Welcome to our Cybersecurity and IT Policy document. We believe in open-sourcing our work whenever possible, and this is no exception! Why hoard the work we’ve done when we can share it with the world, so you don’t have to rebuild it from scratch yourself?! This document is a few years old, so there may be people to credit that we have not explicitly called out. If you find we’re missing someone, please, please, please let us know so we can give them credit. Also, any copy/pasting should come from public domain works – like the US HUD, the California Governor’s Office of Emergency Services, and several universities. We are offering our work under the MIT license: permissive and free. Validate content for inherited licensing prior to use. Disclaimer: use at your own risk, no guarantees.

Authors and contributors include:

* Stephen Semmelroth
* Sean Eyre
* Adrian Tilston

How to use this document:

* You MUST know the company first.
* Begin by reading and understanding it
* Often, the policies will reference themselves or other trackers or external policies such as the Employee Handbook.
* Be judicious when defining change.
* If you haven’t created those other documents, we recommend creating them or removing the references to them.
* Remember that these are governing policies, not technical runbooks.
* Make sure you have HR, Legal, and anyone else important review this before you make it policy!

<<COMPANY>> Cybersecurity and IT Policy

Table of Contents

[2 Policy Statement 6](#_Toc128990066)

[3 Purpose 6](#_Toc128990067)

[4 Scope 6](#_Toc128990068)

[5 Enforcement and Expectation of compliance (HIPAA 1.1.3) 6](#_Toc128990069)

[6 Roles and responsibilities 6](#_Toc128990070)

[7 Policy 7](#_Toc128990071)

[8 Exceptions 8](#_Toc128990072)

[9 Documentation and Control 8](#_Toc128990073)

[9.1 Documents (HIPAA 1.9.1, 1.8, 5.2.1, 5.2.2) 8](#_Toc128990074)

[9.2 Records 8](#_Toc128990075)

[9.3 Distribution and Maintenance 9](#_Toc128990076)

[10 Review and Evaluation (HIPAA 1.1.1, 1.7.4, 1.8, 5.2.3) 9](#_Toc128990077)

[11 Approval 9](#_Toc128990078)

[12 Appendix A: Asset Management 10](#_Toc128990079)

[12.1 Overview and Purpose 10](#_Toc128990080)

[12.2 Scope 10](#_Toc128990081)

[12.3 Enforcement 10](#_Toc128990082)

[12.4 Roles and Responsibilities 10](#_Toc128990083)

[12.5 Acronyms 10](#_Toc128990084)

[12.6 Policy 10](#_Toc128990085)

[12.6.1 Inventory of Computational Assets. 10](#_Toc128990086)

[12.6.2 Inventory of Software and Services 11](#_Toc128990087)

[12.6.3 Inventory of Critical Accounts 12](#_Toc128990088)

[12.6.4 System Criticality (HIPAA 1.7.5) 12](#_Toc128990089)

[12.6.5 Accountability of hardware and assets (HIPAA 2.4.3, 2.4.4) 12](#_Toc128990090)

[12.6.6 Asset Provisioning (and Gold Image) 12](#_Toc128990091)

[12.6.7 Configuration Management and Patch Management 13](#_Toc128990092)

[12.6.8 Tools for Asset Control 13](#_Toc128990093)

[12.6.9 End Point Protection (HIPAA 1.5.2, 1.6.1) 13](#_Toc128990094)

[13 Appendix B: Access Control 14](#_Toc128990095)

[13.1 Overview and Purpose 14](#_Toc128990096)

[13.2 Scope 14](#_Toc128990097)

[13.3 Enforcement 14](#_Toc128990098)

[13.4 Roles and Responsibilities 14](#_Toc128990099)

[13.5 Acronyms 14](#_Toc128990100)

[13.6 Policy 14](#_Toc128990101)

[13.6.1 Employee On-boarding and off-boarding (HIPAA 1.3.3, 1.4.2) 14](#_Toc128990102)

[13.6.2 Role Based Access (HIPAA 1.3.1, 1.4.3, 2.1.3, 2.3) 14](#_Toc128990103)

[13.6.3 Temporary Roles (2.1.3) 15](#_Toc128990104)

[13.6.4 Access, role, and privilege review (HIPAA 1.3.2, 1.4.3) 15](#_Toc128990105)

[13.6.5 Passwords and Authentication (HIPAA 1.5.4, 3.3.1, 3.4) 15](#_Toc128990106)

[13.6.6 Log Aggregation (HIPAA 1.1.4, 1.5.3) 16](#_Toc128990107)

[13.6.7 Log Review (HIPAA 3.2) 16](#_Toc128990108)

[13.6.8 Auxiliary Controls (HIPAA 3.1.3) 17](#_Toc128990109)

