

Tovuti LMS

RegScale# 8

Confidentiality: Moderate

Integrity: Moderate

Availability: Moderate

Tovuti Inc.



Access Control Policy and Procedures

Document Version: 1.0.0

8/10/2023

Prepared by: Tovuti LMS

**DISTRIBUTION IS LIMITED TO U.S. GOVERNMENT AGENCIES AND THEIR CONTRACTORS.
OTHER REQUESTS FOR THIS DOCUMENT MUST BE REFERRED TO: Tovuti LMS**

Change Record

Date	Version	Author	Changes Made / Section(s)
8/10/2023	1.0.0	Tovuti LMS	Initial Document

Table of Contents

1.0	Overview	1
1.1	Purpose	1
1.2	Scope	1
1.3	Roles and Responsibilities.....	1
1.4	Management Commitment	1
1.5	Coordination Among Organization Entities	1
1.6	Compliance	2
2.0	Access Control Policy	2
3.0	Access Control Procedures	2
3.1	Account Management	2
3.2	Access Enforcement.....	4
3.3	Information Flow Enforcement.....	6
3.4	Separation of Duties	6
3.5	Least Privilege	7
3.6	Remote Access	7
3.7	Access Control for Mobile Devices.....	8
3.8	Use of External Systems.....	8
3.9	Information Sharing	9
3.10	Publicly Accessible Content	10

1.0 Overview

Access control policies are high-level requirements that specify how access is managed and who may access information under what circumstances.

This Tovuti LMS Access Control Policy and Procedures addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. This plan has been disseminated to the Tovuti LMS system team, Information System Security Officer (ISSO) and System Owner (SO) via RegScale and will be updated annually. The Tovuti LMS ISSO is responsible for ensuring that the Access Control Policy and Procedures are reviewed annually and posted to the RegScale tool.

1.1 Purpose

It is the purpose of the document to establish the high-level requirements governing the control of access to the Tovuti LMS in compliance with NIST SP 800-53 Revision 5 and to document procedures to facilitate the implementation of the associated security controls.

1.2 Scope

This policy applies to all personnel, processes, and technology components associated with the Tovuti LMS authorization boundary.

1.3 Roles and Responsibilities

Authorizing Official (AO) - Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.

System Owner (SO) – Individual having responsibility for the development, procurement, integration, modification, operation, and maintenance, and/or final disposition of an information system.

Information System Security Officer (ISSO) - Individual with assigned responsibility for maintaining the appropriate operational security posture for an information system or program.

DevOps Engineer - Individual responsible for operating and maintenance of the Tovuti LMS infrastructure while keeping security in mind.

Information Technology (IT) Technical Support - Individual responsible for internal operations, support and maintenance while keeping security in mind.

1.4 Management Commitment

Management is committed to ensuring the confidentiality, integrity, and availability of all information transmitted, stored, and processed by the Tovuti LMS. This policy is reviewed and updated at least annually and approved by the System Owner.

1.5 Coordination Among Organization Entities

This policy and its associated procedures have been coordinated with organizational elements and entities responsible for related plans. The Tovuti LMS ISSO ensures that all applicable stakeholders are included in the annual review and update and that related plans are updated to align with changes to this document.

1.6 Compliance

All personnel with access to the Tovuti LMS are required to comply with this policy and procedures. Violations of this policy may be subject to personnel sanctions up to and including termination.

2.0 Access Control Policy

The following access control policy applies to Tovuti LMS:

- The System Owner shall ensure that the Access Control Policy and Procedures are reviewed and updated **at least annually**.
- The Access Control Policy and Procedures shall be disseminated to **all personnel** with access to the information system.
- The Access Control Policy and Procedures shall be consistent with the requirements outlined in the Federal Information Security Modernization Act (FISMA) and shall comply with the requirements Federal Risk Authorization Management Program (FedRAMP) requirements and the associated security control baselines.
- Organizationally defined security control parameters (i.e., assignment and selection statements) shall be maintained within the RegScale tool and subsequently documented in the Tovuti LMS system security plan (SSP).
- The organization shall maintain an SSP for Tovuti LMS which documents the implementation details of the required FedRAMP access controls commensurate with the effective security categorization for the system.
- The organization shall follow a rigorous process for account management that aligns with CSP-defined policy, procedures, prerequisites, and criteria.
- The organization shall train account managers that validate the need for account creation, secure credentials, monitoring and timely disabling / removal of inactive or unnecessary accounts.
- Access authorization for the system will be enforced for logical access to the systems.
- “Bring your own device” is allowed only for non-confidential data or systems access. Company provided laptops are used to ensure standardization and security requirements are met.
- The organization shall select external systems based on a security assessment and establish a Service Level Agreement, or other documentation to establish terms and conditions and controls for external systems.

