TOVUTI LMS

Customer Secure Configuration Guide

FedRAMP Moderate Impact Level

NIST SP 800-53 Rev. 5 | AWS (US) | Knox Boundary

Classification Public	**Version** 1.1.0
Effective Date June 1st, 2026	**Review Cycle** Annual / Post-Change

Table of Contents

Table of Contents 2
1. Purpose and Scope 4
1.1 Document Conventions 4
1.2 Related Documents 4
3. Pre-Configuration Prerequisites 5
3.1 Governance & Authorization 5
3.2 Required Integrations Before Go-Live 5
4.1 Single Sign-On (SSO) Configuration 6
4.1.1 Configuration Steps 6
4.2 Multi-Factor Authentication (MFA) 6
4.3 Role-Based Access Control (RBAC) and Least Privilege 7
4.3.1 Mandatory RBAC Configuration 7
4.4 Account Lifecycle Management 7
4.4.1 Automated Account Management 8
4.4.2 Account Management Procedures 8
5. Tenant Hardening and Security Configuration 8
5.1 System Use Notification (Federal Login Banner) 8
5.1.1 Enforcing External Authentication 8
5.1.2 FedRAMP-Approved Banner Language 9
5.2 Session Management 9
5.3 Least Functionality — Feature Minimization 10
5.3.1 Features to Evaluate for Disabling 10
5.4 Email Notification Configuration 11
5.5 Acceptable Use Policy (AUP) Enforcement 11
6. Audit Logging and Continuous Monitoring 11
6.1 Audit Log Architecture 12
6.2 SIEM Integration (REQUIRED) 12
6.3 Security Configuration Baseline 12
7. Incident Response 13
7.1 Customer Incident Response Responsibilities 13
7.2 Reporting Contacts 13
8. Security Awareness and Training 13
8.1 Training Requirements 14
9. Customer Configuration Quick Reference 14
10. Continuous Monitoring and Periodic Review Schedule 15
11. Document Control and Revision History 16

1. Purpose and Scope

This Customer Secure Configuration Guide (CSCG) provides mandatory configuration requirements and actionable guidance for organizations deploying Tovuti LMS within the FedRAMP Moderate authorized boundary, hosted on the Knox AWS (US) infrastructure. It is intended for Information System Security Officers (ISSOs), system administrators, and authorizing officials responsible for configuring and maintaining a compliant Tovuti tenant.

The guide delineates customer responsibilities under the Shared Responsibility Model defined in the Tovuti System Security Plan (SSP) and Customer Responsibility Matrix (CRM). It aligns with NIST SP 800-53 Rev. 5 Moderate baseline controls and the FedRAMP Secure Configuration Guide published at fedramp.gov.

> **Scope of Application**
> This guide applies to all Federal agencies, contractors, and organizations operating within the Tovuti FedRAMP Knox environment at the Moderate impact level. Settings described herein are mandatory unless a formal deviation is approved by your Authorizing Official (AO) and documented in a Plan of Action and Milestones (POA&M).

1.1 Document Conventions

Throughout this guide:

- **MUST / REQUIRED:** The configuration is mandatory for FedRAMP Moderate compliance. Failure constitutes a security finding.
- **SHOULD / RECOMMENDED:** The configuration is a best practice strongly recommended by Tovuti and FedRAMP guidance.
- **MAY / OPTIONAL:** The configuration is discretionary and may be enabled based on mission need.
- **Customer:** Refers to the agency, contractor, or organization operating the Tovuti tenant.
- **CSP:** Cloud Service Provider — Tovuti, operating within the Knox AWS GovCloud boundary.

1.2 Related Documents

- Tovuti System Security Plan (SSP) — FedRAMP Rev. 5 Moderate
- Tovuti Customer Responsibility Matrix (CRM)
- NIST SP 800-53 Rev. 5 — Security and Privacy Controls
- NIST SP 800-63-3 — Digital Identity Guidelines
- FedRAMP Secure Configuration Guide — https://www.fedramp.gov/docs/rev5/balance/secure-configuration-guide/
- Tovuti Help Center — https://help.tovutilms.com
- Tovuti API Documentation — https://api.tovuti.com

Tovuti LMS operates under a shared responsibility model. Tovuti (the CSP), Knox on AWS (Tovuti's managed infrastructure provider), and the Customer each bear distinct compliance obligations. Understanding this division is foundational to achieving and maintaining an Authority to Operate (ATO).

