Information Technology (IT)
Policies, Procedures, and Standards

Department: Information Technology (IT)
Owner: Chief Technology Officer
Version: 1.1
Effective:

RevGen' 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 RevGen contact or to the RevGen Chief Technology Officer.

Confidential Information

This document contains information confidential and proprietary to RevGen

TABLE OF CONTENTS

Document History

Date	Revision	Description	Author
12/5/18	1.0		Initial Content
6/24/19	1.1	Contractor version	Steven Martin

SECURITY

IT SECURITY POLICY

Purpose

The purpose of the IT Security Policy is to ensure that the information assets of RevGen (“RevGen” or “the Company”) 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 of the Company’s applications and supporting IT infrastructure are classified by a System Tier level structure as defined in the IT System Ownership Standard.
   2.2. All System Tier 1 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.

3. **User Level Access**
   3.1. User access to the Company’s computing environment is available to employees or authorized contractors. All contractors must sign the 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 Tier 1 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.
      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.
      3.3.6. Password strength configuration parameters by system and application follow company policy (see Security Policy Table at the end of this section).

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. No user should have any expectation of privacy in anything they create, store, send, or receive on or through the Company's computing environment.

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
Microsoft Office 365 apps	Password is ynced with network	Does not expire	Password is synced with network	N/A	10 failed attempts - Duration of 15 minutes

*Note: In addition to the password policy identified above, Microsoft Office 365 apps have Multi-factor Authentication (MFA) enabled to increase the security of information used on laptops, mobile devices, etc.

4. Virus Protection

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

5. Remote Access

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

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

6. System Level Access

6.1. System Tier 1 Application direct database access must be must be approved by the Security Officer and requested as per the IT Security Procedure.

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 contractor devices (i.e. phones and other BYOD devices). Client devices are isolated from RevGen's network.

7.2. Wireless access to the RevGen network is permitted under the following conditions:

7.2.1. Wireless access to the RevGen 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 RevGen's security and antivirus requirements.

8. Communications Over Public Networks

8.1. 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.).

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

9. Disposal of Sensitive Information and Data

9.1. Sensitive information and data from computers, disks, and other equipment or media must be irretrievably erased when disposed of or transferred to another use or done in accordance with client standards, as applicable.

10. Removable Media

10.1. Removable Media should be used in accordance with client standards. If there are no client standards, sensitive data stored on removable media should be, at a minimum, physically secured.

11. Facility

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

12. Incidents

12.1. 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.

13. Annual User Access Review

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

13.2. The user access review is conducted for user access to System Tier 1 Applications, production data, operating systems, external network connections, firewalls, routers, and physical security.

14. Monitoring for Potential Unauthorized Activity

14.1. 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.

14.2. 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 Tier 1 Application, firewall, router, or other key elements of the IT infrastructure.

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

15. Periodic Risk Assessment

15.1. 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.

Exceptions

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

Test Email Accounts: Sharing of individual user IDs and passwords is strictly prohibited unless it has been approved by the Senior Consultant in Managed Services or above 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 contractor agreement 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 RevGen (“RevGen” or “the Company”) 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 Tier 1 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.

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 Tier 1 Applications. (See the IT System Ownership Standard for a list of System Tier 1 Applications.)

2.1.2. Application Owner approval is required for update access to System Tier 1 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 creates a termination ticket which notifies the IT Department and Security Officer, as applicable, such as an IT Department Member.

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 generated ticket to see which accounts should be disabled or deleted.

4.2.1. Regarding all Tier 1 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.

4.3. For each user that has been terminated, the date their system access was terminated is recorded on their most recent IT Security Access Ticket on file.

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. Switch(es)
5.1.5. External Network Connection(s)
5.1.6. System Tier 1 Application(s) and Data
5.1.7. 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 Tier 1 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.

CHANGE CONTROL

IT CHANGE CONTROL POLICY

Purpose

The purpose of the IT Change Control Policy is to ensure that changes to RevGen ("RevGen" or "the Company") computing environment are requested, authorized, and implemented in a controlled manner.

Scope

This policy applies to all System Tier 1 Applications listed in the IT System Ownership Standard and supporting IT infrastructure.

Definition

RevGen defines changes as modifications to a process which alters the way day to day business operations occur.

Policy Statements

1. **Application Ownership**

   1.1. All System Tier 1 Applications must be owned by a designated Application Owner. The change control-related responsibilities of the Application Owner are documented in the IT System Ownership Standard.

2. **Recordkeeping**

   2.1. All changes are recorded in the ticketing system.

3. **Direct Data Updates**

   3.1. Direct data updates to System Tier 1 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 Change Control Form.

4. **Update Access to Production**

   4.1. Update access to production environments hosting System Tier 1 Applications is restricted to the IT Application Support Owner and support personnel, designated backups, and authorized Third-Party Vendors.

5. **Impact Assessment**

   5.1. 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 Change Control Form.

6. **Approval**
   6.1. The requirements for change request approval are based on the impact assessment and is determined using the Approval Matrix in the IT Change Control Procedure. The approval is documented on the IT Change Control Form.