[14 Appendix C: Information Classification and Handling Policy 18](#_Toc128990110)

[14.1 Overview and Purpose 18](#_Toc128990111)

[14.2 Scope 18](#_Toc128990112)

[14.3 Enforcement 18](#_Toc128990113)

[14.4 Roles and Responsibilities 18](#_Toc128990114)

[14.5 Acronyms 18](#_Toc128990115)

[14.6 Policy (HIPAA 2.1.2) 18](#_Toc128990116)

[14.6.1 Classification Categories (HIPAA 3.5.1, 3.5.2, 4.2.1) 18](#_Toc128990117)

[14.6.2 Labeling PHI caveat 20](#_Toc128990118)

[14.6.3 Secure handling of information assets (2.2, 2.3, 2.4.1, 4.2.2) 20](#_Toc128990119)

[14.6.4 Classification by aggregation 21](#_Toc128990120)

[14.6.5 Reduction in classification and media reuse (HIPAA 2.4.2) 21](#_Toc128990121)

[14.6.6 Information or data audit (HIPAA 1.7.5) 21](#_Toc128990122)

[15 Appendix D: Cybersecurity Awareness Training 21](#_Toc128990123)

[15.1 Overview and Purpose 21](#_Toc128990124)

[15.2 Scope 21](#_Toc128990125)

[15.3 Enforcement 22](#_Toc128990126)

[15.4 Roles and Responsibilities 22](#_Toc128990127)

[15.5 Acronyms 22](#_Toc128990128)

[15.6 Policy 22](#_Toc128990129)

[15.6.1 Annual Training Requirement 22](#_Toc128990130)

[15.6.2 Periodic reminders (HIPAA 1.5.1) 22](#_Toc128990131)

[16 Appendix E: Incident Response Policy and Plan 22](#_Toc128990132)

[16.1 Overview and Purpose 22](#_Toc128990133)

[16.2 Scope 22](#_Toc128990134)

[16.3 Enforcement 22](#_Toc128990135)

[16.4 Roles and Responsibilities 22](#_Toc128990136)

[16.5 Acronyms 23](#_Toc128990137)

[16.6 Policy 23](#_Toc128990138)

[16.6.1 Incident Response Team 23](#_Toc128990139)

[16.6.2 Incident Response Team Notification 24](#_Toc128990140)

[16.6.3 Incident Response Team Communications 24](#_Toc128990141)

[16.6.4 Events and Incidents (HIPAA 1.6.1) 24](#_Toc128990142)

[16.6.5 Triage and Escalation 25](#_Toc128990143)

[16.6.6 Tracking and reports 25](#_Toc128990144)

[16.6.7 Incident Categories 25](#_Toc128990145)

[16.6.8 Categories of Functional Impact 26](#_Toc128990146)

[Categories of Information Impact 27](#_Toc128990147)

[16.6.9 Reporting Security Incidents (HIPAA 1.6.1) 27](#_Toc128990148)

[16.6.10 Evidence Retention and Chain of Custody 27](#_Toc128990149)

[16.6.11 Reporting template 28](#_Toc128990150)

[16.6.12 Reporting Incidents to Legal Authority (HIPAA 4.2.4) 30](#_Toc128990151)

[16.6.13 IR Retainer (HIPAA 1.6.1) 30](#_Toc128990152)

[16.7 Process 30](#_Toc128990153)

[17 Appendix F: Disaster Recovery and Emergency Mode Operations Policy and Plan 33](#_Toc128990154)

[17.1 Overview and Purpose 33](#_Toc128990155)

[17.2 Scope 33](#_Toc128990156)

[17.3 Enforcement 33](#_Toc128990157)

[17.4 Roles and Responsibilities 34](#_Toc128990158)

[17.5 Acronyms 34](#_Toc128990159)

[17.6 Policy (HIPAA 3.1.2) 34](#_Toc128990160)

[17.6.1 Backups (1.7.1, HIPAA 1.7.2) 34](#_Toc128990161)

[17.6.2 Data restoration (HIPAA 1.7.2, 1.7.4, 2.11) 34](#_Toc128990162)

[17.6.3 Fail-over (HIPAA 1.7.2, 1.7.4) 34](#_Toc128990163)

[17.6.4 Emergency Communications (HIPAA 1.7.2, 1.7.4) 34](#_Toc128990164)

[17.6.5 Emergency Operations (HIPAA 1.7.2, 1.7.4) 35](#_Toc128990165)

[18 Future Appendix’s 37](#_Toc128990166)

[19 References 38](#_Toc128990167)

# Policy Statement

**<<COMPANY>> (<<COMPANY>>)** shall adopt and follow well-defined and time-tested plans and procedures and lay out cybersecurity objectives to meet its business objectives and ensure continuity of its operations and processes.

