Treasury Software IT Policies

Updated January 21, 2020

http://www.treasurysoftware.com/Public/Policies/IT_Policies.pdf

Table of Contents

1. Access Control Policies / Procedures

2. Purpose

This policy establishes the Access Control Policy, for managing risks from user account management, access enforcement and monitoring, separation of duties, and remote access through the establishment of an Access Control program. The access control program helps Treasury Software implement security best practices with regard to logical security, account management, and remote access.

3. Scope

The scope of this policy is applicable to all Information Technology (IT) resources owned or operated by Treasury Software. This includes any information that is transmitted or stored on Treasury Software IT resources (including e-mail, messages and files). All users (Treasury Software employees, contractors, vendors or others) of IT resources are responsible for adhering to this policy.

4. Requirements

The following subsections outline the Access Control standards that constitute Treasury Software policy.

Access Control Procedures: All Treasury Software Systems must develop, adopt or adhere to a formal, documented access control procedure that addresses purpose, scope, roles and responsibilities.

Account Management: All Treasury Software Systems must:

- Identify account types (i.e., individual, group, system, application, guest/anonymous, and temporary).
- Establish conditions for group membership.
- Identify authorized users of the information asset and specifying access privileges.
- Establish, activate, modify, disable, and remove accounts.
- Specifically authorize and monitor the use of guest/anonymous and temporary accounts.
- Notify account managers when temporary accounts are no longer required and when information asset users are terminated, transferred, or information assets usage or need-to-know/need-to-share changes.
- Deactivate temporary accounts that are no longer required and accounts of terminated or transferred users.
- Review accounts on a periodic basis or at least annually.

Separation of Duties: All Treasury Software Business Systems must:

- Separates duties of individuals as necessary, to prevent malevolent activity without collusion.
- Document separation of duties.
- Implements separation of duties through assigned information asset access authorizations.

Least Privilege: All Treasury Software Business Systems must employ 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 organizational missions and business functions.

Session Lock: All Treasury Software Business Systems must prevent further access to the information asset by initiating a session lock after 120 minutes of inactivity or upon receiving a request from a user. In addition, Treasury Software Business Systems must retain the session lock until the user reestablishes access using established identification and authentication procedures.

Remote Access: All Treasury Software Business Systems must use only approved commercially available solutions for remote access. No exceptions unless another third party application is specified.

Wireless Access: No wireless access is permitted due the development environment at hand. All development and access will be from wired connections.

Access Control for Mobile Devices:
Is only allowed using our external hosted systems:
--email
--trouble tickets

Publicly Accessible Content: All Treasury Software Business Systems must:

- Designate individuals authorized to post information onto an organizational information system that is publicly accessible.
- Train authorized individuals to ensure that publicly accessible information does not contain nonpublic information.
- Review the proposed content of publicly accessible information for nonpublic information prior to posting onto the organizational information system.
- Review the content on the publicly accessible organizational information system for nonpublic information.
- Removes nonpublic information from the publicly accessible organizational information system, if discovered.

5. Enforcement
   Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Definitions – n/a

7. Revision History
   This policy was approved on December 27, 2017

2. Segregation of Duties Policies / Procedures

1. Purpose

Separation of duties is one tool used to ensure the integrity and security of Treasury Software's development environment. Separation of duties is both an IT "best practice" and control standard that reduces the risk of a malicious or inadvertent breach of system security and the disruption of normal business processes. The Company requires that individuals or workgroups not be in a position to control all parts of a transaction or business process.

2. Scope

This policy applies to all employees and contractors who have access to Treasury Software information resources. In addition - this policy applies to all Company information systems and services for which it is responsible. It applies to any computing device owned by the Company that might experience a security incident. It also will apply to any computing device regardless of ownership, which is used to store restricted/confidential Company data, or which, if lost, stolen or compromised, could lead to the unauthorized disclosure of confidential Company data.

3. Requirements

Separation-of-duties requirements include (but are not limited to) the following:

- Non-development staff should not access or modify application code. Code is available for error reporting and support on a 'read-only' basis.
- At each release/build, a line-by-line change review is performed using a software utility such as Winmerge against the prior release/build. This is performed at the director level.
- Access to firewalls and other network security systems should be limited to the director level.

By separating these functions, each area is a "check and balance" of the functions of the other area.

In general - all rights and permissions are issued to the lowest level that is needed to complete the required task at hand.

This prohibits one person from giving an account unauthorized access levels and reviewing system logs or audit reports which could alert an independent reviewer of potential system misuse.

By specific reference, the Treasury Software policy Human Resource Termination Policies and Procedures is incorporated to cover the topic of removing users from access once they are no longer employed with the Company.

4. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Definitions

6. Revision History

This policy was approved on December 27, 2017.

3. Remote Access Policy

1. Purpose

The purpose of this policy is to define standards for connecting to Treasury Software's network from any host using an approved solution. These standards are designed to minimize the potential exposure to Treasury Software from damages which may result from unauthorized use of Treasury Software resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image or damage to critical Treasury Software internal systems.

2. Scope

This policy applies to all Treasury Software employees, contractors, vendors and agents with Treasury Software-owned or personally-owned computer or workstation used to connect to the Treasury Software network. This policy applies to remote access connections used to do work on behalf of Treasury Software.

Currently (December 27, 2017), two individuals are authorized for remote access – and each can only access their workstation.

3. Requirements

- Only a corporate approved third party sanctioned solution may be used for remote access (not named here for security purposes).
- At no time should any Treasury Software employee provide their login or email password to anyone, not even family members.
- Treasury Software employees with remote access privileges must ensure that their computer which is remotely connected to Treasury Software's corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
- Treasury Software employees and contractors with remote access privileges to Treasury Software's corporate network must not use non-Treasury Software email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct Treasury Software business, thereby ensuring that official business is never confused with personal business.
- Personal equipment that is used to connect to Treasury Software's networks must meet the requirements of Treasury Software-owned equipment for remote access.

4. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Definitions

6. Revision History

This policy was approved on December 27, 2017

4. Asset Management Policies / Procedures

1. Purpose

Treasury Software IT Services supports company owned technology equipment, software, and peripherals in ways that ensure an efficient, cost effective, reliable and secure computing environment for the company. To ensure the continued efficiency, reliability, and security of their technology systems, Treasury Software IT Services has established the following guidelines for asset management.

2. Scope

Treasury Software IT Services has established the following guidelines and procedures for all technology purchases.

3. Requirements

Some things to note when purchasing equipment, software, or peripherals include:

- Any computer equipment, software or peripherals that interact with Treasury Software's administrative or financial systems will require a technology and security review prior to purchase.

Treasury Software's ***IT Services can provide only limited support to non-standard computer equipment, software, or peripherals.*** Some things to consider when purchasing or requesting support for technology equipment, software, or peripherals include:

- Treasury Software's technicians have the experience, tools, and certifications to provide support for a limited range of technology vendors, models and versions. In general, Treasury Software's IT Services will not be able to support technology equipment, software, or peripherals outside of these standard models or versions.

- Treasury Software IT Services will not be able to service equipment or support software that is beyond economical repair or support. In general, this includes laptop and desktop computers and consumer-grade printers and peripherals more than three years old as well as older versions of software that do not run on currently supported operating systems.

- As Treasury Software is a Gold Certified Partner – all computers should be running the latest Operating System at all times. As of this writing, this is Windows 10.

4. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Definitions

6. Revision History

This policy was approved on December 27, 2017

5. Antivirus, Malware Policies and Procedures

1. Purpose

This policy is designed to protect the organizational resources against intrusion by viruses and other malware.

2. Scope

This policy applies to all Treasury Software employees, contractors, vendors and agents with Treasury Software-owned or personally-owned computer or workstation used to connect to the Treasury Software network. This policy applies to computers using remote access connections to Treasury Software.

3. Requirements

All computers noted in the scope should have a current copy of Norton Anti-virus running on it. It should be set to scan all incoming and outgoing mail. Anti-virus software will be configured for daily updates and employees will run weekly scans of their computers.

When a virus or malware is found in an inbound email, the policy will be to delete the email and not to notify either the sender or recipient by email. The reason for this is that most viruses fake the sender of the email and sending them a notice that they sent a message with a virus may alarm them unnecessarily since it would not likely be true. If the case appears otherwise, please feel free to notify the originator by phone or other offline method.

The real time protection of the anti-virus should not be disabled at any time.

