Piano Software Public Information Security Policy

Contents

1. Purpose

This Information Security Policy (ISP) is designed to establish administrative, technical and physical safeguards for the protection of Piano's Confidential Information and comply with our obligations under applicable federal, state, and international laws. This ISP sets forth procedures for evaluating and addressing electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting Confidential Information.

This ISP is applicable to all Piano team members, agents, contractors, representatives and other parties that have access to Piano's Confidential Information.

With this ISP, Piano seeks to achieve five core objectives:

- Identify and assess the likelihood and potential damage of reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing Confidential Information;
- Evaluate the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control and mitigate known and reasonably foreseeable risks to Piano;
- Designate and implement a program that puts safeguards in place that are designed to minimize and mitigate the risks identified, consistent with the requirements of applicable data protection laws, including Massachusetts 201 CMR 17.00, EU Personal data protection regulation 679/2016, the US-EU Safe Harbor, US-EU Privacy Shield and other applicable laws and regulations.
- Implement regular monitoring of the effectiveness of those safeguards.

2. Human Resources Security

Appropriate security controls must be implemented to ensure those hired by Piano Software have undergone appropriate pre-employment screening. Employees are informed of security policies and their responsibilities upon hiring and during their term of employment. Access to necessary resources must be provided and removed as appropriate.

2.1. Non-Disclosure Agreements (NDA's)

Contingent workers should be covered under a Non-Disclosure Agreement under the Third Party contract. If persons under a Third Party's responsibility are required to access information classified as Internal or higher, then an individual Confidentiality Agreement should be acknowledged by the individual.

2.2. Termination of contract

When an employee resigns or is terminated, the following should be performed:

The employee's system account(s) must be revoked. All passwords known by the employee on all systems should be changed.

All privileged account passwords known by the employee should be changed.

All Piano property should be collected, including badge/token, workstations, laptops, smartphones.

A termination briefing is planned to remind the employee of their continued responsibilities as defined by the Non-Disclosure Agreements (NDA) and other employment agreements and/or under any applicable local laws.

3. Asset management

Appropriate security controls must be built into Piano Software's information resources. This protection should be commensurate with the resource's value to Piano Software, as determined based on the business requirements.

3.1. Inventory of Assets

Assets should be clearly identified, along with its ownership and location. All assets are assigned an “owner” or “primary user” that has approved management and accountability responsibility.

3.2. Information Classification

Piano Software information and client information entrusted to Piano Software must be classified and protected in a manner commensurate with its sensitivity. This is required no matter where it resides, what technology is used to process or store it, or the purpose for which it is used. All Piano Software staff are responsible for protecting confidential Piano Software and client information from unauthorized access, modification, duplication, destruction or disclosure, whether accidental or intentional.

The classification levels are:

- Public
- Internal
- Confidential

Confidential is information whose unauthorized disclosure, compromise or destruction would directly or indirectly have an adverse impact on Piano Software, its staff or clients. Piano Software Confidential information includes information used in the provision of products and services to clients and prospective clients of Piano Software.

Confidential information may be shared with parties who have a relationship with Piano Software, if they have signed a non-disclosure agreement, have been granted proper authorization and have a need to know. Applicable Piano Software Policies and Procedures relating to the handling, access, use, disposal must be followed. Confidential Information includes, but is not limited to:

- Personal Information
- Sensitive Personal Information
- Information classified as “production”, including all client information when used in system testing environments.
- Client or prospective client information supplied for the provision of Piano Software products and services or business requirements, and other proprietary system design, development or testing documentation.
- Internal and external audit reports
- Regulatory agency reports, unless specified by the regulatory agency as Public information
- Voice mail access codes and passwords
- Passwords
- Any form of security key
- Personal identification numbers
- One-time registration codes
- Challenge/response phrases
- Source Code (example: an application that enhances client sales and retention.)
- Patent and patent applications
- Trade secrets
- Proprietary and confidential information, ideas, media, techniques, sketches, drawings, works of authorship, models, inventions, know-how, processes, apparatuses, equipment, algorithms, software programs, software source documents, and formulae related to the current, future, and proposed products and services, such as information concerning research, experimental work, development, design details and specifications, engineering, financial information, procurement requirements, purchasing, manufacturing, customer lists, investors, team members, business and contractual relationships, business forecasts, sales and merchandising, and marketing plans
- Past, present or future research, development or business activities or the results for such activities

3.3. Handling

No vendors, consultants, or other third parties should be given access to Piano Software or client confidential information, or to systems containing Piano Software or client confidential

information, without having entered into legal contracts containing appropriate security and confidentiality provisions.

