ASURITY

Information Security Policy

Version 3.9

Last Revised: November 22, 2024

1. General

1.1 Overview

Effective security is a team effort involving the participation and support of every Asurity Technologies (Asurity) employee and affiliate who deals with information and/or information systems. This Policy must be adhered to by all Asurity personnel, defined below, and it is the responsibility of every user to learn and know these requirements. For the purpose of this Policy, a user is any person authorized to access an information resource.

1.2 Purpose

The purpose of the Information Security Policy is to protect this organization's information, data, and assets, and the information and data of our clients. This Policy encourages and supports our established culture of openness, trust and integrity, while protecting Asurity users, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

This Policy establishes the overarching security controls and processes all users and Information Technology (IT) administrators are required to follow in order to ensure the integrity and availability of the data environment at Asurity. It serves as a central policy reference document with which all users must be familiar and defines actions and prohibitions that all users must follow. The policy provides IT managers within Asurity with policies and guidelines concerning the acceptable use of Asurity technology equipment, e-mail, electronic communications, Internet connections, bring your own device, future technology resources, information processing and other security related topics.

1.3 Scope

This Policy document defines common security requirements for all Asurity personnel and systems that create, maintain, store, access, process or transmit company information.

Under this Policy, personnel include full time employees, part time employees, project-based employees, contractors, and consultants. This Policy also applies to information resources owned or used by others, such as contractors of Asurity, entities in the private sector, in cases where Asurity has a legal, contractual, or fiduciary duty to protect said resources while in Asurity custody or in the course of performing Asurity business.

This Policy covers Asurity network and application systems which are comprised of various hardware, software, communication equipment and other devices designed to assist Asurity in the creation, receipt, storage, processing, and transmission of information on behalf of its clients and for Asurity as an enterprise. The policy requirements and restrictions defined in this document shall apply to network infrastructures, databases, external media, encryption, hardcopy reports, videos, models, wireless, telecommunication, conversations, and any other methods used to convey knowledge and ideas across all hardware, software, and data transmission mechanisms.

This Policy lays out the expectations of Asurity, however, standalone policies have also been established for certain areas of Asurity operations. Asurity also understands that it must comply with customer policies, but if Asurity policies and customer policies are in conflict, the more restrictive policy will be used where possible. The legal department should be contacted to ensure that all conflicts are resolved without violation of any applicable laws.

1.4 Periodic Review and Update

It is expected that this Policy will change over time, and as such it is subject to periodic review. Asurity will review this Policy formally at a management level no less frequent than annually. Review cycles will be tracked in the revision history section of this document.

This Policy will be distributed to all Asurity employees, and the most recent reviewed version will be published in the Asurity Wiki (Intranet).

1.5 Revision History

Each revision of this Policy shall be dated and version controlled with a summary of changes.

Change Date	Version	Responsible	Summary of Changes
			For revisions prior to 3.0, see earlier versions of this document on the Asurity Wiki (Intranet).
11/09/2022	3.0	David Greenwood	Final version subsequent to review by the Security Team and other key stakeholders.
11/03/2023	3.1	Scott Sykes	Added sections 8.7 and 14.4
11/10/2023	3.2	Scott Sykes	Updated the password section 6.2
01/29/2024	3.3	David Greenwood	Updated the password section 6.2. Revised section 6.3 to more clearly define initial/temporary password guidelines Updated section 6.5
02/01/2024	3.4	David Greenwood	Update to data privacy section 4.2 Update to asset management section 16.6 Update to penetration testing section 18.5 Update to activity log review section 19.3
05/09/2024	3.5	David Greenwood	Replace Application Development section 18 with reference to new SDLC policy
06/28/2024	3.6	David Greenwood	Replace Change Management section 17 with reference to new policy
8/1/2024	3.7	Scott Sykes	Minor updates to the Security Essentials section.
10/7/2024	3.8	Scott Sykes	Updates to CTO/CISO responsibility wording.
11/22/2024	3.9	Scott Sykes	Updated list of reference docs on section 21

1.6 Review History

Each review shall be recorded in the following table and summary of actions recorded.

Review Date	Version	Responsible	Summary of Actions
11/11/2022	3.0	Luke Wimer	COO Executive Review & Approval
11/03/2023	3.1	Luke Wimer David Greenwood	COO and CTO Executive Review & Approval
11/10/2023	3.2	Luke Wimer David Greenwood	COO and CTO Executive Review & Approval
01/29/2024	3.3	Scott Sykes	CISO Review & Approval
02/01/2024	3.4	Scott Sykes	CISO Review & Approval
05/09/2024	3.5	Scott Sykes	CISO Review & Approval
06/28/2024	3.5	Scott Sykes	CISO Review & Approval
08/1/2024	3.7	Scott Sykes	CISO Review & Approval
11/22/2024	3.9	Scott Sykes/David Greenwood	CISO and CTO Review & Approval

Employee Attestation

I, the undersigned, represent that I have fully reviewed and understand the **Information Security Policy** of Asurity Technologies.

I hereby attest, warrant, and agree that I will comply with this Policy for the full duration of my employment contract.

Agreed to by the undersigned:

Signed: ___________________________________

Printed Name: ___________________________________

Date: ___________________________________

Table of Contents

Security Essentials

The following is an abridged list of the *essential requirements* of this Policy, intended to aid in review and understanding. The relevant Policy section references are provided, and the reader is encouraged to review the full document in detail to learn more about the entire scope of Information Security disciplines at Asurity.

Policy Purpose and Scope *Section 1*

The purpose of the *Information Security Policy* is to protect Asurity information, data, and assets, and the information and data of our clients, affiliates, and partners.

The Policy applies to all full-time employees, part time employees, project-based employees, contractors, and consultants as persons, or users, authorized to access information resources.

The Policy applies to all network and application systems owned or managed by Asurity.

Any user found to have knowingly violated the Policy may be subject to disciplinary action, to include termination of employment.

Our Roles in Information Security *Section 2*

Each of us play an important role in helping to secure all information assets and to help prevent, detect, and respond to cyber threats and vulnerabilities.

The CTO and the CISO Security Team are responsible for all information security concerns at Asurity.

It is the responsibility of each user to immediately report all real or perceived security incidents.

Authorized Use of Asurity Systems *Section 3*

Asurity systems are only to be used for business purposes. Accordingly, we shall only collect, use or share information for valid business purposes.

All software programs and documentation generated by or provided to users for the benefit of Asurity remain the property of Asurity.

All electronic communication systems and all information or messages generated on or handled by Asurity-owned or managed equipment are considered the property of Asurity.

Data Privacy and Personal Information *Section 4*

Asurity collects personal information in the normal course of business in order to provide mortgage processing, document, analytical and compliance related services.

Asurity will not sell personal information to anyone and will not disclose personal information to outside parties unless contractually or legally obligated to do so.

Asurity protects the confidentiality and security of all personal information.

Accessing Asurity Systems – IDs and Passwords *Sections 5 & 6*

Users shall have unique logon IDs for identification to access Asurity networks and systems.

Strong passwords are required for authentication on all Asurity networks and systems, and passwords will be changed no less than every 90 days.

Passwords must never be shared with anyone, and passwords must never be stored insecurely.

Under no circumstances are users authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Asurity-owned resources.

For further reference see the *Asurity Access Control Policy*.

Physical Security *Section 7*

All personnel help provide and maintain our physical security in the work environment.

All visitors to Asurity offices must sign in and be accompanied throughout their visit.

Protecting Confidential Information *Section 8*

In the course of working for Asurity, users may handle information which is confidential to Asurity and its clients, affiliates, or partners, and shall exercise reasonable care to prevent others from disclosing or using confidential information.

Users may access, use, or share such confidential information following acceptable use guidelines, and only to the extent it is authorized and necessary to fulfill assigned job duties.

Users have a responsibility to promptly report any actual or suspected theft, loss, or unauthorized disclosure of confidential information.

Users are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure if they leave their computer or work area unattended.

Electronic Communications *Section 9*

All electronic communication systems and all information or messages generated on or handled by Asurity-owned or managed equipment are considered the property of Asurity.

All outbound email is subject to Data Loss Prevention (DLP), which can be used to detect and quarantine suspicious email activity, in order to protect sensitive information and prevent inadvertent or unauthorized disclosure.

Asurity email and messaging accounts should only be used for Asurity business-related purposes.

All Social Media activity, whether using Asurity property and systems or personal computer systems, is subject to restriction and must follow the guidelines outlined in the Policy.

Accessing or attempting to access inappropriate or otherwise illegal Internet sites or services is prohibited.

Any activity that attempts to disrupt or bypass the security, confidentiality, or integrity of Asurity network, systems or data is strictly prohibited.

Data Classification and Use *Section 10*

All confidential information must be handled, maintained, and safeguarded in a manner that ensures its continued protection.

Procedures must be followed to ensure that all data is appropriately handled depending on its data classification level – public, internal-only, external, confidential, restricted, and privileged.

Only personnel with the proper authorization and a need to know are granted access to Asurity systems and their resources.

Use of Mobile Devices *Section 11*

Mobile devices may be used for certain Internet-accessible Asurity systems, such as email or messaging.

Personal mobile devices, so-called Bring Your Own Device or BYOD, are permitted and the user is responsible for ensuring any such device adheres to all Policy requirements.

Mobile devices are not permitted to access internal networks or applications, nor permitted to store any client data.

Asurity will ensure any company data is removed from the user's mobile device upon termination.

System Protections and Updates *Section 12*

Antivirus software is installed on all Asurity desktop computers and servers.

Workstations and servers must have up-to-date operating system security patches installed.