Knox / AWS	Tovuti LMS (CSP)	Customer

Customer Responsibility Matrix (CRM)

The full list of 325+ controls and their assignments is formally captured in the Tovuti CRM. Customers MUST execute and maintain the CRM as a binding commitment prior to system go-live. This guide focuses on the highest-priority customer-owned and shared configurations. Reference your CRM for the complete control inventory.

3. Pre-Configuration Prerequisites

Before configuring your Tovuti tenant, complete the following prerequisites. These steps establish the governance baseline required for all subsequent security configurations.

3.1 Governance & Authorization

- **Appoint an ISSO:** Identify your Information System Security Officer. This individual is the primary point of contact for the security authorization package, manages CRM obligations, and interfaces with your Authorizing Official (AO).
- **Data Categorization:** Formally categorize information to be processed in Tovuti LMS. Document CUI, PII, and any PHI per NIST FIPS 199. Confirm the Moderate impact level is appropriate for your data.
- **ATO Determination:** Determine whether your agency requires an independent ATO or whether you will leverage Tovuti's existing FedRAMP authorization package via an Agency ATO acceptance.
- **Execute the CRM:** Formally sign off on the Customer Responsibility Matrix, acknowledging which of the 325+ controls fall within your scope.
- **Tenant Provisioning:** Submit a change management ticket to Tovuti DevOps to provision your isolated instance in the Knox AWS GovCloud boundary. Do NOT self-provision.

3.2 Required Integrations Before Go-Live

- **Identity Provider (IdP):** Your SSO integration MUST be live and tested before any users are onboarded. Accepted IdPs include Okta, Azure AD, Ping Identity, and other SAML 2.0 / OIDC-compliant providers.
- **SIEM Integration:** Audit log streaming to your agency SIEM (e.g., Splunk, DataDog) MUST be configured before go-live to satisfy continuous monitoring requirements.

- **Incident Response Contacts:** Verify current POCs in your Incident Response plan. Ensure the Tovuti/Knox security team emergency contact details are current.

IAM controls represent the highest-priority customer configuration domain. Misconfiguration in this area constitutes the most significant risk to the confidentiality and integrity of Federal data processed within Tovuti LMS.

4.1 Single Sign-On (SSO) Configuration

NIST Controls: IA-2, IA-2(1), IA-2(2), IA-2(12), IA-8, IA-8(1)

> **REQUIRED**
> All authentication to the Tovuti FedRAMP instance MUST occur through your agency Identity Provider (IdP) via SAML 2.0 or OIDC. Direct local username/password login MUST be disabled after SSO is configured and verified.

Tovuti leverages Okta, a FedRAMP Moderate authorized service, for the underlying SSO and authentication layer. Your agency's IdP federates with Okta to provide seamless authentication. The customer is fully responsible for configuring and enforcing the IdP side of this integration.

4.1.1 Configuration Steps

1. Navigate to Admin Settings > Security > Single Sign-On in your Tovuti admin console.
2. Select your IdP protocol: SAML 2.0 (preferred for PIV/CAC) or OIDC.
3. Import your IdP metadata XML or enter the IdP Entity ID, SSO URL, and certificate.
4. Map IdP attributes to Tovuti user profile fields (email, first name, last name, groups).
5. Test SSO authentication with at least one privileged and one non-privileged account.
6. Disable local login: Contact Tovuti support to enforce SSO-only access for your tenant.

4.2 Multi-Factor Authentication (MFA)

NIST Controls: IA-2(1), IA-2(2), IA-2(6), IA-2(8), IA-2(12)

> **REQUIRED — PIV/CAC Enforcement**
> For Federal agency users, MFA MUST be enforced using PIV/CAC or FIPS 140-2 validated hardware tokens configured in your IdP. Software-based TOTP alone does not satisfy IA-2(12) for Federal personnel. FIPS-compliant MFA must be configured on the IdP side before user onboarding.

