Information Technology (IT)
Policies, Procedures, and Standards

Department: Information Technology (IT)
Owner: Preet Mood
Version: 2.0
Effective: 1/8/2025

“Inteum Company LLC’s” (“Inteum Company LLC” or the “Company”) IT policies, procedures, and standards have been established to enhance the security, stability, recoverability, and overall control of the Company’s IT environment, applications, and data. Compliance is mandatory. Please direct any questions you may have regarding the content of this document or your responsibilities to your supervisor or to the Chief Security Officer (Matt Campbell)

TABLE OF CONTENTS

Document History

Date	Revision	Description	Author	Approver
1/10/18	1.0	Initial Version	Preet Mood	Justin Adair
1/21/19	1.1	Reviewed to see if any changes/updates needed. No changed are needed.	Preet Mood	Justin Adair
8/27/19	1.2	Added Mobile Code Policy	Preet Mood	Ray Dunham
1/21/2020	1.2	Reviewed document	Preet Mood	Ray Dunham
1/12/2021	1.3	Reviewed document	Preet Mood	Ray Dunham
1/19/2021	1.4	Changed password minimum character from 10 to 13 as “This was changed to conform with Australian government policies.	Preet Mood	Justin Adair
1/27/2021	1.5	Updated 18.2 Vulnerability Management risk timeline	Preet Mood	Justin Adair
4/19/2021	1.6	Striped section 3.4.2 in this document	Preet Mood	Justin Adair
1/4/2022	1.7	Reviewed document and no changes are needed	Preet Mood	Justin Adair
1/23/2023	1.8	Reviewed document and no changes are needed	Preet Mood	Matt Campbell
1/16/2024	1.9	Reviewed document and no changes are needed	Preet Mood	Yavuz Alparslan
1/8/2025	2.0	Reviewed document and no changes are needed	Preet Mood	Yavuz Alparslan
1/9/2026	2.0	Reviewed document and no changes are needed	Preet Mood	Yavuz Alparslan

THE REMAINING PORTION OF THIS PAGE IS LEFT INTENTIONALLY BLANK.

Security

IT Security Policy

Purpose

The purpose of the IT Security Policy is to ensure that the information assets of “Inteum Company LLC” are protected from unauthorized access and misuse and that access to information assets is restricted in accordance with business need.

Scope

The scope of this policy applies to all users of the Company’s computing environment and to all applications, data, and supporting IT infrastructure.

Policy Statements

1. **Information Integrity Objectives**
   1.1. Access to the Company’s computing environment is granted based on a business need. If there is an absent legitimate business need, access is denied.

2. **Ownership**
   2.1. All Company applications and supporting IT infrastructure are classified by a System level structure as defined in the IT System Ownership Standard.ITSystemOwnershipStandard
   2.2. All System Applications are assigned an Application Owner and an IT Application Support Owner.
   2.3. The IT System Ownership Standard specifies the security-related responsibilities of the Application Owner and IT Application Support Owner.ITSystemOwnershipStandard

3. **User Level Access**
   3.1. User access to the Company’s computing environment is available to employees or authorized contractors. All users, including non-employees, must sign the Employee Handbook acknowledgement and Acceptable Use Policy prior to receiving access to the Company’s computing environment.
   3.2. The Security Officer or delegated individual has the responsibility and authority for system security. If the Security Officer believes information assets are at risk, the Security Officer is empowered to take appropriate action to protect the information assets through appropriate security measures.
   3.3. User IDs and Passwords
      3.3.1. All System Application users must have a user ID and password.
      3.3.2. Sharing of individual user IDs and passwords is strictly prohibited.

3.3.3. Use of group IDs for user level access is strictly prohibited, except as noted in the Exceptions section.SecurityPolicyExceptions

3.3.4. Users are responsible for all system activity made using their user IDs and passwords.

3.3.5. Assignment of user IDs follows the IT Security Procedure.ITSecurityProcedure

3.3.6. Password strength configuration parameters by system and application follow company policy (see the Security Policy Table at the end of this section).SecurityPolicyTable1

3.3.7. If the application is not capable of automatically enforcing the password strength configuration parameters above, the Company policy is to request user compliance.