Only approved software is permitted to be used on Asurity computers and networks.

Such protections are not foolproof, and users should remain vigilant and immediately report any unexpected or suspicious system activity.

Data Encryption *Section 13*

All servers, desktop computers, including laptops, must be configured to use disk-level encryption.

Data encryption at rest will be employed on all Production and DR databases and file storage.

All sensitive data and files shall be encrypted when transmitted through Asurity networks and environments.

If required by a client or business partner, Asurity will secure attachments in outbound emails.

Telecommuting and Remote Access — *Section 14*

Asurity users who work from their home or from a remote location must abide by all information security requirements and guidance defined in this Policy.

The Asurity requires the use of Virtual Private Network (VPN) software when remotely accessing any Asurity networks or internal resources.

Remote access is restricted to only allow connections originating from within the United States and not internationally.

Security Awareness and Training — *Section 15*

All users upon contract or hire and then at least annually thereafter shall receive appropriate information security awareness training.

Asurity will conduct phishing testing of all users to further enforce awareness training.

Annually, all users will attest to having read and to abide by the Information Security Policy.

The following elements of the Policy are more relevant to only a subset of staff, such as those staff directly involved in systems management, software development, or security operations.

Asset Management — *Section 16*

All electronic assets at Asurity exceeding the asset value threshold must be appropriately tracked in an asset inventory.

Asset disposal processes regardless of asset value must be followed and documented.

Change Management — *Section 17*

Asurity follows a disciplined process to appropriately document, track and manage changes to all production applications, systems, and networks.

All critical changes must be planned, tested, and approved, and ultimately logged for review.

For further reference, see the *Asurity Change and Release Management Policy*.

Application Development and Maintenance — *Section 18*

All software application development and maintenance activity will adhere to the *Asurity Software Development Life Cycle* (SDLC) policy which establishes a standardized and repeatable approach for developing, deploying, and maintaining high-quality software applications.

Audit and Activity Log Review *Section 19*

Asurity will continually assess potential risks and vulnerabilities to protected information in its possession and develop, implement, and maintain appropriate administrative, physical, and technical security measures.

All system and network access and activity is recorded and reviewed for all electronic information resources that contain, access, or transmit data classified as confidential.

Asurity will conduct on a regular basis an internal review of records of system activity to minimize security risk.

Third Party Risk Management *Section 20*

All third-party vendor services critical to the ongoing operation of Asurity solutions are assessed for risk before going to contract and annually thereafter.

If Asurity deems any change to a vendor’s services or service quality to be an unacceptable risk, the vendor will be required to address the concern with a timely mitigation plan.

2. Information Security Policy at Asurity

2.1 Policy Owner

Ownership and management of Information Security Policy and operations at Asurity is the responsibility of the Chief Information Security Office (CISO) in support of the Chief Technology Officer (CTO).

2.2 Security Team

The CISO and the CTO together with other key technology personnel comprise a Security Team with the following members:

Name	Title/Role	Contact Phone	Contact Email
InfoSec Team	- distribution email -	N/A	infosec@asurity.com
David Greenwood	CTO	(804) 415-4476	dgreenwood@asurity.com
Scott Sykes	CISO	(804) 325-1412	ssykes@asurity.com
Eric Krichinsky	Director, Cloud & Infrastructure	(804) 510-0640	ekrichinshy@asurity.com
Brad McFarling	VP. Technology	(214) 220-6634	bradmc@asurity.com
Brett Lewis	VP Software (RiskExec)	(865) 686-8149	blewis@asurity.com

The Security Team is responsible for actively addressing information security concerns or issues in a timely manner and will coordinate with Asurity management to take appropriate actions. It is the responsibility of the Security Team to provide training on any policy or procedural changes that may be required as a result of the investigation of an incident.

2.3 Security Governance

The Security Team will meet quarterly, or as needed, to discuss security issues and to review concerns that arise, to identify areas that should be addressed during annual training, and to review/update security policies and procedures as necessary.

2.4 Reporting Security Incidents

It is the responsibility of each Asurity user to report perceived security incidents to the appropriate supervisor or security person. Users are to report all real or potential security incidents or violations of the security policy immediately to the their immediate supervisor, their department head, or to any member of Security Team.

Reports of security incidents shall be escalated as quickly as possible. Each member of the Security Team must inform the other members as rapidly as possible. Each incident will be analyzed to determine if changes in the existing security structure are necessary. All reported incidents will be logged, investigated, and the remedial action indicated. Refer to the *Asurity Incident Response Plan* document for additional details.

2.5 Reporting Security Breaches

Security breaches shall be promptly reported and investigated in a manner consistent with all Security Incidents. The Security Team will coordinate with Asurity management and business unit executives to address any potential liability matters or to facilitate proper legal processes if matters need to be referred to law enforcement.

2.6 Reporting Software Malfunctions

Users should inform the appropriate Asurity IT personnel when the user's software does not appear to be functioning correctly. The malfunction - whether accidental or deliberate - may pose an information security risk. If the user, or the user's manager or supervisor, suspects a computer virus infection, the Security Team should be notified.

2.7 Non-Compliance

Any user found to have knowingly violated this Information Security policy may be subject to disciplinary action, to include termination of employment or other responses.

3. Acceptable Use

3.1 Acceptable Use Policy

Use of all Asurity systems, including Internet/Intranet/Extranet-related systems, and including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, web browsing, file transfer, or other similar business systems, are only to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

3.2 Property and Ownership

Asurity proprietary information stored on electronic and computing devices whether owned or leased by Asurity, the user or a third party, remains the sole property of Asurity. All users must ensure through legal or technical means that proprietary information is protected in accordance company policy.

All software programs and documentation generated by or provided to users for the benefit of Asurity are the property of Asurity unless covered by a separate contractual agreement. Nothing contained herein applies to software purchased by Asurity users at their own expense. Use of personal software on Asurity equipment is prohibited and all software installed on Asurity computers must be approved by Asurity.

3.3 Acceptable Use

Users may access, use or share Asurity proprietary information only to the extent it is authorized and necessary to fulfill assigned job duties. Users have a responsibility to promptly report the theft, loss or unauthorized disclosure of Asurity proprietary information.

Users are responsible for exercising good judgment regarding the reasonableness of personal use of computing systems. Users should be guided by corporate policies on acceptable use, and if there is any uncertainty, should consult their manager.

For security and network maintenance purposes, authorized individuals within Asurity may monitor equipment, systems and network traffic at any time. Asurity reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

3.4 Unacceptable Use

Under no circumstances are users authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Asurity-owned resources. The following activities are, in general, prohibited. Certain users may be exempted from these restrictions in the course of their legitimate job responsibilities (e.g., systems administration staff, HR staff).

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Asurity.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Asurity does not have an active license is strictly prohibited.
- Accessing data, a server or an account for any purpose other than conducting Asurity business, even if you have authorized access, is prohibited.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using an Asurity computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any Asurity account.
- Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
- Providing information about, or lists of, Asurity users to parties outside of Asurity.
- Sending unsolicited email messages, whether individually or in bulk form, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone, or text messaging, whether through language, frequency, or size of messages.

- Unauthorized use, or forging, of identifying information such as but not limited to email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding “joke emails”, "chain letters", "Ponzi" or other "pyramid" schemes of any type.

4. Data Privacy

4.1 Protecting Privacy

The collection and use of personal, client and borrower information, or data, is central to providing financial services. Therefore, Asurity acknowledges that we shall only collect, use or share such information for valid business purposes. Our relationship with our clients – and in turn their customers – is our most important asset. Asurity understands that we are entrusted with private personal and financial information, and all employees of Asurity will do everything they can to maintain that trust and protect the privacy of individuals.

4.2 Data Privacy Policy

This privacy policy applies broadly to any information or data that we may obtain from any current or former client, vendor, employee, or contractor. Throughout this policy, we refer to that information as “personal information” or commonly, personally identifiable information or PII.

1. ***Asurity will not sell personal information to anyone.***
   Outside of the exceptions noted below, Asurity will not sell or otherwise distribute personal information to outside parties unless specifically directed or contracted to do so.

2. ***Asurity collects personal information in the normal course of business in order to provide mortgage processing, document, analytical and compliance related services.***
   a. *From Clients or Individuals.* Most personal information collected is obtained directly from a client or individual related to a mortgage loan or similar financial product. Information collected may include name, address, phone number, email address, Social Security number, date of birth, marital status, and financial information. Asurity also may collect and store information from consumer reporting agencies.
   b. *From Third Parties.* Additional or supporting personal information may be obtained from third parties as required in the normal course of our business; for example, consumer reporting agencies and employers.

   The extent of personal information collected from clients, individuals and third parties may vary depending upon the type of product or service provided.

3. ***Asurity protects the confidentiality and security of all personal information.***
   a. Asurity maintains *physical, electronic, and procedural safeguards* to protect personal information and ensures that all information remains confidential and secure.
   b. Companies hired by Asurity to provide support services are contractually prohibited under *confidentiality and non-disclosure* agreements from using personal information provided by Asurity for any purposes outside the specific services being provided.
   c. Asurity further restricts access to personal information to select employees and agents who have a need for such information for *business purposes only*. All such employees or agents shall be trained and required to safeguard such information.

4. ***Asurity will not disclose personal information to outside parties, unless one of the following limited exceptions applies:***
   a. Asurity may be *contractually obligated* to use or report personal information, such as loan and transaction data, with financial institutions that contract with Asurity to execute transactions, or to help it process or service transactions or account(s), or act in a custodial capacity related to its services.
   b. Asurity may disclose or report personal information in limited circumstances in which it believes in good faith that disclosure is *required by law*; for example, to cooperate with regulators or law enforcement authorities, resolve consumer disputes, perform credit/authentication checks, or for institutional risk control.
   c. Where contractually permissible, Asurity may share certain personal information with *affiliated business entities*, such as an affiliated law firm or internal business unit, in order to fulfill various quality control and regulatory requirements.