Development – In addition all development code on each build will receive a code differential check, on a line by line basis using a tool such as Winmerge.

4. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Definitions – n/a
6. Revision History

This policy was approved on December 27, 2017

6. Confidentiality Agreements / Non-Disclosure Agreements

1. Purpose

Treasury Software is committed to promoting an environment that retains the full trust and confidence of its clients and employees. To promote a respectful workplace and honor the rights of all clients and employees, it is essential that the confidentiality and privacy of information be maintained. As a Treasury Software employee who has been given access to confidential information, it is your responsibility to protect this sensitive and personal data.

2. Scope

All employees, including contract workers, who have access to data containing personal, sensitive or financial information.

3. Requirements

Confidential information is considered to be all non-public information that can be personally associated with an individual. Treasury Software relies on its employees to maintain this confidentiality and to access, use, discuss, release, and disclose this data only when it is dictated by their job duties. If access to confidential information is not required to perform the job, under no circumstances should it be accessed. If access to confidential information is necessary to carry out job responsibilities, the information should not be divulged to anyone unless it is done so through authorized protocols.

Confidential information can include, but is not limited to: Social Security Numbers, Bank Account Numbers, Routing Numbers, Driver's License Numbers, Credit Card Information, Payroll Information, Passwords, etc.

Confidential information should not be sent unprotected over the Internet, stored unencrypted on an unsecured computer or an unsecured external storage medium or device, or communicated using an unauthorized third party e-mail or social networking system.

Preservation and protection of usernames and passwords ensure that only authorized users have access to our data. Since user access privileges are tailored to an individual's job responsibility, sharing of usernames and passwords is prohibited. Passwords should not be composed so that they may be easily guessed, and should conform to the password creation standards set by Treasury Software [1]. If they should be disclosed to any other person, the employee will be held fully accountable and responsible for any use or misuse by that individual to the same extent as if that employee had performed the act.

In accessing Treasury Software confidential information, the employee acknowledges he/she will:

- Access, distribute and share confidential data only as needed to conduct business as required by his/her job;
- Respect and safeguard the confidentiality and privacy of individuals whose data is accessed;
- Protect confidential information stored or displayed on the workstation;
- Scan all downloads and media for viruses prior to use;
- Immediately report to his/her supervisor any and all security breaches;

In accessing Treasury Software confidential information, the employee also acknowledges that he/she will NOT:

- Discuss verbally or distribute in electronic or print formats, confidential information except as needed to conduct business as required by his/her position;
- Gain or attempt to gain unauthorized access to computing systems;
- Make, accept or use unauthorized copies of software or download any unauthorized programs from the Internet and ensure that license agreements are not purposefully violated;
- Use or allow others to use data for personal gain;
- Engage in any activity that could compromise the security or confidentiality of data;
- Use another's computer sign-on or computer access codes; or provide another the use of such codes to gain access to confidential information without proper authorization;
- Disclose confidential information to those not authorized to receive it.

4. Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Definitions

6. Revision History
This policy was approved on March 14, 2018

Notes (appended March 14, 2018):
1 – Current password creation standards include using LastPass or if manually entered: a minimum length of 8 characters, at least 1 uppercase letter, at least 1 lowercase letter, at least one numeric digit and at least one special character.

7. Change Management, Change Control Policies and Procedures

1. Purpose
The primary goal of the IT change management organization is to accomplish IT changes in the most efficient manner while minimizing the business impact, costs and risks.

2. Scope
This policy applies to all Treasury Software personnel involved in activities that cause or require changes to technology solutions within our environment.

3. Requirements
The purpose of change management is to ensure that standardized methods and procedures are used to alter the production environment to minimize the negative impacts of that change.

The specific objectives of applying a change management system are to:
--Implement changes on schedule
--Publish a calendar that specifies the “maintenance window” (when changes will be allowed)
--Provide a back out plan for all changes

The benefits to be gained from implementation of a change management policy are improved system reliability and availability due to more control and thorough planning for installation of changes, as a result of improved communication and awareness of changes.

The process and procedures shall cover:

- Recording and Acceptance
- Classification
- Authorization
- Coordination and Development
- Approval
- Evaluation

A post-implementation review is conducted to ensure whether the change has achieved the desired goals. Post-implementation actions include deciding to accept, modify or back-out the change; contacting the end user to validate success; and finalizing the change documentation within the company’s selected technology platform.

4. Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Definitions

6. Revision History
This policy was approved on December 27, 2017

8. Audit, Compliance Policies and Procedures

1. Purpose

Internal audit conducts reviews and appraisals of Treasury Software procedures and operations. These reviews provide an independent appraisal of the various operations and systems of control. The reviews also help to ensure that Treasury Software resources are used efficiently and effectively while helping Treasury Software achieve its mission.

2. Scope

While carrying out their duties, the audit staff is responsible for utilizing a systematic, disciplined approach to evaluating and improving the effectiveness of internal controls.

3. Requirements

Internal Audit's primary activity is the implementation of a program of regular audits of the Treasury Software's operation, as outlined below.

- Operational Audits: Operational audits consist of critical reviews of operating processes and procedures and internal controls that mitigate area specific risks. These audits examine the use of resources to determine if they are being used in the most effective and efficient manner to fulfill the Treasury Software mission and objectives.
- Financial Audits: These audits review accounting and financial transactions to determine if commitments, authorizations and the receipt and disbursement of funds are properly and accurately recorded and reported. This type of audit also determines if there are sufficient controls over cash and other assets and that there are adequate process controls over the acquisition and use of resources.
- Investigative audits: These audits are conducted to identify existing control weaknesses, assist in determining the amount of loss and recommending corrective measures to prevent additional losses.
- Compliance: Treasury Software is not required to meet any special legal, regulatory or industry requirements. Year-end policies will review this on an annual basis (audit).

4. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Definitions

6. Revision History

This policy was approved on December 27, 2017.

9. Data Backup Policies / Procedures

1. Purpose

The purpose of this policy is as follows:
To safeguard the information assets of Treasury Software. To prevent the loss of data in the case of an accidental deletion or corruption of data, system failure, or disaster. To permit timely restoration of information and business processes, should such events occur. To manage and secure backup and restoration processes and the media used in the process.

2. Scope

This policy applies to all Treasury Software employees, contractors, vendors and agents.

The retention periods of information contained within system level backups are designed for recoverability and provide a point-in-time snapshot of information as it existed during the time period defined by system backup policies.

3. Policy

Systems will be backed up according to the schedule below. All backups will be in a separate location from their original source. Additional instructions, if needed – are noted.

Website – full backup each month, and before any system-wide changes. Backup data is to be located off-site from original (Go Daddy). After backup, upload/FTP data to Web.com to ensure hot-site / live backup is up-to-date.

Backup email (Outlook pst files) daily.

Backup (export to static help) Notes – Help (http://www.helpconsole.com/) monthly.

Notes: Code for development and version control to be maintained by developers.

Appliances – Avaya phone system, Cisco Router – backed up monthly and before any maintenance.

Storage of backup media:
All media can be backed up to a hard drive backup – and stored either at the office (locked) or can be placed into our Safety Deposit box at Bank of America.

Notes: During transport or changes of media, media will not be left unattended.
Based on the current low cost of hard drives – backups will be saved for at least six months, and then re-used.

Sensitive data
Backups of sensitive data need to be encrypted prior to storage. May use Egnyte account (encrypted) or encrypt data (256 bit AES) prior to storage/archive.

Restoration / Hot Sites
Treasury Software maintains a live hot-site for the domain TreasurySoftware.com. This is an automatic cutover maintained by a third party DNS manager, who is not affiliated with the host of either primary or secondary web sites.

Our development environment has been replicated into a virtual machine and can be run with the proper security from any Windows 8.1 computer with Hyper-V.

Our shopping cart, ticketing system and other web services have established disaster recovery procedures.

Backups and Data Recovery - John Lahrman

Telephone System Backups - Heather Farnsworth

Verification Glenn Fromer
Data backups shall be tested upon the introduction of new procedures or equipment – or at a minimum on an annual basis.

4. Enforcement
   Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Definitions

6. Revision History
This policy was approved on December 27, 2017

10. Data Destruction / Disposal Policies / Procedures

1. Scope
This policy applies to all employees and independent contractors of Treasury Software. It addresses disposal of electronic information storage devices owned by Treasury Software, including those contained within or attached to personal computers, servers, laptops, phones or any other computing/mobile device, accessory equipment, or standalone devices that store electronic data, information, and/or software programs.

