Wasabi Security Policies and Procedures

Table of Contents

Table of Contents

APPLICABLE TO

SECURITY OVERSIGHT
  Security Officer Responsibilities
  Workforce Training
  Supervision of Workforce
  Investigation

SECURITY AWARENESS TRAINING
  General Security Awareness Training
  Initial Security Awareness Training
  Annual Security Awareness Training
  Security Awareness Training for Wasabi Technologies Sub Contractors

NETWORK SECURITY POLICY
  VPN Connections
  Permanent Connections
  Emphasis on Security for Subcontractors

SECURITY INCIDENT RESPONSE POLICY

ENCRYPTION POLICIES AND PROCEDURES
  Data Storage
  Data Transfers
  Access and Use Monitoring
Security Assessments and Audits
Network and Physical Security Requirements
  Basic Security Requirements
  Encryption
  Return or Destruction of Data upon Termination
  Wasabi Encryption Key Management

MEDIA POLICY
  Rules governing the use of transportable media

INFORMATION SYSTEM ACTIVITY REVIEW

REMOVABLE MEDIA POLICY
  General Safeguards
  Workforce Member-Supplied Removable Media
  Company-Supplied Removable Media
  Education/Training

INFORMATION SYSTEM ACTIVITY REVIEW POLICY

RECORD RETENTION AND DESTRUCTION
  Administration
  Suspension of Record Disposal In Event of Litigation or Claims

REMOTE ACCESS POLICY
  Gaining Remote Access
  Equipment, Software, and Hardware
  Security and Privacy
  Enforcement

BREACH NOTIFICATION POLICY
  Discovery of Breach
  Breach Investigation
  Risk Assessment
  Timeliness of Notification
  Delay of Notification Authorized for Law Enforcement Purposes
  Content of the Notice
  Methods of Notification
  Maintenance of Breach Information/Log
  Business Associate Responsibilities
  Workforce Training
  Complaints
  Sanctions
Retaliation/Waiver

DATA MANAGEMENT AND BACKUP
- Data Backup
- Destruction
- Media Movement
- Sanctions

FACILITY ACCESS
- Security of Restricted Areas
- Identification of Persons at Wasabi Technologies
- Persons Allowed in Restricted Areas
- Persons Allowed in Unrestricted Areas
- Enforcement
- Workstation Security
- System/Application Access Control

RISK MANAGEMENT
Risk Assessment
- Step 1. System Characterization
- Step 2. Threat Identification
- Step 3. Vulnerability Identification
- Step 4. Control Analysis
- Step 5. Likelihood Determination
- Step 6. Impact Analysis
- Step 7. Risk Determination
- Step 8. Control Recommendations
- Step 9. Results Documentation
Risk Mitigation
- Step 1. Prioritize Actions
- Step 2. Evaluate Recommended Control Options
- Step 3. Conduct Cost-Benefit Analysis
- Step 4. Select Control(s)
- Step 5. Assign Responsibility
- Step 6. Develop Safeguard Implementation Plan
- Step 7. Implement Selected Controls

BUSINESS CONTINUITY
- Administration of Contingency Plan
Disaster Recovery Team Contact Information
Disaster Recovery Site
Recovery Center/Alternative Site
Prioritized List of Components of System
Current Inventory List
Contact Lists
Contacts for Replacement Hardware/Equipment

Plan Maintenance
  Testing
  Maintenance and Revision
  Responsibility
  Staff Education and Training

SYSTEM ACCESS
  Access Establishment and Modification
  Workforce Clearance Procedures
  Access Authorization
  Person or Entity Authentication
  Unique User Identification
  Password Management
  Automatic Logoff
  Workstation Use
  Workstation Security
  Termination Procedures

DEVICE, MEDIA, AND PAPER RECORD SANITIZATION FOR DISPOSAL OR REUSE

APPLICABLE TO

All workforce members/staff, departments, contractors and business partners of Wasabi Technologies must adhere to the Wasabi Policies and Procedures.

Violation of this policy and its procedures by workforce members may result in corrective disciplinary action, up to and including termination of employment. Violation of this policy and its procedures by others, including providers, providers' offices, business associates and partners may result in termination of the relationship and/or associated privileges. Violation may also result in civil and criminal penalties as determined by federal and state laws and regulations.
SECURITY OVERSIGHT

Security Officer Responsibilities

The Security Officer, in collaboration with the Privacy Officer, is responsible for facilitating the development, implementation, and oversight of all activities pertaining to Wasabi Technologies’ efforts to be compliant with the HIPAA Security Regulations. The intent of all oversight activities includes those necessary to maintain the confidentiality, integrity, and availability of ePHI. These responsibilities are included in the Security Officer’s job description and include, but are not limited to the following:

1. Oversees and enforces all activities necessary to comply with the Security rule and verifies the activities are in alignment with the requirements.
2. Policies and procedures
   a. Establishes, updates, and maintains written policies and procedures to comply with the Security rule.
   b. Retains them for six years from the date of creation or date it was last in effect, whichever is later.
   c. Provides copies of the policies and procedures to management, and has them available to review by all other workforce members to which they apply.
3. Periodically and as necessary, reviews and updates documentation to respond to environmental or operational changes affecting the security of ePHI.
4. Facilitates audits to validate Security compliance efforts throughout the organization.
5. Documents all activities and assessments completed to comply with the Security rule and maintain it for six years from the date of creation or date it was last in effect, whichever is later.
6. Implements procedures for the authorization and/or supervision of workforce members who work with ePHI or in locations where it may be accessed.
7. Maintains a program promoting workforce members to report non-compliance with established Security rule policies and procedures.
   a. Promptly, properly, and consistently investigates and addresses reported violations and takes steps to prevent recurrence.
   b. Work with Human Resources to apply consistent and appropriate sanctions against workforce members who fail to comply with the security policies and procedures of Wasabi Technologies.
   c. Mitigates to the extent practicable, any harmful effect known to Wasabi Technologies of a use or disclosure of ePHI in violation of Wasabi Technologies’ and/or a business associate’s policies and procedures.
8. Reports security efforts and incidents to administration in a timely manner.
9. Assists in the administration and oversight of business associates and agreements in place with them.
Workforce Training

1. Office workforce training must take place upon initial hiring for each employee, annually, and when there are changes to job function of an individual or policy and procedure changes.

2. Training is mandatory for all workforce members.

3. The Security Officer or designee maintains documentation of the training session materials and attendees for a minimum of six years.

4. The training session focuses on, but is not limited to, the following subjects defined in Wasabi Technologies' security policies and procedures:
   a. Wasabi Technologies will monitor access and activities of all workforce members and will address any discrepancies.
   b. Workstations may only be used to perform assigned job responsibilities.
   c. Workforce members may not download software onto Wasabi Technologies' workstations and/or systems without prior approval from the Security Officer or designee.
   d. Workforce members are required to report malicious software to the Security Officer or designee immediately.
   e. Workforce members are required to report unauthorized attempts, uses of, and theft of Wasabi Technologies' systems and/or workstations.
   f. Workforce members are required to report unauthorized access to facilities.
   g. No workforce member may alter ePHI maintained in any system, even if they have the technical ability to do so without specific authorization.
   h. Workforce members will understand that they are responsible for the security of any portable devices that they use. The level of encryption and security must correspond to the most sensitive information stored on the device. Loss or theft must be reported immediately.
   i. Workforce members are required to understand their role in Wasabi Technologies' contingency plan.
   j. Workforce members may not share their usernames nor passwords with anyone.
   k. Workforce member's systems must be designed to require password change and complexity. Workforce members will be trained concerning these requirements.
   l. Workforce members must set all applications that contain or transmit ePHI to automatically log off after “X” minutes of inactivity.
   m. Supervisors are required to report terminations of workforce members and other outside workforce members.
   n. Supervisors are required to report a change in a workforce member’s title, role, department, and/or location.
   o. Workforce members are required to follow procedures to re-use or dispose of any portable media containing ePHI.
   p. The Security Officer facilitates the timely communication of security updates and reminders to all workforce members to which it pertains. Examples of security updates and reminders include, but are not limited to:
   q. Latest malicious software or virus alerts
   r. Wasabi Technologies' requirement to report unauthorized attempts to access ePHI
   s. Changes in creating or changing passwords
5. Additional training is provided to workforce members in the information services department. This training is specific in nature, as to Wasabi Technologies' requirements for their involvement including, but are not limited to:
   a. Data backup plans
   b. System auditing procedures
   c. Redundancy procedures
   d. Contingency plans
   e. Virus protection
   f. Patch management
   g. Media Disposal and/or Re-use
   h. Incidence response
   i. Documentation requirements

Supervision of Workforce

Although the Security Officer is responsible for implementing and overseeing all activities related to compliance to the Security rule, it is the responsibility of all leaders (i.e. team leaders, supervisors, managers, directors, senior leaders, etc.) to supervise all workforce members, including third party vendors, contractors or other users of Wasabi Technologies' systems, applications, servers, workstations, etc. that contain ePHI.

