NACB CYBERSECURITY STANDARDS PREPARED BY IMAGINE TECHNOLOGY GROUP (ITG)

1. Scope

1.1 This standard covers the recommended cyber security practices for the effective defense and protection of private or sensitive customer information along with the practices for bringing people, processes, and technology into information and security compliance.
1.2 *Units*—The values stated in inch-pound units are to be regarded as the standard. The values given in parentheses are mathematical conversions to SI units that are provided for information only and are not considered standard.
1.3 This standard does not purport to address all the security and safety concerns, if any, associated with its use. It is the responsibility of the user of this standard to establish appropriate security, safety, and health practices and determine the applicability of regulatory limitations prior to use.

2. Terminology

2.1 Definitions of Terms Specific to This Standard:

2.1.1 *Information assets, n*— a body of knowledge that is organized as a single asset such as customer records, intellectual property.
2.1.2 *Vulnerability, n*— a weakness present that allows information to be exposed to a threat

2.1.3 *Malware, n - any* program or file that is harmful to a computer such as viruses, worms, spyware and ransomware.
2.1.4 *Boundary defense, n*— control the flow of traffic through network borders, and police content by looking for attacks and evidence. Established multilayered boundary defenses such as perimeter networks, firewalls, and other network tools.
2.1.5 *Incident response, n*— an organized approach to addressing and managing a security breach or cyberattack to limit damage and assist with recovery.
2.1.6 *Penetration test, n*— simulated cyber-attack against a computer system, augments a web application firewall (WAF).
2.1.7 *Chain of Custody, n* – validated process to gather, track and protect any kind of evidence. It is important because it can be used in a court of law.

2.1.8 *Phishing Event, n* – fraudulent practice of sending emails from reputable companies in order to induce or reveal personal information.

2.1.9 *Data Loss Prevention, n* - strategy for making sure that end users do not send sensitive or critical information outside the corporate network. The term is also used to describe software products that help a network administrator control what data end users can

transfer.

3. Significance and Purpose

3.1 Cyber Security. Implementation of an enterprise-wide data privacy and security compliance programs to advise, implement and manage security strategy, core infrastructure security measures and advisory financial risk strategies are in place to prevent data collection and storage of personally identifiable information and other sensitive data from being lost, corrupted or stolen. The appropriate data breach response processes and adequate employee training can expand the protection of the privacy and security of its systems and networks.

In order to accomplish this the organization should *Identify* what information assets to protect (customer records, intellectual property etc.). The use of public wi-fi by employees, loss of paper records, connected smart devices to your Organization's network, email and phishing scams can be a source of vulnerabilities.

3.2 Conduct a Risk Assessment to identify, describe, analyze risks, threats and vulnerabilities.

3.3 Develop strategy and plan to protect critical information assets with security measures and controls.

3.4 Develop security measures and controls. Write SOP's, establish functional requirements for developers/programmers or vendor contracts.

3.5 Implement security measures and controls.

3.6 Active prevention and response planning. Detect, analyze and respond to system intrusions and data breaches.

3.7 Continuous evaluation and improvements.

4. Summary of Standard

4.1 This standard covers the cyber security aspect and includes the required personnel security measures, physical security, security documents, and technical security applicable to the safety, security, and privacy of people, product, currency, and property.

4.2 This standard shall be used to deter the risk of loss, meeting or exceeding the standard of most government regulations; however, no claim is made that this standard meets the regulations of any specific governing body.

5. Acceptable Use Policy

5.1 As the user will be given access to the corporate network, Internet, and other IT resources, the Organization expects the user to use these resources in a responsible manner. The user shall make a concerted effort to avoid accessing network data, files, and information that are not directly related to his or her job function. Existence of access capabilities does not imply permission to use this access.

5.2 Circumvention of Security: Using Organization-owned or Organization-provided computer systems to circumvent any security systems, authentication systems, user-based systems,

or the escalation of privileges is expressly prohibited. Knowingly taking any actions to bypass or circumvent Organization security systems is expressly prohibited. This includes disabling or tampering with any Organization supplied security software.