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

8. **Prioritization**
   8.1. 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 of contractor agreement and possible civil liability and/or criminal prosecution.

IT CHANGE CONTROL PROCEDURE

Purpose

The purpose of the IT Change Control Procedure is to define the procedure for making changes to the RevGen ("RevGen" or "the Company") computing environment.

Scope

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

- System Tier 1 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 Tier 1 Data – New databases or files, changes to database/file structures, and direct data updates to production data.
- System Tier 1 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 Tier 1 Applications.

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.

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 Change Control Form within a ticket and include the following information:

1.5.1. Requestor

1.5.2. Date Requested

1.5.3. Target Date

1.5.4. Impact Assessment (Low, Medium, High)

1.5.5. Change Type (Application, IT Infrastructure, Direct Data Update)

1.5.6. Application(s), IT Infrastructure, and Data affected
1.5.7. Description (of the change request)
1.5.8. Approval(s) – Application Owner, if required
1.5.9. Approval(s) – IT Application Support Owner, if required
1.5.10. Approval(s) – Security Officer/ Delegated Official
1.5.11. 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 Tier 1 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 Tier 1 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 Tier 1 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. Obtain Approval

3.1. For all change requests, approvals are required as shown in the Approval Matrix:

Approval Matrix

Role	High Impact	Medium Impact	Low Impact
Approval to Implement – Applications and Direct Data Updates			
Application Owner	All	All	All
Security Officer/ Delegated Official	All	All	—
Approval to Implement – Operating Systems, External Network Connections, Routers, and Firewall			
Application Owner	All	All	All
Security Officer/ Delegated Official	All	All	—

3.2. Document approval or non-approval in the IT Change Control Ticket.

4. Back-Out Procedure

The steps in this section are performed whenever a change to the Company's computing environment must be backed-out.

4.1. If IT Department personnel determine that a change must be backed out:

4.1.1. IT Department personnel obtain the backup media for the System Tier 1 Application and/or Operating System from storage.

4.1.2. IT Department personnel restore from backup.

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

4.1.4. 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.

IT CHANGE CONTROL FORM

Requestor *Name & title of the change requestor*	Date Requested *Date change requested*	Target Date *Date change desired/ scheduled*	Impact Assessment *Low, Medium, or High assessed impact on the business*

Change Type *Application, IT Infrastructure, Data*	Application Affected *Application Name(s)*	IT Infrastructure Affected *Operating System, Firewall, Router, Switch, Server Hardware, Other*	Data Directly Updated *Application Names(s)*

Description of Change Requested/Made

Provide details of new/updated software version or release; hardware change; or, direct data update made to System Tier 1 Application data as per the requirements of the IT Change Control Policy and IT Change Control Procedure. If space below is insufficient, please attach additional pages as needed.

Is this is a new System Tier 1 Application? Yes / No

(Circle YES or NO. If YES, develop and attach the following documents and check-mark each box.)

□ Implementation Plan □ System Conversion Plan □ Data Conversion Plan □ Testing Plan

□ Rollback Plan

Is this is a new version or release of an existing System Tier 1 Application? Yes / No

(Circle YES or NO. If YES, complete the following confirmation of user acceptance testing.)

Has the Application Owner completed quality assurance of new or modified functionality which is used by the Company?	Yes/No

To be completed by the IT Department employee for each change as appropriate:

Have policies, procedures, and standards affected by the change been updated?	Yes/No/NA
Have the "RevGen-IT Software and Hardware Inventory" spreadsheets been updated?	Yes/No/NA
Have the network security configuration and/or network security control activities been updated?	Yes/No/NA
For Medium and High Impact Assessment ratings, have users been notified of the pending change?	Yes/No/NA
For Medium and High Impact Assessment ratings, has a system backup been taken prior to implementation?	Yes/No/NA
For High Impact Assessment ratings, is implementation scheduled for non-business hours?	Yes/No/NA

Approvals:

Application Owner *Required for all changes to applications owned and all High Impact changes*	Date *Date Application Owner approved/ completed change*	Security Officer *Required for all changes*	Date *Date SO approved/completed change*

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 RevGen (“RevGen” or “the Company”) onsite data.

Scope

This document applies to all of the Company’s computing environments and all System Tier 1 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 Tier 1 Applications.

Policy Statements

1. Backup Frequency

1.1. Backups are to be taken as follows:

1.1.1. System Tier 1 Applications and Data

1.1.1.1. Backups are completed nightly, onsite.

1.1.2. Operating Systems

1.1.2.1. Take full backups after the close of business each night, onsite and offsite.

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 30 days from the date they are taken.

4. Update

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

Exceptions

None.

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 RevGen and RevGen 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 Tier 1 Applications**
   1.1. System Tier 1 Applications are deemed critical to Company operations and have a material impact on revenue generation and financial reporting activities.
   All applications at RevGen are considered critical and therefore are Tier 1.

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
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
10. Backup and recovery of system application components

Exceptions

None.

Noncompliance Penalties

Not applicable