1. Leaders monitor workstations and applications for unauthorized use, tampering, and theft and report non-compliance according to Wasabi Technologies' Security Incident Response policy.
2. Leaders assist the Security Officer to ensure appropriate role-based access is provided to all workforce members.
3. Leaders take all reasonable steps to hire, retain, and promote workforce members and provide access to workforce members who comply with the Security regulation and Wasabi Technologies' security policies and procedures.

Investigation

All workforce members and any others with system access report non-compliance of Wasabi Technologies' policies and procedures to the Security or Compliance Officer or other individual as assigned Officer. Individuals that report violations in good faith may not be subjected to intimidation, threats, coercion, discrimination against, or any other retaliatory action as a consequence.

1. The Security Officer promptly facilitates a thorough investigation of all reported violations of Wasabi Technologies' security policies and procedures. The Security Officer may request the assistance from others such as the workforce member's leader, other workforce members, and/or other vendor/contractors as needed.
   a. Complete an audit trail/log to identify and verify the violation and sequence of events.
   b. Interview any individual that may be aware of or involved in the incident.
   c. All individuals are required to cooperate with the investigation process and provide factual information to those conducting the investigation.
d. Provide individuals suspected of non-compliance of the Security rule and/or Wasabi Technologies’ policies and procedures the opportunity to explain their actions to determine whether it was an unintentional or malicious deviation from established policies and procedures.

e. The designated investigators thoroughly document the investigation in a timely manner. The Security Officer facilitates taking appropriate steps to prevent recurrence of the violation (when possible and feasible).

2. Violation of any security policy or procedure by workforce members may result in corrective disciplinary action, up to and including termination of employment. Violation of this policy and procedures by others, including providers, providers’ offices, business associates and partners may result in termination of the relationship and/or associated privileges. Violation may also result in civil and criminal penalties as determined by federal and state laws and regulations. Refer to Wasabi Technologies’ Sanctions Policy.

3. The Security Officer maintains all documentation of the investigation, sanctions provided, and actions taken to prevent reoccurrence for a minimum of six years after the conclusion of the investigation.

SECURITY AWARENESS TRAINING

General Security Awareness Training

1. The Wasabi Technologies workforce shall receive general security awareness training needed to support Wasabi Technologies security policies and procedures in the course of their normal work. This mandatory, general training may be web-based, and consists of Initial Security Awareness Training and Annual Security Awareness Training.

Initial Security Awareness Training

Newly hired Wasabi Technologies employees and contractors must complete security awareness training as part of their orientation and as a condition of being network access.

Annual Security Awareness Training

All users must complete security awareness training annually. Security Awareness Training must include the following:

1. Acceptable and correct use of information resources
2. How to report an information security incident
3. HIPAA security and privacy requirements
4. General handling of data
5. End User Acceptable Use Policy
6. How to react in case of information security incident
   a. The respective Wasabi Technologies Security Officer shall ensure that their staff and contractors receive training in security awareness and accepted security practices annually and when required by system changes.
   b. The respective Wasabi Technologies Security Officer shall maintain records of the annual security awareness training participation of their staff and contractors.
c. Training content must be refreshed/reviewed annually.
d. Training records shall be maintained to having received the security and awareness training either in writing or electronically as part of the training course completion.
e. Users are required to undergo Security Awareness training after a major system change.

Security Awareness Training for Wasabi Technologies Sub Contractors

1. Wasabi Technologies sub contractors shall conduct initial (for new hires) and annual security awareness training for all staff. This training shall discuss, at a minimum, the requirements listed above.
2. Wasabi Technologies sub contractors shall contact their respective Security Officer to obtain the current security awareness training materials provided to Wasabi Technologies employees and contractors.
   a. Security Officer shall: (a) ensure that all business partner staff complete initial and annual security awareness training, (b) maintain security awareness training records for all business partner staff.

NETWORK SECURITY POLICY

VPN Connections

1. Access to information resources through the internet shall be subject to authorization and authentication by a VPN with an access control system. Direct access without passing through the access control system is prohibited.
2. Systems that allow public access to host computers, including mission-critical servers, warrants additional security at the operating system and application levels. Such systems shall have the capability to monitor activity levels to ensure that public usage does not unacceptably degrade system responsiveness.

Permanent Connections

The security of company systems can be jeopardized from third party locations if security company and resources are inadequate. When there is a need to connect to a third party location, a risk analysis should be conducted. The risk analysis should consider the type of access required, the value of the information, the security measures employed by the third party, and the implications for the security of company systems. The Security Officer or appropriate personnel should be involved in the process, design and approval.

Emphasis on Security for Subcontractors

1. Access to company computer systems or corporate networks should not be granted until a review of the following concerns have been made, and appropriate restrictions or covenants included in a statement of work (“SOW”) with the party requesting access.
a. Applicable sections of the company Information Security Policy have been reviewed and considered.
b. Policies and standards established in the company information security program have been enforced.
c. A risk assessment of the additional liabilities that will attach to each of the parties to the agreement.
d. The right to audit contractual responsibilities should be included in the agreement or SOW.
e. Arrangements for reporting and investigating security incidents must be included in the agreement in order to meet the covenants of the HIPAA Business Associate Agreement.
f. A description of each service to be made available.
g. Each service, access, account, and/or permission made available should only be the minimum necessary for the third party to perform their contractual obligations.
h. A detailed list of users that have access to company computer systems must be maintained and auditable.
i. If required under the contract, permission should be sought to screen authorized users.
j. Dates and times when the service is to be available should be agreed upon in advance.
k. Procedures regarding protection of information resources should be agreed upon in advance and a method of audit and enforcement implemented and approved by both parties.
l. The right to monitor and revoke user activity should be included in each agreement.
m. Language on restrictions on copying and disclosing information should be included in all agreements.
n. Responsibilities regarding hardware and software installation and maintenance should be understood and agreement upon in advance.
o. Measures to ensure the return or destruction of programs and information at the end of the contract should be written into the agreement.
p. If physical protection measures are necessary because of contract stipulations, these should be included in the agreement.
q. A formal method to grant and authorized users who will access to the data collected under the agreement should be formally established before any users are granted access.
r. Mechanisms should be in place to ensure that security measures are being followed by all parties to the agreement.
s. Because annual confidentiality training is required under the HIPAA regulation, a formal procedure should be established to ensure that the training takes place, that there is a method to determine who must take the training, who will administer the training, and the process to determine the content of the training established.
t. A detailed list of the security measures which will be undertaken by all parties to the agreement should be published in advance of the agreement.
SECURITY INCIDENT RESPONSE POLICY

1. Immediately upon observation workforce members must report suspected and known precursors, events, indications, and security incidents to management, the Security Officer or the Privacy Officer.
2. Once an incident is verified, Wasabi Technologies' engineering department will attempt to immediately limit the scope and magnitude of the security incident as well as determine symptoms and cause related to the affected system(s).
3. The technical team will then determine if the affected system(s) have been changed in any way.
   a. If they have, the technical team restores the system to its proper, intended functioning (“last known good”).
      i. Once restored, the team validates that the system functions the way it was intended/had functioned in the past. This may require the involvement of the business unit that owns the affected system(s).
      ii. If operation of the system(s) had been interrupted (i.e., the system(s) had been taken offline or dropped from the network while triaged), restart the restored and validated system(s) and monitor for behavior.
   b. If the system had not been changed in any way, but was taken offline (i.e., operations had been interrupted), restart the system and monitor for proper behavior.
4. Following the remediation of the incident, the team will document the security incident response.
5. The team will maintain all documentation surrounding every security incident, to include all work papers, notes, incident response forms, meeting minutes and other items relevant to the investigation in a secure location for a period of six (6) years.

ENCRYPTION POLICIES AND PROCEDURES

Data Storage
Wasabi stores user Content on secure computers located in a physically secure and controlled data center environment. Wasabi employs technologies that are consistent with industry standards for firewalls and other security technologies to prevent Wasabi computers from being accessed by unauthorized persons. All data is encrypted at rest with AES-256 bit encryption keys.

Data Transfers
Wasabi uses HTTPS standards to protect data integrity during transfers. In addition, Wasabi will maintain at least the following security measures:
   1. HTTP with SSL 256-bit encryption (HTTPS); and
   2. encrypted passwords for the Services.
Access and Use Monitoring

Wasabi will monitor Wasabi’s user access to and use of the Services for security, performance evaluation, and system utilization purposes.

Security Assessments and Audits

If requested by user, Wasabi will cooperate with user in an initial security assessment. In addition, Wasabi will provide user with SSAE16 Reviews from the third party data center providers utilized in the provision of the Services.

Network and Physical Security Requirements

Basic Security Requirements
Subject to the section above, Wasabi will:
1. maintain a working, tuned network firewall to protect user content;
2. regularly install security patches on the services network;
3. ensure authentication to the Service’s network web front-end is encrypted;
4. where applicable, use and regularly update anti-malware prevention tools;
5. maintain a credential management process which includes assigning a unique ID to each person with computer access;
6. track access to systems, generate and store audit trail and logs to help identify malicious activity;
7. regularly test efficiency and health of security controls, systems and processes;
8. maintain a policy that addresses information security for employees and representatives;
9. restrict physical access to systems containing user Content;
10. restrict remote access to the network / devices and employ secure remote access controls to verify the identity of users connecting; and
11. protect backups from unauthorized access during transit and storage.