6. Password Policy

6.1 Password Management: The best security against a password incident is simple. Follow a sound password construction strategy following industry standard best practice guidelines on password construction:

- Use a password manager to assist with the generation unique passwords per account along with the storage of each unique password.
- Do not share or reveal passwords to others.
- Passwords should not be reused.
- Enable multi-factor authentication on all applications/services that support it.
- SMS authentication as a second authentication factor is better than nothing but is known to be vulnerable to SIMSwaps.
- The use of authentication applications or physical hardware tokens is recommended for high value accounts.
- Passwords must be at least 15 characters long.

6.2 Confidentiality: Passwords are considered confidential data and are to be treated with the highest discretion out of any of the organization's proprietary information; Following industry standard best practice guidelines for the confidentiality of organization passwords.

6.3 Change Frequency or Based on Compromise: In order to maintain robust security, passwords shall be periodically changed (within 90-180 days) or are to be changed based on indicators of compromise. This limits the damage an attacker can do as well as helps to frustrate and slow brute force attempts. At a minimum, users shall change passwords as industry standard requires.

7. Confidential Data Policy

7.1 Data Classification: Information assets are assets to the Organization just like physical property. In order to determine the value of the asset and how it should be handled, data shall be classified according to its importance to Organization operations and the confidentiality of its contents. Once this has been determined, the Organization can take steps to ensure that data is treated appropriately. Of concern is confidential, financial, PII, PCI DSS or ePHI. This shall be identified and inventoried in all its forms – electronic, printed, or stored on digital media – and segregated from the Organization's non-confidential data so that access to it can be more tightly controlled and tracked. Any media that contains ePHI shall be catalogued and secured.

7.2 Examples of Confidential Data: The following list is not intended to be exhaustive but should provide the Organization with guidelines on what type of information is typically considered confidential. Confidential data can include:

- Personal Identifiable Information (PII)
- Electronic Protected Health Information (ePHI)
- Medical and healthcare information
- Financial Information
- Credit or debit card (PCI DSS) and other business financial information
- Other business information
- Network diagrams or legal communications

7.3 Inventory: After classification, identify all systems, devices, and media that house, collect, store, and process sensitive information. Determine and document ownership, responsibility, and functions of each system including remote access and removal storage if warranted. Evaluate environment for compliance with other health or financial compliance standards.

7.4 Treatment of Confidential Data: The following sections detail Organization requirements on the storage, transmission, and destruction of confidential data. The Organization shall determine the access control capabilities of each system housing sensitive information to ensure compliance with industry standards. If the standards cannot be met the organization shall upgrade any systems or procedures to meet industry standards.

7.5 Storage: Confidential information shall be stored in appropriate systems that meet security requirements and are not accessible to the public unless deemed necessary.

7.6 Transmission: Implement security controls to ensure sensitive information is sent in a secure manner using available encryption between sender and receiver.

7.7 Destruction: The organization shall ensure there is a retention policy that automates media destruction if possible, if not, media containing confidential data shall be destroyed in a manner that makes recovery of the information impossible.

7.8 Use of Confidential Data: A successful confidential data policy is dependent on the users knowing and adhering to the Organization's standards involving the treatment of confidential data within approved business purposes.

- Sharing Confidential Data: If confidential data is shared with third parties, such as service providers or Business Associates, a written confidential information and/or non-disclosure agreement shall govern the provider's use of confidential information with written agreement with the provider that indicates how the data should be used, secured, and destroyed, with a service provider or other third party, due diligence shall always be performed prior to a provider being selected.

8. Mobile Device Policy

8.1 Physical Security: By nature, a mobile device is more susceptible to loss or theft than a non-mobile system. The Organization shall carefully consider the physical security of its mobile devices and take appropriate protective measures.

8.2 Data Security: When a mobile device is lost or stolen, the data security controls that were implemented on the device are the last line of defense for protecting Organization data. Encrypt

mobile devices whenever possible.

- Organization data should not be made available on personal mobile devices, if this is required, consider implementing a mobile device management platform or providing Organization owned mobile devices.

8.3 Removable Media: This section covers any USB drive, flash drive, memory stick or other removable data storage media that could be connected to Organization systems. Ideally, removable media should not be used. When used, removable media shall always be encrypted.