Piano Software staff must handle Confidential information of the company and its clients with integrity and discretion and in accordance with applicable laws. Information obtained through employment with Piano Software belongs to Piano Software, or to one of its clients.

3.4. Reuse and disposal of computing equipment

Computing or communications equipment (for example laptop) issued to or used by terminated employees for Piano Software business should be examined by the appropriate support group who should re-image the equipment prior to reuse of the device or issuance to another employee.

Computing equipment removed from stock are handled by external providers which ensure the zeroing of data by providing a disposal certificate.

3.5. Unattended user equipment and Clean Screen

All users should lock their workstation when leaving their work area for any reason. Automatic screen lock after idle time must be applied to all unattended workstations to lock the session.

4. Access Control

Piano Software establishes security requirements, in order to ensure controlled access to the information resources of Piano Software that contain sensitive or limited access data. Access must be granted based on the individual's role and must be limited to the minimum necessary to perform the job function.

Initial access to Piano Software information resources will be based on roles defined by the management. These roles will be based on job function. Any user who requires access to specific applications or information resources based on their designated role or job function must request access from their manager.

When granting access, use the concept of "least privileged" access to information and/or resources. This means users should only be granted the access they specifically need to perform their business tasks, and no more.

4.1. Management of Privileged Access Rights

Regular user accounts must never be granted elevated privileges for performing administrative activities. A separate account with elevated privileges must be provisioned and tied to users for the purposes of performing systems administration.

Generic system IDs with elevated privileges (example: root, administrator) or other approved shared IDs may be used by multiple users who have a business need to do so, but the password must be controlled. However, such generic ID cannot be used without any prior authentication with nominative account to ensure the traceability of all access and shall not give access to customer data.

Security logs must be configured to rotate and be sent to a centralized location for aggregation and protection.

4.2. Secret authentication information

Authentication is required for each user account. All authentications must be done using one of three factors:

- Something a person knows - this represents information of which only the legitimate user should have knowledge (e.g., a password)
- Something a person has - this represents a physical object, which is not trivial to duplicate, over which only the legitimate user has possession and control (e.g., hardware token)
- Something a person is or does - this represents a physical attribute which is unique to each user (e.g., fingerprint, retina, face, voice, or signature)
- Multifactor authentication (MFA) is required for remotely accessing Piano Software infrastructure via VPN. Refer to Network and Communications Security Policy for details.

Regular review of user access rights (including privileged accounts) is performed at least on an annual basis.

2.3 Passwords management

User should choose easily remembered passwords which are, at the same time, difficult for unauthorized parties to guess.

Passwords MUST be a minimum of eight (8) characters. Passwords must be comprised of one (1) or more characters from at least three (3) of the following four (4) classes:

- Upper case letters (e.g., A, B, C…Z)
- Lower case letters (e.g., a, b, c…z)
- Numbers (e.g., 0, 1, 2…9)
- Non-alphanumeric special characters (e.g., ?, !, %, $, #, etc.) which can include space(s)

4.3. Password Expiration

The following password expiration requirements should be followed for users, administrators and at the group level:

- Passwords for normal user accounts must have a maximum validity of ninety (90) days or less

Specific policy for Piano Analytics staff is applied:

- Password MUST be a minimum of eight (10) characters
- Password expires after six (6) months

Where possible, an automatic password expiration warning should be given to the user at least seven (7) days, but not more than fifteen (15) days, prior to expiration and at every login during that period.

5. Encryption

All Piano Software and client confidential information must be appropriately encrypted when electronically transmitted outside of company's network. Encryption should be employed to protect the confidentiality of sensitive personal information when being transmitted and/or stored on Piano Software's information resources. The following provides an overview of the appropriate level of encryption based on the classification of the data and method of storage or transmission.

The following guidelines should be followed when transmitting information:

Classification	Protection
Public	No requirement
Internal	Encryption is recommended for transmission over network links containing equipment not owned or controlled by Piano Software (example: the Internet). Encryption is not required for transmission over Piano Software's internal network
Confidential	Encryption must be used for transmission over a network not owned or controlled by Piano Software (example: the Internet). Transmissions over Piano Software's internal network should also be encrypted.

