



THE STANDARD GROUP

Hosted User Applications Policy

Effective 01/01/2026

The Standard Group			
Organization Information Technology		Type Policy	
Subject Hosted Application Policy		Effective Date 01.01.2026	Replaces New
Distribution TBD	Issued By Information Security	Approvals Executive Committee	Next Review 12.1.2026

Table of Contents

- 1. Purpose of this Document 3
- 2. Company and Service Overview 3
- 3. System Boundaries 3
 - 3.1 In Scope..... 3
 - 3.2 Out of Scope 4
- 4. Significant System Components 4
 - 4.1 Infrastructure 4
 - 4.2 Software..... 4
 - 4.3 People 5
 - 4.4 Procedures 5
 - 4.5 Data..... 6
- 5. Purpose and Design of the System 6
 - 5.1 Purpose 6
 - 5.2 Design Principles 6
 - 5.3 High-Level Architecture 7
- 6. Commitments to Customers..... 7
- 7. How This Description Is Made Available..... 7

Document Revision History

Revision	Changes/corrections made from the previous version	Effective Date
1.0	New Release	1/1/2026

Audience: Authorized external users and customers of The Standard Group.

1. Purpose of this Document

This document describes the hosted user applications operated by The Standard Group (TSG) and made available to customers. It defines the boundaries of the system, identifies significant components, and describes the purpose and design of the services. It is made available to authorized external users upon request and via our customer websites and refreshed at least annually or upon material change.

2. Company and Service Overview

The Standard Group provides hosted applications to support our print, marketing and file-transfer workflows. Our hosted user applications are:

- **Pageflex** — a web-to-print and variable-data publishing platform used by customers to create, customize, and order branded print and marketing materials through templated storefronts.
- **Custom Web Storefront** — customer-branded e-commerce storefronts, typically built on and integrated with Pageflex, that allow end users to browse catalogs, personalize products, and place orders.
- **Serv-U FTP** — a hosted managed file transfer service enabling customers to securely exchange files with [Company Name] and their own end users via FTP, FTPS, SFTP, and HTTPS.
- **Insite** — a hosted [Kodak Insite Prepress Portal / equivalent] service that gives customers and their clients web-based access to review, approve, and manage print production jobs and related assets.
- **MailTracker Pro** — a hosted mail-tracking application that provides customers visibility into USPS delivery status for direct-mail campaigns.

Customers access these applications over the public internet via authenticated web and, where applicable, file-transfer protocol interfaces.

3. System Boundaries

3.1 In Scope

The system described here includes:

- The Pageflex platform and any Custom Web Storefronts built on it
- The Serv-U FTP hosted file transfer service
- The Insite prepress portal service
- The MailTracker Pro application
- Customer, order, artwork, job, file, and mail-tracking data stored in the production environment
- Authentication and authorization services supporting the above applications

- Production infrastructure hosted in Lititz , PA datacenter.
- Logging, monitoring, backup, and alerting systems used to operate the above
- Internal administrative tools used by The Standard Group personnel to configure, support, and operate the services
- Personnel, policies, and procedures directly supporting the operation, security, and availability of the services

3.2 Out of Scope

The following are not part of the system boundary:

- Customer-managed endpoints, browsers, FTP clients, and networks
- Customer-hosted or customer-managed integrations that connect to the services (e.g., customer ERP, MIS, or DAM systems)
- Physical print production equipment and post-press operations, except as they consume data from the hosted applications
- USPS systems and other postal or carrier networks referenced by MailTracker Pro
- TSG corporate IT systems not involved in production service delivery (e.g., internal HR, finance, corporate email)
- Sub-processor infrastructure beyond the contracted service interface (see Section 6)

4. Significant System Components

The system is described using the five component categories in the AICPA Trust Services Criteria.