8.4 Connecting Mobile Computers to Unsecured Networks: The use of VPN client software on endpoints is recommended when connecting to unsecured networks. Free Wireless Hotspots should never be used.

8.5 Audits: The Organization shall conduct periodic reviews to ensure policy compliance and to inventory mobile devices. The audit shall involve the inventory and inspection of each mobile device to ensure compliance with Organization security policies.

9. Retention Policy

9.1 Reasons for Data Retention: Some reasons for data retention include:

- Litigation
- Accident investigation
- Security incident investigation
- Regulatory requirements
- Intellectual property preservation

9.2 Personal Data: There are no retention requirements for personal data (non-business related).

9.3 Operational Data: Operational Data includes data for basic business operations, communications with vendors, employees, device logs (if non-confidential), etc. Operational data shall be retained for as long as industry standards dictate.

9.4 Confidential Data: Confidential Data is any information deemed proprietary to the business, including financial, PII or ePHI. See the Confidential Data Policy for more detailed information about how to handle confidential data. Confidential data, including ePHI and other confidential data. Confidential data shall be retained for as long as industry standards dictate.

9.5 Data Destruction: Data destruction is a critical component of a data retention policy. Data destruction shall occur based on company policy or regulatory requirements.

10. Email Policy

10.1 Proper Use of Organization Email Systems: See acceptable use policy.

10.2 Emailing Confidential Data: Any email containing confidential information, regardless of whether the recipient is internal or external to the follows use of strong encryption. Further guidance on the treatment of confidential information exists in the Organization's Confidential Data Policy.

10.3 Retention and Backup: Email shall be retained and backed up in accordance with the applicable policies, which may include but are not limited to Confidential Data Policy, Backup

Policy, and Retention Policy

10.4 Email Account Termination: When a user leaves the Organization, their account should be disabled as quickly as possible.

10.5 Data Leakage: Data loss prevention techniques shall prohibit or limit the sharing of types of classified information, emailing the data to a personal account or otherwise removing it from Organization systems by users are best employed to protect against leakage of confidential data.

11. Backup Policy

11.1 Identification of Critical Data: Critical confidential data shall be identified so that it can be given the highest priority during the backup process. Any data deemed confidential shall be identified so that backups of this data are treated and secured accordingly.

11.2 Data to be Backed Up: A backup policy shall balance the importance of the data to be backed up with the burden such backups place on the users, network resources, and the backup administrator.

11.3 Backup Frequency: Backup frequency is critical to successful data recovery, a backup schedule will allow for sufficient data recovery in the event of an incident, while avoiding an undue burden on the users, network, and backup administrator. Determine an incremental-every day and full-every week back up frequency along with required back up for change or specific event frequency. Data backups shall include storage in offsite locations.

11.4 Backup Storage: Keep backups in a secure offsite location or online for as long as needed to restore business operations.

11.5 Restoration Procedures & Documentation: The data restoration procedures shall be tested and documented. Documentation shall include exactly who is responsible for the restore, how it is performed, under what circumstances it is to be performed, and how long the process should take from request to restoration.

11.6 Restoration Testing: Backup restores shall be tested when any change is made that may affect the backup system, as well as annually.

Network Access and Authentication Policy

11.7 Access Control Account Set Up: Potential personnel are to be screened prior to hire, appropriate to the position, with more in-depth background checks required for personnel with greater responsibilities or access to confidential information. During initial account setup, certain checks shall be performed in order to ensure the integrity of the process. The following policies apply to account setup:

- Positive ID and coordination with Human Resources is required.
- User and network access will be granted only if he or she agrees to the applicable network use policies, such as the Acceptable Use Policy.
- The ability to add, delete, change, and reset user IDs, user credentials, user privileges, and other account-related activities, shall be limited as much as possible, such as to a small group of administrators with specific authority to make these changes.
- During initial account setup, or during a password reset, the account shall be assigned a unique password, which shall be changed immediately after the first use. The Organization shall not

use the same password for every new account or password reset.