# Purpose

The purpose of this policy is to establish cybersecurity guidelines that increases our ability <<COMPANY MISSION STATEMENT>>, to grow within the <<SECTOR>> market, and to outperform our competition.

In establishing a cybersecurity policy, we intend to communicate why we need to guard our information, our partners’ information, and that of our clients and patients. We further lay out what we must do to use security to ensure trust and gain competitive edge as an <<TYPE OF BUSINESS>> as well as how we should implement those countermeasures and manage risk to our organization.

# Scope

This policy applies to <<COMPANY>>, its employees, its IT infrastructure, computing resources, networks, information, and data.

It applies to all information, assets, and data owned, licensed by, or otherwise used by <<COMPANY>>.

# Enforcement and Expectation of compliance (HIPAA 1.1.3)

Any employee or third-party found to have violated these policies may be subject to disciplinary action which may include termination of employment, contract, or other arrangement.

# Roles and responsibilities

**You** – The user, as a member of the <<COMPANY>> staff, you are an integral part of our security program. You maintain appropriate levels of access and privileges and defend <<COMPANY>> with constant vigilance and discipline.

**CEO** – The CEO is responsible for living cybersecurity fundamentals and leading the charge from the front. The CEO establishes priorities and goals for <<COMPANY>>, which the cybersecurity program and policies support.

**Legal Counsel** – <<COMPANY>>’s legal counsel provides a checkpoint for all security programs and ensures that areas such as data retention or emergency mode operations comply with legal and regulatory requirements. They are a primary stakeholder during incident response and are the primary voice of the company between internal stakeholders, any government entity, and partner, client, or patient communications. *Legal counsel will establish policy for and ensure that BAAs, service agreements, and all contracts provide satisfactory assurance that applicable parties will safeguard information and meet the requirements of applicable laws and regulations (1.9.1, 4.1.1, 4.1.2, 4.1.3)*

**CISO** – The CISO leads the cybersecurity department and is responsible for reducing business risk through the judicious application of training, auditing, compliance, governance, and communication across <<COMPANY>>. The CISO role may from time to time include third-parties such as consultants or virtual CISOs. *The CISO is responsible for all policies subordinate to or nested with this one, including the appendices attached here (1.9.1)*

**IT Team** – Support the needs of <<COMPANY>>’s other staff, lead the change control process, and govern identity and access management through the organization. The IT team includes contracted or third-party service providers who directly manage <<COMPANY>>’s assets and infrastructure.

**Facilities Manager** – Responsible for physical access management, key control, and daily security. The office manager coordinates responses to physical incidents and notified cybersecurity and IT personnel. *The facilities manager is responsible for all physical security related policies.* (2.1.2)

**Privileged Users** – Users of <<COMPANY>>’s IT and computing assets with administrative or increased access and permissions. <<COMPANY>> places a high degree of trust and confidence in its privileged users because they have access to more information and resources than other users and have the ability to grant others access to information and resources.

**Third-Party Stakeholders** – People outside the organization that require access to <<COMPANY>>’s information. Those stakeholders, as applicable, must sign non-disclosure agreements, service agreements, and BAAs. They are required to maintain the same levels of diligence to protect the confidentiality, integrity, and availability of our information, systems, and resources.

*See associated RACI Charts, process documents, and personnel documents that define roles and responsibilities more granularly here: [LINK\_TO\_RACI\_DOCS]*

# Policy

<<COMPANY>> strives not just to comply with regulatory frameworks such as HIPAA, but to improve and sustain its operations and ability to serve patients through deliberate risk-management. To this extent, we have an ongoing cybersecurity and risk-management program and will continue to apply and mature it both in scope and in practice. We will employ countermeasures that include but are not limited to:

* End-point protection
* Identity management and identity-focused security
* A judicious use of the principle of least privilege
* A focus on SaaS-based application and a deliberate management of third-party risk
* Email security
* Out-of-band communications
* Risk identification and classification
* Information classification, retention, and disposal
* External audit, assessment, and testing when and where applicable (usually annually)
* Security training
* Change control
* Asset, Vulnerability, and Patch Management
* Incident Response and Incident Management
* Log and Event Management and Retention

# Exceptions

Deviations from or exceptions from these policies shall be submitted to the CISO and IT Team for approval and documentation respectively.

*The CISO and IT Team maintain a repository of approved exemptions and associate risk here: [LINK\_TO\_EXCEPTIONS\_REGISTRY]*

*Note: Access to the exemption repository is controlled based on role and need to know. The link will not work for you if you lack either.*

# Documentation and Control

## Documents (HIPAA 1.9.1, 1.8, 5.2.1, 5.2.2)

The IT and Cybersecurity policy document, all policies or documents contained or referenced herein, and all <<COMPANY>> policies shall be controlled. Version control will be applied to distinguish current versions from all previous revisions. All such policies and documents will be retained in digital form for 6 years from their last effective date in accordance with HIPAA guidelines.

