Security Documentation Overview

Version number	4.0
Last Approved	Mar 2, 2026
Classification	PUBLIC

Applicability

These policies apply to all Company systems and personnel inclusive of Central Services (HR, IT, Finance, Legal, and Facilities) and the Company's Software-as-a-Service ('SaaS') business units:

- Affirmity
- Breezy
- Bridge
- Open LMS
- PeopleFluent
- Preloaded
- Rustici Software
- Watershed Systems

Systems shall be governed by Security policies outlined as part of the this Overview. Hosting systems may require varying or more rigorous security requirements, which may necessitate prevailing Hosting-specific policies.

Purpose

The objective of the Security Documentation Overview is to provide a comprehensive index and provide policy control guidelines.

This overview will act as a *Master Table of Contents*, outlining all Company Security and Privacy polices, each policy will be reviewed at least annually, with its version and changes noted by the author in that policy's Change log.

ISO 27001:2022 Control 7.5.2

When creating and updating documented information the organization shall ensure appropriate:
a) identification and description (e.g. a title, date, author, or reference number);
b) format (e.g. language, software version, graphics) and media (e.g. paper, electronic); and
c) review and approval for suitability and adequacy.

ISO 27001:2022 Control 7.5.3

Documented information required by the information security management system and by this document shall be controlled to ensure:

a) it is available and suitable for use, where and when it is needed; and

b) it is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).

For the control of documented information, the organization shall address the following activities, as applicable:

c) distribution, access, retrieval and use;

d) storage and preservation, including the preservation of legibility;

e) control of changes (e.g. version control); and

f) retention and disposition.

Documented information of external origin, determined by the organization to be necessary for the planning and operation of the information security management system, shall be identified as appropriate, and controlled.

NOTE Access can imply a decision regarding the permission to view the documented information only, or the permission and authority to view and change the documented information, etc.

ISO 42001:2023 Control 7.5.3

Documented information required by the AI management system and by this document shall be controlled to ensure:

a) it is available and suitable for use, where and when it is needed;

b) it is adequately protected (e.g. from loss of confidentiality, improper use or loss of integrity).

For the control of documented information, the organization shall address the following activities, as applicable:

— distribution, access, retrieval and use;

— storage and preservation, including preservation of legibility;

— control of changes (e.g. version control);

— retention and disposition.

Documented information of external origin determined by the organization to be necessary for the planning and operation of the AI management system shall be identified as appropriate and controlled.

Master Table of Contents

The Acceptable Use Policy (AUP) stipulates constraints and practices that Company Personnel must abide by while accessing and using The Company's resources and data, or client data. This policy covers areas which include but are not limited to: hardware, software, email and messaging, data storage, PII, internet, wireless networking, blogging, social media, and third party services.

Access Management Policy

This Access Management policy describes provisioning, management, monitoring, and de-provisioning of user accounts and privileges, operating under the principle of least privilege.

AI Policy

This AI Policy establishes criteria for adoption and use of artificial intelligence (AI) and machine learning (ML) models and making proper use of their results. AI and ML tools and services may include but are not limited to Customer Support & Chatbots (such as ChatGPT and Sentiment Analysis tools), Predictive Analysis tools (such as Churn Prediction or Demand Forecasting), Personalization tools (such as content recommendations and dynamic AI market condition analysis), Data Security tools (such as anomaly detection or fraud detection), Automation or Generative AI tools (such as Zapier or Copilot), and Natural Language Processors (NLP) (such as voice assistants or text analysis tools that analyze customer feedback).

Asset Management Policy

The Asset Management Policy defines roles and responsibilities for maintaining inventory of Company assets and managing the lifecycle of these assets.

Bring Your Own Device (BYOD) Policy

The Bring Your Own Device (BYOD) Policy defines terms for access Company systems using non-Company issued devices.

Business Continuity Planning and Disaster Recovery Policy

The Business Continuity Planning (BCP) and Disaster Recovery (DR) Policy defines the processes by which the Company maintains and tests risk-based resiliency plans for its business and systems.

Disaster Recovery (DR) addresses customer-facing continuity in its hosted systems and is inclusive of customer data.

This policy establishes principles and requirements to ensure that the risk of interruption to its business operations and SaaS services is maintained within tolerable levels that also align with its legal, regulatory, and contractual commitments. The Company will perform regularly scheduled BCP / DR testing to align the Company's capabilities with its risk posture.

