CTO)
All	Second Draft	1/1/2022	Brad Sather (CTO)

2. General Policies

2.1 Overview of Policies

2.1.1 Purpose

The purpose of the EIT Security Policy is to establish security requirements and controls for the protection of information and associated information technology resources. Information security measures at Pinsight® are intended to:

- Protect valuable Pinsight® assets
- Preserve the privacy of Clients, Participants and Pinsight® Employees
- Reduce the risk of unauthorized access, corruption, destruction, delay of Pinsight® data, assets and critical operations
- Protect the legal position of Pinsight®

2.1.2 Scope

Pinsight®'s Information Security Policies apply to information throughout its lifecycle, including creation, distribution, storage and disposal.

These policies are to protect information in all environments in which Pinsight®'s information resides, including information that resides with outside parties such as third-party providers, which is subject to the same controls used to protect information processed internally.

Adherence to this policy is required by all employees, temporaries, interns, contractors, service providers, and agents who use, have access to, or are responsible for Pinsight® assets, and those who design, operate, or are responsible for the computer and manual systems which contain records of the organization's assets.

Resources included in the scope of this security policy statement include but are not limited to: information (data) in any medium or form including, but not limited to: paper, digital, video, and audio representations; computing hardware and software systems which access and manipulate information; and network systems which transport information. Legal constraints directly affect the use of some of these resources. Pinsight® policy may also affect the use of information resources. The multiplicity of needs involving information uses, locations, and protection dictates that a broad spectrum of possible security procedures is necessary. Security risks must be evaluated, and appropriate procedures must be selected and implemented by the individuals responsible for such assets.

2.1.3 Information Assets

Information assets are data and proprietary information in electronic, printed or other forms. They are considered sensitive or critical to Pinsight®'s business objectives.

2.1.4 Information Protection and Privacy

Pinsight® collects the following personal information from users of the Leader Readiness Platform: name, email, telephone number, location (city, state). This information is collected directly from the users when they are completing their user profile. Simulation participants have the option of providing additional information about themselves for EEO and research purposes including their age, race, gender, years of work experience, educational status, company industry and level in the organization. This information is entirely voluntary, and participants are not required to report this. During a simulation, participants create email messages, notes, video voicemail messages and calendar events related to the fictitious simulation scenario. Also, participants engage in interactive video conversations that are recorded and saved to our servers. Pinsight® is subject to regulatory requirements by EU data privacy. All personal information is stored in the United States. Pinsight® participates in the EU-US Privacy Shield.
Information assets will be protected at a level commensurate to their value and potential risk to Pinsight®. Protection will ensure the confidentiality, integrity, and availability of Pinsight®'s EIT assets.

2.1.5 Staff Awareness and Training

Security awareness is necessary for employees and administrators to understand the importance of Pinsight®'s EIT security policies. Pinsight® users (employees, consultants, contractors, and temporaries) must be educated on what security policies exist in the organization, why they exist, and how they are enforced.
All Pinsight® users (employees, consultants, contractors, and temporaries) must be provided with sufficient training and supporting reference materials to allow them to properly protect and otherwise manage Pinsight® data and assets.
All users-employees are responsible for understanding all of Pinsight®'s security policies, and they must sign an acknowledgment once per year that they have read and received and agree to abide by the policies. Users must be educated on security policies and policy changes annually.
Policies must be stored in a central location (e.g., Pinsight®'s SharePoint) and made available for users to review.

2.1.6 Non-Business use of Information and Equipment

Pinsight® information resources (product specifications, databases, mailing lists, internal software, computers, etc.) must only be used for the business purposes specifically allowed by management. Use of these information resources for any other reason will be permitted only after the management has granted written permission.

2.1.7 Availability

Information assets must be available to ensure continued operation of Pinsight®'s business objectives. Appropriate measures must be in place to ensure the timely recovery of all information and access by authorized individuals.

2.1.8 Protection of Records/Integrity of Records

Pinsight® sets aside extra protections for records and information classified as ***PI, Client Confidential, or Company Confidential*** within the "Information and Asset Classification" policy. Information in these categories is stored more securely and with backups in place for recovery. Information assets classified as above must be adequately labeled and protected to ensure completeness and accuracy. Validation measures will be utilized to allow detection of inappropriately modified, deleted, or corrupted information provided this information originates from Pinsight.

2.2 Roles & Responsibilities

2.2.1 Data Protection Officer

Responsible for ensuring that Pinsight®'s ISMS fulfills the requirements of ISO27001, GDPR and Privacy Shield.

2.2.2 Chief Technology Officer

Responsible for monitoring the performance of the ISMS and reporting it to Pinsight® leadership.

2.2.3 Pinsight® Management

Critical business decisions by the Pinsight® management team are dependent on the integrity of information and information systems. The term "***Management***" refers to those Employees who are responsible for directing the activities of other staff.
Responsibilities:

- Accept accountability for all EIT assets under their control.
- Authorize user access to EIT assets as appropriate.
- Ensure compliance with the organization's requirements for information protection by establishing controls that meet or exceed Pinsight®'s EIT Security Policies.
- Assign and track ownership of responsibility for EIT assets.
- Provide sufficient resources to protect Pinsight®'s EIT assets.
- Respond appropriately to information security related exposures and losses.
- Know the nature of information used for decision-making (accuracy, timeliness, relevance, completeness, confidentiality, criticality, etc.).
- Ensure that assigned personnel fulfill responsibilities as Data Stewards, Custodians, and/or Users.

2.2.4 EIT Staff

EIT Staff consists of the DPO, CTO, IT managers, Pinsight® Managers and any other leadership role in Pinsight® that has been designated as EIT Staff. EIT staff is responsible for the overall compliance and leadership initiatives encompassed by this EIT Security Policy.

2.2.5 Data Stewards

Data Stewards are responsible for making overall control and access decisions for entrusted EIT assets. The Data Steward should be the person in the best position to know the organization's business and the value of EIT assets. For example, Sr. Management members can be considered Data Stewards.
Responsibilities:

- Assign value and classify information.
- Ensure and validate the quality and integrity of information.
- Authorize overall access to information and authorize exceptions.
- Define roles and responsibilities for custody of information.
- Specify protective measures to custodians and users of the information.

2.2.6 Custodians

Custodians have authorized control and physical custody of entrusted information and provide proper protection in an operational environment. For example, Computer Operations, Systems & Technology and system administrators can be considered Information Custodians.
Responsibilities:

- Comply with organizational and Data Steward specified protection requirements.
- Provide security tools and mechanisms, and physical and procedural safeguards to protect the information from accidental or intentional, but unauthorized disclosure, modification, or destruction.
- Arrange for backup of vital records and their retention in secure locations.
- Inform Data Stewards of potential and real security exposures and weaknesses.

2.2.7 Users

Users are individuals with management-authorized access to information and/or information systems. While scope of access may differ from system to system, all staff are considered Users of information.
Responsibilities:

- Use information only for authorized business purposes.
- Comply with organizational and Data Steward specified protection requirements including Pinsight®'s Information Security Policies.

- Inform Data Stewards or the DPO about security exposures.
- Report all known breaches to Management.