3.0 Access Control Procedures

The follow subsections provide procedures to facilitate the implantation of the required access controls:

3.1 Account Management

The following sections detail how Tovuti LMS manages user and system accounts.

- **ACCESS AUTHORIZATION:**
 - Before creating a new account, DevOps Engineer or IT Tech Support ensures that there is a valid and justifiable need for the account. This step prevents unnecessary

- or unauthorized account creation, minimizing the potential for security vulnerabilities.
- All user/service accounts start in a Jira ticket in the IT Support project requesting a new user.
- **ACCESS LEVELS:** There are four access levels in the Tovuti LMS system (These can be grouped into learners and administrators):
 - public
 - registered
 - sub administrator
 - site administrator
- **ACCOUNT MANAGERS:** DevOps engineers and IT Tech Support act as account managers to oversee and manage user accounts. Account managers are trained and authorized to handle account-related activities:
 - i. Creation
 - ii. Modification
 - iii. Deletion
 - User profile is selected by the hiring manager by using the Jira ticket template when creating the request in Jira.
 - Users are assigned group and role memberships based on the profile by IT Tech Support or DevOps Engineer.
 - IT Tech Support or DevOps Engineer will create the accounts in google and Okta using Terraform for group and role assignments.
 - IT Tech Support and DevOps ensures the user is only in the onboarding group until employment agreement, employee manual, non-circumvention agreement, proprietary information & Inventions agreements are signed.
- **REQUIRED APPROVALS:**
 - After approval by the requestor's manager, and the ISSO or SO the accounts can be created.
- **ACCOUNT CREATION, ENABLEMENT, MODIFICATION, DISABLEMENT, AND REMOVAL:**
 - After the request has been approved, tickets are worked to either add, modify, or disable accounts. DevOps Engineer or IT Tech Support will be making the changes depending on role and access needed or removed.
- **PROCESS FOR MONITORING USE OF ACCOUNTS:**
 - Quarterly an Auto-ticket is created in Jira
 - The SO or ISSO reviews the ticket and audits active accounts for aged accounts.
 - If any action is needed, the ticket is updated, actions are conducted and the ticket is closed.
- **NOTIFICATION WHEN ACCOUNT ARE NO LONGER REQUIRED:**
 - The employee's manager is responsible for notifying the ISSO and SO when accounts are no longer required.
- **ACCESS AUTHORIZATION:**
 - All user/service accounts start in a Jira ticket requesting a change to access.
 - After approval by the requestor's manager, and the ISSO or SO the accounts can be created or changed.

➤ **REVIEW OF ACCOUNTS:**

- Quarterly an Auto-ticket is created in Jira
- The SO or ISSO reviews the ticket and audits active accounts for aged accounts.
- If any action is needed, the ticket is updated, actions are conducted and the ticket is closed.

➤ **MANAGING SHARED OR GROUP ACCOUNTS:**

- All user/service accounts start in a Jira ticket requesting a change to access.
- After approval by the requestor's manager, and the ISSO or SO the accounts can be created or changed.
- The SO or ISSO reviews the ticket and audits active accounts for aged accounts.
- If any action is needed, the ticket is updated, actions are conducted and the ticket is closed.

➤ **ACCOUNT MANAGEMENT PROCESS IN RELATION TO PERSONNEL
TERMINATION/TRANSFER:**

- Termination
 - i. An offboarding ticket is created by the manager of the departing employee prior to the employee leaving.
 - ii. ISSO reviews current access for the employee leaving, creates a list of all access and equipment.
 - iii. ISSO reports to the manager of the departing employee what equipment the employee has and what needs to come back
 - iv. ISSO Disables accounts at the time the manager specified.
 - v. ISSO records assets back into inventory.
 - vi. ISSO Backs Up the employee data and removes the accounts after 90 days.
- Transfer
 - i. An Employee transfer ticket is created by the new manager the employee is moving to.
 - ii. ISSO reviews current access and what access the employee will need in the new role. The ISSO will communicate with the employee's new manager the different tools/access.
 - iii. ISSO will remove any access that is no longer needed for the new role and add appropriate access for the new role.

3.2 Access Enforcement

Tovuti has implemented a comprehensive process for enforcing logical access to its system resources, strictly in accordance with approved access authorizations and relevant access control policies. This process guarantees that users can only access the specific data and system resources that they have been explicitly authorized to access. This meticulous approach is aimed at reducing the risk of unauthorized data exposure or system breaches. The process involves several key steps:

➤ **User Authentication and Authorization:**

- Users are required to authenticate themselves using their unique credentials, such as usernames and passwords. Once authenticated, the system checks the user's identity

against a centralized authorization mechanism that contains information about the user's roles, permissions, and access rights.