Change Management Policy

This Change Management Policy intends to ensure that changes made to application code and relevant systems are subject to necessary and appropriate controls. Its purpose is threefold: it attempts to mitigate unexpected side-effects, the introduction of defects, and other negative effects of changes through due review; it increases awareness of changes across relevant teams; and it provides a record of changes made to systems and repositories in its scope, where possible. A standard set of minimum requirements are established for changes that are made to production systems and supporting infrastructure across the organization.

Client Data Privacy Compliance Policy

The Client Data Privacy Compliance Policy defines the Company's requirements for maintaining privacy compliance across all applicable laws, regulations and client commitments.

Data Backup Policy

The Data Backup Policy provides minimal guidance on the retention, duration and the backup and restoration methodologies used to securely store copies of systems in a manner that protects the privacy of data and the integrity of copies of the SaaS hosting infrastructure and client data. These guidelines meet industry best practices and ensures The Company retains 'safe' immutable backup copies to prevent data loss due to physical destruction or retroactive modification. The disposition of backup media is covered by the Data Retention, Destruction and Disposal Policy.

Data Classification and Handling Policy

The Data Classification and Handling Policy defines the levels of data classification and the types of information that fall into each category. This policy also defines the appropriate level of security and access controls for each classification and outlines handling requirements, including client data access and manipulation provisions.

Data Encryption Policy

The Data Encryption Policy defines requirements for the use of encryption technologies within the Company.

Data Retention, Destruction and Disposal Policy

The Data Retention, Destruction and Disposal Policy defines how long the Company retains data and how it sanitizes, deletes, and disposes of data related to its Client facing services and physical hardware used in the hosting of these services.

Data Retention (non-client) Policy

The Non-Client Data Retention Policy outlines the Company's standards regarding the data retention of non-client data only.

Encryption Key Management Policy

The Encryption Key Management Policy defines the requirements used to control public and private encryption keys and defines their lifecycle, inclusive of creation, usage, storage, and deletion.

End-of-Life Software Policy

This End-of-Life (EoL) Software Policy outlines the guidelines and procedures for managing software as it approaches the end of its lifecycle and provides guidelines on mandatory maintenance and updates until it's retired.

Information Security Statement

The Information Security Statement provides a framework that will ensure the protection of The Company's assets and its customers' data and privacy. The statement outlines the Information Security Mission and Strategy, as well as the security roles and responsibilities.

Internal Audit and Compliance Policy

The Internal Audit and Compliance Policy establishes the use of audits and/or other evaluation techniques to ensure effective oversight of controls performance.

The Company shall establish a process to ensure that our operations and products are in compliance with applicable laws, regulations, policies, procedures, and the code of conduct.

Password Policy

The Password Policy stipulates constraints and practices that Personnel must abide by while creating and managing passwords.

Physical Security Policy

The Physical Security Policy defines The Company's security controls for offices and data centers and aligns these controls to the principle of least access for all persons visiting our locations. The policy also defines tracking and documentation requirements for all facility access.

Risk Management Policy

We recognize that the Company is exposed to various risks due to the nature of our operations. This policy provides a framework for managing those risks, ensuring the organization's continued success and viability.

Security Baselines Policy

The Security Baselines Policy defines minimally acceptable secure configuration standards applicable to all Company IT systems.

Secure Software Development (SDLC) Policy

The Secure Software Development (SDLC) Policy provides a documented description of how software is built and maintained, emphasizing privacy and security. It describes the various phases of the development process and activities performed during each phase, to the extent applicable.

Security Incident Response Plan

Security incidents present a threat to the confidentiality, integrity, and availability of the Company's systems and data. Successful mitigation of this threat requires not only a best practice approach to managing system vulnerabilities, but also swift and effective response to any security incidents.

The procedures defined in this document ensure that security incident affecting the Company are appropriately and consistently identified and handled.

Vendor Management Policy

This Vendor Management Policy establishes criteria for adoption and qualification of new vendors, evaluation of vendor performance and compliance, risk identification and mitigation, and termination of a vendor relationship.

Vulnerability Management Policy

The Vulnerability Management Policy defines the types of activities for regular vulnerability assessment of hosted / customer-facing systems. Internal vulnerability assessment activities and the time frames for each are defined, as is the use of independent parties for validation and verification. The policy also addresses patching requirements for third party components.