   In all cases, Asurity will disclose any and all such service relationships to its clients.

5. ***Asurity continues to evaluate efforts to protect personal information and make every effort to keep all personal information accurate and up to date.***
   a. If it becomes necessary to disclose any personal information in a way that is inconsistent with this policy, Asurity will notify clients and provide the *opportunity to opt out* of such disclosure to the extent permissible by law.
   b. If Asurity or a client or third party *identifies any inaccuracy* in personal information, efforts will be made to promptly update internal records.

6. ***Asurity will not transform personal information in a manner that results in aggregation, de-identification, derivation, or alteration of such information:***
   a. Under no circumstances will Asurity manipulate or transform personal information under its care with the intent to anonymize such data for broader use.
   b. Asurity will not attempt to re-identify or de-anonymize any individual data record or aggregate data set with the intent to uniquely identify an individual.

c. Asurity may "copy down" production data into lower environments for testing and development purposes after appropriately anonymizing all personal information within the data set.

d. Asurity will remain in compliance with all applicable regulatory data privacy requirements to safeguard all information assets under its care.

5. User Identification and Authentication

5.1 User IDs

Individual users shall have unique logon IDs for identification. An access control system shall identify each user and prevent unauthorized users from entering or using information resources. Security requirements for user identification include:

- All user access to Asurity systems must be reviewed and approved.
- Users shall be responsible for the use and misuse of their individual logon ID.
- All user login IDs are audited at least quarterly or as further defined in the *Asurity Access Control Policy*, and all inactive logon IDs are revoked.
- Asurity Human Resources (HR) department notifies the appropriate personnel upon the departure of all users, at which time login IDs are immediately suspended/revoked.
- The logon ID is locked or revoked after a maximum of three (3) unsuccessful logon attempts which then require the passwords to be reset by the appropriate Administrator.

5.2 User Passwords

Individual users shall use encrypted passwords for authentication in order to gain access to all Asurity networks and workstations. All passwords are restricted to be of a "strong" nature. See Passwords section in this document. When passwords are reset, the user will be automatically prompted to manually change their password at the next logon.

5.3 Access Control

Information resources are protected by the use of access control systems. Access control systems are both internal (i.e., passwords, encryption, access control lists, constrained user interfaces, etc.) and external (i.e., port protection devices, firewalls, host-based authentication, etc.). Rules for access to specific resources will be established by the responsible information/application owner.

5.4 User Entitlement Reviews

No less than annually, the Asurity Security Team shall facilitate entitlement reviews to ensure that all users have the appropriate roles, access, and software necessary to perform their job functions effectively while being limited to the minimum necessary level of access to meet any compliance requirements and protect customer data. See the *Asurity Access Control Policy* for further details.

5.5 Termination of User Logon Account

Upon termination of an employment or contract all user access rights are immediately suspended or revoked. Whether voluntary or involuntary, the Asurity HR Department coordinates with Information Technology about the departure of all users, and makes clear to departing users that no further access will be permitted. If user's termination is voluntary and user provides notice, user's manager shall promptly notify the HR Department of user's last scheduled work day so that their user account(s) can be configured to expire. The user's manager shall be responsible for ensuring that all keys, ID badges, and other access devices as well as Asurity equipment and property is returned to Asurity prior to the user leaving Asurity on their final day of employment.

6. Passwords

6.1 Password Policy

Strong passwords are required to access all computing resources at Asurity, and users should follow the guidelines for password protection and password creation.

6.2 Password Protection

- Passwords must not be shared with anyone. All passwords are to be treated as sensitive, Confidential Asurity information.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Passwords must not be revealed over the phone to anyone.
- Do not reveal a password on questionnaires or security forms.
- Do not hint at the format of a password (for example, "my family name").
- Do not share Asurity passwords with anyone, including help desk personnel, administrative assistants, managers, co-workers, or family members.
- Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.
- Do not use the "Remember Password" feature of applications (for example, web browsers).
- Any user suspecting that his/her password may have been compromised must immediately report the incident and change all passwords.
- The same password(s) should not be used across multiple systems; that is, passwords must be unique across separate and distinct systems. In particular, passwords used to access applications or systems containing sensitive data should not be the same as the passwords used to access corporate resources.
- Password must be unique from the previous 24 passwords of the user.
- Passwords will have a minimum password age of at least 1 day to prevent rapid password recycling.

6.3 Initial/Temporary Passwords

The following guidelines should be followed for initial/temporary passwords.

- The password recipients' identity is to be verified prior to communicating the initial/temporary password or when initiating a password reset.
- Initial/Temporary passwords are to be delivered separately from account information.
- Temporary Passwords are to have a defined expiration period.
- Upon receipt, and enforced within authentication configurations, temporary passwords need to be changed upon initial login.
- Passwords must be changed immediately when an account is believed to be compromised.

6.4 Password Construction Guidelines

Strong passwords should follow the password construction guidelines outlined below to include a combination of upper and lowercase letters, numbers, and special characters. Password complexity for all computer systems in use at Asurity must meet the following minimum requirements, if supported by the system:

- Contain at least 12 alphanumeric characters.
- Contains *at least three* of the following:
  - 1 upper case letter.
  - 1 lower case letter.
  - 1 number (for example, 0-9).
  - 1 special character (for example, !@$%^&*()_+|~-=\`{}[]:";'<>?,/).
- Cannot be found in a dictionary, including foreign language, or exist in a language slang, dialect, or jargon.
- Must not contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
- Must not contain work-related information such as building names, system commands, sites, companies, hardware, or software.
- Must not contain simple patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
- Must not contain common words spelled backward or preceded or followed by a number (for example, terces, secret1 or 1secret).
- Must not be some version of common passwords, such as "Welcome123" "Password123" "Changeme123"
- Where possible, users must not use the same password for various Asurity access needs.

6.5 Password Change

- All user-level passwords (for example, email, web, desktop computer, and so on) expire every 90 days. Users will be notified before expiration.

- For privileged user accounts, passwords expire every 30 days or must require two-factor authentication to authorize account access.
- Any of the previous 24 passwords may not be re-used.
- After 5 unsuccessful sign-in attempts (wrong password), the user will be locked out for a minimum of 15 minutes and will need to request a password change/reset.
- Password cracking or guessing may be performed on a periodic or random basis by the Security Team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the Password Construction Guidelines.

7. Physical Security

7.1 Physical Security Policy

It is the responsibility of all Asurity personnel to take positive action to provide and to help maintain physical security in the work environment.

7.2 Building Security

Asurity ensures that all building access is provided in a secure manner. The following list identifies measures that are in effect at all Asurity locations. All other facilities, if applicable, have similar security appropriate for that location.

- Asurity personnel will be issued a key or access card for secure access to the building.
- Entrance to the building is controlled by a key or access card 7x24. Attempted entrance without a key or access card results in immediate notification to the authorities.
- Only specific Asurity users are given a key or access card for entrance. Loaning or copying of the key or access card for non-users is strictly prohibited.
- The door to the reception area is locked at all times and requires appropriate credentials or escort past the reception or waiting area door(s).
- Video surveillance may be used at building entrances and exits.

7.3 Challenge Unrecognized Personnel

If you see an unrecognized person in a restricted Asurity office location, you should challenge them as to their right to be there. In some situations, non-Asurity personnel, who have signed the confidentiality agreement, do not need to be accompanied at all times. All visitors to Asurity offices must sign in at the front desk. In addition, all visitors must wear a visitor/contractor badge. Any challenged person who does not respond appropriately should be immediately reported to office management and escorted from premises if/as appropriate.

7.4 Avoid Tailgating

Avoid tailgating, in which a second person follows a first person into the facility without showing proper identification, and piggybacking, in which a first person intentionally allows a second person to enter without first checking for proper identification.

8. Protecting Confidential Information

8.1 Confidentiality Policy

In the course of working for Asurity, personnel, including employees, project-based employees, contractors, directors, temporary agency workers, consultants, and vendors, may become aware of information which is confidential to Asurity and its clients. All such confidential information must be handled, maintained, and safeguarded in a manner that ensures its continued protection.

Individuals who act in breach of this obligation may be subject to disciplinary action up to and including termination of employment and may also face civil and/or criminal sanctions.

8.2 Confidential Information

Confidential Information includes, but is not limited to, intellectual property, trademarks, financial information, business plans, product releases, company strategy, operational information, technical data, client information, and/or personal information.

8.3 Protecting Confidential Information

Asurity personnel shall exercise reasonable care to prevent others from disclosing or using Confidential Information.

Asurity personnel shall not knowingly:

- Reveal Confidential Information to anyone outside Asurity except pursuant to a court order or with the consent of Asurity and with client consent, as applicable;
- Reveal Confidential Information of an individual or client to anyone within Asurity who does not have a “need to know” the Confidential Information;
- Use Confidential Information of an individual or client to the disadvantage of the client;
- Use Confidential Information of an individual or client for the advantage of an employee or contractor or advantage or disadvantage of a third person;

8.4 Electronic Transmission of Secured Information

Asurity personnel must distinguish between sensitive and non-sensitive personally identifiable information (“PII”) and determine which PII may be transmitted electronically. If sensitive PII must be electronically transmitted, then it shall not be sent unless it is specifically protected by secure method such as encryption, Public Key Infrastructure (PKI), secure sockets layer (SSL) or some other methodology agreed upon between Asurity and its client. Non-sensitive information may be transmitted in an unprotected form.