Account Type	Required MFA Method	Minimum Password Length (if local fallback)
Privileged (Admin)	PIV/CAC or FIPS 140-2 hardware token (REQUIRED)	14 characters (emergency/break-glass only)

Account Type	Required MFA Method	Minimum Password Length (if local fallback)
Non-Privileged (Standard User)	PIV/CAC or FIPS-compliant MFA via IdP	12 characters minimum (Okta enforced)
Emergency / Break-Glass	Local login permitted only — 14-char password, dual-person control required	14 characters — all printable ASCII

4.3 Role-Based Access Control (RBAC) and Least Privilege

NIST Controls: AC-2, AC-3, AC-5, AC-6, AC-6(1), AC-6(2), AC-6(5), AC-6(7)

Tovuti provides one (1) functional administrator account upon tenant provisioning. The customer is fully responsible for creating all subsequent accounts and managing role assignments for the duration of the authorization period.

4.3.1 Mandatory RBAC Configuration

- **Document all roles:** Before user onboarding, create a Role Definition Matrix that maps each Tovuti role (Learner, Instructor, Manager, Administrator) to your organization's job functions. This document must be maintained and reviewed quarterly for privileged accounts, annually for non-privileged accounts.
- **Enforce least privilege:** Assign users the minimum permissions required to perform their assigned duties. Do not use the Administrator role as a default. Create custom roles where the built-in roles are overly permissive.
- **Separate duties:** Ensure no single user account has the ability to both create content and approve/publish it without a second authorized approver (AC-5, Separation of Duties).
- **Review privileged accounts quarterly:** The FedRAMP Moderate baseline (AC-2(j)) requires quarterly review of all privileged access accounts. Document these reviews for your AO.
- **ITAR & CUI Content Management:** Verify that all CUI and ITAR-regulated materials are hosted strictly within the secure Tovuti LMS tenant boundary or other secure location.
- **Access Enforcement:** Configure explicit Role-Based Access Controls (RBAC) to ensure non-U.S. persons are completely blocked from discovering, searching for, or launching any ITAR-related courses or assets.

> **Account Management Timelines (FedRAMP Mandatory)**
> Disable accounts within 1 hour of discovering high-risk indicators (AC-2(13)). Notify account managers within 24 hours when accounts are no longer required. For terminated or transferred users, notification and disable action must occur within 8 hours. Temporary/emergency accounts must auto-disable after no more than 96 hours from last use (AC-2(2)).

4.4 Account Lifecycle Management

NIST Controls: AC-2, AC-2(1), AC-2(3), AC-2(4), AC-2(5), AC-2(7), AC-2(9), AC-2(12), AC-2(13)

4.4.1 Automated Account Management

Customers SHOULD implement automated account management through the Tovuti REST API or SSO group-to-role mapping. This ensures accounts are provisioned and deprovisioned in sync with your agency's authoritative source of identity (e.g., Active Directory, HR system).

4.4.2 Account Management Procedures

- Creation: Accounts require written approval from a designated account manager prior to provisioning. Document approval in your ticketing system.
- Modification: Role changes require approval at the same level as initial provisioning. Log all changes.
- Inactivity: Disable accounts inactive for 35 days or per your organization's policy, whichever is stricter.
- Termination: Disable immediately upon separation; remove within 24 hours. Recover all government-issued credentials and devices.
- Shared accounts: Prohibited except for technical necessity. If used, change credentials whenever a member leaves the group (AC-2(9), AC-2(k)).

5. Tenant Hardening and Security Configuration

5.1 System Use Notification (Federal Login Banner)

NIST Control: AC-8

> **REQUIRED**
> A compliant System Use Notification banner MUST be displayed to all users before they are granted access to the system. The banner must remain on screen until the user explicitly acknowledges it. This is a mandatory FedRAMP control verified during assessment.

To maintain compliance with mandatory FedRAMP and NIST access control standards, Tovuti MUST NOT be used as a standalone login interface. All users are required to authenticate through an approved Single Sign-On (SSO) or Identity Provider (IDP).

The System Use Notification (Federal Login Banner) is enforced at the IDP level. This ensures that users receive and acknowledge the mandatory legal notification prior to being granted access to the Tovuti environment.