11.8 Account Access Levels: Access levels shall be assigned solely based on job classification or function (role-based access control). Documentation shall be kept that details each user's level of access as well as approval of that access by authorized parties. An access control system shall be utilized that enforces this policy and restricts users' access to data based on defined access levels. This system shall enforce the principle of least access and have a default "denyall" setting for new or unrecognized users.

11.9 Account Changes and Terminations: Accounts shall be audited on interval or as needed based on regulations or compliance requirements to ensure user access levels match expected levels based solely on business need. The Organization shall establish a process for increasing, decreasing, or otherwise changing access levels based on either A) an account audit, or B) a change in user access requirements.

When managing network and user accounts, it is important to stay in communication with the Human Resources department so that when an employee no longer works at the Organization, that employee's account can be disabled. Access for terminated employees shall be immediately revoked. Organization shall audit user accounts every 90 days and remove or disable any accounts that are inactive.

11.10 Authentication: User systems shall be configured with usernames, passwords and multi-factored authentication when possible.

11.11 Time Out Periods: Include appropriate time out periods based on business need, while providing optimal security for unattended devices.

11.12 Minimum Configuration for Access: The organization shall control minimum requirements for configuration and patching levels needed for network access.

11.13 Storage of Login Credentials: Industry best practices state that username and password combinations shall be saved in an encrypted format. Consider a Password Management application.

11.14 Failed Login Attempts: In order to guard against password-guessing and brute-force attempts, the Organization shall lock a user's account after 3-5 unsuccessful logins, implemented as a time-based lockout (for a minimum of 30 minutes) or require a manual reset, at the discretion of the IT Person. Log review for failed password attempts should be reviewed on a regular basis to detect malicious activities.

11.15 Multifactor Authentication: Multifactor Authentication should always be used for network systems as well as SaaS subscriptions.

12. Workforce Security Policy

12.1 Roles and Responsibilities: The Organization shall establish and clearly communicate to employees, roles and responsibilities for all job functions in clear, written job descriptions, and shall ensure that each position has appropriate levels of oversight and training specifically identify all roles and responsibilities that have a business need to access, alter, retrieve, or store ePHI.

12.2 Hiring and Task Assignment: The Organization shall ensure that the employee or contractor has the necessary skills and qualifications to fill the role and meet the qualifications and background against the written job description.

12.3 Implement an employee training program. The training program should contain instruction

on how to identify social engineering attacks as well as periodic campaigns to test the level of understanding.

12.4 Workforce Clearance: Establish a procedure to determine what level of access to confidential information is necessary for the job function, and then establish a procedure to ensure that the access is reasonable and appropriate to the role.

12.5 Granting Access/Termination of Access: Workforce members shall be notified in writing of the access capabilities as well as any expectations required for security and shall agree to the expectations in writing. When access is to be terminated, the Organization shall coordinate procedures with Human Resources to ensure that access is transfer, upgrade, disable immediately, or, better yet, in advance of, employment termination. This should involve the disabling electronically and/or return of access devices, passwords, encryption keys, hardware, software, data involving the deactivation of accounts and remote access capabilities.

13. Incident Response (IR) Policy

13.1 Types of Incidents: A security incident is defined as any attempted or successful unauthorized access, use, disclosure, modification, or destruction of information; or any unauthorized attempted or successful interference with system operations. A security incident, can take one of two forms:

- Electronic: This type of incident can range from an attacker or user accessing the network for unauthorized/malicious purposes, to a virus outbreak, to a suspected Trojan or malware infection. Also covered in this section is the discovery of unauthorized wireless access devices, and alerts generated from intrusion detection, intrusion prevention, and file integrity monitoring systems.
- Physical: A physical IT security incident involves the loss or theft of a laptop, mobile device, tablet computer, smartphone, portable storage device, or other digital apparatus that may contain Organization information. A physical incident can also apply to the loss or theft of data in printed form.

13.2 Preparation: The most important preparation work, obviously, is maintaining good security controls that will prevent or limit damage in the event of an incident. Incident Response roles, responsibilities and procedures should be tested against design basis risk scenarios so that the organization can be prepared for the types of risk which could affect them. Testing to be sure necessary resources are quickly available during an incident and remain in compliance with industry/governmental regulations in addition any agreements with third parties' response agreements.