2. Purpose
When information technology (IT) equipment is in normal use, it is assumed that the entity to which the equipment is assigned (the "Owner") is responsible for guaranteeing appropriate security for all information stored on or maintained by that equipment. When the owner wishes to dispose of that equipment, explicit action must be taken to assure that confidential information does not remain accessible to a new owner. All equipment should be forwarded to the Director of Development for disposal.

Sensitive information includes data required by federal or state law to be protected from disclosure as well as any other confidential data noted by Treasury Software. For purposes of this policy, sensitive information also includes proprietary software that is licensed to Treasury Software, which must be protected against unauthorized distribution.

This policy outlines disposal requirements for protecting these IT assets by either of two methods: (1) destruction of the IT device; or, (2) complete removal of all electronic data from the computer storage device. The Director of Development is responsible that at least one of these actions has been performed.

Disposal requirements

All computer storage devices and removable storage media must be cleaned prior to disposal, regardless of how their owner chooses to dispose of them.

1. All data maintained specifically by the owner and any software programs that are licensed exclusively to the owner must be removed from storage devices and/or media prior to their disposal, except that legally licensed operating system software (e.g., Microsoft Windows) that is tied to a specific computer serial number and which may be legally transferred with the computer to another licensee, may remain on (or may be restored to) the storage device following the cleaning process. (Note: Because of the varying circumstances under which computers may have been acquired, it is the responsibility of the owner to determine, prior to transferring any licensed operating system software, whether it is legally permissible to do so.)

2. Alternatively, if data and/or software programs contained on the storage device and/or media cannot be removed according to the following process, then that device and/or media must be destroyed.

3. To remove data and software from rewritable storage devices or media, the Director of Development, or representative - must use a Department of Defense (DoD) 5220.22-compliant sanitation program or an equivalent method of removal or destruction of data and software (such as high-intensity degaussing of magnetic storage media) that will effectively sanitize the hard drive. To be DoD 5220.22-compliant, programs must use the DoD's "three-pass" process to: (1) overwrite all electronically addressable locations on the device with a character; (2) overwrite it again with the same character's complement bit configuration: and then (3) overwrite it again with

a random character. Finally, the program must perform a verification process to assure that the cleaning has been accomplished.

a) If the data storage device cannot be put through this process because it is not functional or because it is not rewritable, the device must be physically destroyed.

b) All removable storage media must be cleaned using a method such as high-intensity degaussing or must be physically destroyed.

c) The Director of Development will maintain a log on all devices that have been either destroyed or sanitized.

4. Enforcement
   Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Definitions

6. Revision History
   This policy was approved on December 27, 2017

11. Application Development Policies and Procedures

1. Purpose

To keep risk to an acceptable level, Treasury Software shall ensure that the proper security controls will be implemented for each application. This policy addresses the following requirements:

- Application security standards and implementation guidelines.
- The implementation of security controls during the system's lifecycle.
- Security documentation.

2. Scope

This standard applies to all software applications that are being developed or administered by Treasury Software.

3. Requirements

Computer applications should follow a standardized application lifecycle, at a minimum, this should include planning, development, testing, and production phases. Updates, patches, and feature changes should follow the same phases and processes as if the application were being developed from concept.

Specifically, Treasury Software follows an Agile Software development methodology, which utilizes an incremental approach. Iterative development prescribes the construction of small portions of a software project (in prototype) to help all those involved to uncover important issues early before problems or faulty assumptions. The Company targets a minimum of 12 releases annually.

Further, the Company follows a Dynamic systems development method (DSDM), which is an agile project delivery framework. DSDM assumes that users simply can't define requirements for a perfect system until a new system is in place and in use for some time. "Perfection," or complete satisfaction, can only be clearly defined as a set of requirements after what was imagined has actually been used—in other words, the users have to use it to know what they really want in a system.

Principles:

1. Focus on the business need

The main criteria for acceptance of a "deliverable" is delivering a system that addresses the current business needs - on critical functionalities.

2. Deliver on time

Timebox the work - Always meet deadlines

Focus on business priorities

3. Collaborate

User involvement is the main key so that the decisions can be made collaboratively and quickly.

4. Never compromise quality

Set the level of quality at the outset

Design, document and test appropriately

Build in quality by constant review (code review).

Test early and continuously (alpha and beta)

5. Build incrementally and frequently

6. Communicate continuously and clearly

Keep documentation lean and timely

7. Demonstrate control

Use an appropriate level of formality for tracking and reporting

Make plans and progress visible to all

For all systems:
Each individual user (whether a developer, administrator, or user) should have a unique set of credentials for accessing the application. Each process or application role should also have a unique credential.

Only authenticated users should have access to the application. Each user should only be allowed to access the information they require.

Developers should follow best practices for creating secure applications with the intention being to minimize the impact of attacks. A code validation process should be followed to discover and remediate any code errors before an application is approved for production. This may include, but not necessarily limited to peer review, web application scanning, and/or other methods as specified by the application lifecycle process.

The production data source should not be used to develop or test the application.

Quality control - All releases, including interim service packs must undergo both alpha and beta testing. A separate source code line review should be performed using WinMerge or similar application.

Development and testing databases should be redacted if copied from production data sources. A separate data source will be created for each application. Access control procedures should remain the same for the test environment.

Access Control for software
Overview:
http://www.treasurysoftware.com/Help7ACH/login.html

To assign/add a user:
http://www.treasurysoftware.com/Help7ACH/users-add.html

Grant/revoke permissions for Segregation of Duties (client based):
http://www.treasurysoftware.com/Help7ACH/segregation_of_duties.html

Passwords
Strong passwords may be required when adding a user (see above) for internal access as well as defined by the client's SQL Server Database Administrator.

4. Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Definitions

6. Revision History
This policy was approved on December 27, 2017.

12. Secure Coding Policies and Procedures

1. Purpose
   This policy establishes practices to ensure secure code is developed and implemented. This policy's purpose is to reduce the opportunity for malicious code to be inserted in software as well as protect the integrity of the system's data through malicious actions.

2. Scope
   This policy applies to all Treasury Software employees, contractors, vendors and agents with Treasury Software-owned or personally-owned computer or workstation used to connect to the Treasury Software network.

3. Requirements

   Selection of controls is only possible after classifying the data to be protected. For example, controls applicable to low value systems such as blogs and forums are different to the level and number of controls suitable for accounting.

   General principles:
   Confidentiality – only allow access to data for which the user is permitted
   Integrity – ensure data is not tampered or altered by unauthorized users
   Availability – ensure systems and data are available to authorized users when they need it

   Establish secure defaults. Deliver an "out of the box" experience for users that by default, the experience should be secure, and it should be up to the user to reduce their security – if they are allowed.

   Validate input. Validate input from all untrusted data sources. Proper input validation can eliminate the vast majority of software vulnerabilities. Be suspicious of most external data sources, including command line arguments, network interfaces, environmental variables, and user controlled files.

   Architect and design for security policies. Create a software architecture and design your software to implement and enforce security policies. For example, if your system requires different privileges at different times, consider dividing the system into distinct intercommunicating subsystems, each with an appropriate privilege set.

   Keep it simple. Keep the design as simple and small as possible. Complex designs increase the likelihood that errors will be made in their implementation, configuration, and use. Additionally, the effort required to achieve an appropriate level of assurance increases dramatically as security mechanisms become more complex.

   Default deny (a.k.a. fail securely). Base access decisions on permission rather than exclusion. This means that, by default, access is denied and the protection scheme identifies conditions under which access is permitted.

   Adhere to the principle of least privilege. Every process should execute with the least set of privileges necessary to complete the job. Any elevated permission should be held for a minimum time. This approach reduces the opportunities an attacker has to execute arbitrary code with elevated privileges.

   Practice defense in depth. Manage risk with multiple defensive strategies, so that if one layer of defense turns out to be inadequate, another layer of defense can prevent a security flaw from becoming an exploitable vulnerability and/or limit the consequences of a successful

exploit. For example, combining secure programming techniques with secure environments should reduce the opportunity for a vulnerability to run successfully.

Use effective quality assurance techniques. Good quality assurance techniques can be effective in identifying and eliminating vulnerabilities. Fuzz testing, penetration testing, and source code audits should all be incorporated as part of an effective quality assurance program.

All items noted here apply to both to test and production systems. Access to test and production code should be in separate repositories with separate access controls.