Encryption

Wasabi will use cryptographic algorithms that have been published and evaluated by the general cryptographic community with sufficient strength to equate to 256-bit or better.

Return or Destruction of Data upon Termination

1. Wasabi will maintain a documented process that provides for the security and return or destruction of all user Content, including copies stored on backup media, in the event the Agreement is terminated.
2. Notwithstanding the foregoing, with respect to copies of any of the user Content retained by Wasabi that are not easily accessible, Wasabi will continue to maintain such Content on such back-up data or other media subject to the restrictions of the Agreement.
3. In addition, such Content will be destroyed or overwritten by Wasabi in the ordinary course of business for such records.

Wasabi Encryption Key Management
1. Wasabi uses an AES-256 bit symmetric key algorithm to generate the user encryption key.
2. This key is generated per Wasabi domain.
3. This key is generated at the time the user is created.
4. This key is unique to each Wasabi user.
5. This key is stored in a secure key vault

MEDIA POLICY

Rules governing the use of transportable media
1. Data may be exchanged between company workstations/networks and workstations used within the company. The very nature of data exchange requires that under certain situations data be exchanged in this manner.
2. It is permissible to connect transferable media from other businesses or individuals into company networks provided that they have been evaluated to be secure by the DevOps team.
3. No sensitive data should ever be stored on transportable media unless the data is maintained in an encrypted format.
4. When no longer in productive use, all company laptops, workstation, or servers must be wiped of data in a manner which conforms to HIPAA regulations.
   a. All transportable media must be wiped according to the same standards.
   b. For more information refer to the media sanitization policy

INFORMATION SYSTEM ACTIVITY REVIEW
1. The Security Officer shall be responsible for conducting reviews of company’s 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.
2. The Security Officer shall develop a report format to capture the review findings. Such report shall include the reviewer’s name, date and time of performance, and significant findings describing events requiring additional action (e.g., additional investigation, employee training and/or discipline, program adjustments, modifications to safeguards). To the extent possible, such report shall be in a checklist format.
3. Such reviews shall be conducted annually. Audits also shall be conducted if company has reason to suspect wrongdoing. In conducting these reviews, the Information
Technology Services shall examine audit logs for security-significant events including, but not limited to, the following:

a. Logins – Scan successful and unsuccessful login attempts. Identify multiple failed login attempts, account lockouts, and unauthorized access.
b. File accesses – Scan successful and unsuccessful file access attempts. Identify multiple failed access attempts, unauthorized access, and unauthorized file creation, modification, or deletion.
c. Security incidents – Examine records from security devices or system audit logs for events that constitute system compromises, unsuccessful compromise attempts, malicious logic (e.g., viruses, worms), denial of service, or scanning/probing incidents.
d. User Accounts – Review of user accounts within all systems to ensure users that no longer have a business need for information systems no longer have such access to the information and/or system.

4. The Security Officer shall be responsible for maintaining reports.

a. The Security Officer shall consider such reports and recommendations in determining whether to make changes to company’s administrative, physical, and technical safeguards.
b. In the event a security incident is detected through such auditing, such matter shall be addressed pursuant to the breach notification policy.

REMOVABLE MEDIA POLICY

General Safeguards

All Removable Media that create, receive, maintain, or transmit ePHI must comply with the following requirements, regardless of whether the Removable Media is company-supplied or Workforce Member-supplied:

1. Workforce Members shall not access, create, receive, maintain, or transmit ePHI on Removable Media unless:
   a. It is permitted by Wasabi Technologies’ “Remote Access Policy” It is necessary for business purposes;
   b. The Workforce Member has obtained authorization; and
   c. Encryption software is employed for storage and transmission of such ePHI.
2. Removable Media must be appropriately secured when not in use. Appropriate security shall include, but is not limited to, physical security, in accordance with Wasabi Technologies’ Facility Access Policy (described in this document), as applicable, or others methods as determined by Wasabi Technologies
3. Maintain a current and up-to-date anti-malware solution where technically feasible.
4. ePHI stored on Removable Media shall be sanitized, disposed of, or destroyed, as applicable, in the circumstances outlined in, and in accordance with, Wasabi Technologies’ policies and procedures. See “Device, Media, and Paper Record Sanitization for Disposal or Reuse” policy and procedure (described in this document).
5. Removable Media must not be left unattended, or if necessary, must be physically locked away, or secured and hidden from view.
6. Employees must promptly report the loss or theft, or suspected loss, theft, or cyber threat or any other potential breach of any Removable Media on which ePHI is stored to the Wasabi Technologies' Privacy Officer and Security Officer. Failure to report to do so may result in disciplinary action. A “remote Sanitization” should be performed or the device or media should be otherwise rendered inoperable, if possible. If stolen, local law enforcement can be notified and a police report obtained in accordance with Wasabi Technologies’ breach notification policy.
7. The same levels of confidentiality that exist for hard copy PHI, business, and proprietary information apply to ePHI and are extended even after termination or other conclusion of access.
8. ePHI maintained on Removable Media shall not be moved to another device or media only in accordance with Wasabi Technologies' policies and procedures.
9. Wasabi Technologies reserves the right to block, filter, prohibit, or limit access to Removable Media, resources, or content if the Removable Media does not meet the minimum security and technology requirements, or if there are any other concerns about the use of such Removable Media.

Workforce Member-Supplied Removable Media

Workforce Members using their Workforce Member-supplied Removable Media must comply with the following requirements:

1. Workforce Members may only use their Workforce Member-supplied Removable Media to access ePHI upon approval by Wasabi Technologies, and only in the manner specified by Wasabi Technologies.
2. Workforce Members shall follow all security guidelines, and implement any prescribed security controls when using Workforce Member-supplied Removable Media, as required by Wasabi Technologies. Such safeguards shall be substantially similar to those required by company-supplied Removable Media Devices.
3. Workforce Members are responsible for ensuring that their Removable Media are protected from theft, destruction, or unauthorized use and disclosure, and to protect the confidentiality, integrity and accessibility of ePHI.
4. Personal applications and/or software used on the Workforce Member’s Removable Media may not be used to access ePHI, unless approved by Wasabi Technologies.
5. When a Workforce Member will no longer be using his/her Workforce Member-supplied Removable Media, Workforce Member shall Sanitize the Removable Media following the security measures outlined in the Wasabi Technologies' Sanitization policy and procedure. Workforce Member shall not sell, trade-in, give away, or throw away his/her Removable Media without Sanitizing the Removable Media.
6. In addition to other potential sanctions, Workforce Members who violate this policy or other HIPAA policy may have their access to ePHI through their Workforce Member-supplied Removable Media revoked.

Company-Supplied Removable Media

In addition to the general safeguards outlined in Section 1, company-supplied Removable Media must comply with the following requirements:
1. Wasabi Technologies determines which Workforce Members shall have access to company-supplied Removable Media and how such Removable Media may be used.  
2. Wasabi Technologies has established appropriate safeguards and minimum standards for the protection of ePHI on company-supplied Removable Media.  
3. In addition to other potential sanctions, Workforce Members who violate this policy or other HIPAA policy may have their company-supplied Removable Media confiscated and may have their ability to access to PHI through Removable Media revoked.  
4. Wasabi Technologies has the authority to Sanitize any company-supplied Removable Media which may include erasure of personal information.

Education/Training  
1. Wasabi Technologies shall train Workforce Members on appropriate use of Removable Media, compliance with the Privacy Rule and Security Rule, and the risks associated with Portable Handheld Devices, such as theft, loss, vulnerabilities, and cyber threats inherent in the use of Removable Media.  
2. Wasabi Technologies shall inform Workforce Members when there are updates or new versions of Removable Media are available and shall ensure appropriate implementation of such changes.

INFORMATION SYSTEM ACTIVITY REVIEW POLICY  
1. The Security Officer shall be responsible for conducting reviews of company’s 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.  
2. The Security Officer shall develop a report format to capture the review findings. Such report shall include the reviewer’s name, date and time of performance, and significant findings describing events requiring additional action (e.g., additional investigation, employee training and/or discipline, program adjustments, modifications to safeguards). To the extent possible, such report shall be in a checklist format.  
3. Such reviews shall be conducted annually. Audits also shall be conducted if company has reason to suspect wrongdoing. In conducting these reviews, the Information Technology Services shall examine audit logs for security-significant events including, but not limited to, the following:  
   a. Logins – Scan successful and unsuccessful login attempts. Identify multiple failed login attempts, account lockouts, and unauthorized access.  
   b. File accesses – Scan successful and unsuccessful file access attempts. Identify multiple failed access attempts, unauthorized access, and unauthorized file creation, modification, or deletion.  
   c. Security incidents – Examine records from security devices or system audit logs for events that constitute system compromises, unsuccessful compromise
attempts, malicious logic (e.g., viruses, worms), denial of service, or scanning/probing incidents.

d. User Accounts – Review of user accounts within all systems to ensure users that no longer have a business need for information systems no longer have such access to the information and/or system.