2.3 Separation of Duties

Management philosophy must allow for adequate separation of duties and adhere to a "***Need to know***" principle. Where a separation of duties cannot be enforced by logical access controls, other non-information technology related controls must be effective.

2.4 Exceptions

Because policies may be general in nature, there will be situations where economics or other considerations dictate an exception to a policy. In such situations, Sr. Management may decide to accept the risk of not following an established EIT Security Policy or standard. The decision should address the following areas:

- The value of the EIT asset, including the business consequence of its disclosure, destruction, modification, delay or misuse
- The policy to which the exception applies
- A description of the risk and degree of exposure that can result from the exception
- The business reason for non-compliance
- Any compensating controls that will reduce the risk to an acceptable level
- Additional actions, if any, that will lead to compliance and a schedule of those actions

Policy exceptions must be documented, and they must be reviewed annually to determine whether they still need to stand.

3. Security Monitoring

3.1 Accountability for Controls over Information Systems

- Ensure that all personnel using the Pinsight®'s information resources are continuously aware of the importance of EIT assets and of their responsibilities toward protecting these assets. Personnel should consider the following as examples of suspicious behavior:
  - Anyone asking for their own password or authentication credentials.
  - Strange files or programs on their computer or a server.
  - Unusual or inconsistent log entries.
  - Unexpected application or server failure.
  - Unexpected, significant changes in performance, response time, or usability.
- Ensure that changes to software packages, application code, operating systems and overall platform are strictly controlled by EIT management. Access to such pieces of Pinsight®'s infrastructure is on an as needed basis.
- Assess the value or sensitivity of information in order to determine the protection, monitoring, and accountability required.

- Evaluate and specify control and protection requirements for information. Specify ownership. Limit physical and electronic access to information on a strict need-to-access basis. Authorize access based on these criteria.
- Employees shall observe controls to protect physical security and bring any incidents or practices that weaken security to management's attention.
- Clearly define the responsibilities among owners of data, users, and EIT staff.
- Review firewall, intrusion detection system, operating system, and application security logs at least weekly.
- Review performance monitoring trends with regard to security at least twice a month, looking for abnormal bandwidth, disk, or processor use.
- Review change logs quarterly.
- "Prowl around" for suspicious system behavior or unexpected files/accounts at least once a month.
- Compare actual software and operating system patch levels to documented patch levels at least once a quarter.
- Validate that user accounts and permissions match documented (and actual) requirements at least semiannually.
- Identify privileged utility programs such as Prey Protect and Last Pass and ensure that access to those programs is tightly controlled.

3.1.1 Auditing

This section provides the authority for members of Pinsight®'s EIT staff to conduct a security audit on any system at Pinsight.

Audits may be conducted to:

- Ensure integrity, confidentiality, and availability of information and resources.
- Investigate possible security incidents to ensure conformity to Pinsight® security policies.
- Monitor user or system activity where appropriate.

This applies to all computer and communication devices owned, leased, or operated by Pinsight; it also applies to any computer and communications devices connected to Pinsight® assets but which may not be owned or operated by Pinsight.
Audit activity must be approved by Pinsight®'s Data Protection Officer or the CEO. When approved, and for the purpose of performing an audit, any access needed will be provided to members of Pinsight®'s EIT staff.
This access may include the following unless otherwise prohibited by law or other Pinsight® policy:

- User-level and/or system-level access to any computing or communications device.
- Access to work areas (labs, offices, cubicles, storage areas, etc.).
- Access to interactively monitor and log traffic on Pinsight®'s network.
- Access to all security-related events on critical or sensitive systems and devices.

3.1.2 Enterprise Information Technology Escalation Procedures

For the purpose of ensuring the highest possible levels of system security, availability and integrity, Pinsight® will maintain current escalation procedures. Escalation procedures cover a wide scope of systems and types of processing. They include critical system halts, application hangs. The escalation procedures clearly outline the person(s) to contact, the timeline in which to escalate a problem, and documentation of the escalation tasks performed for a given problem. Refer to the Incident Management Policy for more detail.

3.2 Restriction of Privacy Rights

3.2.1 Disclosure of Information to Law Enforcement

By making use of Pinsight® systems, users consent to allow all information they store on Pinsight® systems to be divulged to law enforcement at the discretion of Pinsight® management (Patriot Act).

3.3 Censorship of Data

3.3.1 Right to Censor Data on Organizational Systems

Management reserves the right to censor any data posted to Pinsight® computers or networks. These facilities are private business systems, and not public forums, and as such do not provide First Amendment free speech guarantees.

3.3.2 Right to Remove Offensive Material Without Warning

Pinsight® retains the right to remove from its information systems any material it views as offensive or potentially illegal.

3.3.3 Personal Comments on External Systems

Comments that users post to an electronic mail system, an electronic bulletin board system, or other social media systems are not necessarily formal statements of or the official position of Pinsight. Users should not assume what they read or otherwise observe on Pinsight® systems is necessarily Pinsight® policy.

4. Access Control (Computers/Networks)

4.1 Use of Personal Computers

Pinsight® provides its employees and certain vendors with personal computers (PCs) or Laptops. The primary purpose of the PCs and Laptops is to conduct the business of Pinsight. Use of the PCs constitutes acceptance of this policy.

Employees given the ability to access our system off-site should have a valid need for such access and be closely accounted for. Passwords will adhere to Pinsight®'s password policy. Users are expected to be knowledgeable of these and all policies of Pinsight. Any questions should be directed to EIT Staff. Violations of this or any other Pinsight® policy subjects the user to immediate revocation of system privileges and may result in disciplinary action, up to and including termination.

4.1.1 Account Administration

User accounts, which permit specific system and network access by specific individuals, are an important control point in the overall security model of an organization. If the number and owners of active accounts are not monitored closely, security risk to the organization greatly increases.

The key to effective, secure account administration is adherence to a strict set of policies that describe who is permitted to have accounts, who authorizes accounts, and when accounts expire. Accounts at Pinsight® shall be granted only to individuals meeting criteria and through the approval procedures detailed in the following table.

Table 1: Pinsight® Account Administration

Classification	**Approval procedures for granting account**	**Account Implementation**	**Account expiration**
Pinsight® Employee	Pinsight® supervisor grants permission	Pinsight® EIT staff	Immediately upon termination of employment, instructions from supervisor, or change of role or employment status which no longer requires account
Pinsight® Vendor or Consultant	Pinsight® sponsor or project manager grants permission	Pinsight® EIT staff	Termination of vendor agreement, instructions from project sponsor or project manager, or 120

			days from start date or renewal
Contract/Temporary/Fixed-Term Employee	Pinsight® supervisor grants permission	Pinsight® EIT staff	Termination of contract or instructions from supervisor

- Accounts will be granted only to individuals with a verified business need to access Pinsight® resources.
- Accounts must never be shared.
- Accounts must be granted with the minimum level of access and on the minimum number of systems required for the user to complete his required business tasks.
- Accounts must never be issued to a party whose identity and authorization cannot be positively verified.
- Abuse of accounts or violation of this policy may result in immediate account termination.
- Accounts must be authorized and issued in a planned, thoughtful way to ensure procedural correctness. Accounts must never be authorized or issued under the pressure of time or outside of proper procedure.
- Pinsight® EIT staff will review accounts including user access rights on a regular basis, annually at a minimum.
- Accounts must adhere to the Authentication section of this document.
- Accounts determined to be idle or unused by otherwise active employees, contractors, or consultants for a period of six months must be disabled and the direct supervisor of the account holder notified.
- The Human Resources department is responsible for notifying EIT staff of terminations of all permanent and temporary Pinsight® employees in a regular and timely manner so that their accounts can be disabled in accordance with this policy.