Training and Certification
Developers and testers are encouraged to get their Certified Secure Software Lifecycle Professional (CSSLP) certification. Treasury Software will reimburse approved online courses upon successful passing of the exam. Pre-authorization required.

4. Enforcement
   Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Definitions

6. Revision History
   This policy was approved on December 27, 2017.

13. Email Use and Security Policies / Procedures

1. Purpose

This document outlines the processes used to maintain user accounts on Treasury Software's email systems and to prevent tarnishing the public image of the company. When email goes out from Treasury Software, the general public will tend to view that message as an official statement from the company.

2. Scope

This document covers all employees who use the Treasury Software email systems, including part time employees and contractors who are provided an email account. In addition, it covers any outbound message – including our trouble ticket support system and social media postings.

3. Requirements

- Prohibited Use. The email system should not be used for any illegal or unethical purposes, disruptive or offensive messages, including offensive comments about race, creed, skin color, national origin, gender, disabilities, age, sexual orientation, pornography, religious beliefs and practice or political beliefs. Employees who receive any emails with this content from any other employee at Treasury Software, should report the matter to their supervisor immediately.
- Personal Use. Using a reasonable amount of resources for personal email is acceptable. Sending chain letters or joke emails is unacceptable.
- Monitoring. Employees shall have no expectation of privacy in anything they send, store or receive on the company's email system. Treasury Software may monitor messages without prior notice.
- Access. Email accounts are provided according to the account holder's position. Users who leave for the company for any reason – will not have access to their email account.
- Minimize exposure to viruses. Enable both incoming and outgoing email virus scans. Never click on attachments from unknown senders

- Public Image of Company. All emails should be spell checked and re-read prior to sending. **If a statement is ambiguous, or can be misinterpreted – stop and pick up the phone and call the recipient.** If you are unsure as to grammar, spelling or to content – consult with a colleague or your supervisor. **Spell check is not a substitute for re-reading your email.**

- Response time. In the normal course of business, non-urgent emails should be replied to within the same business day if possible, no later than after one business day. Acknowledge emails from clients – if a full response will not happen within the expected time.
- No passwords of any kind should be sent in an unencrypted email.
- Private data, including credit card numbers and bank account numbers – should never be sent in an email.
- Users are required to follow the security handling methods of sensitive data as noted in Information Security Policies.
- All social media postings are to be reviewed by a Director prior to posting.

Sensitive Data

Emails containing sensitive data attachments: The attachments must be encrypted using 256 bit AES. This is available using your local copy of Winzip (see 14. Encryption).

Emails containing sensitive data must use a secure email server approved by Treasury Software. Please use a SecureInc.com account.

4. Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Definitions

6. Revision History
This policy was approved on December 27, 2017

14. Encryption Policies / Procedures

1. Purpose
   The most reliable way to protect the Company's sensitive data is to avoid handling sensitive data. Sensitive data should be retained or handled only when required. Encryption can be an effective information protection control when it is necessary to possess sensitive data.

   Users should understand that data encryption is not a substitute for other information protection controls, such as access control, authentication, or authorization – and that data encryption should be used in conjunction with those other controls.

2. Scope
   Adherence to these guidelines will better assure the confidentiality and integrity of the Company's sensitive data, should data encryption be used as an information protection control.

   The objective of these guidelines is to provide guidance in understanding the encryption required for maintaining the confidentiality and integrity of the Company's sensitive data, should data encryption be used as an information protection control.

3. Requirements
   All Treasury Software workstations are licensed with a current copy of WinZip. WinZip with AES encryption should be used as the standard tool for any of the items below, unless another tool is specifically mentioned.

   Transmission. In order to protect the confidentiality and integrity of the Company's sensitive data; any data having a required need for confidentiality and/or integrity, shall be transmitted via encryption. While the Company does not currently use public / private keys with any third party – encryption should be performed using WinZip as noted above.

   Physical media included: Note that data needs to be encrypted regardless as to whether it is transmitted over a network or transported on physical media (USB thumb drive, DVD, CD, etc…).

   Storage – Sensitive data can be encrypted using Winzip (file) or the Microsoft Operating System encryption features.

   Encryption Keys
   As of this writing, the Company does not use any public / private keys with any third party.

   Data Labelling – Within any sensitive document, regardless of the storage location or mechanism, the nature of the sensitivity class should be clearly identified at the top of the document.

4. Enforcement
   Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Definitions

6. Revision History
   This policy was approved on December 27, 2017.

15. Human Resource Screening Policies / Procedures

1. Purpose
   The purpose of this policy is to ensure that individuals who join the Company's workforce are qualified for the positions for which they have applied and have accurately presented their qualifications during the hiring process. This policy also ensures that the Company is exercising reasonable care in selecting its employees to promote a safe and productive work environment.

2. Scope
   It is the policy of the Company that all external candidates for employment – as well as all contractors, sub-contractors or anyone having access to Treasury Software Information Assets - have certain credentials, criminal and other background information verified as a condition of employment.

3. Requirements

   All employee finalists at the Company are required to sign a Background Disclosure & Authorization Form to be considered for employment with the Company.

   a. **References and Employment Verification.** Personal and business reference checks resulting in reasonable and satisfactory verification of previous employment and of periods of non-employment (such as enrollment in colleges or universities, etc.).
   b. **Criminal Background Check.** At a minimum, the criminal background check must include the county or counties listed by the candidate as current places of residence and employment, and for past places of residence and employment for the previous ten (10) years. See the Section, c. Social Security Number Cross Check, below, an expanded criminal background check may be required in certain cases.
   c. **Social Security Number Cross Check.** Where the social security number cross check results in the discovery of additional (undisclosed) counties, in such undisclosed counties, the criminal background check for the candidate will include those undisclosed counties.
   d. Employees/candidates may not begin work if any of the Required Pre-screening measures, as set forth above, have not been conducted or if there are disclosed or undisclosed criminal convictions, or pretrial diversion, which violate FDIC Section 19 guidelines (acts of dishonesty or breach of trust, theft); or conviction or pretrial diversion for criminal offenses concerning the manufacture, sale, distribution of or trafficking in controlled substances.

   If the Required Pre-screening measures result in discovery/disclosure of any criminal convictions or pretrial diversion (other than minor traffic offenses) the employee/candidate shall not begin employment.

   A "Pretrial Diversion Program" is defined as any program, whether formal or informal, characterized by a suspension or eventual dismissal of charges or criminal prosecution upon agreement by the accused to treatment, rehabilitation, restitution or other non-criminal or non-punitive alternatives. Examples of pretrial diversion programs include deferred adjudication, suspended imposition of sentence, deferred prosecution, first time offender programs, or dismissal upon payment of court costs.

   Prior to offering an individual employment, the supervisor will ensure the following screening procedures have been completed:
   Review of resume and cover letter.
   Minimum of two interviews.

Minimum of three reference checks including previous supervisors, academic supervisors, and/or professional contacts.
Completion of all hiring package forms.
Criminal records check initiated, if necessary.
Child Welfare check initiated, if necessary.

Due to the timing of Criminal Record Checks being completed potentially after the projected start date of employment, potential employees will be requested during the interview, to disclose any concerns that may result in the Criminal Record Check blocking employment.

If the Criminal Records Check returns with a security concern, the supervisor will meet with the employee to discuss the security concern. The Director, in consultation with the supervisor, will determine if the security concern identified in the Criminal Records Check warrants termination.

4. Enforcement
   Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Definitions

6. Revision History
   This policy was approved on December 27, 2017

16. Human Resource Termination Policies / Procedures

1. Purpose

The goal of this policy is to assure that the Company meets its responsibilities and complies with internal guidelines during the termination process, and to establish a procedure for the separation from employment of employees, whether it is employee or employer initiated.

All employees are what the law terms "at will" employees. This means that employment is a matter of continuing agreement between the employee and the Company. Either the employee or the Company may decide to end the employee's employment here for any reason not prohibited by law, at any time. Nothing in this policy changes an employee's "at will" employment.

2. Scope

Any termination of the employment relationship, whether voluntary or involuntary, must be treated in a confidential, professional manner by all concerned. The termination information will be shared with others in the Company as deemed necessary to complete the termination process and to resolve any issues relating to the termination.

3. Requirements

A: Retirement

Treasury Software does not discriminate against any employee due to age and as such does not have a mandatory age limit for retirement of its employees.