3.4. Monitoring and Privacy

3.4.1. The Company reserves the right to monitor and/or block user email, internet, and system usage.

~~3.4.2. All data created, stored, or transferred on the Company's computing environment is owned exclusively by the Company.~~

3.5. Security Policy Table

Application or System	Minimum Password Length	Password Rotation Period	Password Complexity	Password History	Account Lockout
Inteum Uses Win Active Directory	13	90 days	Yes	24	30 mins

4. Virus Protection

4.1. Antivirus software is installed on all workstations and production servers.

5. Remote Access

5.1. The internal network is protected from unauthorized internet access by a firewall appliance.

5.2. Remote access for privileged functions is allowed for operational functions only

5.3. All remote access must be approved by the Security Officer or delegated official and requested as per the IT Security Procedure.ITSecurityProcedure

6. System Level Access

6.1. System Application direct database access must be approved by the Security Officer and requested as per the IT Security Procedure.ITSecurityProcedure

6.2. All parties granted system level access must comply with the requirements of the User Level Access section above.

6.3. Firewall, Router and Switch Access – Firewalls, routers, and switches contain single instances of passwords that are changed periodically and at any time turnover of knowledgeable IT personnel occurs.

7. Wireless Access

7.1. Access to the internet for non-business use is provided via an Isolated Guest Wi-Fi network for guest, untrusted machines and for personal employee devices (i.e., phones and other BYOD devices). Client devices are isolated from “Inteum Company LLC’s” network.

7.2. Wireless access to the Company’s network is permitted under the following conditions:

7.2.1. Wireless access to the “Inteum Company LLC” network is available via a separate, secured Wi-Fi network. Access is granted only on an as-needed basis, and only to client devices that meet the Company’s security and antivirus requirements.

8. Logical Access

8.1. Three (3) characters are changed when individuals change their passwords

8.2. Inteum privileged users on the production environment will only access the production environment with their privileged account when performing privileged functions otherwise a non-privileged account will be used.

8.3. Production environment is not accessed by personally owned laptops/PCs unless it is accessed through remote desktop login from personally owned laptops/PCs.

8.4. Usage restrictions of laptops are solely for Inteum Company use.

8.5. Sensitive data is not stored on Inteum laptops.

8.6. General user IDs will not be reused for a period of time (2 years)

8.7. An Inteum system administrator will perform a manual process to review the AD for users that haven’t logged in after 90 days (inactivity)

8.8. Terminated users will have their access removed from the production environment on or before their day of termination

8.9. User access reviews for admins are performed annually

9. Communications Over Public Networks

9.1. Sensitive transaction data is only exchanged over a trusted path. Users connecting to the Company’s computing environment via the internet must use access methods which ensure encrypted communications between the user and the system (e.g. DirectAccess, Virtual Private Network (VPN), etc.).

9.2. Confidential and proprietary data or Company information may not be transmitted as an attachment to unsecure email unless the attachment is encrypted.

10. Encryption Usage and Standards

10.1. AES 128 is the minimum

11. Disposal of Sensitive Information and Data

11.1. Sensitive data, including client data, is not stored on Inteum mobile devices (e.g., laptops)

11.2. Sensitive information, including client data, stored on fixed computers (e.g., workstations) must be irretrievably erased when disposed of or transferred to another user.

12. Removable Media

12.1. Sensitive data, including client data, will not be saved to or stored on removable media (e.g., thumb drives, external hard drives).

13. Facility

13.1. Any areas such as server rooms, wiring closets or media storage locations are physically secured, and access is restricted to authorized employees and Third-Party Vendors.

14. Incidents

14.1. All incidents shall be addressed in accordance with client requirements. Additionally, if there is a breach or compromise, the helpdesk and program manager shall be notified immediately for proper action and notification.