4.1.2 Network Administration

Pinsight® networks will be segregated into 4 areas. Corporate Cloud, Staging, Demo and Production. Access to each of these networks is on an as needed basis and can be only granted by appropriate EIT Staff such as the IT manager or DPO. Corporate Cloud may be further segregated as a set of cloud resources, such as Trello, SharePoint, Outlook etc. with access to each of these cloud-based systems also on an as needed basis.

4.1.3 Authentication

Authentication to various Pinsight® resources is done via username and password with MFA. The username and password along with MFA are the responsibility of the individual to whom it is assigned. All users must adhere to the policies spelled out in this section regarding Pinsight®'s use of authentication information. Use of a username and password with MFA by anyone other than the account holder (i.e., family, clients, participants) to gain access to the

Pinsight® network and Internet is strictly prohibited. Violations of this policy are subject to disciplinary action, up to and including termination. Although users will be given a unique username and password, this does not insulate transmissions from employer review for business purposes. If personal computers (PCs) are connected to a Pinsight® asset, when unattended for any significant period of time they must always be logged-off or locked via password protection.

- All accounts, including accounts within major applications, must have a password.
- Mobile devices (e.g., laptops, tablets, smart phones) must be password-protected with at least 8 characters if the device allows for that.
- All system-level passwords (e.g., root, enable, administrator, application administration accounts, etc.), including major application and database administrative passwords, must be changed on at least every 90 days.
- All system-level passwords (e.g., root, enable, administrator, application administration accounts, etc.), including major application and database administrative passwords, must be changed when an EIT staff member is no longer employed by Pinsight.
- All user-level passwords (e.g., email, web, desktop computer, etc.) on systems that allow the user to independently change the password must be changed at least every 90 days.
- User accounts that have system-level privileges must have a unique password from all other accounts held by that user.
- Usernames and Passwords must not be included in unencrypted email messages.
- System-level passwords must be documented and stored in a secure manner.
- Users may be held responsible for system access made with their user accounts.
- All user-level and system-level passwords must conform to the requirements described below.
- MFA is turned on all users accounts.

4.1.3.1 Design of Password

- All user passwords must have a minimum of eight characters, and passwords must fulfill three of the following requirements (in any combination):
  - Upper Case letters (A,B,C etc)
  - Lower Case letters (a,b,c etc)
  - Numbers (0-9)
  - Special Characters (e.g.: $,#, or punctuations characters such as ? or !)

In addition, passwords should:

  - Not be a word in any language, slang, dialect, jargon, etc.
  - Not be based on personal information, names of family, etc.
  - Be easily remembered by the user. One way to do this is to create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: “This May Be One Way To Remember” and the password could be: “TmB1w2R!” or “Tmb1W>r~” or some other variation.
  - Been previously used in the last 3 changes

4.1.3.2 Password Changes After Compromise

Enterprise Information Technology reserves the right to change a user's password if the system is compromised or it is determined that the password does not meet specifications stated above, or if they have reason to believe a user's password has been disclosed to or discovered by unauthorized parties. The affected user will be notified if this occurs. Users are prohibited from storing passwords in written or printed form on or near their PCs.

4.1.3.3 Exception to Password Policies

There are some exceptions to these policies for certain user accounts that relate to the system, not actual end users. These user accounts are used for server service accounts and if password is changed, these services will fail to start automatically, e.g. user account used for backup software etc. Since server consoles are monitored by EIT staff and are in a secure environment, these may not be locked by a password.

4.1.4 Password Management

Pinsight® utilizes LastPass Enterprise to protect all company passwords. LastPass Enterprise offers employees and admins a single, unified experience that combines the power of SAML SSO coupled with enterprise-class password vaulting. LastPass protects our digital assets from the risks associated with employee password re-use and phishing. LastPass Shared Folders allow administrators to easily share credentials for a single website or for a group of sites while retaining the ability to tie activity back to the individual user. Password updates automatically and seamlessly propagate to all assigned users eliminating lock-out caused by version control issues.

In its default state, LastPass Administrators cannot access any data stored in an employee's LastPass account. However, there are some exceptions: (1) the end user can explicitly share data with an Administrator via an individual share or a Shared Folder, or (2) the company can choose to enable either or both of the Super Admin Policies defined here: https://lastpass.com/policy_doc.php. When the Super Admin Policies are enabled, a notification is sent automatically to every LastPass Admin in the Enterprise.

Employee accounts can be instantly disabled when employees leave the organization and administrators can view historical data and can audit employee logins and accesses. LastPass uses multifactor authentication offering increased security. Using an evolved host-proof hosted solution, LastPass employs localized, government-level encryption (256-bit AES implemented in C++ and JavaScript) and local one-way salted hashes to provide complete security with the convenience of syncing through the cloud. All encrypting and decrypting happens on individual computers – no one at LastPass can ever access sensitive corporate data. The LastPass™ Security Challenge also allows users to identify weak account data and provides suggestions for significantly improving online security.

4.1.5 Unattended Systems

Systems left unattended for more than 10 minutes will be automatically locked or otherwise secured.

4.1.6 Personal Use of Personal Computers and Network

As stated previously, the use of PCs in the Pinsight® network is primarily for business purposes. Incidental personal use of the PCs and the LAN/WAN is permitted. However, personal use should not interfere with Pinsight® operations or be in conflict with other established Pinsight® policies, nor should it cause any harm or embarrassment to Pinsight® or its clients. Any personal use is expected to be on the user's own time and is not to interfere with the person's job responsibilities.

4.1.6.1 Configuration of Workstations

Workstations should be configured with best practices. They should have Firewalls enabled, encryption (Bitlocker), and be up-to-date on anti-virus signatures and OS patches. Users should use a non-administrator account for daily activities vs. an administrator account. Workstations should be set for automatic updates.

4.2 Client/Participant Use of Pinsight® Applications

4.2.1 Account Administration

User accounts, which permit specific system access by specific individuals to Pinsight®'s "Leadership Readiness" application, are an important control point in the overall security model of an organization. If the number and owners of active accounts are not monitored closely, security risk to the organization greatly increases.
The key to effective, secure account administration is adherence to a strict set of policies that describe who is permitted to have accounts, who authorizes accounts, and when accounts expire. Access to Pinsight®'s application is based on each contract with our customers. These contracts allow for each partner/client to have the initial owner account created, after that either Pinsight® EIT staff or the client administrators can create/suspend/delete accounts.