B. Voluntary Termination (Resignation)

Prior to submission of notice of resignation, employees are encouraged to discuss the reason for resignation with their immediate supervisor.

All employees are requested to give a minimum two weeks written notice of their resignation.

Treasury Software cannot require that employees take vacation during the notice period and an employee cannot use vacation in lieu of notice.

Employment ends on the last day the employee is physically present at work. Employees cannot take vacation to extend their employment beyond their last day at work

C. Involuntary Termination

An involuntary termination of employment, including layoffs of over 30 days, is a management-initiated dismissal.

The inability of an employee to perform the essential functions of his or her job with or without a reasonable accommodation may also result in an involuntary termination. An employee may also be discharged for any legal reason, e.g., misconduct, tardiness, absenteeism, unsatisfactory performance or inability to perform.

In some cases progressive discipline may be used, prior to termination, to correct a performance problem. However, certain types of employee misconduct are so severe that one incident of misconduct will result in immediate dismissal without prior use of progressive discipline.

Immediate termination may result for:

- Gross misconduct or insubordination
- Sexual harassment

• Performance of assignment(s) while under the influence of alcohol or mind altering drugs
• Theft
• Misappropriation of Treasury Software funds
• Abuse of Treasury Software equipment or materials
• Falsification of Treasury Software records
• Misrepresentation of personal information
• Illegal, violent or unsafe actions
• Abusive treatment of clients or co-workers, either physically or mentally
• Failure or inability to project a positive image of the services of Treasury Software

This is not a comprehensive list, but is intended to clarify understanding of the repercussions for certain behaviors.

Prompt notification to the staff and/or the appropriate employees regarding immediate dismissal of a Treasury Software employee shall be the responsibility of the employee's Director.

F. Return of Property

Upon termination from Treasury Software all employees will be asked to turn in all Treasury Software property. Dismissed employees are not permitted to return to their work area after their last day of work without Supervisor accompaniment.

G. Termination Vacation Pay

Upon termination, remuneration for earned vacation will be paid in direct proportion to the period worked and the allowable vacation providing the individual gives the required notice. Unused sick leave is not paid upon separation from employment.

If more vacation time was taken in the vacation year than was earned, Treasury Software may reduce the final pay check by the amount of time taken over that earned.

Benefits information related to continuation of medical, dental, and vision coverage as required by the Consolidated Omnibus Budget Reconciliation Act (COBRA), and distributions from retirement account plans will be sent directly to the terminating employee's home address following the processing of the termination documents.

H. IT Requirements

It is necessary to involve IT in the employee termination process because a former employee who still has access to a company's network and proprietary corporate data is a security threat.

Moreover, it is smart to preserve certain technological footprints – ie. data, and logs in the event that the former employee or company itself decides to pursue litigation.

The IT (Director's) responsibilities includes researching, documenting, and revoking an employee's access to the company's electronically stored proprietary information and its information systems.

Prudent revocation of access. IT should immediately revoke all computer, network, and data access the former employee has. Remote access should also be removed, and the Company should collect all Company-owned property, including technological resources like a notebook computer and intellectual property, such as corporate files containing customer, sales, and marketing information.

However, in the case of an employee whose end of employment is scheduled at a future date, IT should consult with the employee's manager to determine the appropriate manner in which to stagger the revocation of access over the person's remaining days of employment.

Just as the granting of access and security clearances should be documented for future reference, the revocation of access should also be documented, especially for legal purposes. The goal, of course, should always be to revoke access in ways that make good business sense financially, technologically, and legally.

Preemptive Preservation of Data. While the Company should have data redundancy and retention policies that satisfy its business needs and adhere to applicable laws, such policies address the backup, restoration, and preservation of corporate data in general.

However, the Company should also backup / preserve potentially and particularly sensitive data, records, logs, and other materials that could be of legal significance were the company and former employee to wage a legal battle.

It is especially important to do this in the case of a former employee who held a high-level position and/or left the company under a cloud of suspicion.

The results of this effort should be the greater protection of corporate data as well as better preparedness for litigation regarding corporate data theft, hacking, and other forms of illegal or ill-advised uses of computing technology.

G. Exit Interviews

Upon termination of employment, employees are entitled to an exit interview with the Director of Development. The purpose of this interview is to assess the Treasury Software employment experience. Comments from the interview will be documented, and any disclosures of policy violation must be acted upon.

4. Enforcement
   Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Definitions

6. Revision History
   This policy was approved on December 27, 2017.

17. Security Awareness Training Policies and Procedures

1. Purpose

The Company's security policy sets the standard for the way in which critical business information and systems will be protected from both internal and external threats.

The purpose of the Security Training Policy is to describe the requirements for every employee of Treasury Software – regardless if they are using Information Resources – to ensure that they receive adequate training on computer security issues.

Treasury Software realizes that 'people', not necessarily 'technology', are often the largest threat to the security of sensitive information.

2. Scope
The Treasury Software Security Training Policy applies equally to all individuals that use any Treasury Software Information Resources.

While the Company does not currently have any third parties with access to Company systems – if this situation arises - all third parties with access are required to receive the same training.

3. Requirements
Security awareness training focuses on familiarizing the employees with Treasury Software's security policy. The security awareness focus users includes:
· educating users on the creation and maintenance of good passwords
· do's and don'ts for maintaining workstations
· informing users of email and Internet access policies
· employee responsibility for computer security
· reporting procedures
· emergency procedures

The focus for security awareness for system administrators may include:
· training on how to configure systems securely
· education on user account management policies
· secure remote access for support of systems

Security awareness must also reach the business or non-technical user. Security awareness training for business users may emphasize:
· how to identify social engineering tactics
· how establishing and enforcing security policies can impact the "bottom line" (limiting system downtime, protecting business critical information, etc.)
· public relations impact of DoS attacks, viruses, etc., and how security standards can help limit this risk
· increase in productivity generated by using standard, locked down systems to minimize user downtime

Topics to also include:
Information on known threats.
Security requirements.
Legal responsibilities.
Business controls.
Information on the disciplinary process.
Who to contact for further security advice or to report incidents.

Training includes the importance of security to the individual's life outside of work.

Note: All user workstations must auto-lock (time out) after a period not to exceed 60 minutes.

- All users must sign an acknowledgement stating they have read and understand Treasury Software requirements regarding computer security policies and procedures on an annual basis.

4. Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Definitions

6. Revision History
This policy was approved on December 27, 2017.

18. Incident Response Policy

1. Purpose

This policy is to assure that, in case of an information security incident that threatens the availability, confidentiality, and integrity of Treasury Software information assets, information systems, and the networks that deliver the information - a response is conducted in a consistent manner, with appropriate leadership and technical resources, in order to promptly restore operations impacted by the incident.

Such incidents may include the access to sensitive or confidential data, intellectual property, damage to public image, and/or damage to critical internal systems.

Even the best information security infrastructure cannot guarantee that intrusions or other malicious acts will not occur. When a computer security incident happens, it will be critical for Treasury Software to quickly - recognize, analyze, and respond to an incident, which will limit the damage and lower the cost of recovery.

2. Scope
This policy applies to all Company information systems and services for which it is responsible. It applies to any computing device owned by the Company that might experience a security incident. It also will apply to any computing device regardless of ownership, which is used to store restricted/confidential Company data, or which, if lost, stolen or compromised, could lead to the unauthorized disclosure of confidential Company data.

3. Requirements

1. The staff member who receives the incident notice (or discovered the incident) will contact the Director of Development and include the details of the incident. By default, the Director of Development will convene the Computing Incident Response Team (CIRT).

2. The CIRT will work to determine as to whether:

a) Is the incident real or perceived? Is the incident still in progress?

b) What data or property is threatened and how critical is it?

c) What is the impact on the business, should the attack succeed? Minimal, serious, or critical?

d) What system or systems are targeted, where are they located - physically and on the network?

e) Is the incident inside the trusted network?

f) Is a response urgent?

g) Can the incident be quickly contained?

h) Will the response alert the attacker and do we care?

i) What type of incident is this? Example: virus, worm, intrusion, abuse, damage.

3. Team members will recommend changes to prevent the occurrence from happening again or infecting other systems.

4. Upon management approval, the changes will be implemented.

5. Team members will restore the affected system(s) to the uninfected state. They may do one or more of the following:

a) Re-install the affected system(s) from scratch and restore data from backups if necessary. Preserve evidence before doing this.

b) Make users change passwords if passwords may have been compromised.

c) Confirm the system has been hardened by turning off or uninstalling unused services.

d) Confirm the system is fully patched.

e) Confirm real time virus protection is running.

f) Confirm the system is logging the correct events and to the proper level.