4. The Security Officer shall be responsible for maintaining reports.
   a. The Security Officer shall consider such reports and recommendations in determining whether to make changes to company’s administrative, physical, and technical safeguards.
   b. In the event a security incident is detected through such auditing, such matter shall be addressed pursuant to the breach notification policy

RECORD RETENTION AND DESTRUCTION

Administration

1. The Security Officer is the officer in charge of the administration of this Policy and the implementation of processes and procedures to ensure that the Record Retention Schedule is followed.

2. The Security Officer is also authorized to:
   a. make modifications to the Record Retention Schedule from time to time to ensure:
      i. It is in compliance with local, state and federal laws
      ii. It includes the appropriate document and record categories for Wasabi Technologies
   b. monitor local, state and federal laws affecting record retention; annually review the record retention and disposal program; and monitor compliance with this Policy.

Suspension of Record Disposal In Event of Litigation or Claims

In the event Wasabi Technologies is served with any subpoena or request for documents or any employee becomes aware of a governmental investigation or audit concerning Wasabi Technologies or the commencement of any litigation against or concerning Wasabi Technologies, such employee shall inform the Administrator and any further disposal of documents shall be suspended until shall time as the Administrator, with the advice of counsel, determines otherwise. The Administrator shall take such steps as is necessary to promptly inform all staff of any suspension in the further disposal of documents.
REMOTE ACCESS POLICY

Gaining Remote Access

1. Workforce members shall apply for remote access connections by completing a “System Access Request” form (refer to the System Access Policy). Remote access is strictly controlled and made available only to workforce members with a defined business need, at the discretion of the workforce member's manager, and with approval by the Security Officer or designee.

2. Workforce member is responsible for adhering to all of Wasabi Technologies' policies and procedures, not engaging in illegal activities, and not using remote access for interests other than those for Wasabi Technologies.

3. Business associates, contractors, and vendors may be granted remote access to the network, provided they have a contract or agreement with Wasabi Technologies which clearly defines the type of remote access permitted (i.e., stand-alone host, network server, etc.) as well as other conditions which may be required, such as virus protection software. Such contractual provisions must be reviewed and approved by the Security Officer and/or legal department before remote access will be permitted. Remote access is strictly controlled and made available only to business associates and vendors with a defined business need, at the discretion of and approval by the Security Officer or designee.

4. It is the remote access user’s responsibility to ensure that the remote worksite meets security and configuration standards established by Wasabi Technologies. This includes configuration of personal routers and wireless networks.

Equipment, Software, and Hardware

1. Remote users will be allowed access through the use of equipment owned by or leased to the entity, or through the use of the workforce member’s personal computer system provided it meets the minimum standards developed by Wasabi Technologies, as indicated above. (The Organization must determine minimum standards based on FIPS 140-2 or its successor.)

2. Remote users utilizing personal equipment, software, and hardware are:
   a. Responsible for remote access. Wasabi Technologies will bear no responsibility if the installation or use of any necessary software and/or hardware causes lockups, crashes, or any type of data loss.
   b. Responsible for remote access used to connect to the network and meeting Wasabi Technologies’ requirements for remote access.
   c. Responsible for the purchase, setup, maintenance or support of any equipment not owned by or leased to Wasabi Technologies.

3. Continued service and support of Wasabi Technologies’ owned equipment is completed by engineering workforce members. Troubleshooting of telephone or broadband circuits installed is the primary responsibility of the remote access user and their Internet Service Provider. It is not the responsibility of Wasabi Technologies to work with Internet Service Providers on troubleshooting problems with telephone or broadband circuits not supplied and paid for by Wasabi Technologies.
Security and Privacy

1. Only authorized remote access users are permitted remote access to any of Wasabi Technologies’ computer systems, computer networks, and/or information, and must adhere to all of Wasabi Technologies’ policies.

2. It is the responsibility of the remote access user, including Business Associates and contractors and vendors, to log-off and disconnect from Wasabi Technologies’ network when access is no longer needed to perform job responsibilities.

3. Remote users shall lock the workstation and/or system(s) when unattended so that no other individual is able to access any ePHI or organizationally sensitive information.

4. It is the responsibility of remote access users to ensure that unauthorized individuals do not access the network. At no time will any remote access user provide (share) their user name or password to anyone, nor configure their remote access device to remember or automatically enter their username and password.

5. Remote access users must take necessary precautions to secure all of Wasabi Technologies’ equipment and proprietary information in their possession.

6. Virus Protection software is installed on all Wasabi Technologies’ computers and is set to update the virus pattern on a daily basis. This update is critical to the security of all data, and must be allowed to complete, i.e., remote users may not stop the update process for Virus Protection, on organization’s or the remote user’s workstation.

7. A firewall shall be used and may not be disabled for any reason.

8. Wasabi Technologies maintains logs of all activities performed by remote access users while connected to Wasabi Technologies’ network. System administrators review this documentation and/or use automated intrusion detection systems to detect suspicious activity.

9. Electronic Data Security
   a. Transferring data to Wasabi Technologies requires the use of an approved VPN connection to ensure the confidentiality and integrity of the data being transmitted. Users may not circumvent established procedures when transmitting data to Wasabi Technologies.

Enforcement

1. Remote access users who violate this policy are subject to sanctions and/or disciplinary actions, up to and including termination of employment or contract. Termination of access by remote users is processed in accordance with Wasabi Technologies’ termination policy.

2. Remote access violations by Business Associates and vendors may result in termination of their agreement, denial of access to the Wasabi Technologies’ network, and liability for any damage to property and equipment.
BREACH NOTIFICATION POLICY

Discovery of Breach

1. A breach of PHI shall be treated as “discovered” as of the first day on which such breach is known to the organization, or, by exercising reasonable diligence would have been known to the organization (includes breaches by the organization’s business associates).

2. The organization shall be deemed to have knowledge of a breach if such breach is known or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent (business associate) of the organization (see attachment for examples of breach of unsecured protected health information).

3. Following the discovery of a potential breach, the organization shall begin an investigation (see organizational policies for security incident response and/or risk management incident response), conduct a risk assessment, and based on the results of the risk assessment, begin the process to notify each individual whose PHI has been, or is reasonably believed to by the organization to have been, accessed, acquired, used, or disclosed as a result of the breach.

4. The organization shall also begin the process of determining what external notifications are required or should be made (e.g., Secretary of Department of Health & Human Services (HHS), media outlets, law enforcement officials, etc.).

Breach Investigation

1. The organization shall name an individual to act as the investigator of the breach (e.g., privacy officer, security officer, risk manager, etc.).

2. The investigator shall be responsible for the management of the breach investigation, completion of a risk assessment, and coordinating with others in the organization as appropriate (e.g., administration, security incident response team, human resources, risk management, public relations, legal counsel, etc.)

3. The investigator shall be the key facilitator for all breach notification processes to the appropriate entities (e.g., HHS, media, law enforcement officials, etc.).

4. All documentation related to the breach investigation, including the risk assessment, shall be retained for a minimum of six years.

Risk Assessment

For an acquisition, access, use or disclosure of PHI to constitute a breach, it must constitute a violation of the Privacy Rule. A use or disclosure of PHI that is incident to an otherwise permissible use or disclosure and occurs despite reasonable safeguards and proper minimum necessary procedures would not be a violation of the Privacy Rule and would not qualify as a potential breach. To determine if an impermissible use or disclosure of PHI constitutes a breach and requires further notification to individuals, media, or the HHS secretary under breach notification requirements, the organization will need to perform a risk assessment to determine if there is significant risk of harm to the individual as a result of the impermissible use or
disclosure. The organization shall document the risk assessment as part of the investigation in the incident report form noting the outcome of the risk assessment process. The organization has the burden of proof for demonstrating that all notifications were made as required or that the use or disclosure did not constitute a breach. Based on the outcome of the risk assessment, the organization will determine the need to move forward with breach notification. The risk assessment and the supporting documentation shall be fact specific and address:

1. Consideration of who impermissibly used or to whom the information was impermissibly disclosed.
2. The type and amount of PHI involved.
3. The potential for significant risk of financial, reputational, or other harm.

**Timeliness of Notification**

Upon determination that breach notification is required, the notice shall be made without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach by the organization involved or the business associate involved. It is the responsibility of the organization to demonstrate that all notifications were made as required, including evidence demonstrating the necessity of delay.

**Delay of Notification Authorized for Law Enforcement Purposes**

If a law enforcement official states to the organization that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, the organization shall:

1. If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting of the timer period specified by the official; or
2. If the statement is made orally, document the statement, including the identify of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described above is submitted during that time.