After 6 years from the last effective date of a policy or document, all physical or digital copies of a document or policy will be securely destroyed by shredding and/or secure deletion except when a legal hold or other relevant exception is in place.

*The documentation and control repository can be found here: LINK\_TO\_DOCS\_REPO*

## Records

Records generated as part of the IT and Cybersecurity policy, or a policy contained or referenced herein shall be retained for two years. Records shall be in hard copy or electronic media. The records shall be owned by the respective system administrators and shall be audited once a year. Records shall be encrypted at rest and in transit.

Specific records with a longer retention rate will be maintained for the period outlined by the appropriate laws and statues as to maintain compliance. These include but are not limited to legal actions, insurance settlements, and tax records which have varying requirements for retention.

## Distribution and Maintenance

The IT and Cybersecurity policy document shall be made available to all the employees covered in the scope. All the changes and new releases of this document shall be made available to the persons concerned.

The CEO will be accountable for this document and responsibility for its contents if delegated to the CISO. The CISO will also be responsible and accountable for all subordinate or nested policies.

# Review and Evaluation (HIPAA 1.1.1, 1.7.4, 1.8, 5.2.3)

This IT and Cybersecurity policy will be reviewed and re-approved annually by at least the CISO, CEO, and legal counsel.

In addition to the annual policy review, <<COMPANY>> will review its risk posture and risk management practices where they meet technical and procedural implementation (such as on IT systems or facilities access controls.

Where possible, <<COMPANY>> will contract an unbiased third-party to conduct the risk assessment. If such a third-party cannot be leveraged, <<COMPANY>> will document the reasons why and conduct its risk assessment via either the current Managed IT Service Provider (MSP) or its internal IT team. Regardless of the source of the assessment, <<COMPANY>> will not use the same party to conduct the risk assessment more than two years in a row.

# Approval

Sign and date digitally

# Appendix A: Asset Management

## Overview and Purpose

This policy establishes the principles by which <<COMPANY>> manages its assets including but not limited to computers, servers, software, information, and other critical assets.

## Scope

This policy applies to entities outlines in the Cybersecurity and IT Policy base document/policy.

## Enforcement

See enforcement clause in the Cybersecurity and IT Policy.

## Roles and Responsibilities

The CISO or equivalent person designated in writing is responsible for proper implementation of the Asset Management Policy and accountable for driving the program.

The IT Team is responsible for maintaining accurate inventories and tracking systems for all assets and for deploying, operating, and maintaining asset management tools.

## Acronyms

**Asset management –** The process by which our organization will identify, inventory, maintain, and dispose of physical and virtual assets.

## Policy

### Inventory of Computational Assets.

The IT Team, with the advice and assistance of cybersecurity personnel, will maintain an accurate inventory of all <<COMPANY>>’s assets at all times. To the extent possible, <<COMPANY>> will record the following information for all computation assets.

* Device name
* Device serial number (or equivalent unique identifier for virtual servers)
* Device IP addresses
* Device MAC addresses
* Device FQDN
* Firmware and/or Operating system Version and date
* Date of purchase and/or deployment
* Date when the asset will exceed end of life, warranty, or support
* Date of when service contracts will expire
* Date of when <<COMPANY>> must give notice by to avoid auto renew if applicable
* Date installed
* Classification level
* Department or unit
* Physical location
* Point of contact
* Brief description of role

In addition to an inventory, <<COMPANY>> will maintain a map, diagram, or other pictural representation of how assets are dispositioned or segregated physically and logically.

The Asset Inventory can be found here: LINK\_TO\_ASSET\_INVENTORY

The Network Map can be found here: LINK\_TO\_NETWORK\_DIAGRAM

### Inventory of Software and Services

The IT Team, with the advice and assistance of cybersecurity personnel, will maintain an accurate inventory of all of <<COMPANY>>’s software and services. To the extent possible <<COMPANY>> will record the following information for all software, services, or IT related subscriptions:

* Vendor name
* Internal point of contact
* Vendor point of contact
* Type of software, service, or subscription
* Version number
* Account Number (such as for the license or with the vendor)
* Quantity
* Cost
* Billing Period
* Expiration or renewal date
* End of life or support
* Date of when service contracts will expire
* Date of when <<COMPANY>> must give notice to avoid auto renewal if applicable
* Department or unit
* Description

The software and services inventory should include infrastructure as a service (IaaS) and software as a service (SaaS) services, software deployed on servers or user workstations—both opensource and proprietary—services hosted by third parties, domain names, and other related registrations or subscriptions.