Classification	Approval procedures for granting account	Account Implementation	Account expiration
Admin	Pinsight® Admin grants permission to other Pinsight® or Partner or Customer Admins on a contract by contract basis. Partner/Customer Admins grant permission internally to their own Pinsight® accounts.	Pinsight® EIT staff and Partner/Customer Admins	Immediately upon termination of relationship, with instructions from an approved client representative
Assessor	1. New assessor completes Pinsight® certification program. 2. Pinsight® assessor supervisor/manager grants permission	Pinsight® EIT staff	Immediately upon termination of contract/relationship with Pinsight
Partner Owner (admin)	Pinsight® Admin grants permission	Pinsight® EIT staff	Immediately upon termination of Partner Owner/contract/relationship with Pinsight. Exception: There always has to be a partner owner so if a partner owner is terminated another partner owner will be assigned by a Pinsight® Admin.
Client Owner (admin)	Pinsight® Admin grants permission	Pinsight® EIT staff	Immediately upon termination of Client Owner/contract/relationship with Pinsight. There always has to be a client owner so if a client owner is terminated another client owner will be assigned by a Pinsight® Admin.

Stakeholder	Pinsight® Admin, Partner/Customer Admin grants permission	Pinsight® EIT Staff and Partner/Customer Admins	Immediately upon termination of contract/relationship with Pinsight
Pinsight® Participant	Pinsight® Admin, Partner/Customer Admin grants permission	Pinsight® EIT Staff and Partner/Customer Admins	Termination of participation agreement or termination of client relationship/contract.

Pinsight® clients and participant accounts must adhere to the same authentication guidelines as found in sections 4.1.1 and 4.1.2 of this document.

4.2.2 Application Passwords

- Application passwords must be protected from unauthorized disclosure and modification when stored and transmitted.
- Applications must prevent passwords from being displayed when entered (e.g., asterisks are displayed when a password is being entered).
- Applications must enforce password minimum and maximum lifetime restrictions.
- Applications passwords must be changed every 90 days.

4.2.3 Auto Logout

Application sessions left idle for more than a designated time period will be automatically locked out or otherwise secured. Designated time period is dependent on the application and the customer. Generally 30 minutes is a good guideline.

4.3 HR/Personnel and Third-Party Security

4.3.1 Screening of Critical Staff

Pinsight® obtains signed agreements from all employees and contractors that states adherence to the security policy. All employees receive security awareness training as part of the onboarding process. Pinsight® conducts background checks on employees who have access to financial data. Verification of previous employment and references are conducted for all employees.

4.3.2 Terms and Conditions of Employment

The formal process for approving/granting access to Pinsight® involves employees and contractors reviewing and signing our employment or service provider contract, non-disclosure agreement as well as submitting all necessarily new-hire paperwork which can include a background check screening, before they are granted access. Both, the employment and service provider contracts include information about the company’s and the employee’s/contractor’s responsibilities, the security policies and confidentiality of data. Employees are also given and required to acknowledge receipt of the Pinsight® Employee Handbook.

4.3.3 Information Security Awareness Training

Pinsight®'s security policy is communicated through a recorded webinar, the employee handbook, and online training modules. All relevant parties must certify compliance with our security policy. Our security policy is approved by management, reviewed annually, legally binding and covers the following:

- Code of conduct
- Account management
- Passwords
- Third party information security
- Appropriate email use

4.3.4 Disciplinary Process

Pinsight® has adopted a code of ethics for work employees. Refer to the employee handbook sections on Discipline and Termination of Employment and Internal Complaint Review for more details.

4.3.5 Termination

Pinsight® handles personnel and third-party terminations in the following manner.
For each terminated individual:

- All system account access is revoked.
- An exit interview is conducted.
- When applicable, all physical access to property is collected (e.g., building passes, keys, identification cards).
- All assigned equipment/assets that are property of Pinsight® are returned (I.e. Laptops).
- In addition, Pinsight® retains official documents and records on organizational information systems created by terminated employees.

4.3.6 Access Agreements

Any individual requiring access to Pinsight® systems must complete the appropriate access agreements (e.g., nondisclosure agreement, conflict-of-interest agreement) as deemed appropriate by EIT Leadership. Access agreements will be reviewed as needed, annually at a minimum.

4.3.7 Sanctions

Any individual failing to comply with Pinsight®'s established policies and procedures will face formal sanctions, up to and including termination of employment and/or criminal charges.

4.4 Server Security

No amount of policy or security technology will be effective if Pinsight®'s servers are insecure. This section establishes standards for the base configuration of internal server equipment that is owned and/or operated by Pinsight. Effective implementation of this policy will minimize unauthorized access to Pinsight®'s proprietary information and technology.

- All internal servers deployed at Pinsight® must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by the operational group, based on business needs and approved by Pinsight®'s IT Systems and Security Manager/ DPO.
- Servers must be registered in a Pinsight® server inventory. At a minimum, the following information must be recorded:
    - Primary and backup server contact(s) and location(s)
    - Hardware description and operating system/version
    - Main functions and applications, if applicable
- Information in Pinsight®'s server inventory must be kept up to date; documentation auditing must be conducted periodically to ensure that documentation is current.
- Configuration changes for production servers must follow the appropriate change management procedures.
- Operating system configuration must be in accordance with approved Pinsight® requirements.
- Only EIT staff may add servers to the network.
- Only EIT staff may add services to the servers.
- Services and applications that will not be used must be disabled where practical.
- Access to servers and services must be logged and/or protected through access-control methods, if possible.
- The standard security principle of providing the least required access to perform a function must be used.
- Administrator/root access must not be used when a nonprivileged account will do.
- If a method for secure channel connection is technically feasible, privileged access must be performed over such a secure channel (e.g., encrypted network connections using SSH or IPSec).
- Servers must be physically located in an access-controlled environment. Servers are specifically prohibited from being operated in uncontrolled areas (e.g., cubicles or conference rooms).
- Critical server services must be monitored and EIT staff must be notified of problems via phone or email.
- All security-related events on critical or sensitive systems must be logged and audit trails saved in accordance with the Backups section of this document.
- Security-related events must be reported to EIT Staff who will review logs and report incidents to others as necessary. Corrective measures will be prescribed as needed.

- Audits of server security must be performed on at least a yearly basis using industry-recognized security assessment tools and practices.
- Vulnerability scanning must be performed on a quarterly basis or when significant new vulnerabilities affecting a system are identified and reported. Any vulnerabilities identified as severity High or above based on CVSS V3 Score Range will be addressed with a mitigation plan in place within 48 hours of discovery.
- Network Time Protocol must be used to synchronize time to a centralized time source.

4.5 Pinsight® Employees Remote Access

This section defines standards for connecting to Pinsight®'s infrastructure from remote locations. These standards are designed to minimize the potential exposure to Pinsight® from damages that may result from unauthorized use of Pinsight® resources. Damages may include the loss of sensitive or Pinsight® confidential data, damage to Pinsight®'s image, or damage to critical Pinsight® internal systems.
Only individuals with specific business need may be granted remote access to the Pinsight® network. Requests for remote access by non-employees must be approved by the IT Systems and Security Manager/ DPO and or, CTO following submission of a written request.