**Content of the Notice**

The notice shall be written in plain language and must contain the following information:

1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
2. A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved).
3. Any steps the individual should take to protect themselves from potential harm resulting from the breach.
4. A brief description of what the organization is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches.
5. Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, Web site, or postal address.
Methods of Notification

The method of notification will depend on the individuals/entities to be notified. The following methods must be utilized accordingly:

1. **Notice to Individual(s):** Notice shall be provided promptly and in the following form:
   
a. Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification shall be provided in one or more mailings as information is available. If the organization knows that the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification by first-class mail to the next of kin or person representative shall be carried out.
   
b. Substitute Notice: In the case where there is insufficient or out-of-date contact information (including a phone number, email address, etc.) that precludes direct written or electronic notification, a substitute form of notice reasonably calculated to reach the individual shall be provided. A substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative.
   
i. In a case in which there is insufficient or out-of-date contact information for fewer than 10 individuals, then the substitute notice may be provided by an alternative form of written notice, telephone, or other means.

ii. In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then the substitute notice shall be in the form of either a conspicuous posting for a period of 90 days on the home page of the organization’s website, or a conspicuous notice in a major print or broadcast media in the organization’s geographic areas where the individuals affected by the breach likely reside. The notice shall include a toll-free number that remains active or at least 90 days where an individual can learn whether his or her PHI may be included in the breach.

   c. If the organization determines that notification requires urgency because of possible imminent misuse of unsecured PHI, notification may be provided by telephone or other means, as appropriate in addition to the methods noted above.

2. **Notice to Media:** Notice shall be provided to prominent media outlets serving the state and regional area when the breach of unsecured PHI affects more than 500 patients. The Notice shall be provided in the form of a press release.

3. **Notice to Secretary of HHS:** Notice shall be provided to the Secretary of HHS as follows below. The Secretary shall make available to the public on the HHS Internet website a list identifying covered entities involved in all breaches in which the unsecured PHI of more than 500 patients is accessed, acquired, used, or disclosed.
   
a. For breaches involving 500 or more individuals, the organization shall notify the Secretary of HHS as instructed at www.hhs.gov at the same time notice is made to the individuals.

b. For breaches involving less than 500 individuals, the organization will maintain a log of the breaches and annually submit the log to the Secretary off HHS during the year involved (logged breaches occurring during the preceding calendar year...
to be submitted no later than 60 days after the end of the calendar year). Instructions for submitting the log are provided at www.hhs.gov.

Maintenance of Breach Information/Log
As described above and in addition to the reports created for each incident, the organization shall maintain a process to record or log all breaches of unsecured PHI regardless of the number of patients affected. The following information should be collected/logged for each breach (see sample Breach Notification Log):

1. A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of patients affected, if known.
2. A description of the types of unsecured protected health information that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, etc.).
3. A description of the action taken with regard to notification of patients regarding the breach.
4. Resolution steps taken to mitigate the breach and prevent future occurrences.

Business Associate Responsibilities
The business associate (BA) of the organization that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information shall, without unreasonable delay and in no case later than 60 calendar days after discovery of a breach, notify the organization of such breach. Such notice shall include the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the BA to have been, accessed, acquired, or disclosed during such breach. The BA shall provide the organization with any other available information that the organization is required to include in notification to the individual at the time of the notification or promptly thereafter as information becomes available. Upon notification by the BA of discovery of a breach, the organization will be responsible for notifying affected individuals, unless otherwise agreed upon by the BA to notify the affected individuals (note: it is still the burden of the Covered Entity to document this notification).

Workforce Training
The organization shall train all members of its workforce on the policies and procedures with respect to PHI as necessary and appropriate for the members to carry out their job responsibilities. Workforce members shall also be trained as to how to identify and report breaches within the organization.

Complaints
The organization must provide a process for individuals to make complaints concerning the organization’s patient privacy policies and procedures or its compliance with such policies and procedures. Individuals have the right to complain about the organization’s breach notification processes.
Sanctions
The organization shall have in place and apply appropriate sanctions against members of its workforce who fail to comply with privacy policies and procedures.

Retaliation/Waiver
The organization may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by the individual of any privacy right. The organization may not require individuals to waive their privacy rights under as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

DATA MANAGEMENT AND BACKUP

Data Backup
1. A backup, recovery and testing strategy should be determined based upon the Wasabi Technologies’ Risk Analysis strategy
   a. The Information/HIPAA Security Officer has oversight responsibility and will ensure that further responsibility is properly assigned for the proper management of data.
   b. The Wasabi Technologies’ Operations department is responsible for completing the backups and for ensuring effective training of the workforce members assigned to complete backups, for management of the backup media and for performing periodic testing of restored media.
   c. Wasabi Technologies will perform a daily (at a minimum) backup of all systems that create, receive, maintain, or transmit ePHI. While a vendor may specify or recommend a full backup, an incremental backup, or may not specify, the Chief Technology Officer, will determine the frequency with which back-ups are performed, dependent upon each system.
   d. Data backup systems may be manual or automated.
      i. Automated systems electronically capture back up locations, date/time, etc.
      ii. If the process is manual, documentation of the backup should include:
         1. Site/location name
         2. Name of the system
         3. Type of data
         4. Date & time of backup
         5. Where backup stored (or to whom it was provided)
         6. Signature of individual that completed the back up
2. Stored data must be accessible and retrievable at all times.
3. Proper management of situations concerning data back-up/data recovery, such as emergencies or other occurrences, should be addressed in the Wasabi Technologies’ Disaster Recovery and Business Continuity Plans.
Destruction

Wasabi Technologies will determine a record retention policy and data backup retention schedule. This schedule should include a timeline for ultimate destruction (tapes maintained and destroyed) of storage media.

Media Movement

It is not possible or economically practical to control all media that enter and leave an organization. Wasabi Technologies makes all reasonable and prudent efforts to control media entering and leaving the organization. Workforce members are trained to recognize that media containing ePHI is handled in a manner to protect the confidentiality of the data contained on it. Media that contains PHI that is no longer useful or useable should be sanitized consistent with the “Device, Media, and Paper Record Sanitization for Disposal or Reuse” policy.

Sanctions

1. Failure to backup a system in the absence of a system failure is a violation of this policy and may result in corrective disciplinary action, up to and including termination of employment.
2. Violation of this policy and its procedures by workforce members may result in corrective disciplinary action, up to and including termination of employment.
3. Violation of this policy and procedures by others, including providers, providers’ offices, business associates and partners may result in termination of the relationship and/or associated privileges.
4. Violation may also result in civil and criminal penalties to Wasabi Technologies as determined by federal and state laws and regulations related to loss of data.
5. Violation may also result in liability to Wasabi Technologies related to loss of data.

FACILITY ACCESS

Security of Restricted Areas

1. Restricted areas and facilities are locked and alarmed when unattended (where feasible).
2. Only authorized workforce members receive keys to access restricted areas (as determined by the Security Officer through Departmental requests).
   a. Workforce members are required to return the key(s) to the Human Resources department (or Supervisor) on their last day of employment/last day of contracted work or services being provided.
3. Workforce members must report a lost and/or stolen key(s) to the Security Officer.
   a. The Security Officer facilitates the changing of the lock(s) within 24 hours of a key being reported lost/stolen
Identification of Persons at Wasabi Technologies

1. All persons wear identification badges in addition to their own organization’s id badges they may have.
   a. Workforce members wear a identification badge at all times while at any Wasabi Technologies facility.
      i. Workforce members are required to return their identification badge to the Human Resources department (or Supervisor) on their last day of employment/last day of contracted work or services being provided.
   b. Visiting vendors register (sign in and out) and obtain Visitor identification badges from the department they are visiting. Vendors are instructed to return the Visitor identification badge and sign out prior to leaving the premises.

Persons Allowed in Restricted Areas

1. Workforce members as approved by their supervisor and as needed to perform their job duties.
2. Vendors (wearing a Wasabi Technologies Visitor ID badge) with a workforce member’s escort into and out of the areas.
3. Vendors at Wasabi Technologies on a long-term contract (wearing a Wasabi Technologies Visitor ID badge), once acclimated to the areas, without an escort.

Persons Allowed in Unrestricted Areas

1. Workforce members.
2. Vendors.
3. Workforce family members and friends.
4. All visitors.

Enforcement

1. Escort violators out of restricted areas immediately and either have them register and obtain a visitor ID badge or escort them to the area they are trying to get to.
2. Report violations of this policy to the restricted area’s department team leader, supervisor, manager, or director, or the Privacy Officer.
3. Workforce members in violation of this policy are subject to disciplinary action, up to and including termination.
4. Visitors in violation of this policy are subject to loss of vendor privileges and/or termination of services from Wasabi Technologies.

Workstation Security

1. Workstations may only be accessed and utilized by authorized workforce members to complete assigned job/contract responsibilities. Third parties may be authorized by the Security Officer to access systems/applications on an as needed basis.
2. All workforce members are required to monitor workstations and report unauthorized users and/or unauthorized attempts to access systems/applications as per the System Access Policy.
3. All Wasabi Technologies computer mainframes, servers, and network hardware are maintained in secured, locked, environmentally conditioned rooms with 24 hour per day monitoring devices which alert the Security Officer of any problems. Access to these rooms is limited to authorized IS and facility services workforce as required to perform job responsibilities to maintain these rooms and/or the equipment within these rooms. Access by anyone else is granted only by approval from a member of the DevOps team or the Security Officer and only with an escort by an authorized IS or facility services workforce member.