➤ **Role-Based Access Control (RBAC) Implementation:**

- Tovuti employs a role-based access control (RBAC) model to define and manage user access privileges. Different roles are created based on job functions, responsibilities, and clearance levels within the organization. Each role is associated with specific permissions and access rights that determine what resources a user with that role can interact with.

➤ **Access Request and Approval Workflow:**

- When a user needs access to certain resources, they initiate a formal access request. This request is routed through an approval workflow that involves appropriate stakeholders. Typically, supervisors or designated approvers review the request and verify its legitimacy based on the user's job requirements and security clearance.

➤ **Access Control Lists (ACLs) and Resource Permissions:**

- Tovuti employs access control lists (ACLs) to define fine-grained permissions for specific resources, such as files, databases, or applications. These ACLs specify which users or roles have read, write, or execute permissions on a particular resource.

➤ **Regular Access Reviews and Audits:**

- To maintain the integrity of access controls, Tovuti conducts regular access reviews and audits. These assessments involve reviewing user roles, permissions, and access logs to ensure that they are aligned with the organization's needs and that no unauthorized access has occurred.

➤ **Automated Enforcement and Monitoring:**

- Automated mechanisms are in place to enforce access controls in real-time. These mechanisms ensure that access permissions are consistently applied and that any attempts to violate these controls trigger alerts or security measures.
- Okta, Tovuti's authentication provider is configured with Okta ThreatInsight which analyzes sign-in activity across the customer base. This detects potentially malicious IP addresses, prevents credential-based attacks such as password spraying, credential stuffing and brute-force cryptographic attacks.
- Accounts are configured to be locked out if the ThreatInsight is over the current threshold.
- Tovuti customers have the flexibility to change these enforcements through their IDP.

➤ **Revocation of Access:**

- Access authorizations are not static; they are subject to change as user roles and responsibilities evolve. When a user changes roles or leaves the organization, their access rights are promptly revoked or adjusted to prevent any lingering access to resources that are no longer relevant to their current responsibilities.

3.3 Information Flow Enforcement

Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information.

Internal to Tovuti LMS, all information is permitted and authorized to flow freely under the following conditions:

- Information remains at the same classification level.
- All users have a valid need to know, or if separation of users is required; information will be protected with access controls.
- All information remains internal to Tovuti LMS

Approved authorizations are based on user access. If a user has a valid account on Tovuti LMS, they are considered authorized to access the information.

External to Tovuti LMS, all information is permitted and authorized to flow freely under the following conditions:

- Information remains at the same classification level.
- All users have a valid need to know, or if separation of users is required; information will be protected with access controls.
- If information does not cross an external boundary, it must only connect to another system within the internal enclave.
- If information does cross an external boundary, it must be mediated through a proxy, firewall or DMZ.
- Ports, Protocols and Services must be identified in the architecture diagram.
- Sensitive or classified information must be encrypted.
- Any information containing credentials must be encrypted.

Approved authorizations are based on user or system access. If a user has a valid account on Tovuti LMS, they are considered authorized to access the information. If Tovuti LMS interconnects with another trusted system, it is considered authorized.

3.4 Separation of Duties

Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example: (i) dividing mission functions and information system support functions among different individuals and/or roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions.

Tovuti LMS has defined the below duties that require separation:

Role	Duty	Role in Use?	Separation Implemented
Standard User	Managed Device: Limited access to authorized information	Yes ☒ No ☐	Yes ☒ No ☐

Foreign National	Limited access to authorized information	Yes ☐ No ☒	Yes ☒ No ☐
Local Administrator	Managed Device: Manage the local system	Yes ☒ No ☐	Yes ☒ No ☐
Information System Security Officer (ISSO)	Security functions, e.g. audit log review	Yes ☒ No ☐	Yes ☒ No ☐
DevOps Engineer	Operation and Maintenance of Infrastructure	Yes ☒ No ☐	Yes ☒ No ☐
IT Tech Support	Operation and Support	Yes ☒ No ☐	Yes ☒ No ☐
Public	TovutiLMS Anonymous users not registered	Yes ☒ No ☐	Yes ☒ No ☐
Registered	TovutiLMS Training users (Students)	Yes ☒ No ☐	Yes ☒ No ☐
Sub Administrator	TovutiLMS Some configurations, but limited and customizable	Yes ☒ No ☐	Yes ☒ No ☐
Site Administrator	TovutiLMS See Everything Super Admin	Yes ☒ No ☐	Yes ☒ No ☐
AWS Role: AWSReadOnlyAccess	AWS Read Only access	Yes ☒ No ☐	Yes ☒ No ☐
AWS Role: TovutiAdministratorsAccess	AWS Full Administrator Access	Yes ☒ No ☐	Yes ☒ No ☐
AWS Role: TovutiSecurityAccess	AWS Tovuti Access	Yes ☒ No ☐	Yes ☒ No ☐
AWS Role: TovutiWorkspaceAdminAccess	AWS Workspace admin	Yes ☒ No ☐	Yes ☒ No ☐