5.1.1 Enforcing External Authentication

Since Tovuti does not feature a global "Disable Local Login" toggle, Administrators must ensure compliance by following these configuration guardrails:

1. **Enforce SSO-Only Workflows:** Do not provide learners with the standard Tovuti login URL (e.g., yourdomain.tovuti.io/login). Instead, all published access points, bookmarks, and navigation links must point to the **SSO-Enabled Deep Link** or the IDP-initiated login URL.
2. **Externalize the Banner:** Configure your agency's authorized IDP (Okta, Azure AD, etc.) to display the FedRAMP-approved banner text. The banner must require explicit acknowledgment before the IDP issues the SAML/OIDC assertion to Tovuti.
3. **Deprioritize Local Login UI:** * Navigate to **Admin > Portals > [Select Portal] > Details**.
    - Ensure the "Login Form" is removed from the landing page or replaced with a "Login with [Agency SSO]" button.
    - This ensures that the only visible path to entry for a user is through the compliant, banner-protected IDP.
4. **Credential Management:** To prevent "backdoor" local access, users should be provisioned via the SSO/JIT (Just-In-Time) process without a local Tovuti password. Without a local password, the Tovuti local login form is effectively disabled for those users.
5. **Verification:** Periodically audit the system to ensure that no "local-only" accounts exist for federal learners and that all successful logins are originating from the authorized SSO provider.

5.1.2 FedRAMP-Approved Banner Language

WARNING — U.S. GOVERNMENT SYSTEM

This is a U.S. Government information system, which includes: (1) this computer, (2) this network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only.

Unauthorized or improper use of this system is prohibited and may result in disciplinary action and/or civil and criminal penalties. By using this information system, you understand and consent to the following:

You have no reasonable expectation of privacy regarding any communication or data transiting or stored on this information system. At any time, the government may monitor, intercept, search, and seize any communication or data transiting or stored on this information system. Any communications or data transiting or stored on this information system may be disclosed or used for any U.S. Government-authorized purpose.

5.2 Session Management

NIST Controls: AC-11, AC-11(1), AC-12

Tovuti is configured to terminate application sessions after 15 minutes of inactivity at the platform level. However, the customer MUST also enforce session timeout at the IdP/SSO layer to ensure complete compliance.

- **IdP Session Timeout (REQUIRED):** Configure your IdP to enforce a maximum session lifetime of 15 minutes of inactivity. This must be set independently in your identity provider (e.g., Okta, Azure AD) and tested after configuration.
- **Device Lock (REQUIRED):** The agency's endpoint management policy (e.g., GPO, MDM) MUST enforce a 15-minute device lock timeout on any workstation used to access Tovuti LMS (AC-11).

- **Logon Attempt Limits:** configure IdP to lock accounts after 3 consecutive invalid login attempts within 15 minutes, with a 3-hour lockout or administrator unlock. Customers MUST ensure their IdP aligns with or is more restrictive than this threshold (AC-7).

5.3 Least Functionality — Feature Minimization

NIST Control: CM-7, CM-7(1)

Federal agencies MUST configure the Tovuti instance to enable only those features, integrations, and modules strictly required for mission accomplishment. Disabling unnecessary capabilities directly reduces the attack surface and is a core FedRAMP configuration requirement.

> **Practical Guidance**
> Begin with all optional features disabled. Enable each feature only after documented mission justification and approval by your ISSO. Review enabled features quarterly and disable any that are no longer in active use.

5.3.1 Features to Evaluate for Disabling

Review and disable the following unless there is a documented mission need:

Access & Authentication Control

- **Native Password Management:** Enforce SSO-only authentication; disable or hide native login fields and "Change Password" functionality to prevent bypass of centralized identity controls.
- **Guest / Anonymous Access:** Disable all "Public" visibility settings for catalogs, courses, and landing pages to ensure only authenticated users can view content.
- **User Directory / Member Search:** Disable the ability for users to search for or view profiles of other learners to prevent PII harvesting.

> **Important - Authentication**
> Because some features (like Native Authentication) cannot be technically deleted from the software's codebase, customers MUST implement "Compensating Controls." This includes using the Tovuti "Brand Identity" settings to hide UI elements and configuring "Global Redirects" to ensure users are automatically routed to the agency's authorized Identity Provider (IdP).