For development processes, the development department leader is responsible for tracking all software dependencies and packages in use throughout the development and production pipeline and environments and reporting those inventories to IT for tracking. This supports the concept of a software bill of materials (SBOM) and which allows the team to understand inventory risk.

The Software and Services inventory can be found here: [LINK\_TO\_ASSET INVENTORY]

### Inventory of Critical Accounts

Critical or privileged accounts, either for users, administrators, or automation, will be tracked and managed with the same scrutiny as other assets and will be considered critical to <<COMPANY>> accomplishing its mission and winning in the market.

Critical accounts include but are not limited to any key provided to a third party to access <<COMPANY>>’s systems, root or system level credentials of any kind, AWS root credentials, and the personal credentials of any company level executive.

An inventory of Critical Accounts will record:

* Name
* Account name
* Date provisioned
* All people with access to that account or credential
* Privilege level
* Date of last review or audit

The Critical Account inventory can be found here: [LINK\_TO\_ASSET\_INVENTORY]

### System Criticality (HIPAA 1.7.5)

The IT Team will maintain an accurate inventory of all systems in accordance with the asset management policy. All systems and services will also be inventoried in terms of their classification level and their criticality for operations.

<<COMPANY>> will use three criticality levels:

1. Essential – <<COMPANY>> cannot function without these systems
2. Critical – <<COMPANY>>’s operations are seriously hindered without these systems but <<COMPANY>> can still function.
3. Low – <<COMPANY>> can function with little to no impact if this system or service is lost

### Accountability of hardware and assets (HIPAA 2.4.3, 2.4.4)

When a physical asset is moved from one location to another a record will be recorded of the move with signatures and names recorded at the source and destination.

Before information may be copied onto storage media for transportation or movement, the individual creating the copy must ensure that a backup of the data exists.

*The information audit or asset inventory will maintain an accurate record of the current physical locations of all digital storage media including computer workstations. The inventory may be found here: LINK*

### Asset Provisioning (and Gold Image)

The IT team will establish “gold images” for all configurable assets <<COMPANY>> relies on.

<<COMPANY>> will establish a gold image for at least each of its servers, baseline container images, and user workstations and will review each gold image when it is changed or updated to ensure that any vulnerabilities or security issues are properly documented and mitigated. Each image will be reviewed at least annually.

When a new asset is acquired or deployed, it will be configured using <<COMPANY>>’s gold images and confirmed before it is deployed to development, staging, or production environments. To the extent possible, IT will manage code, scripts, or other automated means to deploy gold images, set initial configurations, and provide updates.

<<COMPANY>>’s gold images are stored and documented here: LINK\_TO\_GOLD\_IMAGE\_LIST

### Configuration Management and Patch Management

<<COMPANY>> has a vested interest in investing in the care and feeding (lifecycle management) of its assets. Using Gold Images is the correct place to start. Keeping those Gold Images and all their deployed subordinates up to date is nontrivial.

An IT Team with a solid configuration management program manages the Gold Images and deploys configuration updates through that management. This means that patches happen as an outcome of a define-once-deploy-many configurations management program rather than a box-to-box patching program.

### Tools for Asset Control

The IT team, with the advice and assistance of the information security team and relevant third parties, will establish tools for monitoring the state and health of assets. Such tools will be deployed to all <<COMPANY>> assets which can receive them and will be used to track:

* What asset is active and where (at least to a logical, network level)
* What the asset’s running state is
* What accounts, services, or personas are leveraging the asset
* What software, services, or libraries are present or active on the asset

Where possible, asset control tools will also provide end point protection and enable the collection of logs and other artifacts relevant to asset management and incident response.

Further documentation regarding <<COMPANY>>’s asset management tools can be found here: [LINK\_TO\_EDR\_OR\_RMM\_TOOLS\_DOCS]

### End Point Protection (HIPAA 1.5.2, 1.6.1)

The IT team will deploy and manage an end-point protection and response (EDR) tool that allows them to detect and respond to and remediate malware and more advanced threats.

The IT team will tune end-point protection and will respond to alerts, events, and incidents highlighted by the tool. The IT Team will ensure that the EDR tool is deployed to all <<COMPANY>> assets and will maintain a list of assets which cannot support the tool and why.

Details of the EDR Tool deployment may be found here: [LINK\_TO\_EDR\_INVENTORY AND DOCUMENTATION]

# Appendix B: Access Control

## Overview and Purpose

The purpose of this policy is to establish risk mitigations and access controls for all <<COMPANY>> assets and personnel and to ensure that all activity—especially unauthorized activity—is fully and accurately recorded for remediation.

## Scope

This policy applies to entities outlines in the Cybersecurity and IT Policy base document/policy.

## Enforcement

See enforcement clause in the Cybersecurity and IT Policy.

