TIDEWELL FINANCIAL

Technology Governance Program

Software Asset and License Management Standard

Standard No. TGP-STD-350

Version 1.1 | Effective September 1, 2026

Portfolio writing sample by David Parker Jr. Tidewell Financial is a fictional organization; all names, document numbers, and requirements in this document are invented for illustration.

Contents

1 Purpose
2 Scope and Authority
3 Adherence Reporting
4 Compliance
5 Exceptions and Risk Acceptance
6 References
7 Standard
    7.1 Software Inventory
    7.2 Approved Software Catalog
    7.3 Acquisition
    7.4 License Compliance
    7.5 Reclamation and Renewal
    7.6 Unauthorized and End-of-Support Software
    7.7 Monitoring and Reporting
8 RACI Matrix
9 Terms and Definitions
10 Reviewers and Approvers
11 Revision History
Appendix A Software Lifecycle Status Definitions

1 Purpose

This Standard sets the requirements for tracking, acquiring, licensing, and retiring software used by Tidewell Financial. Following it keeps the organization within the terms of its software contracts, avoids paying for licenses that are not used, and removes software that is unauthorized or no longer receives security updates.

2 Scope and Authority

This Standard is issued under the authority of the *Technology Governance Policy (TGP-POL-100)*. It applies to all software used to conduct Tidewell Financial business, whether installed on Tidewell-owned or managed devices, hosted in Tidewell-managed cloud environments, or provided as a subscription service (SaaS). It applies to all employees, contractors, and third parties who request, buy, install, or manage that software.

Physical hardware assets are governed by the Hardware Asset Management Standard (TGP-STD-355). Software developed in-house is out of scope except for the third-party components it includes.

3 Adherence Reporting

The Standard owner must be able to show that the requirements in Section 7 are being met. The SAM Office will test the evidence in Figure 1 each quarter and report results to the Technology Governance Committee.

Figure 1. Adherence evidence

Requirement area	Evidence tested
Software inventory (7.1)	Discovery coverage report shows at least 98% of managed endpoints and servers reported inventory in the past 7 days; SaaS reconciliation is on file for each month in the period.
Approved software catalog (7.2)	Sample of installed titles shows each has a catalog entry and a lifecycle status, and that no Prohibited title is present.
Acquisition (7.3)	Sample of software purchases shows each was made through Procurement and its entitlement record was entered within 10 business days.
License compliance (7.4)	Signed reconciliation for each top-20 vendor for the quarter, with any shortfall resolved within 30 days.
Reclamation and renewal (7.5)	Renewal notices were issued 120 days ahead and owner decisions were recorded at least 60 days before each renewal date.
Unauthorized and end-of-support software (7.6)	Removal tickets for unauthorized installs closed within the required time; retirement plans or approved exceptions exist for all end-of-support titles.

4 Compliance

All software introduced after this Standard takes effect must meet its requirements before it is deployed. Software already in use must also comply. Where a title or process does not comply, the

Software Owner must submit a remediation plan to the SAM Office within 30 days, listing the actions, owners, and target dates needed to reach compliance.

5 Exceptions and Risk Acceptance

When a requirement cannot be met, the Software Owner must request an exception through the Technology Risk exception process. Each request must describe:

- the requirement that cannot be met and why;
- the compensating controls in place, such as network isolation for unsupported software;
- the plan and target date for reaching compliance.

Exceptions are granted for no more than 12 months. A Senior Director or above who is accountable for the affected business function must accept the residual risk in writing.

6 References

This Standard must be read and maintained in conjunction with the following documents.

Tidewell Financial documents

- TGP-POL-100 Technology Governance Policy
- TGP-STD-310 IT Change Management Standard
- TGP-STD-355 Hardware Asset Management Standard
- PROC-POL-020 Procurement Policy

External frameworks

- ISO/IEC 19770-1, IT asset management systems
- NIST SP 800-53 Rev. 5, controls CM-8 (System Component Inventory), CM-10 (Software Usage Restrictions), and CM-11 (User-Installed Software)
- CIS Critical Security Controls v8, Control 2 (Inventory and Control of Software Assets)

7 Standard

7.1 Software Inventory

7.1.1 All installed software and all SaaS subscriptions used for Tidewell Financial business must be recorded in the software asset repository.

7.1.2 IT Operations must run automated discovery on all managed endpoints and servers at least daily. The SAM Office must reconcile SaaS subscriptions monthly against accounts payable records and single sign-on application logs.

7.1.3 Each software title must have a named Software Owner. When a Software Owner leaves their role, their leader must assign a new owner within 30 days.

7.2 Approved Software Catalog

7.2.1 The SAM Office must maintain a catalog of software titles and assign each one a lifecycle status as defined in Appendix A.

7.2.2 Only software with a status of Approved, or Restricted with Software Owner approval, may be installed in production.