External Connectivity & Integrations

- **Third-Party Integrations:** Disable any non-authorized applications or "Marketplace" apps (e.g., Zapier, Salesforce) that are not within the authorized boundary.
- **Video Conferencing:** Disable integrations with external platforms that are not FedRAMP Moderate (Zoom, Teams, WebEx) if not required for synchronous instruction.
- **Corporate Whitelisting:** Explicitly add any domains (e.g., *.bizlibrary.com for bizlibrary) to the organization's local corporate network firewall, web proxy, and egress whitelist filters to permit inbound/outbound asset traffic.

- **Platform Exception Request**: Submit a formal technical service request to Tovuti DevOps to append the vendor's designated streaming domains to the tenant's environment-level Content Security Policy (CSP) allowed origins list.

- **External Notifications:** Disable third-party SMS or non-authorized email relay platforms to prevent data exfiltration.

Social & Collaboration Tools

- **Community & Forum Features:** Disable social walls, peer-to-peer discussions, and public forums to minimize the risk of unauthorized information sharing or lateral movement.
- **In-App Messaging:** Disable internal "Inbox" or chat features to prevent unmonitored communication and potential phishing vectors.
- **User-Generated Content (UGC):** Restrict or disable unrestricted file uploads by learners to prevent the introduction of malicious binaries or unvetted data.

Commerce & Data Privacy

- **E-commerce & Marketplace:** Disable all "Point of Sale," shopping carts, and payment gateway integrations (Stripe, PayPal) for internal-only mission sets.
- **Social Media Metadata:** Disable "Social Share" buttons and Open Graph metadata tags to prevent internal course information from being indexed by public crawlers.

5.4 Email Notification Configuration

> **Important — Email Compliance Gap**
> By default, Tovuti email notifications are NOT configured for FedRAMP compliance. Customer MUST review and configure all outbound email settings to ensure notifications do not transmit CUI outside the authorized boundary. Disable any notification that could route sensitive data through a non-FIPS-compliant email relay.

- **Review all email notification templates:** Ensure no CUI or PII is embedded in subject lines or email body content routed through external SMTP relays.
- **Configure SMTP:** If using a third-party SMTP provider, verify it is FedRAMP authorized or operates under a signed interconnection agreement.
- **Disable non-essential notifications:** Limit automated emails to operationally necessary events only.

5.5 Acceptable Use Policy (AUP) Enforcement

NIST Controls: PL-4, PS-6

Customers MUST ensure an organizational Acceptable Use Policy (AUP) is in place and aligned with the Federal login banner content. All users MUST formally acknowledge the AUP as a prerequisite to system access. Document AUP acknowledgments and retain records per AU-11 (minimum 1 year online, 7 years total).

6. Audit Logging and Continuous Monitoring

6.1 Audit Log Architecture

NIST Controls: AU-2, AU-3, AU-4, AU-6, AU-6(1), AU-9, AU-11, AU-12

Tovuti generates and retains audit logs for a minimum of seven (7) years in accordance with FedRAMP requirements. Ninety (90) days of logs are immediately accessible in the Tovuti admin interface. Logs beyond 90 days are archived in S3 and available upon request.

Log Type	CSP Retention	Customer Action Required
Application audit logs (LMS events)	7 years (90 days online, remainder S3 archive)	Stream to SIEM; manage retrieval requests for archived logs.
Infrastructure CloudTrail	7 days in DataDog, then S3 archive	Ingest via API if agency requires consolidated view.
Access logs (Okta/IdP)	90 days in DataDog, then S3 archive	Ingest if agency requires retention beyond 90 days.

6.2 SIEM Integration (REQUIRED)

Customers MUST configure Tovuti application audit logs to stream in real-time to their agency-approved SIEM. This is required for continuous monitoring (CA-7) and audit record review (AU-6) at the FedRAMP Moderate baseline.

- **Use the Tovuti REST API:** Application-level audit events are available via the Tovuti REST API for ingestion into your SIEM (Splunk, DataDog, Microsoft Sentinel, etc.). Configure API polling or webhook delivery per your SIEM's ingestion method.
- **Review frequency:** FedRAMP requires audit log review at least weekly (AU-6). Configure automated alerting in your SIEM for high-priority events (failed logins, privilege escalation, bulk data access).
- **Correlation:** Correlate Tovuti application logs with IdP logs, endpoint logs, and network flow data in accordance with AU-6(3).