6. Evidence Preservation—make copies of logs, email, and other communication. Keep lists of witnesses if applicable. Keep evidence as long as necessary to complete prosecution.

7. Notify proper external agencies—notify the police and other appropriate agencies if prosecution of the intruder is possible.

8. Assess damage and cost—assess the damage to the organization and estimate both the damage cost and the cost of the containment efforts.

9. Review response and update policies—plan and take preventative steps so the intrusion can't happen again.

a) Consider whether a procedure or policy was not followed which allowed the intrusion, and then consider what could be changed to ensure that the procedure or policy is followed in the future.

b) Was the incident response appropriate? How could it be improved?

c) Was every appropriate party informed in a timely manner?

d) Were the incident-response procedures detailed and did they cover the entire situation? How can they be improved?

e) Have changes been made to prevent a re-infection? Have all systems been patched, systems locked down, passwords changed, anti-virus updated, email policies set, etc.?

f) Have changes been made to prevent a new or similar infection?

g) Should any security policies be updated?

h) What lessons have been learned from this experience?

4. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Definitions

6. Revision History

This policy was approved on December 27, 2017

19. Information Security Policies / Procedures

1. Purpose

Treasury Software possesses information that is sensitive and valuable, such as personally identifiable information, financial data, software code and other information that is considered sensitive.

Some information is protected by federal and state laws, and other information is protected by contractual obligations that prohibit its unauthorized use or disclosure. The exposure of sensitive information to unauthorized individuals could cause irreparable harm to the Company and to our clients and partners. Additionally, if Company information were tampered with or made unavailable, it could impair the Company's ability to conduct business. The Company therefore requires all employees to diligently protect information as appropriate for its sensitivity level.

2. Scope

This policy applies to all employees and contractors who have access to Treasury Software information resources. In addition - this policy applies to all Company information systems and services for which it is responsible. It applies to any computing device owned by the Company that might experience a security incident. It also will apply to any computing device regardless of ownership, which is used to store restricted/confidential Company data, or which, if lost, stolen or compromised, could lead to the unauthorized disclosure of confidential Company data.

3. Requirements

Summary of responsibilities - All employees and contractors

--Use of Company IT resources including hardware, software, services – including e-mail and Internet connectivity, is intended for Company business purposes, with limited personnel use. The privilege of limited personal use may be revoked or limited at any time.

--You may only access information needed to perform your legitimate duties as a Company employee and only when authorized by the appropriate Information Guardian.

--You are expected to ascertain and understand the sensitivity level of information to which you have access through training, other resources or by consultation with your manager or the Information Guardian.

--You may not in any way divulge, copy, release, sell, loan, alter or destroy any information except as authorized by the Information Guardian within the scope of your professional activities.

--You must understand and comply with the Company’s requirements related to personally identifiable information.

--You must adhere to the Company’s requirements for protecting any computer used to conduct Company business regardless of the sensitivity level of the information held on that system.

--You must protect the confidentiality, integrity and availability of the Company's information as appropriate for the information's sensitivity level wherever the information is located, e.g., held on physical documents, stored on computer media, communicated over voice or data networks, exchanged in conversation, etc.

--You must not install software on a Company computer without prior approval from the Director of Development. Person-to-Person (P2P) applications, Voice Over IP (VOIP), instant messenger (IM) and remote access applications pose a high risk to the company and their unauthorized use is strictly prohibited.

--You must safeguard any physical key, ID card or computer/network account that allows you to access Company information. This includes creating difficult-to-guess computer passwords.

--You must not upload, download or share files in violation of U.S. Patent, trademark or copyright laws.

--Intellectual property, including source code, that is created for the Company by its employees, vendors, contractors, consultants and others – is the property of the Company, unless otherwise specifically agreed upon by means of a third party agreements or contracts.

--You must destroy or render unusable any confidential or highly confidential information contained in any physical document (e.g., memos, reports) or any electronic, magnetic or optical storage medium (e.g., USB key, CD, hard disk) before it is discarded.

In regards to sensitive data (such as personally identifiable information, financial data, software code and other information that is considered sensitive):
--You must report any activities that you suspect may compromise sensitive information to your supervisor or to the Director of Development.

--Where applicable, your obligation to protect sensitive information continues after you leave the Company.

4. Enforcement
   Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Definitions

6. Revision History
   This policy was approved on December 27, 2017.

20. Social Media, Mobile Media, Device Policies and Procedures

1. Purpose

As Treasury Software possesses information that is sensitive, it realizes that this data may be stored on a computer or device other than a traditional computer located within the Treasury Software office.

In addition, Treasury Software realizes that certain information (although never sensitive) is posted on Social Media sites.

This goal of this policy is to help minimize the risk associated with these areas.

Note: It is not the intent of the Company to manage or specify content but to ensure users of social media are in compliance with existing policies and have access to best practices as mentioned below.

2. Scope

This policy applies to all employees and contractors who have access to Treasury Software information resources. In addition - this policy applies to all Company information systems and services for which it is responsible. It applies to any computing device owned by the Company that might experience a security incident. It also will apply to any computing device regardless of ownership, which is used to store restricted/confidential Company data, or which, if lost, stolen or compromised, could lead to the unauthorized disclosure of confidential Company data.

3. Requirements

Social Media

Social media tools can have a significant impact on organizational and professional reputations. Social media platforms are designed to create social interaction, using highly accessible and scalable publishing techniques. Examples include but are not limited to LinkedIn, Twitter, Facebook, YouTube, and Instagram.

Best Practices

This section applies to those posting on behalf of the Company, though the guidelines may be helpful for anyone posting on social media in any capacity.

Think twice before posting: Privacy does not exist in the world of social media. Consider what could happen if a post becomes widely known and how that may reflect both on the account administrators and the Company. Search engines can turn up posts years after they are created, and comments can be forwarded or copied. If you wouldn't say it at a conference or to a member of the media, consider whether you should post it online. If you are unsure about posting something or responding to a comment, ask your supervisor for input or contact the Director of Development.

Strive for accuracy: Get the facts straight before posting them on social media. Review content for grammatical and spelling errors. This is especially important if posting on behalf of the Company in any capacity.

Be respectful: Understand that content contributed to a social media site could encourage comments or discussion of opposing ideas. Responses should be considered carefully in light of how they would reflect on the account administrators and/or the Company.

Remember your audiences: Be aware that a presence in the social media world is or easily can be made available to the public at large. This includes prospective and current clients, prospective and current employees, bank colleagues and peers within the industry. Consider this before publishing to ensure the post will not alienate, harm, or provoke any of these groups.

Photography: Remember that photographs posted on social media sites easily can be saved by visitors and used without your consent. Most people will click on a picture before they will read information so it is best to use visual pictures/images as often as possible.

Personal Posts: Identify your views as your own. If you identify yourself as a Company employee, it should be clear that the views expressed are not necessarily those of the Company.

Mobile Media and Devices

Employees may use their mobile devices to access the following Company resources: Email, calendars, contacts, trouble tickets and the licensing system. When accessing these system on a public network (airports, hotels, coffee shops, etc…), the connection must be secured with the use of a Virtual Private Network (VPN).

Employees should never retain locally saved copies of documents or other sensitive data on a mobile device, unless specifically authorized in writing from the Director of Development. If an exception is authorized, the data must be stored in an encrypted format.

Note: This includes not only mobile devices, but mobile/removable storage as well – such as USB (thumb drives), DVD's and CD's.

Retirement of Mobile Devices and Removable storage – by specific reference, the Treasury Software Disposal of Computer Storage Devices Policy is incorporated into this policy.

Cloud storage
All data stored on a third-party cloud storage facility should be encrypted. The use of personal cloud-based storage systems for professional purposes is specifically prohibited.

Treasury Software has a zero-tolerance policy for texting or emailing while driving and only hands-free talking while driving is permitted.

4. Enforcement
   Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Definitions

6. Revision History
   This policy was approved on December 27, 2017

21. Network Security Management Policies and Procedures

1. Purpose
   The goal of this Network Security Management Procedures is to limit information access to authorized users, protect information against unauthorized modification, and ensure that information is accessible when needed.

2. Scope
   This policy applies to all Treasury Software personnel. The policy applies to all IT systems, to include hardware, software, media, and facilities.