The following guidelines should be followed when storing information (data at rest):

Classification	Protection
Public	No requirement
Internal	No requirement
Confidential	Use an approved encryption algorithm, unless the resource has compliant user authentication, least privilege access controls, logging and time outs

Key Management will follow NIST 800-57 Recommendations for Key Management.

Piano Software uses AWS Key management service for infrastructure key management, which is managed based on the documentation:

- https://docs.aws.amazon.com/kms/latest/developerguide/overview.html

Customer data stored on AWS S3 are encrypted using AES 256 algorithm.

Piano Software uses Snowflake default encryption for Piano Analytics, which is managed based on the documentation:

- https://docs.snowflake.com/en/user-guide/security-encryption-end-to-end.html

6. Physical and Environmental Security

Piano Software facilities and information resources must have appropriate physical access controls to protect against unauthorized physical access, safeguard against foreseeable environmental hazards, and protect associates and authorized visitors.

To ensure the protection of Piano Software employees, visitors, assets, client data (including: Sensitive Personal information), funds, intellectual property, and the Piano Software brand, access to any Piano's facility including the headquarters, Service Centers, offices and information processing facilities, must be controlled and managed appropriately. Example: Make sure others do not "tailgate" into a facility behind authorized personnel.

Access to facilities must be physically restricted with access granted to those employees, contingent workers and vendors who have legitimate business responsibilities within the facility. Any observed or reported incident of unauthorized access should be reported immediately to the CSO or CSO's delegates or the employee's manager. Clients, representatives of clients, or other third parties are restricted from entry to any area of the

facility deemed a ‘restricted area’. A restricted area is defined as an area which limits general access via a key.

7. Operations security

Operating procedures are used in all day to day maintenance and operations of Piano Software in-scope infrastructure and services. These operating procedures are documented or/ and referenced to an appropriate level of detail for the team that will be using them.

There is a set of complex monitoring and alarming tools that are used to monitor resources. In addition to monitoring, regular architecture meetings are conducted as part of product development to identify potential bottlenecks, performance issues, and other capacity and performance related issues.

7.1. Protection from malware

All Piano Software end user devices must have anti-malware software installed and always be running while in operation.

The anti-malware product shall be operated in real time on all end user devices. The product shall be configured for real time protection. The anti-malware solution will be configured for users devices to updated on a daily basis. Automatic scans shall be done at least weekly on all end user devices.

7.2. Patch management

All servers will have all security patches applied every 60 days. Public facing servers will be patched timely. All devices will have all critical and security updates applied every 90 days. Public facing devices will be patched within one week of release or within 24 hours if the patch is security related. Any exception to this policy will be documented and forwarded to CSO for review.

7.3. Management of technical vulnerabilities

Piano Software aligns its standard security baselines with security best practices and vendor recommendations such as CIS Benchmark. Hardening policy has been defined for servers systems.

7.4. Logging and monitoring

Logs are created in line with the requirements and are reviewed using an automated review process to enable oversight of security related events. Logs contain records of system and network security and therefore must be protected from breaches of their confidentiality and integrity.

Log protection shall be controlled by:

- Attempts to access the logging systems shall be logged and the audit records shall be protected from modification and deletion;
- Access to logging systems and systems audit tools should be limited to those who require access for their job function considering the segregation of duties.

8. Network and Communications Security

Access between Piano Software's internal networks and any other network, public or private, must be through appropriately secured connections which support strategic business initiatives. This policy applies to employees and contingent workers, who are individuals providing services to Piano Software on a provisional or non-permanent basis, such as temporary workers, contract workers, independent contractors, or consultants worldwide. It sets a minimum standard. It may be supplemented by other policies and procedures which state additional requirements in certain geographic regions where applicable laws impose stricter requirements on Piano Software.

Networks must be segregated or divided into separate logical segments, so access between segments can be controlled by means of network secure devices. Servers which access external networks or are accessed from external networks should be logically isolated from Piano Software's internal networks.

All external entities which require access to Piano Software information resources for business purposes must be sponsored by a Piano Software manager and approved by the CSO. Access should not be granted until the approval is received. All new connections to external public networks must be approved by the CSO.

Information may be transferred digitally or physically for the secure transfer of business information between Piano Software and external parties.