8.4.1 Personally Identifiable Information (“PII”)

The term personally identifiable information refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc.

8.4.2 Sensitive Information

Sensitive information is defined as PII which, when disclosed, could result in harm to the individual whose name or identity is linked to the information. Further, in determining what PII is sensitive, the context in which the PII is used must be considered.

For the purpose of determining which PII may be electronically transmitted, the following types of PII are considered sensitive when they are associated with an individual. Secure methods must be employed in transmitting this data when associated with an individual:

- Place of birth
- Date of birth
- Mother’s maiden name
- Social Security Number
- Personal financial information
- Credit card or purchase card account numbers
- Any information that may stigmatize or adversely affect an individual.

This list is not exhaustive, and other data may be sensitive depending on specific circumstances.

Note that Social Security Numbers (SSNs), including truncated SSNs that include only the last four digits, are sensitive regardless of whether they are associated with an individual. If it is determined that such transmission is required, then secure methods must be employed.

8.4.3 Non-Sensitive information

The following additional types of PII may be transmitted electronically without protection because they are not considered sufficiently sensitive to require protection.

- Work, home and cell phone numbers
- Work and home addresses
- Work and personal e-mail addresses

Note that the determination that certain information is non-sensitive does not mean that it is publicly releasable. The determination to publicly release any information can only be made by an Asurity official or agent authorized to make such determinations. The electronic transmission of non-sensitive information is equivalent to transmitting the same information by the U.S. mail, a private delivery service, courier, facsimile, or voice. Although each of these methods has vulnerabilities, the transmitted information can only be compromised as a result of theft, fraud, or other illegal activity.

8.4.4 Methods of Transmission of PII

Asurity provides several methods of secured transmission if required by a client, such as secure email, secure FTP, custom integrations (using web services), or other services such as secure file shares. Other methods of secure transmission may be less used. See section below on Data Encryption and Secure Data Transmission for additional considerations.

8.5 Clean Desk - Safeguarding Documents and Other Materials

Users are required to ensure that all sensitive/confidential information in hardcopy or electronic form is secure in their work area at the end of the day and when they are expected to be gone for an extended period. Users are responsible for ensuring:

- Removal of Restricted or Sensitive information from the desk and the material locked in a drawer when the desk is unoccupied and at the end of the work day.
- File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.
- Keys used for access to Restricted or Sensitive information must not be left at an unattended desk or made easily accessible.
- Printouts containing Restricted or Sensitive information should be immediately removed from the printer.
- Restricted and/or Sensitive documents are shredded in the official shredder bins or placed in the lock confidential disposal bins.
- Whiteboards containing Restricted and/or Sensitive information are erased after use.
- Lock away or securely tether portable computing devices such as laptops and tablets.
- Secure mass storage devices such as CD-ROM, DVD or portable USB drives should be locked away in a drawer at the end of the working day, even if they are encrypted.
- Computers and laptops must not be left logged on when unattended.
- If sensitive or confidential information is being worked on, the screen must be closed, minimized, or locked when unauthorized persons are in close proximity to the screen if practical, or they should be asked to move away.

8.6 Disposal of Information

When disposing of portable storage devices containing sensitive information (USB drives, printed materials, hard drives, CDs), adhere to the following guidelines:

8.6.1 Printed Materials:

- Shred documents using a cross-cut shredder.
- Disperse shredded pieces to prevent reconstruction.
- Promptly dispose of shredded materials in secure waste receptacles.

8.6.2 USB Drives:

- Physically destroy the drive using a specialized shredder or by drilling holes through it.

8.6.3CDs:

- Physically destroy the disc using a CD shredder or by drilling holes through it.
- Crush the disc into small pieces.

8.6.4 Hard Drives:

- Physically destroy the drive using a specialized hard drive shredder or by drilling holes through it.
- Utilize data wiping software to overwrite data multiple times.
- Perform a low-level format to further erase data.

8.7 Unattended Computers

Unattended computers must enable the screen lock by the user when leaving the work area (Hold Windows Key and Press L). The automatic lock feature must be set to automatically turn on after no more than 15 minutes of inactivity. If a user observes that their screen is not locking automatically after 15 minutes, they should immediately contact IT for assistance.

8.8 Automatic Session Logoff

Asurity systems – workstations and servers – will be configured to automatically logoff (terminate) the user session when the session is finished. For remote terminals and remote desktop sessions, the session will be considered finished if disconnected, and automatically terminated.

9. Electronic Communication

9.1 Electronic Communication Policy

All electronic communication systems and all messages generated on or handled by Asurity owned or managed equipment are considered the property of Asurity. All such systems are to be used in a manner consistent with Asurity policies and procedures of ethical conduct, safety, compliance with applicable laws, and proper business practices.

9.2 Monitoring

All email is subject to Data Loss Prevention (DLP) in order to protect sensitive information and prevent inadvertent disclosure. Incoming and outgoing email containing sensitive information may be inspected and quarantined for review. All email is also subject to spam and malware detection.

Generally, while it is NOT the policy of Asurity to monitor the content of any non-email electronic communication, Asurity is responsible for servicing and protecting all equipment, networks, data, and resource availability and therefore may be required to access and/or monitor electronic communications from time to time.

Authorized information system support personnel, or others authorized by the Asurity Security Team, may test the resiliency of a system. Such personnel may test for susceptibility to hardware or software failure, security against hacker attacks, and system infection.

9.3 Email and Messaging

Asurity email and messaging accounts should be used primarily for Asurity business-related purposes and adhere to the following guidelines.

- Asurity users shall have no expectation of privacy in anything they store, send or receive on the company’s email or messaging systems.
- Asurity may monitor messages without prior notice. Asurity is not obliged to monitor email messages.
- Email and messaging should be retained only if it qualifies as an Asurity business record, where there exists a legitimate and ongoing business reason to preserve the information contained in the email, in accordance with the data retention policy.
- The Asurity email and messaging systems shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Users who receive any emails with this content from any Asurity user should report the matter to their supervisor immediately.
- Users are prohibited from automatically forwarding Asurity email or messages to a third-party email system such as Gmail, Yahoo Mail, AOL, or other third-party systems.
- Users are prohibited from using personal accounts for third-party email, messaging systems and storage servers such as Google, Yahoo, etc. to conduct Asurity business, to create or memorialize any binding transactions, or to store or retain email or documents on behalf of Asurity. Such communications and transactions should be conducted through proper channels using Asurity-approved processes and services.
- Personal communication is permitted on a reasonable basis, but non-Asurity related commercial uses are prohibited. Using a reasonable amount of Asurity resources for personal emails is acceptable, but non-work-related email shall be saved in a separate folder from work related email.
- Users must use extreme caution when opening e-mail attachments received from any sender, because it may contain malware.

9.4 Social Media

Social media includes all means of communicating or posting information or content of any sort on the Internet, including to your own or someone else’s blog, journal, or diary, personal or otherwise-associated web site, social networking or affinity web site, web bulletin board, or a chat room, whether or not associated or affiliated with Asurity, as well as similar forms of electronic communication. Such activity may be referred to as “posting” information.

Social Media activity, whether using Asurity property and systems or personal computer systems, are subject to the terms and restrictions set forth in this Policy.

- Limited and occasional use of Asurity systems to engage in social media is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Asurity policy, is not detrimental to Asurity best interests, and does not interfere with a user's regular work duties.
- Asurity Confidential Information policy also applies to social media. As such, users are prohibited from revealing or posting any Asurity confidential or proprietary information, trade secrets or any other material covered under Confidential Information.
- Users shall not engage in any social media that may harm or tarnish the image, reputation and/or goodwill of Asurity and/or any of its users. Users are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments, or otherwise engaging in any conduct prohibited by non-discrimination and anti-harassment policies as outlined in the Asurity Employee Handbook.
- Users may not attribute personal statements, opinions, or beliefs to Asurity. If a user is expressing his or her beliefs and/or opinions, the user may not, expressly, or implicitly, represent themselves as an employee or representative of Asurity.
- Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, Asurity trademarks, logos and any other Asurity intellectual property may also not be used in connection with any social media activity.

9.5 Internet Access

Internet access is provided for Asurity users and is considered a great resource for the organization. This resource is costly to operate and maintain, and is allocated primarily to those with business, administrative or contract needs.

Internet access provided by Asurity should not be used for bandwidth-intensive entertainment such as online games or streaming movies. While seemingly trivial to a single user, company wide use of these non-business sites may consume a large amount of Internet bandwidth, which could then impact responsible use. Users must understand that individual Internet usage is monitored, and if a user is found to be spending an excessive amount of time or consuming large amounts of bandwidth for personal use, disciplinary action may be taken.

Many inappropriate Internet sites, such as games, peer-to-peer file sharing applications, chat rooms, and on-line music sharing applications, have already been blocked by Asurity security infrastructure. Other inappropriate uses or illegal or potentially illegal uses may include:

- Accessing sites or distributing materials containing derogatory or sexual content or language, such as pornography, vulgarities, obscenities, sexually explicit language, and adult entertainment;
- Accessing sites that contain content that could potentially incite a hostile work environment, e.g., militancy, racism, weapons, violence, or derogatory, defamatory, discriminatory, or harassing statements;

- Accessing a site that contains illegal or potentially illegal content, such as sites relating to drugs, gambling, alcohol, and hacking; and
- Using the internet/intranet, including the transmission of material, information, or software, for purposes that are in violation of any local, state, or federal law.