System/Application Access Control
1. All systems/applications purchased by Wasabi Technologies are the property of Wasabi Technologies and are distributed to users by the Information Systems department only.
2. Prior to downloading, all software must be registered to Wasabi Technologies and must be approved in advance by the IS department. To prevent computer viruses from being transmitted through Wasabi Technologies' information systems, there will be no unauthorized downloading of any unauthorized software.
3. The Information Systems department is responsible for downloading all upgrades, testing upgrades, and for supporting Wasabi Technologies systems/applications.

RISK MANAGEMENT

The implementation, execution, and maintenance of the information security risk analysis and risk management process is the responsibility of Wasabi Technologies’ Information Security Officer (or other designated employee), and the identified Risk Management Team.

Risk Assessment
The intent of completing a risk assessment is to determine potential threats and vulnerabilities and the likelihood and impact should they occur. The output of this process helps to identify appropriate controls for reducing or eliminating risk.

Step 1. System Characterization
1. The first step in assessing risk is to define the scope of the effort. To do this, identify where ePHI is created, received, maintained, processed, or transmitted. Using information-gathering techniques, the IT system boundaries are identified, as well as the resources and the information that constitute the system. Take into consideration policies, laws, the remote work force and telecommuters, and removable media and portable computing devices (e.g., laptops, removable media, and backup media).
2. Output – Characterization of the IT system assessed, a good picture of the IT system environment, and delineation of system boundaries.

Step 2. Threat Identification
1. In this step, potential threats (the potential for threat-sources to successfully exercise a particular vulnerability) are identified and documented. Consider all potential threat-sources through the review of historical incidents and data from intelligence
agencies, the government, etc., to help generate a list of potential threats. The list should be based on the individual organization and its processing environment.

2. **Output** – A threat statement containing a list of threat-sources that could exploit system vulnerabilities.

**Step 3. Vulnerability Identification**

1. The goal of this step is to develop a list of technical and non-technical system vulnerabilities (flaws or weaknesses) that could be exploited or triggered by the potential threat-sources. Vulnerabilities can range from incomplete or conflicting policies that govern an organization’s computer usage to insufficient safeguards to protect facilities that house computer equipment to any number of software, hardware, or other deficiencies that comprise an organization’s computer network.

2. **Output** – A list of the system vulnerabilities (observations) that could be exercised by the potential threat-sources.

**Step 4. Control Analysis**

1. The goal of this step is to document and assess the effectiveness of technical and non-technical controls that have been or will be implemented by the organization to minimize or eliminate the likelihood (or probability) of a threat-source exploiting a system vulnerability.

2. **Output** – List of current or planned controls (policies, procedures, training, technical mechanisms, insurance, etc.) used for the IT system to mitigate the likelihood of a vulnerability being exercised and reduce the impact of such an adverse event.

**Step 5. Likelihood Determination**

1. The goal of this step is to determine the overall likelihood rating that indicates the probability that a vulnerability could be exploited by a threat-source given the existing or planned security controls.

2. **Output** – Likelihood rating of low (.1), medium (.5), or high (1). Refer to the NIST SP 800-30 definitions of low, medium, and high.

**Step 6. Impact Analysis**

1. The goal of this step is to determine the level of adverse impact that would result from a threat successfully exploiting a vulnerability. Factors of the data and systems to consider should include the importance to the organization’s mission; sensitivity and criticality (value or importance); costs associated; loss of confidentiality, integrity, and availability of systems and data.

2. **Output** – Magnitude of impact rating of low (10), medium (50), or high (100). Refer to the NIST SP 800-30 definitions of low, medium, and high.

**Step 7. Risk Determination**

1. This step is intended to establish a risk level. By multiplying the ratings from the likelihood determination and impact analysis, a risk level is determined. This represents the degree or level of risk to which an IT system, facility, or procedure might be exposed if a given vulnerability were exercised. The risk rating also presents actions that senior management (the mission owners) must take for each risk level. (See “Risk Analysis &

2. **Output** – Risk level of low (1-10), medium (>10-50) or high (>50-100). Refer to the NIST SP 800-30 definitions of low, medium, and high.

**Step 8. Control Recommendations**

1. The purpose of this step is to identify controls that could reduce or eliminate the identified risks, as appropriate to the organization’s operations to an acceptable level. Factors to consider when developing controls may include effectiveness of recommended options (i.e., system compatibility), legislation and regulation, organizational policy, operational impact, and safety and reliability. Control recommendations provide input to the risk mitigation process, during which the recommended procedural and technical security controls are evaluated, prioritized, and implemented.

2. **Output** – Recommendation of control(s) and alternative solutions to mitigate risk.

**Step 9. Results Documentation**

1. Results of the risk assessment are documented in an official report or briefing and provided to senior management (the mission owners) to make decisions on policy, procedure, budget, and system operational and management changes.

2. **Output** – A risk assessment report that describes the threats and vulnerabilities, measures the risk, and provides recommendations for control implementation.

**Risk Mitigation**

Risk mitigation involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process to ensure the confidentiality, integrity and availability of ePHI. Determination of appropriate controls to reduce risk is dependent upon the risk tolerance of the organization consistent with its goals and mission.

**Step 1. Prioritize Actions**

1. Using results from Step 7 of the Risk Assessment, sort the threat and vulnerability pairs according to their risk-levels in descending order. This establishes a prioritized list of actions needing to be taken, with the pairs at the top of the list getting/requiring the most immediate attention and top priority in allocating resources.

2. **Output** – Actions ranked from high to low

**Step 2. Evaluate Recommended Control Options**

1. Although possible controls for each threat and vulnerability pair are arrived at in Step 8 of the Risk Assessment, review the recommended control(s) and alternative solutions for reasonableness and appropriateness. The feasibility (e.g., compatibility, user acceptance, etc.) and effectiveness (e.g., degree of protection and level of risk mitigation) of the recommended controls should be analyzed. In the end, select a “most appropriate” control option for each threat and vulnerability pair.
2. **Output** – list of feasible controls

**Step 3. Conduct Cost-Benefit Analysis**

1. Determine the extent to which a control is cost-effective. Compare the benefit (e.g., risk reduction) of applying a control with its subsequent cost of application. Controls that are not cost-effective are also identified during this step. Analyzing each control or set of controls in this manner, and prioritizing across all controls being considered, can greatly aid in the decision-making process.

2. **Output** – Documented cost-benefit analysis of either implementing or not implementing each specific control.

**Step 4. Select Control(s)**

1. Taking into account the information and results from previous steps, the Wasabi Technologies’ mission, and other important criteria, the Risk Management Team determines the best control(s) for reducing risks to the information systems and to the confidentiality, integrity, and availability of ePHI. These controls may consist of a mix of administrative, physical, and/or technical safeguards.

2. **Output** – Selected control(s).

**Step 5. Assign Responsibility**

1. Identify the individual(s) or team with the skills necessary to implement each of the specific controls outlined in the previous step, and assign their responsibilities. Also identify the equipment, training and other resources needed for the successful implementation of controls. Resources may include time, money, equipment, etc.

2. **Output** – List of resources, responsible persons and their assignments

**Step 6. Develop Safeguard Implementation Plan**

1. Develop an overall implementation or action plan and individual project plans needed to implement the safeguards and controls identified. The Implementation Plan should contain the following information:
   a. Each risk or vulnerability/threat pair and risk level
   b. Prioritized actions
   c. The recommended feasible control(s) for each identified risk
   d. Required resources for implementation of selected controls
   e. Team member responsible for implementation of each control
   f. Start date for implementation
   g. Target date for completion of implementation
   h. Maintenance requirements.

2. The overall implementation plan provides a broad overview of the safeguard implementation, identifying important milestones and timeframes, resource requirements (staff and other individuals’ time, budget, etc.), interrelationships between projects, and any other relevant information. Regular status reporting of the plan, along with key metrics and success indicators should be reported to the organization’s executive management/leadership team (e.g. the Board, senior management, and other key stakeholders).
3. Individual project plans for safeguard implementation may be developed and contain
detailed steps that resources assigned carry out to meet implementation timeframes and
expectations (often referred to as a work breakdown structure). Additionally, consider
including items in individual project plans such as a project scope, a list deliverables, key
assumptions, objectives, task completion dates and project requirements.

4. Output – Safeguard Implementation Plan

Step 7. Implement Selected Controls
As controls are implemented, monitor the affected system(s) to verify that the implemented
controls continue to meet expectations. Elimination of all risk is not practical. Depending on
individual situations, implemented controls may lower a risk level but not completely eliminate
the risk.

1. Continually and consistently communicate expectations to all Risk Management Team
members, as well as senior management and other key people throughout the risk
mitigation process. Identify when new risks are identified and when controls lower or
offset risk rather than eliminate it.

2. Additional monitoring is especially crucial during times of major environmental changes,
organizational or process changes, or major facilities changes.

3. If risk reduction expectations are not met, then repeat all or a part of the risk
management process so that additional controls needed to lower risk to an acceptable
level can be identified.

4. Output – Residual Risk

Risk Management Schedule
The two principal components of the risk management process - risk assessment and risk
mitigation - will be carried out according to the following schedule to ensure the continued
adequacy and continuous improvement of Wasabi Technologies’ information security program:

1. Scheduled Basis – an overall risk assessment of Wasabi Technologies’ information
system infrastructure will be conducted annually. The assessment process should be
completed in a timely fashion so that risk mitigation strategies can be determined and
included in the corporate budgeting process.