15. Annual User Access Review

15.1. The Security Officer, or their delegate, performs at least an annual review of user access capabilities and corrects inappropriate user access.

15.2. The user access review is conducted for user access to System Applications, production data, operating systems, external network connections, firewalls, routers, and physical security.

16. Monitoring for Potential Unauthorized Activity

16.1. IT Department personnel review security events from key elements of the IT infrastructure, including server operating system event logs, semi-annually to identify potential unauthorized activity and documents the review and results in the IT ticketing system.

16.2. Potential unauthorized activity is defined to be, in part, password guessing. Password guessing appears in event logs as multiple failed attempts to logon to a server, System Application, firewall, router, or other key elements of the IT infrastructure.

16.3. Potential unauthorized activity found is investigated, followed-up, and communicated to the Security Officer or a member of Executive Management.

17. Periodic Risk Assessment

17.1. The Security Officer and other applicable department heads will conduct a risk assessment annually or when significant changes that could impact security are made to the Company's computing environment. If warranted, a third-party service provider may be engaged to assess and report security risks and vulnerabilities. The Security Officer takes corrective action to reduce risk to an acceptable level.

18. Vulnerability Management

18.1. Vulnerability management policy has been established for identifying and mitigating vulnerabilities. IT Security Manager is responsible to monitor security advisories.

18.2. Remediation of vulnerabilities are handled in accordance with the risk

Risks	Days
Critical/High	30 days
Medium	60 days
Low	90 days

19. Mobile Code Policy

19.1. Inteum does not allow unsigned mobile code to execute on Inteum Systems. Mobile code is also disabled from running on production servers.

Exceptions

The Security Officer, unless delegated, must approve all exceptions and changes to the IT Security Policy.ITSecurityPolicy

Test Email Accounts: Sharing of individual user IDs and passwords is strictly prohibited unless it has been approved by the Security Officer to test the use of an email account.

Non-Compliance Penalties

Violators of this policy are subject to disciplinary action, up to and including termination of employment and possible civil liability and/or criminal prosecution.

IT Security Procedure

Purpose

The purpose of the IT Security Procedure is to define the process for obtaining user access to the "Inteum Company LLC's" computing environment, including initiating a request, obtaining approval, and processing the request. It also covers the procedure for terminating user access, obtaining emergency access and periodically reviewing, and approving or correcting user access.

Scope

This process applies to user access to the Company's computing environment, including:

- Production Server(s) Operating System(s)
- System Application(s)
- Firewall(s)
- Router(s)
- Switch(es)
- Physically-Secured IT Area(s)
- VPN
- Enterprise Wireless Network

Procedure Statements

1. **Initiate Request**
   1.1. The user's supervisor or system owner creates a ticket within the ticketing system.ITSecurityAccessForm
      1.1.1. For new users and changes to existing users, the requestor must specify the application(s) and access level to be provided to the user.

2. **Obtain Approval**
   2.1. IT Department personnel review the IT Security Access Ticket for compliance with the requirements of IT policies, procedures, and standards.
      2.1.1. Application Owner[1] approval is required for new user access and existing user access changes to System Applications. (See the IT System Ownership Standard for a list of System Applications.)
      2.1.2. Application Owner approval is required for update access to System Application data outside the application.

2.1.3. Security Officer approval is required for administrator-level access to production servers, firewalls, routers, switches and any access to physical premises where IT equipment, wiring, and/or media is secured.

2.2. In emergency situations where Application Owner approval is not readily available, verbal or email approval will be permitted with formal Application Owner approval after-the-fact.

3. Process Requests

3.1. IT Department personnel or the Application Owner build account(s) in systems and/or applications, based on roles and responsibilities requested and approved.

3.2. IT Department personnel or the Application Owner create appropriate access in each system and/or application.

3.3. IT Department personnel or the Application Owner notify the requestor and user that the user account(s) has/have been created and closes and files the IT Security Access Ticket.