13.3 Confidentiality: All information related to an electronic or physical security incident shall be treated as confidential information until the incident is fully contained and investigated. This will serve both to protect employees' reputations (if an incident is due to an error, negligence, or carelessness), and to control the release of information to the media and/or customers until the scope and damage of the incident can be assessed.

- Electronic Incidents: When an electronic incident is suspected, the goal is to recover as quickly as possible, limit the damage done, secure the network, and preserve evidence of the incident. Remove the compromised or unauthorized device from the network by unplugging or disabling network connection. Do not power down the system, disable the compromised account(s)

as appropriate; report the incident to the IT Person and physically secure the compromised system.

- If prosecution of the incident is desired, chain of custody and preservation of evidence are critical, log each step taken during this process, including chain of custody for the compromised system, hard drives, media, and/or logs. Notify applicable authorities if prosecution is desired and possible based on the evidence collected.
- Based on information gathered, determine the effectiveness of the policy and incident response processes, procedures, and personnel. Make changes that are necessary to strengthen response capabilities.

- Physical Incidents: Prepare for an incident by mandating the use of strong encryption to secure confidential data when stored on Organization systems, mobile or otherwise. Applicable policies, such as those covering encryption and confidential data, should be reviewed for guidance. Physical security incidents are sometimes the result of a random theft or inadvertent loss by a user or intentional. Survey on a quarterly basis the Organization's laptops and mobile devices to assess the Organization's risk if one were to be lost or stolen.

13.4 Response: Review of physical evidence, data forensics or logs can provide insights as to the extent of the incident.

13.5 Loss Contained: First, change any user names, passwords, account information, encryption keys, passphrases, etc. that were stored on, or used by, the system. Notify the IT or IR Person. Notify the applicable authorities if an incident/breach/loss has occurred.

13.6 Data Loss Suspected: First, notify the executive team, legal counsel, and/or public relations group so that each team can evaluate and prepare a response in their area.

13.7 Notification: Notify the applicable authorities using their notification and breach notification policies.

13.8 Managing Risk: Managing risk of a security incident or data loss is the primary reason to create and maintain a comprehensive security policy. Protecting critical and confidential data and key systems from these risks is of paramount importance in the industry. An Incident Response Policy is not effective at managing risk if it is not maintained and kept current, thus any policy shall be reviewed and tested at least annually or based on changing risk variables within the environment

13.9 Organization shall conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of the Organization's critical or confidential information as identified in the Confidential Data Policy. The process shall be performed annually or based on changing risk variables within the environment.

13.10 Risk Management Program: A formal risk management program shall be implemented to cover any risks known to the Organization (which have been identified through a risk assessment), and to ensure that reasonable security measures are in place to mitigate any identified risks to a level that will ensure the continued confidentiality, integrity, and availability of the Organization's confidential and critical data.

14. External Connection Policy

14.1 Encryption: Site-to-site VPNs shall utilize strong encryption to protect data during transmission. Encryption algorithms shall meet or exceed current industry standards for strong encryption.

14.2 Authentication: Site-to-site VPNs shall utilize a strong password, pre-shared key, certificate, or other means of authentication to verify the identity of the remote entity. The strongest authentication method available shall be used, which can vary from product-to-product.

14.3 Implementation: When site-to-site VPNs or WAN connections are implemented, they shall adhere to the principle of least access, providing access limited to only what is required for business purposes. Further, systems that will be accessed over the site-to-site VPN or WAN connection should be located in a demilitarized zone (DMZ), if possible, to segment access from the Organization's trusted network.

14.4 Management: The Organization shall manage its own VPN gateways, meaning that a third party shall not provide and manage both sides of the site-to-site VPN.

14.5 Logging and Monitoring: Depending on the nature of the site-to-site VPN or WAN connection, the IT Person will use his or her discretion as to whether additional logging and monitoring is warranted.

14.6 Managing Risk: Risk for a VPN or WAN should be weight based on the business requirements and the potential risk.

14.7 Restricting Third Party Access: Best practices for connection to a third party require that the link be held to higher security standards than an intra-Organization connection

15. Guest Access Policy

15.1 Granting Guest Access: Guest access will be provided on a case-by-case basis to any person who can demonstrate a reasonable business need to access the network or access the Internet from the Organization network.