3. Requirements
   --**Access – Unless otherwise noted below – no access is permitted to the Company network, other than by Company IT resources, physically located at a Company office via a hard-wired Ethernet cable, installed by Treasury Software.**

   --Wireless Access – Based on the security needs of the Company's development environment, does not allow for any wireless connection at this time.

   --Remote Access – Based on the security needs of the Company's development environment, the Company minimizes its external facing footprint – and only allows remote access on a very limited basis. The Company as of this writing, only authorizes two users to use remote access – and that is to their own workstations. Please see our Remote Access Policy for updates and details.

   --IP Addresses – Are assigned dynamically, except when required for equipment (printers, phones, etc…). Using or attempting to use a different IP address than the one assigned is prohibited.

   --Network Abuse: Interfering or attempting to interfere with the normal operation of networks and systems within or external to the Company is prohibited. Examples of this type of abuse include unreasonable use of resources, denial of service, scanning, monitoring, interception, impersonation, or modification of systems or data without authorization or consent of the system or data owner.

   --Network Authoritative Services: Operation of network-authoritative services (DNS, DHCP, and routing-related services) without authorization from the Director of Development is prohibited.

   ---Commercial Use: Use of Company Network connections to host services for unauthorized commercial purposes is prohibited.

   By specific reference, the Company's Incident Response Plan and Information Security Policy are incorporated into this Policy.

4. Enforcement
   Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Definitions

6. Revision History
   This policy was approved on December 27, 2017

22. IT Operations Policies / Procedures

1. Purpose

To maximize the availability for accessing and using information technology resources, while minimizing interruptions from information technology resource operations and/or maintenance activities.

2. Scope

All employees, contractors, and all other authorized users are responsible for complying with this policy on information technology operations.

3. Requirements

Information technology resources shall be operated and maintained in a manner that supports high availability for utilization and minimizes the risk of business interruption. To the fullest extent possible, non-emergency maintenance activities shall be performed in time periods during which a resource is not typically utilized for business purposes (i.e. Internal Systems - after 5 p.m., Website – on weekends, etc.)

All shared communications and processing resources, network routers, shall be installed with a surge protector and with a back-up UPS (uninterrupted power supply) with sufficient capacity to prevent an equipment failure if the main power supply fails.

The main website TreasurySoftware.com should be maintained on a hot server, ready to auto-fail to, should the primary fail. The hot server should be completely independent of the primary hosting company (two separate hosting companies). The third party DNS manager should ping the primary website at least every ten minutes, and auto-fail to the backup server automatically when appropriate.

Operating policies and procedures for business and IT processes should be fully documented to provide for proper coverage, in case of absence by the employee primarily responsible to perform these tasks.

By specific reference, the Company's Incident Response Plan, Information Security Policy and Change Management Policy are incorporated into this Policy.

4. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Definitions

6. Revision History

This policy was approved on December 27, 2017.

23. Patch Management Policies and Procedures

1. Purpose

Treasury Software's Patch Management policy is to review, evaluate, and appropriately apply software patches in a timely manner.

2. Scope

This policy applies to all equipment that is owned or leased by Treasury Software such as all electronic devices, servers, application software, computers, peripherals, routers, and switches.

3. Requirements

Microsoft Windows Updates (only)
All non-development computers should have their settings set to automatically download and install. Development machines can set their computers to automatically download and notify, with the requirement that any security updates be installed immediately.

All other Patches and Updates
Treasury Software IT is responsible for the overall patch management implementation, operations, and procedures. While safeguarding the network is every user's job, Treasury Software IT is responsible to ensure that all known and reasonable defenses are in place to reduce network vulnerabilities while keeping the network operating. This responsibility includes the tasks detailed below.

- Monitoring: Treasury Software will review vendor notifications and Web sites, and research specific public Web sites for the release of new patches. Monitoring will include, but not be limited to, the following:
    - Scanning Treasury Software's network to identify known vulnerabilities.
    - Identifying and communicating identified vulnerabilities and/or security breaches to Treasury Software IT department.

- Review and evaluation: Once alerted to a new patch, Treasury Software will download and review the new patch. Treasury Software will categorize the criticality of the patch according to the following:
    - Emergency—an imminent threat to Treasury Software network
    - Critical—targets a security vulnerability
    - Not Critical—a standard patch release update
    - Not applicable to Treasury Software environment

- Risk assessment and testing: Treasury Software will assess the effect of a patch prior to its deployment.

4. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Definitions

6. Revision History

This policy was approved on December 27, 2017.

24. Physical Security Policies / Procedures

1. Purpose
   Treasury Software offices that include computers and other types of information technology resources must be safeguarded against unlawful and unauthorized physical intrusion, as well as fire, flood and other physical threats.

2. Scope

   Shared responsibility for security rests with all employees of Treasury Software. An employee shall report any activity, suspected or real, of a criminal nature or any suspicious activity immediately to their supervisor or the Director of Development.

   Physical Security requires appropriate 'layering' of physical and technical security such as appropriate office layout, suitable emergency preparedness, reliable power supplies, adequate climate control and alarm systems.

3. Requirements

   A. Visitors
   All visitors and guests to Treasury Software offices must be accompanied at all times by their employee sponsor. A Visitor cannot sponsor another Visitor.

   B. Limit of Physical Access
   The IT Department will designate and physically limit access to sensitive IT equipment.

   C. Keys + Fobs
   Keys and fobs to the office and floors are provided for active employees only.
   Keys and fobs must be appropriately protected, not shared or transferred and returned when no longer needed. Lost or stolen keys/fobs must be reported immediately.

   D. Lockdown of computers
   Equipment which cannot be moved to a secure location – such as a development computer (or any computer with sensitive data) should be locked to a physical structure within the office. Laptops should be locked down using a Kensington or similar device while in the office.

   E. Storage of Backups
   While backups are rotated off-site, backups will exist on-site as well. On-site backups should be securely stored.

4. Enforcement
   Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Definitions

6. Revision History
   This policy was approved on December 27, 2017.

25. Risk Management / Risk Assessment Program Policies / Procedures

1. Purpose

The Company has business processes and sensitive data that depend on IT assets, which the Company cannot afford to lose or have exposed. Unfortunately, these IT assets are subject to an increasing number of threats, attacks and vulnerabilities, against which more protection is continually required. These threats can come from individuals (internal and external, hackers, competitors, user errors), technical threats (crashes, overloads, viruses), and/or environmental threats (natural disasters, floods, hurricanes, earthquakes).

A formal Information Security Risk Management (ISRM) program consistently identifies and tracks information security risks, implements plans for remediation, and provides guidance for strategic resource planning.

2. Scope

Information Security Risk Management is the process with which Treasury Software identifies information security risks and determines their likelihood and impact; incorporates the implementation of plans for remediation; and provides guidance for strategic resource planning.

3. Requirements

Risk refers to the probability of an event and potential consequences to an organization associated with that event's occurrence. Risks do not necessarily exist in isolation from other risks; as a result, a series of risk events may result in a collective set of consequences that is more impactful than the discrete set of consequences associated with risk events taking place in isolation.

Risk is inherent to any activity. It is neither possible, nor advantageous, to entirely eliminate risk from an activity without ceasing that activity. The safest ships are the ones that do not sail, but that is not what they are designed for.

The goal of risk treatment is to reduce risk(s) to the lowest acceptable residual risk level. Risk treatment also includes prioritizing risks and implementing the treatment measures identified during the assessment.

The Director of Development is responsible for identifying and tracking security risks and an ongoing basis, and is responsible for updating this list as changes occur. Note: Updates should be made at least quarterly.

Risk/asset categorize as follows:

Low Risk Systems or data that if compromised (data viewed by unauthorized personnel, data corrupted, or data lost) would not disrupt the business or cause legal or financial ramifications. The targeted system or data can be easily restored and does not permit further access of other systems.

Medium Risk Systems or data that if compromised (data viewed by unauthorized personnel, data corrupted, or data lost) would cause a moderate disruption in the business, minor legal or financial ramifications, or provide further access to other systems. The targeted system or data requires a moderate effort to restore or the restoration process is disruptive to the system.

High Risk Systems or data that if compromised (data viewed by unauthorized personnel, data corrupted, or data lost) would cause an extreme disruption in the business, cause major legal or financial ramifications, or threaten the health and safety of a person. The targeted system or data requires significant effort to restore or the restoration process is disruptive to the business or other systems.