3.4. If the request is denied, IT Department personnel or the Application Owner notify the requestor that the request was denied and closes and files the IT Security Access Ticket.

4. Process Terminations

4.1. A member of Management notifies the HR Department. The HR Department sends email notifying to IT Security Officer and IT Security Officer will then create a case in Axosoft and follow it till closure.

4.2. IT Department personnel or the Application Owner review active system and application user accounts along with the termination list found within an email to see which accounts should be disabled or deleted.

4.2.1. Regarding all Applications, Firewall/Router/Switch/Wifi and Physical access, when IT Department personnel terminate or a Third-Party Vendor relationship is terminated, IT Department personnel assess whether the individual has firewall, router or switch access that needs to be disabled. Disabling may require the firewall, router, switch or wifi password to be changed.

4.2.2. Regarding physical access to IT areas, when IT Department personnel terminate or a Third-Party Vendor relationship is terminated, IT Department personnel assess whether the individual has physical access that needs to be revoked.

5. Periodic Access Review

5.1. The scope of the periodic access review includes the:

5.1.1. Production Server(s)

5.1.2. Firewall(s)

5.1.3. Router(s)

5.1.4. External Network Connection(s)

5.1.5. System Application(s) and Data

5.1.6. Physical security of the computer room(s), network equipment, and media storage area(s)

5.2. IT Department personnel create or obtain user ID/role listings for the areas in scope.

5.3. Obtain approval of access to:

5.3.1. IT Infrastructure – Security Officer/ Delegated Officer

5.3.2. System Applications - Application Owner

5.3.3. Physical security of IT areas – Security Officer/ Delegated Officer

5.4. Conduct the review annually near the end of each calendar year.

5.5. Document the review by retaining approved, signed, and dated printouts evidencing the review.

THE REMAINING PORTION OF THIS PAGE IS LEFT INTENTIONALLY BLANK.

Change Control

IT Change Control Policy

Purpose

The purpose of the IT Change Control Policy is to ensure that changes proposed or to be made to the Company's computing environment are requested, authorized, and implemented in a controlled manner.

Scope

This policy applies to all System Applications listed in the IT System Ownership Standard and supporting IT infrastructure.ITSystemOwnershipStandard

Definition

"Inteum Company LLC" defines changes as modifications to a process which alters the way day to day business operations occur.

Policy Statements

1. **Recordkeeping**
   1.1. All changes are recorded in the ticketing system.

2. **Direct Data Updates**
   2.1. Direct data updates to System Application data made outside of the application are considered to be changes and are recorded as per the IT Change Control Procedure and using the IT Processing and Managing Change Requests through Axosoft Tool.ITChangeControlProcedureITChangeControlForm

3. **Update Access to Production**
   3.1. Update access to production environments hosting System Applications is restricted to the IT Application Support Owner and support personnel, designated backups, and authorized Third-Party Vendors.

4. **Impact Assessment**
   4.1. The impact of each change request is assessed using the Impact Assessment Matrix in the IT Change Control Procedure to determine the appropriate impact (priority). The impact assessment

is documented on the IT Processing and Managing Change Requests through Axosoft Tool.ITChangeControlProcedureITChangeControlForm

5. **Approval**
   5.1. The requirements for change request approval are based on the impact assessment and is determined by the Application Owner and CTO/CEO in the IT Change Control Procedure. The approval is documented on the IT Processing and Managing Change Requests through Axosoft Tool.ITChangeControlApprovalMatrixITChangeControlProcedureITChangeControlForm

6. **Third-Party Vendor Access**
   6.1. The Security Officer or delegated official authorizes Third-Party Vendor access to the Company's computing environment according to the process documented in the IT Change Control Procedure.ITChangeControlProcedure

7. **Prioritization**
   7.1. The Security Officer or delegated official is responsible for establishing and communicating the priority of change requests.

Exceptions

None.

Non-Compliance Penalties

Violators of this policy are subject to disciplinary action, up to and including termination and possible civil liability and/or criminal prosecution.