## Roles and Responsibilities

See base Cybersecurity and IT Policy

## Acronyms

None for this policy

## Policy

### Employee On-boarding and off-boarding (HIPAA 1.3.3, 1.4.2)

New <<COMPANY>> employees will be automatically added to <<COMPANY>>’s IT systems based on their department and need to access specific information.

HR will create a ticket with IT specifying the identity of the employee, their department, job title, duties, and current contact information. IT will assign the new user a unique user identification number and username and will establish and maintain automated systems to provision access and privileges for new employees in accordance with restrictions established in this policy and will activate such systems upon receiving the ticket from HR.

The IT team will establish an automated system for revoking access to all <<COMPANY>> systems, including third-party systems, services, subscriptions, or tools and will activate such systems *immediately* upon termination of employment *regardless of the reason for termination.*

Such automatic access granting and revoking systems will also apply to PHI access.

### Role Based Access (HIPAA 1.3.1, 1.4.3, 2.1.3, 2.3)

The IT team will manage access to all information—especially PHI—based on the user’s role and department.

All users will be managed in groups in both active director and in Office 365. Groups will reflect the department or organizational units of <<COMPANY>>, and the usernames of all staff assigned to each department will be members of the group for the department.

Permission to access or modify information will be determined based on the departments’ need to access information and will reflect the principle of least privilege. Permissions or privileges will be assigned to the group and inherited by the user; they will not be assigned to individual users.

### Temporary Roles (2.1.3)

As required, the IT Team will document and provide for visitors by establishing temporary user accounts which automatically deactivate at the end of the visit.

Besides the temporary nature of this account, visitor accounts will be managed with the same level of caution and attention to role-based access and least privilege as all other accounts.

### Access, role, and privilege review (HIPAA 1.3.2, 1.4.3)

Supervisors and human resource personnel will review the membership of each group against the membership of each department quarterly and ensure that no users remain in groups who are not members of <<COMPANY>>.

The IT team will review access to information and prioritize access to PHI to determine which groups and associated users have access to what information. Groups without a need to access information or PHI and users accessing information directly instead of via a group will have their permissions removed.

As appropriate, IT will create groups or add group permissions to ensure that all staff members have access to the information they need to accomplish their duties.

### Passwords and Authentication (HIPAA 1.5.4, 3.3.1, 3.4)

All users will protect accounts or access with strong passwords that meet the following criteria:

1. Must be 20 or more characters long.
2. Must contain at least one each of capital letters, numbers, and special characters

The IT team will automate enforcement of this criteria in Active Directory using a group policy object and will facilitate users’ creating strong password by recommending/providing password managers. <<COMPANY>> recommends/provides the following password managers:

1. Opt 1
2. Opt 2
3. Opt 3

When working from home, users will protect all accounts with multi-factor authentication using tools which the IT team will approve for them. The IT team will provide and ensure that the following tools function for users and are auditable by the IT team:

1. Auth tool 1
2. Auth tool 2

SMS (text messages) may be used for <<COMPANY>> accounts for multi-factor authentication only if a one-time password feature is not available.

Users will not share accounts and accesses, including passwords, with anyone at any time including the IT team, other personnel, family, or friends. A user providing access to another individual, either deliberately or through a failure to secure access, is a violation of this policy.

In some cases, a shared account may be authorized to co-manage services that do not support identity access management or role-based controls. In such cases, the shared account must be approved by the CISO and documented by the IT Team. Credentials for all such shared accounts will be stored in an <<COMPANY>> provided password manager in such a way that the IT Team can enforce and monitor role-based access of the shared credentials.

Passwords and other credentials must be changed from their initial or default value as soon as users acquire them. Should an account, access, credential, or password ever be compromised or disclosed, that credential must be immediately changed.

**ePHI –** All access to PHI will require authentication and will meet the same password and multifactor requirements as established above. If a single sign-on solution is not used, systems with PHI must allow the IT team to establish unique identifiers and usernames for all users to support attribution and non-repudiation.

Where possible, the unique identifiers and usernames for PHI systems will be the same as for other systems <<COMPANY>> controls, but will have different passwords and unique multifactor authentication registrations (e.g. unique one-time password generators)

### Log Aggregation (HIPAA 1.1.4, 1.5.3)

The IT team will establish and maintain a log aggregation solution that allows for logs to be collected from user workstations, electronic health systems, and network devices including but not limited to firewalls and switches.

The log aggregator will store at least the following logs:

* Network authentication logs
* All remote access logs
* Workstation or endpoint authentication logs
* Authentication logs for any ePHI system
* Data level access logs for any ePHI (e.g. at the cell level of a database)
* Data level modification logs for any ePHI
* Data level deletion logs for any ePHI

The log aggregator will store all logs for no less than 2 years. Logs related to ePHI access, deletion, or modification will be stored for 6 years. Logs will be indexed and immediately accessible for 3 months (90 days), after which time they may be retain in in-active or “cold” storage.