- Remote access must be strictly controlled.
- All computers including personal computers, that are connected to Pinsight®'s infrastructure must follow policies spelled out in Section 4.1.6.
- At no time may remote login information be shared with anyone.
- All remote access achieved through the Internet (such as cyber-cafes and public access terminals) must utilize encryption to protect all data during transmission. No unencrypted communication channels will be permitted across public networks.
- Pinsight® employees and contractors with remote access privileges must ensure that their Pinsight-owned or personal computer or workstation that is remotely connected to Pinsight®'s infrastructure is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
- All computers, including personal computers, that are connected to Pinsight®'s infrastructure via remote access channels must use antivirus software in accordance with the Malicious Software section of this document.
- All computers, including personally owned computers, that are connected to Pinsight®'s infrastructure via remote access channels must be patched with the latest security patches and hotfixes in accordance with the Managing Software Patches and Upgrades section of this document.
- All remote access with designated time limits will only be available during the specified times. Any changes to the scope of remote access time requires the approval of Pinsight®'s EIT Staff.
- Any violations of these guidelines may result in the termination of the remote access channel, and Pinsight® may pursue legal remedies if access is used inappropriately.

4.6 Mobile Devices/Removable Media

Pinsight® is comprised entirely from employees who are mobile and remote. It is critical that Pinsight® employees take extra security measures to ensure that data on mobile devices and removable media is secure. This protects the privacy and security of Pinsight, its employees, and its clients.

- Pinsight® Confidential or otherwise sensitive information must be encrypted using an encryption program approved by the EIT team before it can be placed onto a mobile device or removable media.
- All portable devices containing any Pinsight® information must be configured to use a password-protected screensaver that activates after a period of inactivity.
- Pinsight® installs Prey Protect on all company laptops. Prey Protect is an anti-theft protection software that monitors company computer locations and helps recover them if lost or stolen. After installing the software, Prey runs in the background and can be activated by an administrator as needed. Prey allows for remote lock down of devices and to delete stored passwords.

4.7 Communication Services - Policy

It is the responsibility of each Pinsight® employee prevent any loss or damage to devices assigned to them or used by them for Pinsight® business. This includes but is not limited to telephones, laptops, voice mail, fax machines, modems, videoconferencing equipment, cell phones.

4.8 Use of Electronic Mail

Pinsight® provides its employees and certain vendors (employee-users) with electronic mail communications. The primary purpose of the electronic mail system is to expedite necessary business communication between two or more individuals. As such, the use of electronic mail is for Pinsight®'s business purposes. Use of e-mail is a privilege and may be revoked at any time. Use of e-mail constitutes acceptance of this policy.
Employee-users are expected to be knowledgeable of these and all policies of Pinsight. Any questions should be directed to EIT Staff.

4.8.1 E-Mail Accounts

An electronic mail "account" is assigned to each employee-user. Any communication sent from this account is the responsibility of the employee-user assigned to that account. Employee-users are prohibited from allowing other individuals to send electronic mail from their account and may not use another account to send e-mail communications for their own purposes. Employee-users should not expect that electronic mail communications made through the Pinsight® system are confidential.

4.8.2 Personal Use

As stated previously, the use of electronic mail in the Pinsight® network is primarily for business purposes. Incidental personal use of the electronic mail system is permitted. However, the personal use of e-mail should not interfere with Pinsight® operations, nor should it cause any harm or embarrassment to Pinsight® or its Clients and Participants. Any personal use of e-mail is expected to be on the employee-user's own time and is not to interfere with the person's job responsibilities.

4.8.3 E-Mail Security Awareness

Employee-users should take extreme caution when using e-mail. All files should be passed through virus protection programs prior downloading. Failure to detect viruses could result in corruption or damage to files and/or unauthorized entry into Pinsight®'s infrastructure. It is mandatory that employee-users comply with copyright and trademark laws when downloading materials from the Internet
If the employee-user finds that any damage occurred as a result of downloading files, the incident should be reported immediately to EIT staff.

Encrypted email must be used: When sending or discussing confidential, strategic, non-public, or classified business information. When sending or discussing any type of client confidential, privileged, or private information. When sending any kind of PII (Personal Identifiable Information) of a client or employee.

Spam email is an unwanted email that is sent without the permission of the recipient. Pinsight® must implement and maintain an email filter mechanism to filter out common forms of email spam.

5. Software

5.1 Copyrights and Maintenance Agreements

5.1.1 Pinsight® Adherence to Copyright Law

Pinsight® purchases or licenses the use of copies of computer software from a variety of outside companies. Pinsight® does not own the copyright to this software or its related documentation and, unless authorized by the software developer, does not have the right to reproduce it for use on more than one computer.

5.2 Operational Control Policy

5.2.1 Separation of Operations

Pinsight® will have physically and logically separated staging/demo/production and corporate environments. Controls will be in place for securing each one independently. Access to each will be controlled on as needed basis by EIT Staff.

5.2.2 Server and Host System Changes

All requests to change any application or host or client / server system parameters must be submitted in writing via Trello.
EIT staff will maintain a change control Trello board, for the purpose of documenting change history. The change control board will contain the signed approval, the specifications of the form, and the date and time the change was implemented. The change control file will be reviewed as necessary.

5.2.3 Operating System Change Control

Prior to loading any new operating system releases, a change control process will be adhered to via Trello.
Included in this process will be:

- A review of the criticality of the change
- Confirmation with critical application providers, that their software is certified for the operating system release being installed.
- Preliminary testing of the Operating System and support applications in a test environment, prior to installation on Production mainframes/servers.
- Performance Monitoring and Benchmarking where possible, to ensure that Pinsight® systems continue to run optimally.
- Technical review of applications after operating systems changes.

5.2.4 Application Change Control

Pinsight® shall adhere to a release management process controlled within Azure Devops. Application change control will consist of the following:

- Large Features: These are deployed on a bi-monthly basis, usually on the Monday. These are not necessarily monthly releases.
- Fixes and small features: These are deployed on a weekly basis, usually on Monday if the live simulation schedule does not have any conflicts. If a scheduling conflict arises, the release is scheduled for the following day.

- Hot fixes: These are deployed ASAP and are of an urgent nature. Hot Fixes take a different path than the other two release types and can be pushed out in a matter of hours if necessary.

5.2.5 System Acceptance Testing

Systems acceptance testing shall be carried out by the Development, Stake Holders and the Product Management team prior to each release. Automated tools shall be used for first phase of acceptance testing in the staging environment. Review of changes are also done in production immediately after a release by the product management team and stakeholders.

5.2.6 Capacity Planning

Pinsight® uses Azure Monitoring and Cloudflare to monitor its production environment and measure the performance. All capacity planning is done based on using the Azure Monitoring and Cloudflare plus the corporate outlook for each year as it pertains to growth. Number of Simulations is the key metric used when predicting Pinsight®'s capacity needs for the future.

5.2.6.1 Information Systems Audit Control

Pinsight® shall leverage audit controls (such as Azure monitoring) that do not interfere with systems productivity or performance.

5.3 Software Development and Change Control

5.3.1 Development Process

Application Development is the primary responsibility of Pinsight® programming staff. They maintain the responsibility for understanding, adhering to, and supporting the Policies. These policies apply to internal development staff and all third-party vendors or contract developers.

- Authentication methods and access authorization must be appropriate for each user's level of access and sensitivity of data in the application.
- All untrusted input, including all user input, must be validated in software.
- All sensitive data crossing the Internet should be encrypted in transit using strong encryption.
- All new applications must follow the OWASP Guidelines and those in the subsections below.
- Pipeline scans will be performed on code and libraries as part of every new release of Pinsight®'s Leader Readiness Platform.
- System security testing shall be continuous during development activities assuring no anonymous access is ever possible.
- Unique, individually-identifiable end-user logins must be used for all applications.