7.2.3 A new title must complete security, architecture, and procurement review before it is given Approved status. Deploying it to production must follow the IT Change Management Standard (TGP-STD-310).

7.3 Acquisition

7.3.1 Software, including free trials that convert to paid subscriptions, must be acquired through Procurement. Software must not be bought with personal funds or expensed.

7.3.2 Before a new purchase, the SAM Office must confirm that no unused licenses for the same product are available to reassign.

7.3.3 The SAM Office must enter the entitlement record, including the contract, quantity, license metric, term, and renewal date, within 10 business days of contract execution.

7.4 License Compliance

7.4.1 The SAM Office must reconcile deployments against entitlements each quarter for the 20 vendors with the highest annual spend, and at least annually for all other vendors. The Software Owner must sign off on each reconciliation.

7.4.2 Any shortfall identified in a reconciliation must be resolved within 30 days, either by removing installations or by acquiring additional licenses.

7.4.3 Any request from a vendor to audit software use must be sent to the SAM Office and Legal within two business days of receipt. No one may provide usage data to a vendor or its auditor without approval from Legal.

7.5 Reclamation and Renewal

7.5.1 Licenses that have not been used for 90 days must be reclaimed unless the Software Owner documents a business need to keep them.

7.5.2 The SAM Office must notify the Software Owner at least 120 days before a contract renewal date. The Software Owner must record a decision to renew, resize, or cancel at least 60 days before that date.

7.6 Unauthorized and End-of-Support Software

7.6.1 Software with a status of Prohibited, or with no catalog entry, must be removed within five business days of detection. If Information Security determines it presents an active security risk, it must be removed or isolated within 24 hours.

7.6.2 Where a vendor has announced an end-of-support date, the SAM Office must change the title’s status to Retiring at least 12 months before that date, and the Software Owner must submit an upgrade or retirement plan.

7.6.3 Software that remains in use after its end-of-support date requires an approved exception under Section 5.

7.7 Monitoring and Reporting

7.7.1 The SAM Office must report the following metrics to the Technology Governance Committee each quarter: inventory coverage, license position for the top 20 vendors, savings from reclaimed and cancelled licenses, unauthorized installations detected and removed, and end-of-support titles still in use.

8 RACI Matrix

Figure 2 identifies who is Responsible, Accountable, Consulted, and Informed for each section of this Standard.

Figure 2. Roles and responsibilities

Section	Software Owner	SAM Office	Procurement	Info Security	IT Operations
7.1 Software Inventory	C	A/R	I	C	R
7.2 Approved Software Catalog	R	A	I	C	I
7.3 Acquisition	R	C	A	I	I
7.4 License Compliance	R	A	C	I	C
7.5 Reclamation and Renewal	A	R	C	I	R
7.6 Unauthorized and End-of-Support Software	A	C	I	R	R
7.7 Monitoring and Reporting	I	A/R	I	C	I

R = Responsible A = Accountable C = Consulted I = Informed

9 Terms and Definitions

Term	Definition
End of support	The date after which a vendor no longer provides security updates for a software version.
Entitlement	The rights Tidewell Financial has purchased to use a software product, as defined by the contract, quantity, license metric, and term.
License metric	The unit by which use of a product is counted, such as per user, per device, or per processor core.
Reclamation	Removing an unused license from one user or device so it can be reassigned or retired.
SAM Office	The Software Asset Management Office, which owns this Standard and the software asset repository.

Term	Definition
Software asset repository	The system of record for software inventory, catalog entries, and entitlement records.
Software Owner	The person accountable for a software title's business use, cost, and lifecycle.
True-up	A periodic payment to a vendor to cover use beyond the licenses originally purchased.

10 Reviewers and Approvers

Role	Title
Standard Owner	Manager, Software Asset Management Office
Reviewer	Director, Strategic Sourcing
Reviewer	Senior Manager, Information Security
Reviewer	Associate General Counsel, Technology Contracts
Approver	Chief Technology Officer

11 Revision History

Date	Version	Summary of change	Updated by	Approved by
09/02/2025	1.0	Initial release.	SAM Office	CTO
08/10/2026	1.1	Added SaaS reconciliation (7.1.2) and free-trial conversions (7.3.1). Added Legal approval for vendor audit data (7.4.3).	SAM Office	CTO

Appendix A Software Lifecycle Status Definitions

Status	Meaning	Installation allowed
Approved	Reviewed and supported for general use.	Yes
Restricted	Approved for named roles or use cases only, often because of cost or data sensitivity.	With Software Owner approval
Under Review	Evaluation is in progress.	Non-production evaluation only
Retiring	Scheduled for removal; a replacement or exit date has been set.	No new installations
Prohibited	Must not be used because of security, legal, or licensing risk.	No; remove if found