2. Throughout a System’s Development Life Cycle – from the time that a need for a new
information system is identified through the time it is disposed of, ongoing assessments
of the potential threats to a system and its vulnerabilities should be undertaken as a part
of the maintenance of the system.

3. As Needed – the Security Officer (or other designated employee) or Risk Management
Team may call for a full or partial risk assessment in response to changes in business
strategies, information technology, information sensitivity, threats, legal liabilities, or
other significant factors that affect Wasabi Technologies’ information systems.

Process Documentation
Maintain documentation of all risk assessment, risk management, and risk mitigation efforts for
a minimum of six years.
BUSINESS CONTINUITY

Administration of Contingency Plan

1. Chain of Command: In situations that affect single systems, the Security Officer, or a designee should determine the appropriate response and implementation.

2. Communication Strategies: Wasabi Technologies should determine the need to identify and develop needed communication strategies during a disaster.
   a. IS Disaster Recovery Team Status Report: The DRC will determine the need to complete status reports. The Disaster Recovery Team and all other disaster recovery support team leaders will be responsible for completing the report when requested by the DRC. The DRC will compile information from the status report(s) to use in communicating to senior administrative leadership, corporate resources, and other external contacts and stakeholders (a blank template of this form is available as an attachment to this plan – Appendices 1 and 2).
   b. Administration: The administrative leader assigned to the disaster recovery process shall act as a liaison between the DRC/Team and administration. The leader will be responsible for communicating disaster recovery activities on an as needed basis.
   c. Corporate/System Level: The DRC will determine the need for notification of the corporate oversight structure and/or IS staff. The Corporate Office shall be notified of any disaster/security incident that:
      i. Results in adverse patient care outcomes or impact operational functions;
      ii. Requires additional IS resources and support beyond the scope of the local organization’s IS staff;
      iii. Impacts more than one organization or facility;
      iv. Results in critical/key ePHI systems being down for more than (one hour);
      v. Requires involvement with local, state or federal law enforcement agencies; and
      vi. Results in adverse publicity and requires media relations skills.
   The DRC may also request assistance from other affiliated organizations for IS support. The Coordinator may contact Wasabi Technologiess directly or request assistance from corporate IS in coordinating supporting services and resources from the other organizations.
   d. Media/Public Relations: All IS disaster related information (spoken or written) shall be coordinated and issued to members of the media by a designated media relations contact such as a Communications Coordinator or a member of senior leadership. Certain types of information security incidents may generate the attention of the news media, and there are instances in which Wasabi Technologies may also choose to initiate contact with the news media. For example, local radio and television stations may be utilized to report closings or new hours of facilities.

Wasabi Technologies’s designated media relations contact should serve as a liaison between Wasabi Technologies and the news media (or a single point of
contact for the news media). This will eliminate the need to involve the Disaster Recovery Team members and leaves them free to manage the security incident. The DRC, IS leader or other member of the Disaster Recovery Team should be prepared to share information with the media relations contact. Key considerations when working with the media relations contact person or the news media include:

1. Ensuring that the contact has a clear understanding of the technical issues so that they may communicate effectively and accurately with the press. False or misleading information may ultimately cause more damage to Wasabi Technologies’s reputation.

2. Contacting Wasabi Technologies’s legal counsel if unsure of legal issues.

3. Establishing a single point of contact (if no official media relations contact person exists) when working with the news media to ensure that all inquiries and statements are coordinated.

4. Keeping the level of technical detail low – do not provide attackers with information.

5. Being as accurate as possible.

6. Avoiding speculation.

7. Ensuring that any details about the incident that may be used as evidence are not disclosed without the approval of investigative agencies.

8. Contacting the Privacy Officer should information released to media (need to) contain patient specific information to ensure required authorizations are in place prior to the release.

Disaster Recovery Team Contact Information

Members of the IS Disaster Recovery Team shall be contacted immediately once the IS DRP has been activated. The following information should be provided at the time of contact:

i. A Brief Description of the Problem (e.g., Facilities/Systems Down)

ii. Location of the IS Disaster Recovery Command Center

iii. Phone Number of the IS Disaster Recovery Command Center

iv. Identification of Immediate Support Required (e.g., Services, Equipment, Backup Tapes, etc.)

v. Information Regarding How the Facility Can be Entered (Need for Badge/Identification)

Disaster Recovery Site

1. Wasabi Technologies shall determine appropriate recovery site needs for the IS Disaster Recovery Command Center.

2. The Command Center should function as the centralized location for IS disaster recovery processes.
Recovery Center/Alternative Site

1. The DRC shall make the determination as to whether or not recovery activities should be relocated to an alternative site.

Prioritized List of Components of System

1. Wasabi Technologies shall prioritize based on business impact/criticality analysis and system interdependencies to determine what applications, systems, and/or networks are recovered first. It is recommended that this be determined in advance and approved by Wasabi Technologies's senior leadership.

Current Inventory List

1. Wasabi Technologies shall have compiled an inventory list of IS equipment, hardware, software, and key application, system, and network information/specifications. This list could be a part of a database that stores information about many key IS components, associated contacts, etc.

Contact Lists

1. Wasabi Technologies shall have compiled contact lists for key workforce members, business associates, stakeholders, utilities management, disaster recovery specialists, emergency government contacts, radio and TV stations, etc.

Contacts for Replacement Hardware/Equipment

1. Wasabi Technologies shall ensure the access and availability of this information during an IS disaster. Consider maintaining this documentation electronically as well as in hard-copy.

Plan Maintenance

Testing

1. Wasabi Technologies shall determine the scope and how often the plan shall be tested.
2. Testing will be done on an annual basis.
3. A “table top” drill allows examining alternatives without actually interfering with any daily operations.

Maintenance and Revision

1. The DRP should be reviewed and revised as necessary on an annual basis to ensure that the information it contains is up-to-date and reflects current workforce information (titles, names, and contact information), systems, vendors, and other external contacts information. Additionally, after each disaster incident, whether
a planned drill or actual disaster, the plan should be reviewed and revised to address practical application issues.

Responsibility

1. Wasabi Technologies shall designate the Security Officer for maintenance and revision of the plan. Wasabi Technologies might consider the following individuals or structures to be responsible for the plan:

Staff Education and Training

1. Members of Wasabi Technologies’s workforce shall be provided education and training in emergency preparedness and disaster recovery upon hire and as needed to reflect any significant changes to Wasabi Technologies’s emergency preparedness/disaster recovery practices including information system disaster events and security incidents.
2. Workforce members with specific responsibilities for IS disaster recovery shall receive the necessary education and training required to ensure that they can carry out their assigned duties in the event of an IS disaster events.

SYSTEM ACCESS

Access Establishment and Modification

1. All requests for access to any of the organization’s information systems and applications must be approved by the requestor’s immediate supervisor.
   a. Access will not be granted until signed “Confidentiality and Information Access Agreement” forms are received, reviewed, and additional approval is obtained if required.
   b. Training related to security, confidentiality, and incident reporting must occur before login credentials are issued.
   c. The “Confidentiality and Information Access Agreement” and the “System Access Request Change” forms are maintained by the Security Officer.
2. The Managing Supervisor is responsible for notifying the Security Officer of employees transferred into a new department or new role.
3. The Security Officer is responsible for changing the user’s access to information systems based on the user’s new role.

Workforce Clearance Procedures

1. The level of security assigned to a user to the organization’s information systems is based on the minimum necessary information (amount of data) access required to carry out legitimate job responsibilities assigned to a user’s job classification and/or to a user needing access to carry out treatment, payment, or healthcare operations.
2. All access requests are treated on a ‘least-access principle”; blanket access is not provided for any user.
3. Any access not specifically authorized is prohibited.
Access Authorization

1. Role based access categories for each information system/application are pre-approved by the Devops Team. Categories are defined by the importance of the applications running on the information system, the value or sensitivity of the ePHI on the information system, security controls on the information system, security controls on the workstation utilized to access the information system, and the extent to which the information system is connected to other information systems. Any access must be based on the minimum necessary information needed for the user’s role.

2. The Devops Team grants the level of access to users based on these pre-determined categories.

3. Refer to the remote access policy for details relating to remote access.

Person or Entity Authentication

Each user has and uses a unique User Login ID and password that identifies him/her as the user of the information system.

Unique User Identification

1. Access to the organization’s information systems/applications is controlled by requiring unique User Login ID’s and passwords for each individual user.

2. Password requirements should be based on current industry and NIST standards whenever possible (for example 8 character minimum with upper and lower case letters, numbers, and symbols).

3. Passwords are not displayed at any time. Password characters are replaced with asterisks “*” or other characters when typed.

4. Users should not select passwords that may be easily guessed or obtained using personal information (i.e., names, favorite sports team, etc.).

5. The DevOps Team assigns a User Login ID and generic password for each user to utilize for first time access into each information system. The User Login ID and password are forwarded to the user securely (e.g., in a sealed envelope).

6. Each information system automatically requires users to change their password upon first-time use of the information system.