5.3.1.1 Application Logging and Auditing

- Pinsight® Applications should provide detailed audit trails for significant events, including all individual access to sensitive information, actions taken by individuals with elevated privileges, access to audit trails, and all authentication attempts.
- Audit trails created by applications should include at least the following entries: unique user identification, type of event, date/timestamp, success or failure indication, source of event, and identification of affected data, system, or resource.
- Access to application audit trails should be limited to those with job-related need.
- Audit logs should be retained for as long as legally required, or at least one year, with a minimum of three months available online.
- Audit logs should NOT contain sensitive information such as SSN or DOB.
- Production applications should not log in debug mode.

5.3.1.2 Database Security

- Applications should connect to the database using as low privilege a Service Account as possible.
- Applications should connect to the database with different credentials for every trust distinction (e.g., user, read-only user, administrators) and permissions applied to those tables and databases to prevent unauthorized access and modification.
- Test and Demo database shall NEVER contain any live or PII data. All databases shall be physically separated from each other on different servers and networks. Data shall never be restored from production into test or demo, nor shall any real PII data be entered into the test or demo database.

5.3.1.3 Input Validation

- An application developed in any programming language can have input vulnerabilities, so all input from users and other untrusted sources should be validated. Standard validation libraries should be used.
- Input validation should specifically address the possibility of embedded browser-executable code (such as HTML, Javascript, etc.) to prevent cross-site scripting (XSS) attacks.
- A periodic review of the content of key fields or data files should be performed to confirm their validity and integrity.
- Validate all client provided data before processing, including all parameters, URLs and HTTP header content (e.g. Cookie names and values).

5.3.1.4 Encryption

- Where possible, all sensitive data should be encrypted in transit on any network using strong encryption.
- Applications storing credentials at rest should store those credentials securely, ideally in an encrypted format.

5.3.1.6 Standardization

It will be Pinsight®'s practice to define and utilize EIT standards wherever reasonably possible in its development process.
Development standards include:

- File naming conventions
- Job/Programming documentation conventions
- Source control standards
- Source archival standards
- Variable naming conventions
- Reasonable coding standards to facilitate readability (structure, etc).

5.3.2 Access to Source Code

Source code is securely stored at Azure Devops. Access to the source code is strictly controlled through Azure AD and MFA. Source code has audit trail for all actions carried out. Developers must follow all policies spelled out in this EIT policy section 4 regarding management of authentication protocols.

5.3.3 Use of Development Tools/Equipment

Certain tools may be utilized in the development cycle. These tools may be either software or hardware and must be approved for use by EIT Staff prior to use at Pinsight.
These tools may include test PC's and servers upon which software is to be developed and tested prior to any code being introduced into the production environment.

5.3.3.1 Software Tools

The following software products are currently approved and in use by Pinsight® programming staff, and approved contract developers:

- Atom
- PHP
- Nginx
- PHPStorm
- WEBStorm
- Composer Package Manager
- Doctrine ORM
- Babel
- MySQL (CE)

5.3.4 Use of Diagnostic Tools

Only personnel authorized for testing and development may use diagnostic test hardware and software. Access to such tools (hardware or software) is to be strictly controlled.

5.3.5 Certification

A third-party application and infrastructure review is required every two years.

5.3.6 Developer Training

Pinsight® developers will undergo annual “Secure Code Training” to ensure that OWASP Guidelines are being adhered to.

5.4 Disclaimer of Responsibility for Damage

Pinsight® uses access controls and other security measures to protect the confidentiality, integrity, and availability of the information handled by computers and communications systems. In keeping with these objectives, management maintains the authority to:
Restrict or revoke any user's privileges to inspect, copy, remove, or otherwise alter any data, program, or other system resource that may undermine these objectives and take any other steps deemed necessary to manage and protect its information systems.
This authority may be exercised with or without notice to the involved users.

5.5 Operating Systems Security

The security and performance of operating system software is critical to a production-application environment. Key vulnerabilities for operating systems software include loopholes, bugs, and support. The systems architecture needs to be documented and periodically reviewed (minimum yearly), to ensure loopholes are known and then either closed or closely monitored. Operating systems' software problems need to be documented, prioritized, and corrected through a problem/change management program.

- Operating system security policy must be derived primarily from the information security needs and mandates of the users. The technical staff builds and maintains the infrastructure to accomplish that mandate, deploying sound techniques and technologies and recommending it.
- Fundamental to the security and performance of operating systems software is the person(s) directly responsible for individual products as well as an accountable manager/supervisor. Where possible the manager/supervisor is different from the applications and production managers.

5.6 Security Monitoring via Software

Compliance with all security policy aspects will be monitored with appropriate software controls. Software Access controls such as passwords are covered in section 2 of this document: Access Controls. Additional controls, such as logging of internal system level events or activity by individuals may also be utilized

5.6.1 Logging and Data Collection Processes

5.6.1.1 Relevant Security Events in System Logs

Computer systems handling confidential, valuable, or critical information must securely log significant computer security relevant events. This should include things like SSH login, root access login, password guessing attempts.

5.6.1.2 Log File Retention

Logs containing computer security events must be retained for at least 90 days. During this period, such logs must be secured in such a manner that they cannot be modified, and such that only authorized persons can read them. These logs are important for error correction, forensic auditing, security breach recovery, and related efforts.

5.6.1.3 Log File Protections

Mechanisms to detect and record significant computer security events must be resistant to attacks. These attacks include attempts to deactivate, modify, or delete the logging software and/or the logs themselves.

5.6.1.4 Authorization to View Logs

All system and application logs must be maintained in a form that cannot readily be viewed by unauthorized persons. A person is authorized if he or she is an EIT staff member. Unauthorized users must obtain written permission from EIT Staff prior to being granted such access.

5.6.1.5 Regular and Prompt Review of System Logs

To allow proper remedial action, EIT staff must review records reflecting security relevant events on multi-user machines in a periodic and timely manner.

5.6.1.6 Users Notification About Logging

Users must be put on notice about the specific actions that constitute security violations. Users must also be informed that such violations will be logged.

5.6.1.7 Contact with Authorities and Special Interest Groups

To obtain and keep up to date on system vulnerabilities of information systems, Pinsight® currently subscribes to the security news sources for Facebook and Twitter as well as the Azure security alerts. Internal Company Content

5.6.2 Ownership of Company Content

Unless approved in advance by EIT Staff, all content posted to internal Pinsight® applications is the property of Pinsight. These applications include SharePoint, Teams, Trello, Office 365 and any other internally used corporate applications.

5.6.3 Ownership of Company Information

All information posted to Pinsight® internal applications must have a designated owner. Upon release of an employee's role through job change, termination, or attrition, it is the employee's manager's responsibility to assure continuance of these duties within their department.

5.6.4 Access to Internal Systems by Third Parties

All third-party access to Pinsight® internal systems must be approved in advance by EIT Staff.

5.6.5 Forwarding of Company Information

The Pinsight® internal applications are for the exclusive use of authorized persons. Unlike the Internet, information on the internal applications may be disseminated only to authorized persons. Users must not forward information appearing on internal applications to third parties without going through the appropriate internal channels (such as Human Resources, Marketing, or Public Relations).