6.3 Security Configuration Baseline

NIST Controls: CM-2, CM-3, CM-6

Customers MUST document and maintain a Security Configuration Baseline (SCB) for their Tovuti tenant. This baseline records the approved configuration state of all settings described in this guide.

- Document the baseline before go-live, covering at minimum: SSO settings, MFA enforcement, login banner text, session timeout values, enabled features/integrations, RBAC role definitions, and email notification settings.
- Audit the baseline quarterly and after any significant configuration change.
- Record deviations in your POA&M and report to your AO.
- Align baseline review schedule with your agency's continuous monitoring strategy per CA-7.

7. Incident Response

NIST Controls: IR-2, IR-3, IR-4, IR-5, IR-6, IR-6(1), IR-7, IR-8, IR-9

> **The 1-Hour Rule — FedRAMP Mandatory**
> Upon discovery or reasonable suspicion of a security incident involving the Tovuti FedRAMP environment, the customer MUST report the incident to both the Tovuti/Knox security team AND to CISA within ONE (1) HOUR. This timeline is non-negotiable under FedRAMP. Failure to report within this window constitutes a compliance violation.

7.1 Customer Incident Response Responsibilities

- **Maintain a current IR plan:** Your agency Incident Response Plan MUST address incidents involving the Tovuti FedRAMP environment. Include Tovuti/Knox POC details and the CISA reporting mechanism. Verify POC accuracy at least annually.
- **Train IR personnel:** Privileged users must complete IR training within 10 days of assuming IR responsibilities. All IR team members must complete annual refresher training (IR-2).
- **Test annually:** Conduct annual IR exercises that include scenarios specific to the Tovuti LMS environment (data spillage, unauthorized account access, CUI exfiltration). Coordinate exercises with Tovuti if required (IR-3, IR-3(2)).
- **Information spillage:** If CUI is exposed to unauthorized parties via Tovuti, follow IR-9 procedures. Identify affected individuals, isolate affected content, notify affected parties per agency policy, and coordinate with Tovuti support for technical containment.

7.2 Reporting Contacts

Party	Contact Method	Reporting Timeline
Tovuti/Knox Security Team	Verify current POC from your onboarding documentation. Do NOT use general support line for security incidents.	**Within 1 hour of discovery**
CISA (US-CERT)	https://www.cisa.gov/report / 1-888-282-0870	**Within 1 hour of discovery**

Party	Contact Method	Reporting Timeline
Agency AO / ISSO	Per your agency IR plan notification chain.	Per agency IR plan

8. Security Awareness and Training

NIST Controls: AT-2, AT-2(2), AT-2(3), AT-3, AT-4

Customers are responsible for ensuring all personnel with access to the Tovuti FedRAMP environment complete the required security awareness and role-based training. Tovuti provides the training delivery platform; the customer provides and manages training content and completion records.

8.1 Training Requirements

Training Type	Audience	Frequency	Control
Security Awareness	All users before system access	Annually	**AT-2**
Insider Threat	All users	Annually	**AT-2(2)**
Social Engineering	All users	Annually	**AT-2(3)**
Role-Based (ISSO, IR, Admin)	Privileged users, ISSO, IR roles	Before access + Annually	**AT-3**

Maintain training records in Tovuti LMS. Completion records must be retained for a minimum of three (3) years and made available to your AO upon request (AT-4).

9. Customer Configuration Quick Reference

The following table summarizes the highest-priority customer-owned configurations with their associated NIST controls. Use this as a checklist during initial configuration and quarterly reviews.

Control	Requirement	Customer Action	Responsibility
AC-2	Account management procedures, approval, review	Implement account lifecycle process; review privileged accounts quarterly, non-privileged annually	**Customer**
AC-2(2)	Temp/emergency accounts disable after 96 hrs last use	Configure automated account expiration in IdP for all temporary accounts	**Customer**