15.2 AUP Acceptance: Guests shall agree to and sign the Organization's Acceptable Use Policy (AUP) before being granted access.

15.3 Approval: Guest need for access will be evaluated and provided on a case-by-case basis. This shall involve management approval if the request is non-standard or access to business systems.

15.4 Account Use: Guest accounts, if offered, are only to be used by guests. Guest accounts shall have specific expiration dates that correlate to the business need for the individual guest's access. The account expiration date is not to exceed either A) the expected duration of the guest's need for access or, B) thirty days, whichever is sooner.

15.5 Security of Guest Systems: Guests are expected to be responsible for maintaining the security of his or her system, and to ensure that it is free of viruses, Trojans, malware, etc. The Organization reserves the right to inspect the system if a security problem is suspected but does not deem it necessary to inspect each guest's system prior to accessing the network.

15.6 Guest Access Infrastructure Requirements: Best practices dictate that guest access be kept separate, either logically or physically, from corporate network, since guests have typically not undergone the same amount of scrutiny as the Organization's employees. Guest access shall be provided prudently and monitored for appropriateness of use.

15.7 Monitoring of Guest Access: Since guests are not employees of the Organization, they are not considered trusted users. As such, the Organization will monitor guest access to ensure that the Organization's interests are protected, and its security policies are adhered to.

16. Wireless Access Policy

16.1 Security Configuration

- The Service Set Identifier (SSID) of the access point shall be changed from the factory default.
- If possible, though not required, the wireless access point should utilize MAC address filtering so that only known wireless NICs are able to connect to the wireless network.
- Encryption shall be used to secure communications on wireless networks.
- Administrative access to wireless access points shall utilize strong passwords or two-factor authentication.
- Change all default passwords to access the device
- If possible, hide the SSID
- All logging features shall be enabled on the Organization's access points.

16.2 Audits: The wireless network shall be audited quarterly to ensure that this policy is being followed. Specific audit points can include: location of access points, signal strength, SSID, SSID broadcast, and use of strong encryption.

17. Network Security Policy

17.1 Network Device Authentication: Passwords that are used to secure these devices, such as routers, switches, and servers, shall be held to higher standards than user-level or desktop system passwords and the utilization of multi-factor authentication.

17.2 Network Device Password Construction: See password creation policy for strong, unique password per network/security device. The utilization of vault or password manager technology can help with this and sharing credentials that might need access based on business need.

17.3 Failed Logins to Network Devices: Repeated login failures can indicate an attempt to 'crack' a password and surreptitiously access a network account. In order to guard against password-guessing and brute-force attempts, the Organization shall lock a user's account after 5 unsuccessful logins

17.4 Password Policy Enforcement: Where passwords are used, technology shall be implemented that enforces the Organization's password policies on construction, changes, re-use, lockout, etc.

17.5 Administrative Password Guidelines: As a general rule, administrative (also known as "root") access to systems shall be limited to only those who have a legitimate business need for this type of access. Any administrative access to network devices shall be logged. Administrators should have a secondary account for non-administrative functions with limited rights and privileges.

17.6 Logging: Logs contained on application servers, network devices, and critical systems may all contain different data, but all contain valuable information that the Organization shall record. Thus, the Organization requires that logging on network-level devices shall be enabled to the fullest degree possible. Passwords shall not be contained in the logs. Logs should be reviewed on a regular basis to review for malicious activity.

17.7 Audit Trails: Audit trails are typically chronological and designed to allow for the reconstruction and examination of the activities surrounding network and system events and with documented and clear written communication to the appropriate personnel responsible.

17.8 Audit Trail Process: The Organization shall establish a process for linking all access to system components, particularly access done with administrative privileges, back to individual users, evaluation of existing infrastructure and if insufficient, invest in and implement the necessary tools to accomplish the required tasks

17.9 Audit trails shall be retained for based on business or compliance requirements.

17.10 What to Record: The Organization shall record at least the user identification, event type, date and time of event, origination and success or failure indicator and identity or name of affected data, system component and resources for all system components to provide detail of the potential compromise for quick identification to investigate the situation.