4.1 Infrastructure

- **Hosting environment:** Located in the Print and Technology facility in Lititz, PA.
- **Network:** Fortinet perimeter firewalls, load balancers, VPN for administrative access, segmented VLANs / VPCs separating production, management, and corporate traffic.
- **Servers:** VMware / Windows Server hosts running application, database, and file-transfer workloads
- **Databases:** Microsoft SQL Server, MySQL supporting Pageflex, Insite, and MailTracker Pro
- **File storage:** Secure SAN / NAS / object storage for artwork, job files, PDFs, and transferred files
- **Backup infrastructure:** Veeam Backup with File Replication

4.2 Software

- **Pageflex** (web-to-print platform) and Custom Web Storefront front-ends built on it
- **Serv-U MFT / Serv-U FTP Server** for managed file transfer
- **Insite** prepress portal software
- **MailTracker Pro** application

- Supporting software: web servers ([IIS / Apache / nginx]), database engines, operating systems, anti-malware, backup software, monitoring agents
- Administrative tooling used by TSG staff for tenant provisioning and support

4.3 People

Roles with responsibilities for the system include:

- **Executive leadership** — accountability for security, availability, and confidentiality commitments
- **IT / Systems Administration** — operates infrastructure, servers, patching, backups
- **Application Administration** — configures and supports Pageflex, Insite, Serv-U, and MailTracker Pro tenants
- **Development** — maintains Custom Web Storefronts and any internally developed integrations
- **Security / Compliance** — maintains policies, monitors controls, coordinates audits and incident response
- **Customer Support** — assists customers and escalates production issues
- **Prepress / Production liaison** — coordinates hand-off from Insite/Pageflex into print production (interface only; production itself is out of scope)

NOTE: Access to production systems is restricted to personnel with a documented business need.

4.4 Procedures

Documented procedures govern:

- Change management and application/software deployment
- Storefront provisioning and customer onboarding
- Access provisioning, periodic review, and de-provisioning
- Incident detection, response, and post-incident review
- Vulnerability management and patching for OS, database, and application layers
- Backup, restoration testing, and disaster recovery
- File-transfer account management for Serv-U (creation, expiration, credential rotation)
- Vendor and sub-processor risk management
- Data retention and secure disposal of customer artwork, files, and mail data

4.5 Data

- **Customer artwork and job files** — PDFs, images, templates, and production files handled by Pageflex, Custom Web Storefronts, and Insite
- **Order and transaction data** — orders placed through Pageflex and Custom Web Storefronts
- **Transferred files** — files uploaded to and downloaded from Serv-U FTP
- **Mail campaign and tracking data** — mail-piece records and delivery scan data in MailTracker Pro
- **User account and authentication data** — user identifiers, hashed credentials, session information
- **Operational data** — system logs, access logs, monitoring metrics, audit trails
- **Configuration data** — tenant, storefront, workflow, and integration settings

Data is encrypted in transit (TLS 1.2 or higher; SFTP/FTPS for file transfer) and at rest (full-disk / database TDE / object-storage encryption).

5. Purpose and Design of the System

5.1 Purpose

The hosted applications exist to enable customers to run branded print and marketing operations, exchange production files securely, coordinate prepress approval workflows, and track direct-mail delivery. The system is designed to meet commitments made to customers in Master Service Agreements, order forms, and public documentation regarding security, availability, and confidentiality of customer data.

5.2 Design Principles

The system is designed around:

- **Tenant isolation** between customer storefronts, Insite sites, Serv-U accounts, and MailTracker Pro instances
- **Least-privilege access** for both external users and internal personnel
- **Defense in depth** across network, host, application, and data layers
- **Encryption by default** for data in transit and at rest
- **Observability** through centralized logging, monitoring, and alerting
- **Controlled change management** with peer review and testing before production deployment
- **Redundancy and recoverability** through Veeam backups and server HA / failover approach, sized to meet availability commitments

5.3 High-Level Architecture

Customers reach the applications through the public internet. Web traffic for Pageflex, Custom Web Storefronts, Insite, and MailTracker Pro terminates at load balancers or reverse proxies in the production perimeter, which forward requests to the application servers. Application servers authenticate users, apply tenant scoping, and read/write to databases and file storage in a segmented production network. Serv-U FTP exposes SFTP/FTPS/HTTPS endpoints for file transfer, with per-customer accounts and directory isolation. All administrative access to production occurs through [bastion / VPN + MFA]. Access, authentication, and administrative actions generate logs shipped to a centralized logging system.

6. Commitments to Customers

We commit to customers, through contracts and public documentation, to:

- Protect customer data through the controls described above
- Maintain [target availability, e.g., 99.9%] for the production applications
- Notify customers of security incidents affecting their data in accordance with contractual and legal obligations
- Provide the ability for customers to retrieve and, upon request, delete their data in accordance with retention terms

7. How This Description Is Made Available

This System Description is published on our customer-facing websites and is made available to authorized external users on an ongoing basis. It is communicated through:

- Direct communication from Customer Success and Account Management upon request
- Notifications to customers when material updates are published