3.5 Least Privilege

Tovuti LMS utilizes the account management process documented in section 3.1 to implement the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with mission and business functions.

3.6 Remote Access

Remote access is only allowed from company devices that meet our requirements.

Before allowing remote connections, Tovuti ensures each type of remote access to the system is authorized. A Request ticket is created by the individual, or their manager. After approval by the manager, and the ISSO or SO, the DevOps team will assign access. An application will need to be installed on the employee's computer that meets specific requirements such as virus scanning, encrypted hard drive.

3.7 Access Control for Mobile Devices

While we support a 'Bring Your Own Device' policy for mobile devices, company-provided laptops are used to ensure standardization and enhanced security. Mobile devices such as mobile phones, are not able to access AWS Infrastructure.

Mobile Devices are not permitted to connect to AWS Infrastructure.

3.8 Use of External Systems

To ensure the security and integrity of organization-controlled information, the following procedure is followed:

- **Identification of Need:**
 - The process begins with the identification of a specific need or requirement for using an external system. This could be driven by business processes, collaboration needs, or specialized functionalities that the organization's internal systems do not provide.
- **Risk Assessment and Selection:**
 - Before adopting any external system, a thorough risk assessment is conducted. This assessment evaluates the security posture, data protection measures, compliance with FEDRAMP requirements, and the potential impact on the organization's overall security. Based on the assessment, a suitable external system is selected that aligns with the organization's security standards and requirements.
- **Terms and Conditions:**
 - Once an external system is selected, the Cloud Service Provider (CSP) establishes specific terms and conditions for using the external system. These terms include contractual agreements, service level agreements (SLAs), data handling practices, and access control requirements.
- **Access Control Configuration:**
 - The CSP configures access controls for the external system, ensuring that authorized individuals have appropriate access permissions while unauthorized access is restricted. This involves implementing role-based access control (RBAC), multi-factor authentication (MFA), and other security mechanisms to authenticate and authorize users.
- **Data Handling Guidelines:**
 - The organization and the CSP establish guidelines for handling organization-controlled information within the external system. This includes data encryption, data segregation, and the process for transmitting, storing, and processing data in accordance with FEDRAMP standards.
- **User Training and Awareness:**
 - Authorized users who will be accessing the external system undergo training on the proper usage, security practices, and compliance requirements. This ensures that users understand their responsibilities and how to interact with the system securely.
- **Monitoring and Auditing:**
 - Ongoing monitoring and auditing of the external system's usage are conducted to detect and respond to any anomalies or security incidents promptly. Access logs and audit trails are maintained to track user activities, changes, and potential security breaches.

- **Incident Response and Reporting:**
 - In the event of any security incident, unauthorized access, or breach related to the external system, an incident response plan is triggered. The CSP, along with the organization's security team, investigates the incident, takes appropriate actions, and reports the incident to relevant stakeholders and authorities, as required.
- **Regular Review and Assessment:**
 - Periodic reviews and assessments are conducted to ensure that the external system continues to meet FEDRAMP standards and aligns with the organization's security needs. If there are any changes in the system, its usage, or the threat landscape, the risk assessment and controls are adjusted accordingly.
- **End of Usage or Transition:**
 - When the need for the external system diminishes or changes, or if there are security concerns, the organization and CSP follow a controlled process to terminate or transition away from using the external system. This process includes data migration, ensuring data is securely transferred, and disabling access appropriately.

3.9 Information Sharing

Information sharing applies to information that may be restricted in some manner based on some formal or administrative determination. Examples of such information include contract-sensitive information, classified information related to special access programs or compartments, privileged information, proprietary information, and personally identifiable information.