8.1. Information transfer

A formal information transfer agreement should be set up prior to transferring to include:

- specific reference to identified data flows, means of transfer, security requirement (relevant to the transfer/flow), incident reporting procedures and contact details for the lead contacts in each participating party.
- Be signed and dated by each key contact.

Information transfer must be in accordance with contractual, legal and regulatory requirements.

9. Supplier Relationship Risk Management

Piano Software will determine prior to engagement if the third-party vendor, in performing its contractual services, will either maintain, store, process, transmit sensitive data, including client data.

Standard 'baseline' contractual agreements containing appropriate vendor/partner assurance terms and conditions are required to be executed in Piano Software's Data Processor Agreement (DPA) for all third-party engagements where the relationship requires that the third-party processes client data. The following general security requirements should be included, where applicable, in agreements with third party vendors:

- Processing of Company Personal Data
- Third Party Personnel
- Security
- Sub-Processing
- Data Subject Rights
- Personal Data Breach
- Data Protection Impact Assessment and Prior Consultation
- Deletion or Return of Company Personal Data
- Audit Rights
- Transfers
- Processing Records
- Liability

10. Security Incident Management

The Security Incident Management is implemented with an Incident Response Plan ("Plan"). The Plan formalizes Piano's internal processes, including the actions to be taken in the event of an actual or suspected incident involving the unauthorized access, use or disclosure of confidential information or an attack on Piano's systems and data that might, or does, jeopardize the integrity of Personal Information or other confidential information held by Piano.

10.1. Incident Response Team

Promptly following implementation of this Plan, Piano will create and maintain an active Piano-wide Incident Response Team ("IRT"). In cases where there has been an actual or suspected security incident, attack or security breach (often referred to below as a "breach") the IRT will be immediately called together when possible, or at a minimum the Team Leader will be notified.

The IRT's basic duties in the case of an attack or breach (as further described in this Plan) are as follows:

- To determine if in fact an attack or breach is taking/has taken place.
- Close down all services that are being used in a suspected breach or attack.
- Determine the extent of the damage caused by the attack or security breach.
- Coordinate with senior management regarding the findings of investigations and on actions being taken.

IRT members will coordinate with management via the CSO, who will keep Piano's executive team informed and liaise with Piano's internal and outside attorneys to ensure all statutory notifications are made.

- Where third party confidential data has been compromised, coordinate and work with the third party and external agencies (banks, financial institutions, law enforcement, etc.) in order to mitigate the loss of confidential data, and to assist in external investigations.
- Prepare a detailed report about the incident. This report must cover the nature of the attack or breach, how it happened, what if anything was lost or compromised, who was responsible, and what actions have been taken to ensure it doesn't happen again.
- Review current security mechanisms and make adjustments where required to both policies and their implementation to ensure that such an attack cannot be repeated.
- Coordinate and cooperate with third party security reviews following an incident.

10.2. Action Plan

Following are the steps Piano should take if a security incident/ breach is suspected:

- Validate and Contain
- Convene Incident Response Team
- Notify Outside Parties
- Debrief and Review

10.3. Enforcement

Piano will notify its employees that:

a) Any staff failing to immediately report suspected or actual attacks and security breaches will be considered derelict in their duties and may be subject to disciplinary action, including the possibility of dismissal.
b) Failure to report such incidents may lead to them being suspected of involvement and therefore liable to investigation by the relevant legal authorities.
c) Failure by members of the IRT or other employees with specific duties under this Plan may lead to disciplinary actions.

11. System acquisition, development and maintenance

11.1. Change Management and Secure Software development

Change Management is the process to manage the introduction of any enhancement, modification, update, installation, or removal of any hardware, software, interface, or database that will impact the existing production environment. The goal of change management is to increase awareness and understanding of proposed changes across an organization and ensure that all changes are made in a thoughtful way that minimizes negative impact to services and customers.

Piano Software's application development and management methodology must incorporate appropriate security controls into each stage of the system development life cycle.

11.2. Types of Changes

Piano Software uses three definitions of changes:

Standard change

A standard change is a pre-authorized change that is low risk, relatively common and follows a specified process. A standard change is one that is frequently implemented, has repeatable implementation steps, and has a proven history of success. As Standard changes are pre-approved, they follow a streamlined process in which Architecture board authorization steps are not required.