Cold storage must allow <<COMPANY>> to re-load and re-index logs into active storage when needed.

### Log Review (HIPAA 3.2)

At least monthly, the IT Team will review access logs of all systems containing PHI such as Electronic Medical Records and databases associated with medical tools to ensure that no unauthorized access has occurred.

After review of PHI logs is complete, the IT Team will also review access logs from all other systems for evidence of inappropriate use or unauthorized access to minimize risk to PHI on or interacting with those systems.

This log review applies to all on premises and third-party or cloud hosted tools which <<COMPANY>> has direct access to.

Where possible, the IT team will automate such review and create alerts for inappropriate access or unauthorized access.

The IT Team will provide the results of each monthly review to the CISO in writing.

### Auxiliary Controls (HIPAA 3.1.3)

**Automatic lockouts** – The IT Team will establish technical controls such as group policy objects for active directory and Office365 that cause users to automatically lock and log out of all active log-ins after a period of inactivity.

The IT Team will ensure that screens and log-ins lock after 10 minutes of inactivity and require re-authentication to resume the session. Accounts will automatically log out after 60 minutes of inactivity.

The IT Team will ensure that all “stale” accounts which have not been logged into after 30 days are deactivated. A user must communicate with an admin to restore use of the account. The IT Team will automate the deletion of accounts which have been stale for 60 days (90 days of inactivity total).

**Full Disk Encryption (HIPAA 3.1.4) –** The IT Team will ensure that all machines which support Full Disk Encryption have it activated and that restoration keys are backed up and maintained under the control of the IT Team. The IT Team will document all machines which cannot be encrypted for the review and approval of the CISO.

# Appendix C: Information Classification and Handling Policy

## Overview and Purpose

To provide for patients, ensure continuity of operations and patient care, and to meet its business objectives, <<COMPANY>> shall adopt and follow well-defined and time-tested plans and procedures to ensure that sensitive or critical information is classified correctly and handled according to <<COMPANY>>’s policies.

Information, particularly Personal Health Information (PHI), is considered a primary asset for <<COMPANY>>. <<COMPANY>> uses different types of information assets and the sensitivity of these information assets may vary, as will their handling mechanisms.

The purpose of this policy is to ensure personal information, PHI, and confidential information are protected from unauthorized use and disclosure. This policy helps to facilitate the identification of information to support routine disclosure and active dissemination of information. It also helps protect <<COMPANY>>’s intellectual property.

## Scope

This policy applies to entities outlines in the Cybersecurity and IT Policy base document/policy.

## Enforcement

See enforcement clause in the Cybersecurity and IT Policy.

## Roles and Responsibilities

The CISO or equivalent person designated in writing is responsible for proper implementation of the Information Classification and Handling Policy in conjunction with appropriate other stakeholders such as the Legal Counsel. This role is accountable for proper implementation of the Information Classification and Handling Policy with various other department leads assuming responsibility for implementing the policy within their respective departments.

## Acronyms

None for this policy

## Policy (HIPAA 2.1.2)

This policy inherits its privacy from the base policy. Portions of this policy may, by exception, be held at a higher, more restrictive classification level and stored separately in accordance with access control policies as governed by that more restrictive classification level.

### Classification Categories (HIPAA 3.5.1, 3.5.2, 4.2.1)

<<COMPANY>> categorizes information into four classes: Public, Internal, Confidential, and Secret.

1. **Public** – *Definition*: Information or assets intended for disclosure to or interaction with the public or that, if disclosed, poses no risk or damage to <<COMPANY>>.   
     
   Public information includes information assets that do not have any confidentiality or regulatory requirements or that can be disseminated to the public.   
     
   Examples include press releases, annual financial reports, marketing material, social media, and <<COMPANY>>’s website.
2. **Internal** – *Definition*: Information or assets that are not intended for public release but that do not necessarily pose a risk or damage to <<COMPANY>> if released.   
     
   Internal information includes information necessary for the organization and operation of <<COMPANY>> that is not necessarily confidential or information that can be circulated freely within all offices or departments in <<COMPANY>> but not necessarily the public.   
     
   Examples include personnel assignments, office orders, internal circulars, movement of personnel or equipment, or invoices.
3. **Confidential** – *Definition*: Information or assets that pertain to the specific needs of a project, team, department, or business process or that pose a risk or damage to <<COMPANY>> if improperly disclosed.   
     
   Confidential information includes information necessary for the business operations of departments or units, information that cannot be freely circulated within <<COMPANY>>, PII, PHI, or PCI data, or that contain sensitive or proprietary information. Confidential information must only be accessible to members of the concerned department, project, or business process and must be backed up and archived. It must be encrypted when transmitted or password protected when encryption is not possible.   
     