The list of inappropriate sites is constantly monitored and updated as necessary. Additionally, any user bypassing these site/content filtering controls will be disciplined and may be terminated.

9.6 Unauthorized Network Activity

The follow activities are strictly prohibited on the network or using the Internet to facilitate such activities:

- The willful, unauthorized access or inspection of confidential or sensitive information to which you have not been approved on a "need to know" basis is prohibited.
- Violating or attempting to violate the terms of use or license agreement of any software product used by Asurity is strictly prohibited.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Port scanning or security scanning is expressly prohibited by Asurity users outside the Security Team, unless otherwise authorized by the Asurity CISO or CTO in writing.
- Executing any form of network monitoring which will intercept data not intended for the users’ host unless this activity is a part of the users’ normal job/duty.
- Circumventing user authentication or security of any host, network, or account.
- Introducing honeypots, honeynets, keylogging, or similar technology on the network.
- Interfering with or denying service to any user (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with or disable a user's terminal session.

9.7 Data Integrity

Asurity shall implement and maintain appropriate security mechanisms to corroborate that any information has not been altered or destroyed in an unauthorized manner. To prevent transmission errors as data passes from one computer to another, Asurity will use encryption, as determined to be appropriate, to preserve the integrity of data.

10. Data Classification

10.1 Information Classification

Asurity outlines six levels of information sensitivity as follows.

- PUBLIC – This classification applies to information that has been approved by Asurity management for release to the public. By definition, there is no such thing as unauthorized disclosure of this type of information, and it may be disseminated without potential harm.
- INTERNAL-ONLY – This classification applies to non-sensitive business information that is generally only intended for use within Asurity. Such "internal use only" information can be considered routine work-related communications, including emails, presentations, spreadsheets, and other business documents.
- EXTERNAL – This classification applies to non-sensitive business information that is communicated externally to/with clients, business partners or other third parties. Such information can be considered work-related communications used in the normal course of doing business with external parties.
- CONFIDENTIAL – This classification applies to business information that contains either proprietary internal information or sensitive client-related data, including PII (see section 8.4.2). Such confidential information is intended for use only within Asurity or only *as needed* to be shared externally with clients or business partners. Its unauthorized disclosure could adversely impact Asurity or its customers, suppliers, business partners, or employees.
- RESTRICTED – This classification applies to the most sensitive business information that is intended for use strictly within Asurity and by a limited, authorized audience. Its unauthorized disclosure could seriously and adversely impact Asurity, its customers, its business partners, and its suppliers.
- PRIVILEGED – This classification applies to any communications, both internal and external, sent in connection with the delivery, the request for, and/or the receipt of *legal advice* or the sharing of documents or other work product prepared by, or at the direction of, an attorney.

10.2 Information Labeling Procedures

The following procedures must be followed to ensure that all data is appropriately labeled depending on its classification level. In all cases, the information creator/owner should always consider both "need to know" and granted access requirements as outlined in section 10.3 before sharing any information internally or externally.

- PUBLIC – Information classified as *PUBLIC* requires no specific labeling.
- INTERNAL-ONLY – Information classified as *INTERNAL-ONLY* does not require any specific labeling. Optionally, when the creator/owner desires to make it absolutely clear that the content of the email or business document should *never* be shared externally, the label "Internal Use Only" must be proactively applied in either the email subject line or as a decoration to the document file name.
- EXTERNAL – Information classified as *EXTERNAL* does require specific labeling as outlined immediately below. Nothing in this Policy or outlined herein with respect to

labeling procedures is intended to impede timely business communication with customers, suppliers, or business partners.

  - Outbound email does not require any specific labeling to indicate an external communication.
  - Inbound email may be *automatically* labeled by the email system, with the text "[External]" prepended to the subject line, or a similar notification banner added to the email body. This labeling approach will aid the recipient by alerting that the communication is originating from an external source, and, therefore, the recipient should take appropriate precautions before opening to avoid external threats such as potential phishing or other similar adversarial tactics.

- CONFIDENTIAL – Information classified as *CONFIDENTIAL* does require appropriate labeling as follows:
  - Email, either sent internal or external, must include the text "[Confidential]" in the beginning of the email subject line. Any file attachments to the email should also be appropriately labeled (see below).
  - Non-mortgage loan-related documents must include the text "Confidential" on both the cover page of the document (if appropriate) and in the footer of every page within the document. To aid the recipient of such documents in the appropriate handling, it is required that the document file name include the word "confidential", e.g., Quarterly-Revenue-Results [Confidential].xlsx. When file formats do not readily facilitate labeling within the body of the document (e.g., Excel spreadsheets, or PDF documents received from another party), the file name decoration is a sufficient label.
  - Mortgage loan-related documents must always adhere to the format and content determined by local, state and federal regulatory requirements and *should not* be altered or unnecessarily labeled or decorated in any way. Examples of such mortgage loan documents include cover letters, disclosures, loan estimates, closing estimates, affidavits, lender documents, investor documents, compliance certificates, or other documents typically included in a loan document package.
- RESTRICTED – Information classified as *RESTRICTED* does require appropriate labeling. These highly sensitive, strictly internal-only documents require clear labeling as follows:
  - Email must include the text "[Restricted]" in the beginning of the email subject line. Any file attachments to the email should also be appropriately labeled (see below).
  - Non-mortgage loan-related documents must include the text "Restricted" on both the cover page of the document (if appropriate) and in the footer of every page within the document. To aid the recipient of such documents in the appropriate handling, it is required that the document file name include the word "restricted", e.g., Acquisition-Target-ProForma [Restricted].pptx. When file formats do not

readily facilitate labeling within the body of the document (e.g., Excel spreadsheets, or PDF documents received from another party), the file name decoration is a sufficient label.
    - Mortgage loan-related documents are never classified as restricted. See CONFIDENTIAL above for appropriate labeling requirements.
- PRIVILEGED – Information classified as *PRIVILEGED* does require appropriate labeling as follows:
    - Email must include the text "[Privileged]" in the beginning of the email subject line. Any file attachments to the email should also be appropriately labeled (see below).
    - Non-mortgage loan-related documents must include the text "Privileged" on both the cover page of the document (if appropriate) and in the footer of every page within the document. To aid the recipient of such documents in the appropriate handling, it is required that the document file name include the word "privileged", e.g., Legal-Review [Privileged].pptx. When file formats do not readily facilitate labeling within the body of the document (e.g., Excel spreadsheets, or PDF documents received from another party), the file name decoration is a sufficient label.
    - Mortgage loan-related documents are never classified as privileged. See CONFIDENTIAL above for appropriate labeling requirements. Legal consultation about mortgage loan-related documents sent via email is covered by the handling procedures described above.

See section 13 on Data Encryption and Secure Data Transmission for additional considerations, specifically, the use the secure email attachment and file sharing solutions that support the external communication of confidential documents in a secure manner.

10.3 Access Control

The following access controls ensure that only personnel with the proper authorization and a need to know are granted access to Asurity systems and their resources:

- Need to Know – Information must be disclosed only to those people who have a legitimate business need for the information.
- System Access – proper controls shall be in place to authenticate the identity of users and to validate each user's authorization before allowing the user to access information or services on the system.
- Access Granting Decisions – Access to Asurity sensitive information is provided only after the authorization of the Information Owner or their delegate has been obtained. The list of individuals with access to Confidential or Restricted data must be reviewed for accuracy by the relevant Information Owner.

See the *Access Control Policy* for additional considerations regarding account management, including segregation of duties, account types, and account changes.

10.4 Information Owners

All electronic information managed by Asurity must have a designated Information Owner, and they are responsible for assigning appropriate information sensitivity classifications as defined above. Information Owners do not legally own the information entrusted to their care. They are instead designated members of the Asurity team who act as data stewards, and who supervise the ways in which certain types of information are used and protected.

Information Owners must make decisions about who will be permitted to gain access to information, and the intended uses of such information. Asurity must take steps to ensure that appropriate controls are utilized in the storage, handling, distribution, and regular usage of all electronic information.

10.5 Media Reuse and Disposal

Storage media containing sensitive (i.e. restricted or confidential) information shall be completely empty before reassigning that medium to a different user or disposing of it when no longer used. Simply deleting the data from the media is not sufficient. A method must be used that completely erases all data. When disposing of media containing data that cannot be completely erased, the media must be destroyed in a manner dictated by the technology disposal policy. See the Media and Equipment Disposal section of this document.

10.6 Device Security

If Restricted information is going to be stored or viewed on a personal computer, mobile device, personal digital assistant, or any other single-user system, the system must conform to data access control and encryption safeguards approved by Asurity. When not currently accessing or otherwise actively using the restricted information on such a device, users must not leave the device unattended without logging off, invoking a password protected screen saver, or otherwise restricting access to the restricted information.

10.7 Transfer of Sensitive/Confidential Information

When confidential or sensitive information from one individual is received by another individual while conducting official business, the receiving individual shall maintain the confidentiality or sensitivity of the information in accordance with the conditions imposed by the providing individual. All users must recognize the sensitive nature of data maintained by Asurity and hold all data in the strictest confidence. Any purposeful release of sensitive or confidential data to which a user may have access is a violation of Asurity policy and will result in personnel action, including legal action.

11. Mobile Devices

11.1 Mobile Device Policy

All company-provided mobile devices, smartphones and tablets (not including corporate IT-managed laptops) that have access to corporate networks, data or systems will be managed using a Mobile Device Management (MDM) solution.

Note: the MDM solution currently in use at Asurity is the Microsoft InTune platform.

11.2 BYOD

Asurity encourages employees to purchase and use smartphones and tablets of their choosing at work for their convenience – so called “Bring Your Own Device” or BYOD. Asurity may provide nominal reimbursement for the expense of personal mobile device usage. Asurity reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below when using their personal devices to access Asurity resources.