Example of standard change: patch installation, version update

Emergency change

A change that must be implemented as soon as possible, for example to resolve a major incident or implement a security patch. It is of such a high priority that it bypasses group and peer review and approval and goes straight to the Authorization state for approval by the Architecture board approval group.

Emergency changes cover the following types of emergencies (but are not limited to):

- Fix on fail or retroactive situations where the impact to service has already been experienced.
- Failures or situations where the impact to service is imminent if action is not taken.

These changes do not follow the complete life cycle of a normal change due to the speed with which they must be authorized.

Normal change

Any service change that is not a standard change or an emergency change. Normal change requests follow a prescriptive process which requires approval before being implemented, reviewed and closed. These changes require an assessment and authorization to ensure completeness, accuracy, and the least possible disruption to service. These changes are most often scheduled outside of defined change blackout windows or during defined maintenance windows. The normal type is used to implement beneficial change for any change to a service that is not a standard or emergency change.

11.3. Scope of Changes

There are many IT tasks performed that do not fall under the process of Change Management. Tasks that are outside the scope of Change Management process include:

- Contingency/Continuity/Disaster Recovery
- Patch management
- Changes to non-production elements or resources
- Changes made within the daily administrative process. Examples of daily administrative tasks include but are not limited to: - Password resets of non-critical user accounts - User add/deletes - User modifications, Adding, deleting or revising AD or Unix group changes, File permission change - Desktop support tasks (software installs/un-installs such as Word, Excel, etc.)

The Architecture board (arc) may modify the scope periodically to include items in the scope of the Change Management process.

11.4. Addressing Risks of Web Based Applications

To ensure the risks associated with the development of web based applications are minimized, additional controls should be employed. These controls address the privacy requirements (e.g. EU GDPR, California Consumer Privacy Act (CCPA), etc.) which affect client applications.

The following security controls should be implemented for client applications:

- Client and service-related data must be protected appropriately as per Information Classification requirements
- Applications must be tested for information security issues (secure code review, penetration test performed at least annually, vulnerability scanning).
- Interfaces between web servers, back-end systems, and client side should be restricted to those services required by the application, based on documented Application Programming Interfaces (APIs), and supported by mutual authentication
- Feasibility studies should be conducted to ensure technology solutions are designed to support business requirements such as throughput, user load and traffic loads

- Testing processes should include volume testing and other systems testing to ensure architecture can support the expected usage of the applications
- Developers must receive secure coding training
- Segregating functions by server (e.g. web servers, application servers, and database servers should be implemented on separate servers)
- Segregating server roles to network locations (e.g. DB servers to Private zones, Application servers to App zones, and Web servers to DMZ)
- A privacy review must be conducted to ensure appropriate privacy notices and data security controls are in place
- All domain names and websites registered by Piano Software must be reviewed on a regular basis. Additionally, a process should be instituted to monitor potential illegitimate websites for protection against phishing and other potential threats
- Developers should not have any access to production information resources, which includes but are not limited to: the server operating system, databases, web services, APIs, etc. which would allow access to client information, or would affect a change to the production environment. Any exception to this rule should be handled through a risk management program.

11.5. Sanitization of Production Data for Testing Purposes

Client data is not used for development, testing, training presentations or any purpose other than providing production services, client-specific acceptance testing, or production diagnostics.

11.6. Source Code Management Systems

In order to reduce the potential for software corruption and restrict access to only those individuals who need direct access to source code, source code management systems must be used.

All code access and changes must be tracked (check-in, check-out, branches, configuration changes, etc.) and each code change must be associated with the individual who committed the change, the date and the time.

Access to a source code repository follows the least privilege principle. Individuals should only receive access to the parts of the source code required to complete the individual's tasks. Authorized personnel must not transfer or share code with other individuals who are not authorized to handle the corresponding source code.

Revision History

Date of Change	Responsible	Version	Description of change
25.05.2016	Stuart Ashford	Version 1.0	Creation
27.09.2017	Stuart Ashford	Version 1.0 (3)	Added vetting of 3rd parties
4.12.2019	Stuart Ashford	Version 1.1	Revision of document
27.06.2022	Stuart Ashford	Version 1.2	Merge with Piano Analytics
24.10.2022	Stuart Ashford	Version 1.3	Revision of document
21.11.2022	Stuart Ashford	Version 1.3 (2)	Added SDLC and privileged account details