17.11 Security of Audit Trails: An attacker will often try to erase records of what he or she changed on a system. For that reason, the Organization shall secure audit trails such that they cannot be altered.

17.12 Configuration: The following statements apply to the Organization's implementation of firewall technology:

- A firewall or firewalls shall be configured by default to block inbound access to the network from external sources.
- Firewall rules shall be as restrictive as possible while still providing the necessary access required for business operations.
- Firewalls shall provide secure administrative access (through the use of strong encryption) with management access limited to only networks where management connections would be expected to originate.
- No unnecessary services or applications can be enabled on firewalls. The Organization shall use 'hardened' systems for firewall platforms or use pre-hardened appliances.
- Firewall rule sets shall be documented and audited every six months. Documentation shall include details of each rule, including business justification for all services and protocols allowed. Documentation of any protocols considered to be insecure shall include a description of the security features implemented to mitigate risk to acceptable levels. Audits shall cover each rule, what it is for, if it is still necessary, and if it can be implemented more securely. All documentation shall be approved and maintained by the IT Person.

17.13 Outbound Traffic Filtering: Firewalls shall be configured to block inbound and outbound or "egress traffic filtering" connections from external sources letting outbound connections from the network, security can be greatly improved. By specifying exactly what outbound traffic to allow, all other outbound traffic is blocked

17.14 Networking Hardware: Networking hardware, such as routers, switches, bridges, and access points, shall be implemented in a consistent manner.

17.15 Network Servers: Servers typically accept connections from a number of sources, both internal and external, access should be determined based on business need and use case.

- Only services, daemons, protocols, scripts, drivers, and features necessary for the system to perform the intended business functions are to be enabled on any system. All other services,

daemons, protocols, scripts, drivers and features shall be disabled. If possible, follow a server-hardening guide consistent with industry best practices.

- Network servers, even those meant to accept public connections, shall be protected by a firewall or access control list.
- Implement only one primary function per server. This will ensure that applications with different security levels do not exist on the same server.
- A standard installation hardening system security parameter process shall be developed for the Organization's network servers. This will provide consistency across servers no matter what employee or contractor handles the installation.

17.16 Security Review: The Organization shall periodically review its network, infrastructure, and security processes to ensure that the deployed controls and personnel are capable of performing the required tasks, network architecture and data flow diagrams are kept current. and is able to accomplish security goals. Pay particular attention to the extent that each area is covered by data protection regulations.

17.17 Security Testing: The goal of this testing is to review all security controls and determine their efficacy at meeting the Organization's security needs, as well as fulfilling applicable regulations. Security testing Should occur on a regular basis and should include all relevant stakeholders. The organization shall review the results and mitigate and identified security or compliance issues. Testing can be conducted by internal or external teams depending on the skills and experience needed. Testing should include vulnerability testing to ensure all systems are within an acceptable score in relation to the Common Vulnerability Scoring System (CVSS)

17.18 Antivirus/Anti-Malware: The Organization needs to ensure the use and updating of antivirus/anti- malware software on all computer devices.

17.19 Operating System Security: All operating Systems should be updated with the most current Security and Critical Updates. Policy should be put in place to automatically apply critical security patches.

17.20 Software Use Policy: The company should consider setting up standards and guidelines for software use taking into about any required license agreements. Security testing should include the testing of software for vulnerabilities and misconfigurations.

17.21 Change Management: The Organization shall document hardware and/or configuration changes to software configuration or devices in a "change log". Changes should be discussed with relevant stakeholders to discuss the reasons, risk and rollback strategies for potential changes.

17.22 Security Policy Management: Security strategy shall be documented and maintained to be effective, particularly in the event of a security incident. Therefore, the Organization shall continually implement and review its policies, processes, and procedures to ensure efficacy and compliance with applicable regulations. The specific requirements:

18. Encryption Policy

18.1 Applicability of Encryption: Employ encryption can for sensitive data and implement encryption and decryption procedures to the fullest extent possible. Guidelines herein should be viewed as the minimum acceptable requirements. Since many policies contain requirements pertaining to encryption, this section summarizes those requirements from other policies:

18.2 Remote Access: The Organization requires that remote access to the network be secured

with strong encryption for both users and administrators. Encryption shall be initiated prior to the administrative password being changed.