THE REMAINING PORTION OF THIS PAGE IS LEFT INTENTIONALLY BLANK.

IT Change Control Procedure

Purpose

The purpose of the IT Change Control Procedure is to define the procedure for making changes to the Company's computing environment.

Scope

The scope of this procedure includes the following types of changes:

- System Applications – New applications, new releases of existing applications, and all other updates EXCEPT patches to correct security exposures and patches to correct software defects.
- System Data – New databases or files, changes to database/file structures, and direct data updates to production data.
- System Operating Systems – New operating systems, new releases of existing operating systems, and all other updates EXCEPT patches to correct security exposures and patches to correct software defects.
- Configuration Changes – New hardware including production servers, firewalls, and routers; changes to configuration settings including firewall rules, router tables, and external network connections.

The scope of this document is ALL changes and includes both emergency and non-emergency changes. The IT System Ownership Standard contains a list of System Applications.ITSystemOwnershipStandard

Procedure Statements

1. **Initiate Request**
   1.1. The SO or delegated official receives, reviews, and considers change requests from multiple sources (e.g., IT Department personnel, users, third-party vendors, etc.).
   1.2. The SO or delegated official assesses the business impact of the change request (High, Medium, or Low) using the Impact Assessment Matrix.ITChangeControlImpactAssessmentMatrix
   1.3. The SO or delegated official determines whether the change request is emergency or non-emergency.
   Note: IT Department personnel may deviate from the normal change control process in emergencies, if time constraints so dictate in their judgment or that of Executive Management. The change should still be captured and approved after the change is made.
   1.4. The SO or delegated official evaluates the desirability of the change and establishes a target date for implementation of desired changes.

1.5. IT Department personnel should use the information within the IT Processing and Managing Change Requests through Axosoft Tool within a ticket and include the following information:ITChangeControlForm

1.5.1. Requested By
1.5.2. Start Date
1.5.3. Completion Date
1.5.4. Severity (Low, Medium, High)
1.5.5. Project (Application, IT Infrastructure, Direct Data Update)
1.5.6. Description (of the change request)
1.5.7. Other required information.

2. Assess Business Impact

2.1. For all change requests, an impact assessment is required as shown in the Impact Assessment Matrix:

Impact Assessment Matrix

Assessment Criteria	Low	Medium	High
Affects user's ability to perform their job	Single User	Multiple Users	All Users
Affects functionality of a System Application	Functionality is minimally impacted	Functionality is moderately impacted	Functionality is significantly impacted

2.2. Evaluate the assessment criteria for each change request, and weight functionality more heavily to determine the impact.

Examples:

High Impact

- New System Application
- Production Server Operating System: A migration to a new production server operating system or a full restore of data from backup media
- New firewall, router, switch, or server hardware

Medium Impact

- New version or release of existing System Application
- Production Server Operating System: Operating system upgrade
- Firewall: Upgrade or changes to firewall rules
- Router: Upgrade or changes to router rules

Low Impact

- Single User Upgrade

3. Back-Out Procedure

The steps in this section are performed whenever a change to the Company's computing environment must be backed-out. If IT Department personnel determine that a change must be backed out:

3.1.1. IT Department personnel obtain the backup media for the System Application and/or Operating System from storage.

3.1.2. IT Department personnel restore from backup.

3.1.3. IT Department personnel perform tests to confirm that the Company's computing environment functions as expected.

3.1.4. IT Department personnel create a record of the restore, testing performed, and test results in the IT Change Control Ticket of the change requiring back-out.

THE REMAINING PORTION OF THIS PAGE IS LEFT INTENTIONALLY BLANK.

IT Processing and Managing Change Requests Through Axosoft Tool

A new feature enhancement request or any issues/bugs identified by the Customer or new software installation requirements are submitted in Axosoft Tool.