Options for dealing with risk:

Tolerate – if we cannot reduce the risk in a specific area (or if doing so is out of proportion to the risk) we can decide to tolerate the risk; ie do nothing further to reduce the risk. This option is rarely used, although can be addressed for very low probability events.

Treat – if we can reduce the risk in a sensible way by identifying mitigating actions and implementing them, we should do so. For most risks, this is what we are doing.

Transfer – here risks might be transferred to other organizations, for example by use of insurance or transferring out an area of work (ie. hosting an online store by a third party with expertise in PCI compliance).

Terminate – this applies to risks we cannot mitigate other than by not doing work in that specific area. So if a particular project is very high risk and these risks cannot be mitigated.

4. Enforcement

   Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Definitions

6. Revision History

   This policy was approved on December 27, 2017.

26. Data Retention Policies / Procedures

1. Purpose

   A data retention policy weighs legal and privacy concerns against economics and need-to-know concerns - to determine the retention time, archival rules and the permissible means of storage, access, and encryption.

   This policy reviews the policies of persistent data and records management for meeting legal and business data archival requirements.

2. Scope

   This policy establishes the retention period of data within systems owned by Treasury Software and for which Treasury Software is responsible for the disposition of deleted data.

3. Requirements

   As of this writing, other than financial data (seven years) and personnel records (three years after termination) – the Company is not aware of any data minimum or maximum requirements required by any government regulation, industry standard, contractual agreement or any legal obligation.

   Absent any of these requirements, the Company will establish a commonsense approach and archive all non-sensitive data that is currently available and store all backed up data in a secure environment.

   Any sensitive or private data, including personnel files, client information and personnel files shall be archived in an encrypted environment.

   Development – Code for development will be retained by development and proper version history will be maintained using version control solutions such as Perforce or Subversion (SVN).

4. Enforcement

   Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Definitions

6. Revision History

   This policy was approved on December 27, 2017.

27. Third Party Management Policies / Procedures

1. Purpose

The Vendor/Third Party Access Policy informs Treasury Software employees and vendors about the requirements that vendors need to follow in order to access Treasury Software Information Systems. The policy defines the responsibilities for all parties for the mutual protection of Treasury Software and the vendor.

2. Scope

This Policy applies to all individuals and/or parties that are responsible for the installation of new Treasury Software Information System assets, the operations and maintenance of existing Treasury Software Information Systems - and those who allow vendor access for support, maintenance, monitoring and/or troubleshooting purposes.

3. Requirements

a) Vendor access to Treasury Software Information Resources is granted solely for the work contracted and for no other purposes.

b) Vendors must comply with all applicable Treasury Software policies, practice standards and agreements.

c) Prior to granting any access or performing work, Treasury Software will perform a risk analysis on the vendor/project and hold the vendor/project up to the same standards as if this were performed by an employee of Treasury Software. This policy by specific reference, incorporates Treasury Software Policy - Risk Management Policies and Procedures.

d) Vendor agreements and contracts must specify:

- The Treasury Software information the vendor should have access to. If, at the time of contract negations this is unknown or ambiguous, mention of this should be made in the agreement.
- How Treasury Software information is to be protected by the vendor. A copy of the Vendor's Security and Privacy Policy should be made available to Treasury Software where appropriate.
- Acceptable methods for the return, destruction or disposal of Treasury Software information in the vendor's possession at the end of the contract.
- Agreement that the Vendor must only use Treasury Software information and Information Systems for the purpose of the business agreement.
- Any other Treasury Software information acquired by the vendor in the course of the contract cannot be used for the vendor's own purposes or divulged to others.

e) Prior to the start of the engagement, the proposed work must be clearly identified and authorized by a Director within the Company.

f) Vendors work activities on Treasury Software systems may be monitored and logged for comparison.

g) Each vendor must provide Treasury Software with a list of all employee names working on the contract. The list must be updated and provided to Treasury Software within 24 hours of staff changes, wherever possible.

h) Vendor access must be uniquely identifiable and password management must comply with the Treasury Software Password Policy.

i) All vendor maintenance equipment on the Treasury Software network that connects to the internet via any means, and all vendor accounts, will remain disabled except when in use for authorized maintenance.

j) Upon departure of a vendor or vendor employee from the contract for any reason, the vendor will ensure that all sensitive information is collected and returned to Treasury Software or destroyed within 24 hours.

k) Each vendor granted access to any Treasury Software Information System must sign a statement that they have:
- Read and understand this policy
- Understands the responsibility to comply.
- Understands the consequences of an infraction.

4. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Any vendor found to have violated this policy may be subject to termination of the current and/or future contracts as well as legal action.

5. Definitions

6. Revision History

This policy was approved on December 27, 2017

28. Business Continuity Plan

1. Purpose

The purpose of this Business Continuity Plan is to provide processes for the prevention and mitigation of potential threats - and to enable ongoing operations. In summary, to help keep the company resilient during threats.

2. Scope

This Policy applies to all individuals and/or parties that are responsible for the continuity of operations.

This section is an extract for IT Policies (public) - from the corporate disaster continuity plan and subsequent disaster recovery plan. This section is intended as a high level overview for external vendor management review and other requirements. Information regarding third-party providers, logins and other details have been redacted from this document.

3. Business Impact Analysis

As Treasury Software is an installed application at our client locations, there are no central points of failure that would prohibit full use or access of the software for existing clients.

There are no cloud-based web components or data storage that we provide, that enable or hinder use of the software.

As the product is fully distributed at our client locations, this section focuses on ancillary functions, including risk mitigation and prioritization for restoration and recovery – as well as for testing and updating of this policy.

a. Recovery strategies, plan details and testing by function.

In terms of natural and man-made disasters (cyber-attacks, etc…) – both external and internal - their impact on us would be as follows:

Customer and prospect support:

Treasurysoftware.com website
Our primary site is hosted by a leading service provider – and we maintain a full working backup hot-site at another leading service provider.

We have engaged a DNS service provider to 'ping' our primary site every three minutes.

Should a ping fail, a secondary ping is automatically initiated. Should both fail – the DNS is automatically updated and all traffic is sent to the backup site.

Multiple notifications are sent to operations (ticketing) and to development. The system will fall back automatically to the original primary site once it is back up.
Testing/updates – Every two months, with the exception of licensing, which is tested/updated at every build (monthly).

Phone System
Treasury Software hosts its own VoiceOver IP Phone (VOIP) system. Should this system go down (extended power outage, Internet outage, local phone access outage, equipment failure), incoming calls from the toll-free service can be routed to our answering service.

Note: This answering service is used daily for overflow calls and after hours calls. All messages are sent to Treasury Software by a trouble ticket system.

When operating in this capacity, we are considered in 'call-back' mode – and all calls are returned by representatives using their cell phones.

If we anticipate to be in call-back mode greater than one day, mitigation efforts include displaying a notification banner to be placed on the website requesting clients and prospects to contact us via chat, web-form or email.

Each employee has a full company phone list with cell phone numbers.

Disaster recovery: Emergency contact numbers for phone providers is documented.

Testing/updates – lists updated as part of new hire and termination processes. Answering service is used daily.

Answering Service
Overflow and weekday after-hours calls are passed to the answering service in an 'attended transfer', rather than a blind transfer. The difference being that if the attended transfer is not successful, the system will recapture the call and place it in queue.

If the answering service is down/unable to take the call in time, the transfer will time out and the call will be returned to our in-house system for call handling. The caller will have the option of leaving a voice message.
Testing/updates – As weekend calls are not transferred to the answering service, but are handled by the voice messaging system, it is functionally tested weekly.

Internal operations:

File Servers
Treasury Software utilizes external file servers (ie. Box, etc…) which maintain off-site. Backups of critical files are performed on a regular basis (see backup) and can be restored locally if needed.
Testing/updates – annually.

Lack of access to building
All Treasury Software employees are telecommute ready. All have remote access and VOIP phones and can fully operate if access to the office is limited.
Testing/updates – (daily) as employees routinely work remotely

Development
Our development team maintains all code in off-site storage and has access to backups to restore their development environments.

Gap Analysis
There are no gaps currently identified for business critical operations, nor are there any long-term consequences associated with any of the strategies above.

4. Enforcement
   Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Any vendor found to have violated this policy may be subject to termination of the current and/or future contracts as well as legal action.

5. Definitions

6. Revision History
   This policy was extracted from Internal Operations and approved on December 17, 2019