5.7 Downloads & Uploads

5.7.1 Downloading Confidential Information

Confidential Pinsight® information may be downloaded from a production (live) server to another device such as laptop or PC only after two conditions have been fulfilled. For this data transfer to take place, a clear business and legal need must exist AND advance permission from an EIT Staff Member must be obtained. This policy is not intended to cover electronic mail or memos, but does apply to databases, master files, and other information stored on remote servers, and other multi-user machines.

5.7.2 Handling Software and Files Downloaded From Internet

All software and files downloaded from non-Pinsight® sources via the Internet (or any other public network) must be screened with virus detection software. This screening must take place prior to being run or examined via another program such as a word processing package.

5.7.3 Reliability of Information Downloaded from Internet

All information taken off the Internet should be considered suspect until confirmed by another source. There is no quality control process on the Internet, and a considerable amount of Internet information is outdated, inaccurate, or deliberately misleading.

5.7.4 Uploading Software to Other Machines Via the Internet

Users must not upload software that has been licensed from a third party, or software that has been developed by Pinsight, to any computer via the Internet unless authorization from the Pinsight® EIT Staff has first been obtained.

5.8 Cryptography

Technology is providing new and faster methods of transferring data between businesses and clients or participants. While it is desirable to take advantage of these new technologies, our first responsibility is to maintain our clients and participants' privacy. To do so, may require encryption of data being transferred in to or out of Pinsight. However, this process must be managed to ensure that appropriate controls are being used, and to ensure that the encryption process does not allow other adverse effects, such as data loss.

5.8.1 Use of Encryption Processes

256-bit or better encryption processes will be used for transmittal of any member data inter-institutionally, on a non-secured line (i.e., Internet). This includes human resource data, client information, or participant information, to name a few examples. EIT will maintain responsibility for all secure certificates, and all other cryptographic software applications.

5.8.2 Encryption Key Management

5.8.2.1 Disclosure of Encryption Keys

Encryption keys are private, and access to such keys must be strictly limited to those who have a need-to-know. Unless the approval of EIT Staff is obtained, private encryption keys must not be revealed to staff, clients, participants, consultants, contractors, or other third parties.

5.8.3 Miscellaneous Encryption Matters

5.8.3.1 Deletion of Readable Data After Encryption

Whenever encryption is used, users must not delete the sole readable version of data unless they have first demonstrated that the encryption process is able to reestablish a readable version of the data.

5.9 Malicious Software

All Employees, contractors, vendors, and any other person using or accessing Pinsight®'s systems must take appropriate measures to prevent the introduction or spread of malicious software.
Introduction of virus code into any computer owned or operated by Pinsight® is strictly prohibited. Users must not intentionally write, generate, compile, copy, propagate, execute or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of the computer's or Pinsight® network's memory, file system, or software. Violation of this policy subjects the user to immediate termination and/or criminal/civil penalties.
Pinsight®'s production/staging/demo infrastructure is protected by antivirus software. Pinsight® uses clam AV (https://www.clamav.net/) with automatic testing set for 6am each day, including new files uploaded by users. All uploaded files will be scanned in real-time. However, virus protection software does not necessarily prevent the introduction of a virus into a computer or the network. Symptoms of a virus include considerably slower response time, inexplicable loss of files, changed modification dates for files, increased file sizes, and total system failure. Any user noticing symptoms such as these is to notify EIT staff. Because some viruses are very complex, the user should not attempt to eradicate it on his or her own. Such attempts could result in the further spread of the virus through the network. If the user is notified by virus protection software installed on the network that a virus or other malicious software is present, that person is to immediately notify EIT staff.
Occasionally, virus protection software on the infrastructure will update when the user logs on. No user should attempt to terminate this update from occurring. In addition, users are prohibited from attempting to disable the virus protection software on their computer.
Virus protection software must be installed and maintained on all systems connected to Pinsight®'s network. Pinsight®'s email system must be configured to scan and filter the content of messages to prevent the spread of viruses, worms, Trojan horses, or other executable items that could pose a threat to the security of systems and networks.

- Virus protection software must be installed and maintained on all systems.
- Virus protection software updates must be downloaded and installed as they become available.
- Virus protection software must be configured to scan for viruses in real time.

- Files or macros attached to an email from an unknown, suspicious, or untrustworthy source must never be opened. These attachments must be deleted immediately, and then "double deleted" by emptying the Trash.
- Files must never be downloaded from unknown or suspicious sources.
- Direct workstation disk sharing with read/write access must never be done unless there is an absolute business requirement to do so.
- Removable storage media from unknown sources must always be scanned for viruses before being used.

5.10 Patch/Upgrade Management

All systems must be patched to current levels. Pinsight®'s EIT staff is responsible for daily monitoring of patch and upgrade announcements from all vendors whose software products are in use in the organization. EIT staff must meet as needed to prioritize patches and upgrades, placing those with significant security impact at the top of the list.

- Security related patches must be reviewed within 72 hours.
- Critical patches must be applied within 10 days.
- Non-critical patches must be applied within 30 days.
- All patches must be thoroughly tested before being applied to production systems.
- Only patches from verified, known, reputable sources may be applied to systems.
- All new systems must be at current patch levels prior to being added to Pinsight®'s network.
- EIT staff must keep a log of patch applications.
- Regular auditing of patch compliance must be conducted to ensure proper policy compliance and system integrity.

6. HARDWARE

6.1 Hardware Acquisition

All acquisitions of computer assets and software must be acquired through EIT staff. Software and hardware acquisition is based on business need and conforms to established configuration and security standards.

6.2 Approval for Establishment of Servers

Before they are connected to the Azure network, all Pinsight® Servers must be reviewed by EIT staff and pre-authorized by EIT Staff.

6.3 Maintenance and Service Agreements

Pinsight® and its employees are responsible for maintaining equipment in a responsible manner, and routine preventive and regular maintenance on Pinsight® systems must be documented in accordance with manufacturer or vendor specifications and/or organization-specific maintenance requirements. Precautions are to be taken against abuse or negligence of all Enterprise Information Technology hardware.

6.4 Physical Protection

- All Pinsight® mission critical servers and services will be housed in SOC 2 Type II compliant data centers.
- Unauthorized personnel are not allowed entry to Pinsight® facilities, data centers, etc.
- In the event of a disaster, Pinsight®'s Disaster Procedure must be followed.

Refer to the Pinsight® Security Document for more details on specific data centers and controls.

6.5 Asset Management

All hardware and software used on Pinsight®'s information systems is managed by EIT Staff. EIT staff is responsible for the physical inventory and maintenance of these assets.

6.5.1 Inventory of Assets

Pinsight® keeps a complete inventory of all assets both for personal use as well as for the platform. Inventory of assets is held in a number of documents including personal Inventory Assets and the Pinsight® Inventory document and the Information and Asset Classification Policy.

6.5.2 Ownership of Assets

All assets identified in the inventory documents are considered to be "Owned" or "Controlled" by Pinsight. I.e. while we do not physically own the servers at Azure, Pinsight® does own complete stewardship and control of those assets.