11.3 Mobile Device Requirements

Mobile devices used to access Asurity systems shall have the following requirements and restrictions:

- Currently only Apple iPhone and Android phones are permissible.
- Devices must maintain an up-to-date version of the platform operating system (e.g. Apple iOS, Google Android).
- Devices may be required to install the corporate MDM software and be properly configured for access to certain Asurity resources.
- Devices must be configured with a secure password that complies with the Asurity password policy and/or utilizes a biometric fingerprint to access the device. This password must not be the same as any other credentials used within the organization. Note, not all devices support biometric fingerprint security.
- With the exception of those devices managed by IT, devices are not allowed to be connected directly to the internal corporate network. Guest WiFi access is permissible.
- Users must only load data essential to their role onto their mobile device(s).
- Users must report all lost or stolen devices to Asurity IT immediately.
- If a user suspects that unauthorized access to company data has taken place via a mobile device, the user must report the incident in alignment with the Security Incident handling process.
- Devices must not be “jailbroken” or have any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the user. To jailbreak a mobile device is to remove the limitations imposed by the manufacturer. This gives access to the operating system, thereby unlocking all its features and enabling the installation of unauthorized software.
- Users must not load pirated software or illegal content onto their devices.

- Applications must only be installed from official platform-owner approved sources (e.g. Apple App Store, Google Play store). Installation of code from un-trusted sources is forbidden. If you are unsure if an application is from an approved source, contact Asurity IT for assistance.
- Devices must be kept up to date with manufacturer or network provided patches. As a minimum, patches should be checked for weekly and applied at least once a month.
- Devices must not be connected to a PC which does not have up-to-date and enabled anti-virus protection and which does not comply with corporate policy.
- Users must be cautious about the merging of personal and work email accounts on their devices, and take particular care to ensure that company data is only sent through the corporate email system. If users suspect that company data has been sent from or to a personal email account, they must notify Asurity IT immediately.
- Users must not use corporate workstations to backup or synchronize device content such as media files unless such content is required for legitimate business purposes.

11.3 Termination

Upon termination of a user, whether voluntary or involuntary, mobile devices used to access Asurity resources will be remotely wiped if provisioned with MDM. Note that Microsoft InTune only “wipes”/removes any corporate data associated with corporate email, applications, and related documents, but does not remove any personal data or other applications. In the absence of MDM, the user may be asked to demonstrate that all Asurity-related applications and data have been successfully removed from the mobile device.

12. System Protections and Updates

12.1 Antivirus, Malware, and Vulnerabilities

Antivirus software will be installed on all Asurity workstations and servers. The current anti-virus software solution is Sophos Endpoint Protection. The Sophos solution centralizes deployment and management, with virus and malware patterns updated daily on Asurity servers and workstations. Asurity utilizes malware detection on all user email accounts to automatically detect and quarantine suspicious attachments. The Digital Defense Inc. (DDI) solution is used to independently scan for vulnerabilities and determine whether server systems may be vulnerable.

Procedures for virus and malware detection, containment, and remediation are fully described in the *Asurity Incident Response Plan*.

12.2 Monitoring and Reporting

Appropriate IT administrative staff are responsible for providing reports for auditing and emergency situations as requested by the Asurity Security Team or appropriate personnel. Administratively, automated tools are used to alert the Security Team when antivirus is out of date or potential vulnerabilities are detected.

Asurity IT will regularly monitor security mailing lists, 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 Asurity networks to identify known or potential vulnerabilities.
- Identifying and communicating identified vulnerabilities and/or security concerns.
- Monitoring CERT, notifications, and Web sites of all vendors that have hardware or software operating in the Asurity environment.

12.3 Patch Management

Workstations and servers owned by Asurity must have up-to-date operating system security patches installed to protect the asset from known vulnerabilities. This includes all laptops, desktops, and servers owned and managed by Asurity. Desktops and laptops must have automatic updates enabled for operating system patches. This is the default configuration for all workstations provisioned by Asurity. Servers, including virtual servers or VMs, must comply with the minimum baseline requirements that have been approved by Asurity IT. These minimum baseline requirements define the default operating system level, service pack, hotfix, and patch level required to ensure the security of the Asurity asset and the data that resides on the system. Any exception to these standards must be documented and forwarded to the Asurity Security Team for review and approval.

12.4 Approved Software

Only software created by Asurity application staff, if applicable, or licensed software approved by the Asurity Security Team or appropriate personnel will be used on internal computers and networks. All new software will be tested by appropriate personnel in order to ensure compatibility with currently installed software and network configurations.

Personal software shall not be used on Asurity computers or networks. If a need for specific software exists, submit a request to your supervisor or department head. Users shall not use Asurity purchased software on home or on non-Asurity computers or equipment.

12.5 Use of Shareware/Freeware

Although shareware and freeware can often be useful sources of work-related programs, the use and/or acquisition of such software must be approved by the Asurity Security Team. Because the software is often provided in an open distribution environment, special precautions must be taken before it is installed on Asurity computers and networks. These precautions include determining that the software does not, because of faulty design, “misbehave” and interfere with or damage Asurity hardware, software, or data, and that the software does not contain viruses, either originating with the software designer or acquired in the process of distribution.

12.6 Virus Scanning

All data and program files that have been electronically transmitted to a Asurity computer or network from another location must be scanned for viruses immediately after being received. Contact the appropriate Asurity IT personnel for instructions for scanning files for viruses.

Every portable media device is a potential source for a computer virus. Therefore, every CD-ROM, DVD and USB device must be scanned for virus infection prior to copying information to a Asurity computer or network.

12.7 Bootable Media

Computers shall never be “booted” from a portable media device received from an outside source. Users shall always remove any such media or device from the computer when not in use. This is to ensure that the media or device is not in the computer when the machine is powered on. A CD-ROM, DVD or USB device infected with a boot virus may infect a computer in that manner, even if the media or device is not “bootable”.

13. Data Encryption

13.1 Device Encryption

Servers, desktop computers, including laptops, must be configured to use disk-level encryption. This ensures that any files or data stored on the hard drive of each machine is encrypted at rest.

- Windows-based desktop and laptop computers must have BitLocker enabled.
- MacOS X-based laptop computers must have FileVault enabled.
- Production servers and systems and any related Disaster Recovery (DR) systems must use encrypted storage.

13.2 Database Encryption

Asurity utilizes data encryption on all Production and DR databases. In this manner, all Production data stored in a database is encrypted at rest.

13.3 Encryption Keys

Asurity manages all Production and DR encryption keys using a FIPS 140-2 compliant secure key management solution – currently, Azure Key Vault. See https://learn.microsoft.com/en-us/azure/security/fundamentals/key-management for futher details.

13.4 Secure Data Transmission

All sensitive data and files shall be encrypted when transmitted through Asurity networks and environments. When encrypted data are transferred between organizations, the organizations shall devise a mutually agreeable procedure for secure data transmission. Asurity can employ several common methods of secure data transmission, such as the use of secure file shares, secure File Transfer Protocol (sftp/ftps), or other file encryption techniques.

13.5 Secure Email Attachments

If required by a client or business partner to secure the attachments in outbound emails, Asurity can support delivery whereby file attachments are removed and securely stored, and the email message body is augmented with embedded URL link(s). The resulting link(s) can be then accessed by the recipient to download the attachment. The sender may also elect to enable a 'password' feature, which further secures access to the file(s). When uniquely required by a client or business partner, use of alternative attachment delivery methods may be configured, as outlined in 13.4. For additional information regarding secure email attachment handling, please contact IT Support.

13.6 Email Encryption

Asurity utilizes third party service providers (Google Workspace and Office365) for standard office e-mail. By default, these services are configured to connect with external mail servers using Transport Layer Security (TLS), a secure communications protocol, if available. However, if requested by a client, these services also support the use of the Mandatory Transport Layer Security (MTLS) option, which *requires* the use of TLS for communication.

13.7 Facsimile

Sending sensitive information by facsimile is permissible and often required for valid business purposes. However, to comply with this Policy regarding data privacy and confidentiality, it is required that the sender alerts the designated recipient in advance if sensitive personal information or confidential information is being sent and that it is known that the designated equipment is in a secure area accessible only to the intended recipient or approved client personnel.

13.8 File Sharing Services

Asurity utilizes the Citrix ShareFile file sharing service for securely exchanging files both internally and with external parties. Any Asurity staff member who desires to utilize this technology may request a ShareFile account from the Asurity Security Team or appropriate personnel. Note that Google Drive, which is used as part of the Google Workspace application suite available to some Asurity staff, has the ability to enable file sharing and Asurity prohibits its use with external parties. The use of any other cloud-based file sharing services such as Box.com, Dropbox, or similar services is strictly prohibited.

13.9 File Transfer Protocol (FTP)

Files may be transferred to secure FTP sites through the use of appropriate security precautions. The use of SFTP is preferred over FTPS and the encryption must meet at a minimum the requirements defined in the Data Encryption section of this policy. Requests for any FTP transfers should be directed to the Asurity Security Team or appropriate personnel.

13.10 Secure Socket Layer (SSL)

All web sites and web services that contain any sensitive data, as defined in the Data Classification section of this policy, shall transmit data using SSL or TLS encryption – often referred to as HTTPS or HTTP over SSL. Asurity currently requires use of the TLS 1.2 or higher standard which supersedes SSLv3. The encryption algorithm must meet the minimum standards defined below. Appropriate digital certificates can be requested from the Asurity Security Team. All servers and applications using SSL or TLS must have the digital certificates signed by a known, trusted provider.