- **Identify Collaboration Needs:**
 - Organizations identify the need for information sharing when collaborating with external entities, government agencies, partners, or stakeholders. This could involve the exchange of data, reports, insights, or strategic information to achieve common goals.
- **Assess Data Sensitivity and Purpose:**
 - Before sharing any information, the organization assesses the sensitivity of the data to be shared. They also define the purpose of the sharing, ensuring that it aligns with the organization's mission and objectives.
- **Determine Legal and Regulatory Requirements:**
 - Organizations identify any legal, regulatory, or contractual requirements that may impact the sharing of specific types of information. This step ensures that the sharing process remains compliant with relevant laws and standards, including FEDRAMP.
- **Classify Information:**
 - The data to be shared is classified based on its sensitivity, value, and potential impact if compromised. Data classification helps determine the appropriate level of security measures required for sharing.
- **Identify Authorized Recipients:**
 - The organization identifies the authorized recipients who need access to the shared information. Recipients are determined based on their roles, responsibilities, and their need to know the information for collaborative purposes.
- **Assess External Party's Security Posture:**

- If sharing with an external party, an assessment is conducted to evaluate their security posture. This assessment includes their adherence to security standards, such as FEDRAMP, to ensure that the shared information will be handled securely.
- **Evaluate Data Handling Procedures:**
 - The organization assesses the external party's data handling procedures, including encryption methods, access controls, data retention policies, and incident response plans. This evaluation ensures that the shared information will be protected throughout its lifecycle.
- **Define Terms and Conditions:**
 - Organizations and external parties establish formal agreements that outline the terms, conditions, and controls for sharing information. These agreements include specifics on access rights, data usage, data retention, incident reporting, and compliance with FEDRAMP.
- **Implement Access Controls:**
 - Access controls are configured to ensure that only authorized individuals within the organization and the external party can access the shared information. Role-based permissions, encryption, and authentication mechanisms are set up as needed.
- **Secure Data Transmission:**
 - Data is transmitted using secure and encrypted communication channels. This prevents unauthorized interception and ensures the confidentiality of the shared information during transit.
- **Regular Monitoring and Auditing:**
 - The sharing of information is monitored and audited regularly. Audit logs track who accessed the data, when, and for what purpose, enabling the identification of any unauthorized or unusual activities.
- **Review and Update Sharing Agreements:**
 - Sharing agreements are periodically reviewed and updated to reflect changes in security requirements, compliance regulations, or collaborative objectives. This ensures that the information sharing process remains relevant and effective.
- **End of Sharing or Transition:**
 - When the collaboration concludes or the need for information sharing changes, a process is followed to terminate the sharing agreement. Access to shared data is revoked, and any residual data is handled and disposed of securely.

3.10 Publicly Accessible Content

This process outlines how publicly accessible content is reviewed and approved before posting to publicly accessible systems, ensuring that non-public information is not disclosed.

- **Designation of Responsible Individuals:**
 - Designated individuals or a team, including communication specialists, content managers, and subject matter experts, are responsible for making information publicly accessible. This aligns with our commitment to safeguard client data and offers them the discretion to choose what information they wish to make public.
- **Training for Non-Public Information Handling:**

- Individuals involved in preparing content for public access undergo training in accordance with our comprehensive policy. This policy ensures that personnel are adept at managing data via Tovuti-managed devices and understand the significance of data security and privacy.
- **Review of Proposed Content:**
 - The proposed content undergoes a meticulous review process that aligns with our focus on secure software solutions:
- **Content Drafting:**
 - Content is drafted, ensuring the exclusion of non-public information.
- **Initial Review:**
 - Content creators review the draft to identify potential non-public information. This process echoes our commitment to offering robust mechanisms to safeguard client data.
- **Subject Matter Expert (SME) Review:**
 - Subject matter experts in relevant areas review the draft for accuracy, relevance, and the absence of non-public information. Their involvement assures our clients of the high quality and security of the content.
- **Legal and Compliance Review:**
 - Legal and compliance teams validate that the content adheres to our commitment and organizational standards. They ensure accuracy and compliance with relevant regulations.
- **Non-Public Information Check:**
 - A final check ensures that no non-public information is included, aligning with our promise to maintain the security and privacy of client data.
- **Scheduled Reviews:**
 - Designated individuals periodically review publicly accessible content for non-public information. This commitment to regular review maintains the security and privacy of non-public information.
 - Audit and Monitoring: Automated tools and manual audits further ensure the adherence to our commitment. These tools uphold our focus on providing secure software solutions.
 - User Feedback: Users are encouraged to provide feedback on any potential discrepancies they encounter. This user-centric approach helps identify and rectify issues promptly, reinforcing our dedication to delivering a reliable service.
- **Incident Response:**
 - If non-public information is identified within publicly accessible content, our incident response plan is enacted promptly. Content is removed or corrected, and an investigation is conducted to prevent similar incidents, in line with our promise of discretion and data security.