6.5.3 Acceptable use of assets

Acceptable use of Pinsight® assets is defined in several policy and procedure documents, including the employee handbook, the Company Security Policy and the EIT Security Policy. Employees must acknowledge and signify they understand these policies and procedures as part of their employment. See section 4.3 of EIT Security Policy for more details.

6.5.4 Return of Assets

Per section 4.3.5 of EIT Security Policy, all employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement. Laptops, keycards, company cell phones etc.

6.5.5 Personal Computer Assets

The following are measures utilized by Pinsight® to physically protect personal computer assets from theft, damage or unauthorized access.

- Prey Protect is installed on all laptops.
- If the personal computer is configured with a hard disk on which data and software are stored, it should be secured against access, tampering or removal
- If the personal computer is not configured with a hard disk, then the data and software used on the machine should be secured when not in use, e.g., locked in a cabinet, safe, desk, etc.
- Personal computers or workstations and their disks, with critical and sensitive data stored on them or accessible through them should be further secured against unauthorized use even by someone who has legitimate access to the physical space.
- Personal computers should be clearly marked for ownership.

6.5.6 Classification of Information

Information is classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification. Refer to the Information and Asset Classification Policy for more details.

6.6 Computer Location and Facilities

6.6.1 Equipment Management

6.6.1.1 Alteration/Expansion of Pinsight® Computers

Computer equipment provided by Pinsight® must not be altered or added to in any way (e.g., upgraded processor, expanded memory, or extra circuit boards) without knowledge and written authorization by EIT staff.

6.6.1.2 Moving Equipment

Computer equipment (PCs, LAN servers, etc.) must not be moved or relocated without the prior approval of EIT.

6.6.1.3 Equipment Damage

Users must promptly report to their manager any damage to or loss of Pinsight® computer hardware, software, or information that has been entrusted to their care.

6.6.1.4 Equipment Disposal

When equipment is retired after reaching end-of-life, or if it is replaced because of failure or the need for repair, it is extremely important that it be disposed of and/or moved in a secure manner to avoid disclosing Pinsight® data unknowingly to parties that come into possession of the equipment in the future.
Before any Pinsight-owned or managed hard disk or system containing a hard disk is transferred, donated, or disposed of, it must be sanitized by reformatting the hard drive in a secure manner or by using an approved wipeout utility. Portable media may be reused after overwriting or re-formatting, or it may be destroyed. Simply deleting a file is not sufficient to prevent someone from undeleting the file later.
Hardware that is moved off-site for repair can only be done so after approval by the EIT team.

- The EIT team must use an approved sanitization program on all systems before they are sent out for donation or disposal.
- Hard disks of server systems must be wiped of all information and software in a secure manner, or removed and physically destroyed by crushing, drilling, or incinerating.
- Portable media, thumb drives and CD-ROMs, may be destroyed by crushing, incinerating, shredding, or melting. If it is to be reused, portable media must be erased using a secure program before being reused by other parties.
- Damaged storage devices containing very sensitive data may require a risk assessment to determine whether the item must be destroyed, repaired, or discarded.
- All hardware and media disposal must be tracked.

6.6.2 Physical Security or Encryption of Confidential Information

All information storage media containing confidential information must be physically secured when not in use. An exception will be made if this information is protected via an encryption system approved by EIT staff.

7. BUSINESS CONTINUANCE POLICY

7.1 Operational Units

Each manager within Pinsight® is responsible for developing a departmental plan to resume normal operations within a defined period of the occurrence of a natural disaster or human act of destruction that effects a particular business or functional team. Pinsight® is a remote operating company with no corporate headquarters. Each manager must ensure that their team and employees have an ability to recover their own operations in the event of a disaster:

7.1.1.1 Critical Applications

All current customers and users of the computation facility need to be inventoried and updated *annually*. Each application needs to be assessed from a risk perspective. How many days before normal operations must resume? This is all defined in the ***Business Continuity Plan***.

7.1.1.2 Facilities

Disaster recovery alternatives must include resuming operations at a warm standby site, cold site or sister location. Pinsight® has created working accounts with Azure to provide a standby site, refer to the **Business Continuity Plan** for more details.

7.1.1.3 Testing

Annually, a walk-through or table top test of the Business Continuity plan is performed. These drills test different cases and/or segments and the appropriate documentation is updated.

7.2 Backup and Restoration of Software and Data

A major security concern for Pinsight® is the ability to maintain computer system availability. If the data or software is destroyed inadvertently or maliciously on a system, there must be copies of the data and software available that can be restored to allow continuation of processing with a minimum of effort on the part of the user. This implies that data and software must be copied to a separate backup medium on a regular cycle for contingent use.

7.2.1 Critical Systems Backup:

Critical systems include Pinsight®'s production system, source code system, test system, secure servers, and other business critical servers.

- General backup (DB // server configs // frontend and backend – grandfather-father-son scheme backed up to Amazon S3 Bucket) https://www.handybackup.net/grandfather-father-son-backup.shtml
- Daily and Weekly snapshots of the Azure VM's.
- Backups are encrypted at rest on AWS.
- Full system backup media must NEVER be overwritten as long as the system remains in use. Once a system has been retired, its full system backup media may be eligible for recycling (if the data is no longer useful to Pinsight) after two years.
- Firewalls and state-full network equipment configurations must be backed up on a weekly basis and prior to and following major changes made to that equipment.
- Critical data must be backed up in such a manner that it can be restored in full up to 90 days following the day it was backed up. Critical operating system data must be backed up in such a manner that it can be restored in full up to 30 days following the day it was backed up.
- On-site backup media must be stored in a physically secure, climate-controlled location.

- Only EIT staff may physically handle on- or off-site backup media.
- Every backup must be labeled so as to identify its contents.
- Backup sets must be verified at least annually to verify restoration capability.
- Deviations from these requirements may be allowed where other Pinsight® policy requires that data not be backed up or archived as described above.

7.2.2 Restoration:

Annual restoration exercises shall be performed to validate that prompt recovery from system failures can be achieved.

- Restore from snapshots to validate ability to be up and running in less than 24 hours (unofficially in less than 4 hours).
- Restore from general backup (in case we also lose snapshots) to validate the ability to be up and running in less than 48 hours (unofficially in less than 8 hours).

7.3 Incident Response

It is Pinsight®'s policy to take a pro-active approach to Information and Systems Security. However, in the event of a critical systems problem, an internal misuse of information or systems or external attacks upon our systems, we must be responsive.

7.3.1 Incident Reporting

All Employees have responsibility to ensure the security of computer systems they have access. Staff must report problems or suspected activity to EIT staff in a timely manner.
Computer security related incidents other than direct attacks will be escalated based on Member or organizational impact.

7.3.1.1 Hacker Attacks

Any indication that our systems/servers are being impacted by hacker attacks, are to be reported immediately to EIT staff. EIT staff will appraise the situation and determine the controls to be utilized to remove the risk.
It is the responsibility of the IT Systems and Security Manager/ DPO or the CTO to provide appropriate notification of the incident to the CEO, and to ensure that measures are being taken to protect Pinsight®'s systems and information.

7.4 Incident Management

Any reported incident shall immediately be subjected to the ***Incident Management Policy***, refer to policy for more details.