13.11 Encryption Algorithms

Asurity utilizes the Advanced Encryption Standard (AES) encryption standard for all confidential and sensitive data communications and requires a minimum key length of 256 bits. For password encryption or applications where hash functions are commonly used, Asurity utilizes the SHA-2 standard.

14. Telecommuting and Remote Access

14.1 Telecommuting and Work From Home

The Asurity considers telecommuting or so-called “work from home” to be an acceptable work arrangement in certain circumstances. Asurity users who work from their home full or part time, or users on temporary travel, or users who work from a remote office location, or any user who connects to Asurity network and/or hosted systems, if applicable, from a remote location is considered a telecommuting user under this policy and must abide by all information security requirements.

14.2 General Requirements

With the increased availability of broadband access and VPNs, telecommuting has become more viable for many organizations. While telecommuting can be an advantage for users and for the organization in general, it presents new risks in the areas of confidentiality and security of data. Workers linked to the Asurity network become an extension of the wide area network and present additional environments that must be protected against the danger of spreading Trojans, viruses, or other malware. This arrangement also exposes corporate as well as customer data to risks not present in the traditional work environment.

Telecommuting workers are required to follow, as applicable, all information security guidance defined in this policy. Additional telecommuting and remote access security requirements and protections are defined below.

14.3 Home Networks and Wireless Access

All home wireless infrastructure devices that provide direct access to a Asurity network, such as those behind Enterprise Teleworker (ECT) or hardware VPN, must adhere to the following:

- Use WPA2 with AES, WPA with AES or WPA with Temporal Key Integrity Protocol (TKIP)
- Use a complex WPA2 or WPA shared secret key (at least 20 characters) on the wireless client and the wireless access point
- Change the default SSID name
- Disable SSID broadcasting
- Disable administration through wireless communications
- Change the default administrative login and password

14.4 Dual Network Restriction

It is prohibited to be connected to both a wired and wireless network at the same time. Asurity workstations will be configured to restrict any such multiple connections. Note that Asurity servers or virtual server machines hosted in the datacenter or cloud do not have wireless capabilities.

14.5 Required Telecommuting Equipment and Setup

Users approved for telecommuting must understand that Asurity will not provide all equipment necessary to ensure proper protection of information to which the user has access; however, the following lists define the equipment and environment required.

Asurity provided:

- Asurity supplied workstation or laptop
- (Optional) Asurity supplied mobile device if approved by management
- (Optional) Virtual Private Network (VPN) access to internal resources (see 13.5.1)

User provided:

- Broadband connection that meets the following network performance standards:
  - At least 25 Mbits download speed. Higher speeds are strongly recommended.
  - At least 10 Mbits upload speed. Higher speeds are strongly recommended.

  Contact Asurity IT for assistance with selecting or configuring a broadband service.
- Secure office environment isolated from visitors and family.
- Optional, if required as part of your job duties:
  - Office printer
  - Paper shredder
  - A lockable file cabinet or safe to secure work-related documents when away from the home office

14.6 Security Protections

14.6.1 VPN Use

The Asurity requires the use of Virtual Private Network (VPN) software when remotely accessing any Asurity networks or internal resources.

14.6.2 Lock Screens

No matter what location, always lock the screen before walking away from the workstation. Be sure the automatic lock feature has been set to automatically turn on after no more than 15 minutes of inactivity.

14.6.3 Bluetooth Devices

No Bluetooth device shall be deployed on Asurity equipment that does not meet a minimum Bluetooth v5.1 specification without written authorization from the Asurity Security Team.. Any Bluetooth equipment purchased prior to this Policy must reasonably comply with all parts of this policy except the Bluetooth version specifications.

- Pins and Pairing
  - When pairing your Bluetooth unit to your Bluetooth enabled equipment (i.e. phone, laptop, etc.), ensure that you are not in a public area where your PIN can be compromised.
  - Use a minimum PIN length of 4. A longer PIN provides more security.
  - If your Bluetooth enabled equipment asks for you to re-enter your pin after you have initially paired it, you must refuse the pairing request and report it to the Asurity Security Team, through your Help Desk, immediately.
- Device Security Settings
  - All Bluetooth devices shall employ 'security mode 3' which encrypts traffic in both directions, between your Bluetooth Device and its paired equipment.
  - Switch the Bluetooth device to use the hidden mode (non-discoverable)
  - Bluetooth should be disabled by default and enabled only when it is needed.
  - Ensure device firmware is up-to-date.
  - Users must only access Asurity information systems using approved Bluetooth device hardware, software, solutions, and connections.

14.7 Data Protection

14.7.1 Transferring Data to Asurity

Transferring of data to Asurity requires the use of an approved VPN connection or an approved secure file transfer mechanism to ensure the confidentiality and integrity of the data being transmitted. Do not circumvent established procedures, nor create your own method, when transferring data to Asurity.

14.7.2 External System Access

If users require access to an external system, contact your supervisor or department head. Asurity Security Team or appropriate personnel will assist in establishing a secure method of access to the external system.

14.7.3 Non-Asurity Networks

Extreme care must be taken when connecting Asurity equipment to a home or hotel network. Although Asurity actively monitors its security status and maintains organization wide protection policies to protect the data within all contracts, Asurity has no ability to monitor or control the security procedures on non-Asurity networks.

14.7.4 Hard Copy Reports or Work Papers

Never leave paper records around your work area. Lock all paper records in a file cabinet at night or when you leave your work area. See Clean Desk section of this policy for more details.

14.7.5 Document Disposal

All paper documents which contain sensitive information that are no longer needed must be shredded before being disposed. Do not place in a trash container without first shredding. All users working from home, or other non-Asurity work environment, must have direct access to a shredder.

14.7.6 Data Entry When in a Public Location

Do not perform work tasks which require the use of sensitive corporate or customer information when you are in a public area, i.e. airports, airplanes, hotel lobbies. Computer screens can easily be viewed from beside or behind you.

14.7.7 Sending Data Outside Asurity

All external transfer of data must be associated with an official contract, non-disclosure agreement, or appropriate Business Associate Agreement. Do not give or transfer any customer information to anyone outside Asurity without the written approval of your supervisor. Only use approved methods outlined in the Electronic Communications Policy of this document.

14.7.8 Transferring Software or Files Between Home and Work

Asurity proprietary data, including but not limited to customer financial information, IT Systems information or human resource data, shall not be placed on any computer that is not the property of Asurity without written consent of the respective supervisor or department head. It is crucial to Asurity to protect all data and, in order to do that effectively we must control the systems in which it is contained. In the event that a supervisor or department head receives a request to transfer Asurity data to a non-Asurity Computer System, the supervisor or department head should notify the Asurity Security Team or appropriate personnel of the intentions and the need for such a transfer of data.

15. Security Awareness and Training

15.1 Annual Training Requirement

Asurity has established a security awareness and training program for all users of its systems, including management personnel. All users upon contract or hire and then at least annually thereafter shall receive appropriate training concerning security policies and procedures. General Asurity users will be trained using prepared materials. Application Developers, IT Administrators, and Asurity Security team members will be given the security awareness training and all additional training that has been determined by role type; e.g., secure software development concepts for developers.

15.2 Phishing Testing

As part of the security awareness and training program, Asurity will no less than annually conduct phishing testing of all users. Phishing is the fraudulent practice of sending emails purporting to be from reputable users or companies in order to induce the recipient to reveal sensitive information. Phish testing, then, is the process of intentionally sending realistic but fake emails to employees in order to see how they respond, and to gauge the effectiveness of security awareness training programs that are designed to help employees spot phishing emails and to handle them appropriately. Users that fall prey to the phish test are then provided additional training.

15.3 Periodic Reminders

The Asurity Security Team shall generate and distribute routine security reminders to all workforce members on a regular basis. Periodic reminders shall address topics such as password security, malicious software, incident identification and response, and access control. The Asurity Security Team may provide such reminders through formal training, e-mail messages, and discussions during staff meetings.

15.4 Key Training Concepts

The Asurity Security Team shall provide training concerning the important elements of this policy, as well as ensure general familiarity with topical security concerns.

Asurity security awareness training shall address the following:

- (Un)Acceptable Use
- Identification and Authentication
- Passwords
- Physical Security
- Data Privacy
- Protecting Confidential Information
- Email and Messaging
- Internet Security
- Social Engineering and Phishing

- Viruses, Malware, and Ransomware
- Social Media
- Mobile Devices
- Data Encryption
- Telecommuting and Remote Access
- Reporting Incidents

16. Asset Management

16.1 Overview

Asset management at Asurity includes processes for receiving, inventorying, and eventually disposing of equipment. Maintaining an accurate asset control posture is critically important to ensure computer equipment locations and dispositions are well known. Lost or stolen equipment may contain sensitive data and therefore proper asset management procedures provide relevant documentation that aid in recovery, replacement, or investigative activities.

16.2 Policy

All electronic assets (equipment) at Asurity exceeding the asset value threshold must be appropriately tracked in an asset inventory. Asset disposal processes regardless of asset value must be followed and documented.

16.2 Asset Value

Assets which cost less than $250 shall not be tracked, including computer peripheral components such as monitors, keyboards, or mice. However, assets, which store data regardless of cost, shall be tracked either as part of a computing device or as a part of network attached storage.