18.3 Mobile Devices: Mobile devices, such as laptops, mobile computers, removable storage media, and tablets, shall, at a minimum, use an encrypted partition to store Organization data. Whole disk encryption should be considered if the data on the device is especially sensitive.

18.4 Email and Instant Messaging: Confidential information shall never be sent via email or any other end-user messaging technologies without the use of strong encryption, regardless of recipient. Sensitive data shall never be sent via end-user messaging, regardless of encryption.

18.5 Backups: Confidential data shall be stored in encrypted form using industry-standard strong encryption algorithms to protect the Organization against data loss.

18.6 Authentication: Authentication credentials shall be encrypted during transmission across any network, whether the transmission occurs internal to the Organization network or across a public network such as the Internet.

18.7 Site-to-site VPNs: Site-to-site VPNs shall utilize strong encryption to protect data during transmission. Encryption algorithms shall meet or exceed current minimum industry standards.

18.8 Confidential Data: Strong encryption shall be used for confidential data transmitted external to the Organization (where such transmission is absolutely necessary for business operations). Confidential data shall always be stored in encrypted form.

18.9 Only the strongest encryption algorithms shall be used to secure this data during transmission and update as needed.

18.10 Firewall Configuration: Firewalls shall provide secure administrative access (through the use of strong encryption) with management access limited to only networks where management connections would be expected to originate.

18.11 Network Hardware: Networking hardware shall provide secure administrative access (through the use of strong encryption) with management access limited, if possible, to only networks where management connections would be expected to originate.

18.12 Encryption Key Management: The use of technologies like key management or vaults should be utilized to help secure and manage encryption keys.

- For secure key storage the Organization shall use split knowledge or dual control (for example, requiring two or three people each knowing only their key component, to reconstruct the whole key). Any person responsible for an encryption key, in whole or in part, shall formally acknowledge and commit to their responsibilities as a key custodian.
- Cryptographic keys shall be changed when they have reached the end of their crypto period – which is typically a set period of time or after a certain amount of encryption has been performed – or quarterly, whichever time frame is shorter. The Organization shall follow relevant guidelines from the application vendor or industry best practices for key expiration.
- The selected technology shall prevent the unauthorized substitution of encryption keys.

18.13 Acceptable Encryption Algorithms: The Organization shall only use “strong encryption” when implementing encryption. Strong encryption is that which is based on industry-tested and accepted algorithms, along with strong key lengths and proper key-management practices. Acceptable algorithms should be reevaluated as encryption technology changes.

18.14 Legal Use: Some governments have regulations applying to the use and import/export of encryption technology. The Organization shall conform with encryption regulations of the local

or applicable government. The Organization specifically forbids the use of encryption to hide illegal, immoral, or unethical acts. Anyone doing so is in violation of this policy and will face immediate consequences per the Enforcement section of this document.

19. Physical Security Policy

19.1 Physical Risk Assessment: When possible, thought should be given to selecting a site for IT Operations that is secure and free of unnecessary environmental challenges.
After the assessment, the Organization shall assign a risk rating to each vulnerability and rank them by degree of potential impact and the risk of each occurrence. The Organization shall identify and perform corrective and mitigating activities (to the extent possible). Assign and document responsibility to certain individuals for corrective actions. Test and review security controls after mitigation activities.

19.2 Access control: The Organization shall keep and maintain records of any work done to the physical access controls, including: locks, keys, keypads, doors, walls, etc. The Organization shall review physical security after any repairs or work is performed that may affect any items identified, or that may introduce new risks. An assessment should be performed annually, or after any changes, and the findings documented. Correct and re-assess as needed.

19.3 Physical System Security: In addition to protecting the data on the Organization's information technology assets, this policy provides the guidelines below on keeping the systems themselves secure from damage or theft.

19.4 Minimizing Risk of Loss and Theft: Secure electronic and physical media from unneeded exposure and unsecured public access.