- If it is a new “Feature” enhancement request Configuration Manager will review and provide the details to the QA Lead to open a related Feature(s) in Axosoft.
- If it is a “Bug/Issue” the Configuration Manager will assign the support case to the QA Lead. QA will try to reproduce the issue and if the issue was reproduced a new related BUG will be opened in Axosoft.
- If it is a software installation/update, the system administrator will open a related Feature(s) in Axosoft and once the installation/update is complete, the respective “Feature” will be updated and closed by the system administrator.

The Inteum Configuration Manager and QA will make sure the support cases are tracked till the closure.

THE REMAINING PORTION OF THIS PAGE IS LEFT INTENTIONALLY BLANK.

Data Backup

IT Data Backup Policy

Purpose

The purpose of the IT Data Backup Policy is to describe the policies for backing up and retaining the Company's onsite data.

Scope

This document applies to all Company's computing environments and all System Applications, data, and related system software, including operating systems. It is updated when the backup policy changes. See the IT System Ownership Standard for a list of System Applications.ITSystemOwnershipStandard

Policy Statements

1. **Backup Frequency**
   - 1.1. Backups are to be taken as follows:
     - 1.1.1. System Applications and Data
       - 1.1.1.1. Backups are completed nightly, onsite.

2. **Storage**
   - 2.1. Backups are to be stored as follows:
     - 2.1.1. Onsite
       - 2.1.1.1. Store the primary backup media onsite in the same location as the server/storage.
     - 2.1.2. Offsite
       - 2.1.2.1. Store the secondary backup media in an alternate location that is sufficiently distant from the primary location.
       - 2.1.2.2. Backups under IT department management are not stored on removable media and rotated to an offsite storage location. Rather, backups are copied or replicated to offsite storage.

3. **Retention**
   - 3.1. Backups are to be retained as follows:
     - 3.1.1.1. Retain backups for a minimum of 4 weeks from the date they are taken.

4. **Update**
   4.1. The backup procedure is reviewed annually and updated as appropriate.

Exceptions

None.

THE REMAINING PORTION OF THIS PAGE IS LEFT INTENTIONALLY BLANK.

IT System Ownership Standard

Purpose

The IT System Ownership Standard specifies the Application Owner and IT Application Support Owner of each application and their responsibilities.

Scope

The IT System Ownership Standard is applicable to all applications of “Inteum Company LLC” and “Inteum Company LLC” clients. The Company’s applications may be further defined at the module level, where ownership may change by location or by business unit.

Standard Statements

Each application is required to have both an Application Owner and an IT Application Support Owner.

1. **System Applications**
   1.1. System Applications are deemed critical to Company operations and have a material impact on revenue generation and financial reporting activities.
   1.2. All applications at “Inteum Company LLC” are considered critical.

The responsibilities of the Application Owner and IT Application Support Owner are described below.

Application Owner Responsibilities

Responsibilities of this position may be delegated; however, the assigned application owner retains ultimate accountability. For applications owned, these responsibilities include:

1. Designing application controls that ensure data integrity;
2. Authorizing access to secure/proprietary data and systems;
3. Periodically reviewing access to applications owned;
4. Approving upgrades, changes, or modifications to systems;
5. Approving exceptions to standards; and
6. Recommending disciplinary actions for infringement of policy or standards.

IT Application Support Owner Responsibilities

Responsibilities of this position may be delegated; however, the IT application support owner retains ultimate accountability. For applications owned, these responsibilities include:

1. Custodial responsibilities for the system;

2. Protection of physical assets;
3. System installations and updates to production;
4. Operational usage, monitoring, and capacity planning;
5. Licensing usage and monitoring;
6. Retirement/discontinuance/replacement of system;
7. Authority for data (system) access as per the application owner's instructions;
8. Compliance with change control standards for system certification (testing);
9. Suspension of access privileges if suspicious activities could compromise the security of the Company's computing environment; and
10. Backup and recovery of system application components.

Exceptions

None.

Noncompliance Penalties

Not applicable

THE REMAINING PORTION OF THIS PAGE IS LEFT INTENTIONALLY BLANK.