16.3 Asset Types

The list of assets that will be tracked include, but are not limited to:

- Desktop workstations
- Laptop mobile computers
- Tablet devices
- Printers, copiers, fax machines, and multifunction print devices
- Handheld devices
- Scanners
- Servers
- Network appliances (e.g. firewalls, routers, switches, Uninterruptible Power Supplies (UPS), endpoint network hardware, and storage)
- Private Branch Exchange (PBX) and Voice over Internet Protocol (VOIP) Telephony Systems and Components
- Internet Protocol (IP) Enabled Video and Security Devices
- Memory devices

16.4 Asset Tracking Requirements

The following are the standard requirements for asset tracking, which shall minimally include if available:

- Date of purchase
- Make, model, and descriptor
- Serial Number
- Location
- Type of asset
- Owner
- Department
- Purchase Order number
- Removal
- Disposition

All asset information must be centrally maintained in an asset tracking inventory, which may take the form of a database or spreadsheet or similar mechanism.

16.5 Asset Removal

Removal and/or disposal of any assets as outlined in section 15.3 requires direct approval from either the Asurity Security Team or their delegate. Such approval and authorization shall be provided by email and noted in the relevant asset inventory as appropriate.

16.6 Asset Disposal

16.6.1 External Media

It should be assumed that any external media in the possession of a user is likely to contain either protected information or other sensitive information. Accordingly, external media (CD-ROMs, DVDs, USB drives) should be disposed of in a method that ensures that there will be no loss of data and that the confidentiality and security of that data will not be compromised.

When no longer needed, all forms of external media are to be sent to IT or appropriate personnel for proper disposal. External media should never be thrown in the trash. All external media must be sanitized or destroyed following appropriate destruction methods are used based on National Institute of Standards and Technology (NIST) 800-88 guidelines.

16.6.2 Electronic Equipment

When Technology assets have reached the end of their useful life, they should be sent to the Asurity Security Team or IT for proper disposal (see E-Recycling Option below). All electronic or computer equipment to be disposed of will be wiped of all data, and all settings and configurations will be reset to factory defaults.

Electronic Equipment refers to desktop, laptop, tablet or netbook computers, printers, copiers, monitors, servers, handheld devices, telephones, cell phones, disc drives or any storage device, network switches, routers, wireless access points, batteries, backup tapes.

The Asurity Security Team or IT will securely erase all storage mediums in accordance with current industry best practices. All data including all files and licensed software shall be removed from equipment using disk sanitizing software that cleans the media following National Institute of Standards and Technology (NIST) 800-88 guidelines and meeting Department of Defense standards.

No computer or technology equipment may be sold to any individual, and no computer equipment should be disposed of via skips, dumps, landfill, or office trash bins.

16.6.3 E-Recycling Option

Asurity IT may arrange for final disposal of electronic equipment through certified e-recycling vendors. Such vendors can provide a full range of services including secure transport, data destruction, and in certain cases asset value recovery. If data destruction services are required, the vendor must follow procedures that adhere to US Department of Defense (DoD) and National Institute of Standards and Technology (NIST) standards for removal of sensitive data. Prior to leaving Asurity premises, all equipment must be updated in the appropriate asset inventory to affirm its status and removal. The e-recycling vendor must provide documentation confirming the asset disposition. Any asset value recovery will be coordinated with Finance.

16.6.4 Client Notification and Asset Tracking

If the asset to be disposed contains electronic media that is known to contain client data:

- The affected client should be notified prior to commencing the disposal process on the subject decommissioned asset.
- A chain of custody record should be maintained for audit and tracking purposes throughout the asset disposal process.
- A final report certifying data destruction may be provided to the client upon request.

17. Change Management

17.1 Change and Release Management Policy

All changes will adhere to the *Asurity Change and Release Management Policy* which outlines a standardized process for proposing, evaluating, implementing, reviewing, approving, deploying, and monitoring changes to Asurity production systems and application environments. The policy defines a disciplined process to manage all changes to production systems and infrastructure, including but not limited to software applications, databases, operating systems, firewalls, network infrastructure, patches, and configurations. The policy fosters collaboration between IT, development, testing, information security, and business stakeholders before production changes occur, minimizes disruption to business operations, ensures proper validation and authorization for change, and helps to maintain the integrity of the production environment.

18. Application Development and Maintenance

18.1 Software Development Life Cycle (SDLC)

All software application development and maintenance activity will adhere to the *Asurity Software Development Life Cycle* (SDLC) policy which establishes a standardized and repeatable approach for developing, deploying, and maintaining high-quality software applications. The policy champions the adoption of an agile development methodology to deliver high-quality software solutions efficiently and iteratively, adheres to industry best-practices for software development and delivery, and outlines the different stages a software project goes through from conception to deployment and beyond.

19. Audit and Activity Log Review

19.1 Audit Controls

Asurity is committed to routinely auditing users' activities in order to continually assess potential risks and vulnerabilities to protect information in its possession. As such, Asurity will continually assess potential risks and vulnerabilities to protected information in its possession and develop, implement, and maintain appropriate administrative, physical, and technical security measures.

Audit controls ensure that Asurity implements hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain protected information. Audit Controls are technical mechanisms that track and record computer activities. An audit trail determines if a security violation occurred by providing a chronological series of logged computer events that relate to an operating system, an application, or user activities.

19.2 Security Logging

Procedures must be in place to ensure that all security access and activity is recorded and reviewed for all electronic information resources that contain, access, or transmit data classified as confidential.

a. Logging must be enabled at the operating system, application/database, and system/workstation level.
b. Logs must be reviewed in response to suspected or reported security problems on systems containing confidential data or as requested by the Security Team.
c. The Security Team is responsible for determining which systems require scheduled log review.
d. Log review shall include investigation of suspicious activity, including escalation to the Incident Response team.
e. Individuals shall not be assigned to be the sole reviewers of their own activity.

19.3 Suspicious Activity

Asurity actively monitors all systems and networks to detect and alert on suspicious activity. Please refer to the *Asurity Incident Response Plan* for more information, outlining the metrics, thresholds, and heuristics utilized for threat intelligence to maintain a robust security posture.

19.4 Activity Log Review

Activity reviews must be conducted on a periodic basis as an operational review including, but not limited to, user accounts, system access, file access, security incidents, audit logs, and access reports. Asurity shall conduct on a regular basis an internal review of records of system activity to minimize security risk.

The Asurity Security Team shall be responsible for conducting reviews of Asurity information systems' activities. Such person(s) shall have the appropriate technical skills with respect to the operating system and applications to access and interpret audit logs and related information appropriately. Audits shall also be conducted if Asurity has reason to suspect wrongdoing.

20. Third Party Risk Management

20.1 Vendor Risk Management

Asurity maintains responsibility and accountability for overseeing third-party vendor, or service organization (SOs), relationships and ensures that they remain aligned with our strategic objectives and appropriately manage risk.

Asurity leverages a number of industry standard methodologies to routinely assess vendor risk, including the Vendor Risk Management Maturity Model (VRMMM) from SharedAssessments.org, the FFIEC's IT Examination Handbook for Vendor and Third-Party Management, and, ideally, available SSAE 18 SOC 2 Type II audit reports.

Vendors are assessed for risk before going to contract, and annually thereafter, so that appropriate due diligence steps can be taken to ensure that Business Continuity, Information Security, Physical Security, and other key components have been properly assessed.

20.2 Change Management

Should there be any significant change in the services provided by an existing third-party vendor outside of the standard annual review period outlined in section 5.3, a review of the relationship is then required. Changes that warrant a vendor risk review include but are not limited to a change in the service pricing model, a change in service location(s), a change in how the service is provisioned, a discernable change in service quality, or an information security event affecting the vendor, its staff, or the underlying technologies utilized by that vendor.

If Asurity deems any change to be an unacceptable risk, the vendor will be required to address the concern with a timely mitigation plan. If a mitigation plan cannot be provided or met, Asurity will then seek alternative service providers.

20.3 Risk Review

All third-party vendors or service organizations that have a direct impact on a business unit's ability to continue to deliver its most important products and services will be required to either provide a SOC audit report or complete a VRMMM Standard Information Gathering (SIG) template or verifying annually their ongoing compliance with SSAE information security and operational standards.

Any gaps in a vendor's processes or procedures will be risk scored and assessed for potential business impact, and the resulting remediation activity will be monitored and tracked for risk mitigation and closure. The Asurity Security Team together with Business Unit Sponsors will engage appropriate stakeholders in the organization throughout the process including information security, legal, human resources, business operations, technical operations, and line management teams within each business unit.

20.4 Risk Acceptance

Risk Acceptance is the practice of simply allowing the business to operate with a known risk. Many low risks are simply accepted. Risks that have an extremely high cost to mitigate are also often accepted. Each business will utilize a risk assessment framework and identify those risks that it has accepted and the rationale for acceptance.

To ensure consistency in vendor assessment and reporting, a Vendor / Service Organization Report Review Summary Template is provided in the *Asurity Risk Management Framework* document.

20.5 Risk Reporting

Using the risk management framework outlined above, business risks and risk management strategies must be clearly reported and summarized into a management reporting package, and will be utilized as part of the overall governance process. See the *Asurity Risk Management Framework* document for additional details.

21. Supporting Documents

The following is a list of related policies and procedures that complement and support this Information Security Policy. All documents listed here are available on the Asurity Wiki (Intranet).

- *Asurity Employee Handbook*
- *Asurity Access Control Policy*
- *Asurity Business Continuity Program, Policy, and Plan*
- *Asurity Incident Response Plan*
- *Asurity Software Development Life Cycle (SDLC)*
- *Asurity Change and Release Management Policy*
- *Asurity Vendor Risk Management Procedures*
- *Asurity Overview of Security Awareness Training*
- *Asurity External Threat Management Process*
- *Asurity Data Retention Policy*
- *Asurity Backup and Recovery Management Policy*

END OF DOCUMENT