Additional Information - Continuity and Oversight

The following statements on *Oversight, Disciplinary Actions*, *Exceptions*, and *Questions* contained within this policy are applicable and enforced throughout the above listed policies, statements, and measures.

Executive Security Steering Committee Oversight

Changes to these policies will be communicated to the Executive Security Steering Committee as necessary.

Disciplinary Actions

Violation of the above policies may result in disciplinary action which may include termination of employment, dismissal, or suspension. Additionally, personnel who violate this policy may be subject to civil and criminal prosecution.

Exceptions

The Company's Information Security Policies (and the procedures developed and approved to implement them) should be applicable in most circumstances. However, the Company recognizes that some circumstances require deviations from standard policies and procedures. Exceptions must be rare and must be based on sound rationale. An exception register will be maintained by the Security Team and will be reviewed at least annually.

Recent Acquisitions

Products or companies acquired within the last 6 months that otherwise would be in scope must develop a transitionary plan and may continue to operate under their prior information security policies so long as they do not conflict with the spirit of these documents. The acquired product(s) must transition to this plan, either by adoption as it stands or by proposing changes to this policy that meet the spirit and intent and will not jeopardize compliance of other product lines. After a period of six months, any acquired products or companies will fall within the scope of the most recent revision of this policy.

Questions

Any questions about this document should be directed to the GRC Team.

Document control

This policy is only controlled in its live, digital format. Any other format or export of this policy is an uncontrolled version of this document

Document Owner	Art Machado	
Author(s)	Art Machado, Angelina Kilmer, Paul Gordon	
Required Approver(s) and Approval Date	Art Machado - VP Information Security	Mar 2, 2026
Review cycle	ANNUAL	
Next review date	Mar 2, 2027	

Version History

Date	Author(s)	Version	Changes
Mar 2, 2026	Angelina Kilmer Paul Gordon	4.0	Annual Review
Aug 12, 2025	Art Machado Angelina Kilmer Paul Gordon	3.3	Streamlined language, updated GRC contact email, and automated excerpts.
Apr 9, 2025	Paul Gordon	3.2	References to ISO 42001
Mar 7, 2025	Paul Gordon	3.1	Removal of duplicate paragraph
Feb 25, 2025	Art Machado Angelina Kilmer Paul Gordon	3.0	Annual review
Nov 1, 2024	Angelina Kilmer	2.5	Changed Policy classification from Confidential to Public
May 9, 2024	Sarah Zwicker Art Machado	2.4	Added LTG Central Services to Applicability statement
Mar 13, 2024	Art Machado Sarah Zwicker Paul Gordon	2.3	Annual review; update Company legal entity and scoping considerations; inclusion of IT policies
Mar 11, 2024	Sarah Zwicker	2.2	Updated Disciplinary Action language
Jan 16, 2024	Sarah Zwicker	2.1	Moved to Global Policy Register, updated applicability statement
Apr 14, 2023	Sarah Zwicker Art Machado	2.0	Applicability statement clarifications
Feb 23, 2023	Sarah Zwicker	1.9	Annual review + logo change
Nov 15, 2022	Sarah Zwicker	1.8	Added “Bridge Advance Video” to Instilled’s name
Apr 22, 2022	Sarah Zwicker	1.7	Additions of PF-ISMS-0019, PF-ISMS-0020, PF-ISMS-0021; Added Privacy considerations

Mar 16, 2022	Sarah Zwicker Art Machado	1.6	Annual Review; Changes to Applicability to reflect acquisitions; Title change for VP InfoSec
Nov 18, 2021	Sarah Zwicker	1.5	Changed name of PF-ISMS-0008 after policy was modified to include Data Retention
Nov 12, 2021	Sarah Zwicker	1.4	Added PF-ISMS-0018
Jul 28, 2021	Sarah Zwicker	1.3	Updated Policy Titles
Apr 9, 2021	Sarah Zwicker	1.2	Inclusion of applicable ISO controls
Mar 15, 2021	Sarah Zwicker	1.1	Changed owner Changed ISMS Required Approvers and Dates Deprecation of PF-ISMS-0012, and is now addressed within PF-ISMS-0009 Depreciation of PF-ISMS-0015, and is now included within PF-HOST-0015
Feb 2, 2021	Sarah Zwicker Art Machado	1.0	Original version