Control	Requirement	Customer Action	Responsibility
AC-2(13)	Disable high-risk accounts within 1 hour of discovery	Establish and document process; assign responsibility; test annually	**Customer**
AC-6	Least privilege — restrict permissions to minimum required	Define and enforce RBAC roles; no default admin access; Define and enforce RBAC roles; implement SSO attribute mapping to restrict ITAR content strictly to verified U.S. Persons if needed.	**Customer**
AC-7	Lock account after 3 failed attempts / 15-min window	Verify IdP enforces matching or stricter lockout policy	**Shared**
AC-8	Federal login banner before system access	Enable and configure banner in Tovuti admin; use approved text	**Shared**
AC-11	Device lock after 15 min inactivity	Enforce via MDM/GPO on all endpoints accessing Tovuti	**Customer**
AC-12	Session termination after 15 min inactivity	Configure 15-min session timeout in IdP/SSO	**Shared**
AU-6	Audit log review at least weekly	Configure SIEM with automated alerts; document weekly review	**Customer**
AU-11	Log retention: 1 yr online, 7 yr total	Ingest logs via API for agency-side retention as needed	**Shared**
CA-7	Continuous monitoring per agency ConMon strategy	Define and execute ConMon plan; quarterly config baseline audit	**Customer**
CM-7	Disable features not required for mission	Review and disable non-mission-essential Tovuti features; For authorized external content platforms (e.g., BizLibrary), add the streaming domains to the internal corporate network whitelist and submit a platform CSP exception request to Tovuti DevOps.	**Customer**
IA-2(1)	MFA for all privileged accounts	Enforce PIV/CAC or FIPS 140-2 hardware MFA in IdP	**Customer**
IA-2(2)	MFA for all non-privileged accounts	Enforce FIPS-compliant MFA for all users in IdP	**Customer**
IA-2(12)	Accept PIV credentials	Configure IdP to accept PIV/CAC; disable non-PIV login paths	**Customer**

Control	Requirement	Customer Action	Responsibility
IA-5	Authenticator management	Enforce password reset on first use; manage emergency accounts	**Shared**
IR-6	Report incidents within 1 hour to CSP and CISA	Maintain current IR plan with Tovuti/Knox POC and CISA contacts	**Customer**
AT-2	Annual security awareness training for all users	Assign and track completion in Tovuti LMS; retain records	**Customer**
PL-4	Acceptable Use Policy acknowledgment	Ensure AUP aligns with login banner; require acknowledgment pre-access	**Customer**

10. Continuous Monitoring and Periodic Review Schedule

Frequency	Activity	Details	Controls
Weekly	Audit log review	Review SIEM alerts and logs for anomalous activity; document findings	**AU-6**
Monthly	Account audit spot-check	Verify no unauthorized accounts or role escalations	**AC-2**
Quarterly	Privileged access review	Full review of all admin/privileged accounts; remove unnecessary access	**AC-2(j), AC-6(7)**
Quarterly	Security configuration baseline audit	Compare current tenant configuration against documented baseline; document any drift	**CM-2, CM-6, CA-7**
Quarterly	Feature/integration review	Verify no unauthorized features or integrations have been enabled	**CM-7**
Annually	Non-privileged access review	Full review of all user accounts for continued need and appropriate roles	**AC-2(j)**
Annually	Security awareness training	Ensure 100% completion for all active users; update training content	**AT-2, AT-3, AT-4**
Annually	IR plan review & test	Update POC list; conduct tabletop or functional exercise	**IR-3, IR-8**
Annually	CRM review	Review Customer Responsibility Matrix for	**CA-7**

Frequency	Activity	Details	Controls
		changes due to system updates	
Post-change	Configuration verification	After any significant configuration change, verify against security baseline	**CM-3, CM-6**

11. Document Control and Revision History

Version	Date	Description of Change	Author
1.0.0	02/26/2026	Initial release. Aligned to NIST SP 800-53 Rev. 5 Moderate, FedRAMP Rev. 5, and Tovuti SSP / CRM dated January/February 2026.	Tovuti Security Team
1.0.1	03/16/2026	Fixed table of content links, other minor items.	Tovuti Security Team
1.1.0	06/01/2026	Updated Sections 4.3.1 and 5.3.1 to incorporate ITAR U.S. Person gating requirements via RBAC, and established the Content Security Policy (CSP) permit-by-exception framework for non-CUI commercial content partners (ex. BizLibrary)	Tovuti Security Team

For questions about this guide or your FedRAMP compliance obligations, contact the Tovuti Security Team via the Tovuti Help Center at help.tovutilms.com or your designated Tovuti account security representative.