Password Management

1. User Login IDs and passwords are used to control access to the organization’s information systems and should not be disclosed. Under rare circumstances IT support may need a user ID and password. When that happens the password may be shared but should be changed to a new password as soon as possible.

2. Users may not allow anyone for any reason to have access to any information system using another user’s unique User Login ID and password with the exception of IT support as outlined above.

3. Users that do not recall their password may contact DevOps. The DevOps Team provides the employee with a temporary, one-time use password which must be changed on first use.
4. Passwords are inactivated upon an employee’s termination (refer to the termination procedures in this policy).
5. If a user believes their User Login ID has been compromised, they are required to immediately report the incident to the Security Officer.

**Automatic Logoff**

1. Users are required to make information systems inaccessible by any other individual when unattended by the users (i.e., locking or logging off the systems; if the device is used only by a single individual with a unique log in, it may be locked).
2. Users must log off information systems/applications at the end of their shift, or at the end of their need to use the system/application, whichever is sooner.
3. Information systems should automatically log users off the systems after 60 minutes of inactivity. Shortened automatic log off times should be implemented for workstations located in public or high traffic areas or for portable devices. Each organization must choose the number of minutes for automatic logoff based on its risk analysis.
4. The Technical Security & Privacy Officers approve exceptions to automatic log off requirements.

**Workstation Use**

1. Workstations should only be used for authorized business purposes.
2. When possible workstations should be placed in secure areas. Workstations in patient rooms or public areas must be logged off or locked when not in use. Users must take actions to prevent unauthorized viewing (e.g. privacy screens, minimizing sessions, closing laptops, and so on).
3. All users are responsible for practicing precautions to protect the confidentiality, integrity, and availability of ePHI in the information systems at all times.
4. Workstations may not be used to engage in any activity that is illegal or is in violation of organization’s policies.
   a. Access may not be used for transmitting, retrieving, or storage of any communications of a discriminatory or harassing nature or materials that are obscene or “X-rated”. Harassment of any kind is prohibited. No messages with derogatory or inflammatory remarks about an individual’s race, age, disability, religion, national origin, physical attributes, sexual preference, political affiliation, or health condition shall be transmitted or maintained. No abusive, hostile, profane, or offensive language is to be transmitted through organization’s system.
   b. Information systems/applications also may not be used for any other purpose that is illegal, unethical, or against company policies or contrary to organization’s best interests. Messages containing information related to a lawsuit or investigation may not be sent without prior approval.
   c. Solicitation of non-company business, or any use of organization’s information systems/applications for personal gain is prohibited.
   d. Participation in chain letters and other such activities is also prohibited.
   e. Transmitted messages may not contain material that criticizes organization, its providers, its employees, or others.
f. Users may not misrepresent, obscure, suppress, or replace another user’s identity in transmitted or stored messages.

g. I understand that I have neither ownership interest nor expectation of privacy in any information accessed or created by me during my relationship with Wasabi Technologies. Wasabi Technologies may audit, log, access, review, and otherwise utilize information stored on or passing through its systems for many reasons, including to maintain the confidentiality, security, and availability of Confidential Information. Any exceptions for personal incidental use of Wasabi Technologies computers or communications systems must have the approval of the department director or higher-level management. Such exceptions can only be approved when such use does not:
   i. Consume more than a trivial amount of resources that could otherwise be used for business purposes;
   ii. Interfere with workforce member productivity;
   iii. Preempt any business activity;
   iv. Violate any restrictions noted in these or other company policies;
   v. Engage in inappropriate behavior (e.g. written attacks, threats, harassment, acquisition and/or use of materials or information inconsistent with Wasabi Technologies' Mission, Vision and Values);
   vi. Violate any laws or regulations governing such usage;
   vii. Potentially embarrass Wasabi Technologies or any of its affiliates.
   viii. Require changes to firewall, proxies, or other systems or devices

Workstation Security

1. Users may access and utilize workstations as assigned by their supervisor.
2. All users must report unauthorized workstation use to the Technical Security Officer or designee.
3. The organization must install on all workstations anti-virus software to prevent transmission of malicious software. This software is regularly updated.
4. Portable workstations (e.g. laptops, mobile devices etc.) are also subject to the same safeguards and protections. Portable workstations are maintained in a safe and secure manner when transported. Any portable device that contains PHI must be encrypted. Portable media is also subject to the same requirements.
5. Networks are secured with a Firewall.
   a. Network access is limited to legitimate or established connections. An established connection is return traffic in response to an application request submitted from within the secure network.
   b. Firewall console and other management ports are appropriately secured or disabled and are located in a physically secure environment.
   c. Mechanisms to log failed access attempts are in place.
   d. The configuration of firewalls used to protect networks is approved by the Technical Security Officer or designee and maintained by the DevOps department.
   e. Firewalls need to be maintained as staff change positions.
   f. Servers are located in a physically secure environment and are on a secure network with firewall protection.
      i. The system administrator or root account is password protected.
ii. A security patch and update procedure is established and implemented to ensure that all relevant security patches and updates are promptly applied based on the severity of the vulnerability corrected.

iii. All unused or unnecessary services are disabled.

**Termination Procedures**

1. The Managing Supervisor is required to notify network administration upon completion and/or termination of access needs and facilitating completion of the “Termination Checklist”.

2. The Managing Supervisor is required to notify the network administration to terminate a user’s access rights if there is evidence or reason to believe the following (these incidents are also reported on an incident report and are filed with the Privacy Officer):
   a. The user has been using their access rights inappropriately,
   b. A user’s password has been compromised (a new password may be provided to the user if the user is not identified as the individual compromising the original password)
   c. An unauthorized individual is using a user’s Login ID and password (a new password may be provided to the user if the user is not identified as providing the unauthorized individual with the User Login ID and password).

3. Network administration will terminate users’ access rights immediately upon notification.

4. The DevOps Department audits and may terminate access of users that have not logged into organization’s information systems/applications for a period of over 12 months.

**DEVICE, MEDIA, AND PAPER RECORD SANITIZATION FOR DISPOSAL OR REUSE**

1. All destruction/disposal of media will be done in accordance with federal and state laws and regulations and pursuant to the organization's written retention policy/schedule. Records that have satisfied the period of retention will be destroyed/disposed of in an appropriate manner.

2. Records involved in any open investigation, audit or litigation should not be destroyed/disposed of. If notification is received that any of the above situations have occurred or there is the potential for such, the record retention schedule shall be suspended for these records until such time as the situation has been resolved. If the records have been requested in the course of a judicial or administrative hearing, a qualified protective order will be obtained to ensure that the records are returned to the organization or properly destroyed/disposed of by the requesting party.

3. Before reuse of any recordable and erasable media, for example hard disks, tapes, cartridges, USB drives, smart phones, SAN disks, SD and similar cards, all ePHI must be rendered inaccessible, cleaned, or scrubbed. Standard approaches include one or all of the following methods:
   a. Overwrite the data (for example, through software utilities).
   b. Degauss the media.

4. Records scheduled for destruction/disposal should be secured against unauthorized or inappropriate access until the destruction/disposal of PHI is complete.
5. The business associate agreement must provide that, upon termination of the contract, the business associate will return or destroy/dispose of all patient health information. If such return or destruction/disposal is not feasible, the contract must limit the use and disclosure of the information to the purposes that prevent its return or destruction/disposal.

6. A record of all PHI media sanitization should be made and retained by the organization. The organization has the responsibility to retain the burden of proof for any media destruction regardless of whether destruction is done by the organization or by a contractor. Retention is required because the records of destruction/disposal may become necessary to demonstrate that the patient information records were destroyed/disposed of in the regular course of business. Records of destruction/disposal, such as a certificate of destruction, should include:
   a. Date of destruction/disposal.
   b. Method of destruction/disposal.
   c. Description of the destroyed/disposed record series or medium.
   d. Inclusive dates covered.
   e. A statement that the patient information records were destroyed/disposed of in the normal course of business.
   f. The signatures of the individuals supervising and witnessing the destruction/disposal.

7. Copies of documents and images that contain PHI and are not originals that do not require retention based on retention policies (e.g., provider copies, schedule print outs etc.) shall be destroyed/disposed of by shredding or other acceptable manner as outlined in this policy. Certification of destruction is not required.

8. If destruction/disposal services are contracted, the contract must provide that the organization’s business associate will establish the permitted and required uses and disclosures of information by the business associate as set forth in the federal and state law (outlined in organization’s HIPAA Business Associate Agreement/Contract). The BAA should also set minimum acceptable standards for the sanitization of media containing PHI. The BAA or contract should include but not be limited to the following:
   a. Specify the method of destruction/disposal.
   b. Specify the time that will elapse between acquisition and destruction/disposal of data/media.
   c. Establish safeguards against unauthorized disclosures of PHI.
   d. Indemnify the organization from loss due to unauthorized disclosure.
   e. Require that the business associate maintain liability insurance in specified amounts at all times the contract is in effect.
   f. Provide proof of destruction/disposal (e.g. certificate of destruction).

9. The methods of destruction, disposal, and reuse should be reassessed periodically, based on current technology, accepted practices, and availability of timely and cost-effective destruction, disposal, and reuse technologies and services.