   Examples include the processes which implement procedures or responsibilities, information that would reduce <<COMPANY>>’s ability to go to win in the market, business strategy, plans for mergers or acquisitions, PCI data, personnel files, service or other agreements, or other techniques or procedures not secret but not appropriate for public release.
4. **Secret –** *Definition:* Information or assets that have a high confidentiality value or which pose a severe risk or damage to <<COMPANY>> if improperly disclosed, specifically PHI  
     
   Secret information includes information **such as PHI** and <<COMPANY>>’s specific intellectual property which shall not be publicly disclosed except when directed to by laws, regulations, or legal direction. **This data is backed up, archived, and encrypted when stored or transmitted. Only a limited set of authorized users shall access these information assets.**  
   Examples include <<COMPANY>>’s specific intellectual property, information from clients that requires special handling, information under specific legal order or regulation, and PHI.

### Labeling PHI caveat

All media containing PHI will also be labeled with the designation “PHI” in the same place and manner as its classification label.

### Secure handling of information assets (2.2, 2.3, 2.4.1, 4.2.2)

1. All information will be labeled according to its classification label in the header and footer of the document and clearly within the file name. In the case of physical storage media, it will be physically labeled with the highest level of information stored therein.
2. All information must be at least logically separate from information of lower classifications and will be physically separated where possible. PHI shall be treated as its own classification category when determining how to segregate it from other secret information.
3. Some classification levels may require approval from the CISO, CEO, or legal counsel prior to transmission.
4. Secret and confidential information must be stored behind digital and physical access controls when not attended, such as in a locked cabinet or safe at the end of the business day.
5. Secret information shall only be accessed in a manner which prevents eavesdropping or shoulder surfing such as by using privacy protecting screen protectors or ensuring monitors face walls without window or opening
6. Appropriate access restrictions shall be applied to prevent access from unauthorized personnel.
7. Restrict mailing and/or shipment of confidential information through only trusted mail services or couriers who must show authentication.
8. Hard copy confidential or secret information must be shredded at the end of its life.
9. Take prudent cautions to prevent unauthorized personnel from accessing higher levels of restricted information.
10. Limit access control both by role and by person/entity.
11. Similarly treat confidential information as you would with both chains of custody and custodial responsibility.
12. Encrypt spooled data and validate user identity and permission prior to printing.
13. Limit distribution to “need to know” and “need to use.”
14. Review persona and entity access monthly and at the end of major project phases.
15. The approval authority for downgrading an information asset’s classification level resides with department leads, and when a classification level is in question, department leads are to consult with the owner of this policy, legal counsel, and or other executive stakeholders.

See associated charts, process documents, and controls more granularly here: [LINK\_TO\_INFO INVENTORY]

### Classification by aggregation

Aggregating data or information can change the classification level of that data. Converting data into information can change the classification of this newly created information asset. This is because information aggregation both represents an intellectual property base and can provide insights into the company’s internal workings that could cause the company to lose in a competitive market.

When information is aggregated it will be classified at the highest level amongst all the information aggregated. For example, when information of internal classification is aggregated with information of confidential classification, the aggregated information is controlled as confidential.

If several items at the same classification level are aggregated, the aggregated information will instead be classified as one level higher than the information aggregated. For example, several pieces of confidential information aggregated into one document will be controlled as secret.

### Reduction in classification and media reuse (HIPAA 2.4.2)

Digital storage media may be reused at the same classification if data stored on the media which is no longer needed is deleted and physical control of the storage media is consistently maintained.

Before any digital storage media may be reused at a lower classification level it must be cryptographically wiped such that all data (every individual bit) is overwritten with random, cryptographic information at least three times before the media is recirculated for use.

Media that has been cryptographically wiped is considered classified as and subsequently labeled as “internal” until data of a higher level has been stored on it again.

### Information or data audit (HIPAA 1.7.5)

The IT Team will maintain an accurate audit of all information on <<COMPANY>>’s network and Office365 setup according to the above classification levels.

The IT Team will review the information audit and ensure not only its accuracy but also that all data and information are protected adequately according to this information classification, handling, and retention policy.

# Appendix D: Cybersecurity Awareness Training

## Overview and Purpose

This policy exists to drive staff vigilance against incidents and motivate the team to report both potential and confirmed incidents.

## Scope

This policy applies to entities as outlined in the Cybersecurity and IT Policy base document.

All <<COMPANY>> users and external entities with access to <<COMPANY>> information or information systems must receive training.

## Enforcement

See enforcement clause in the Cybersecurity and IT Policy.

## Roles and Responsibilities

The CISO is responsible for this program, its direction, and its effectiveness with input from legal, HR, and the IT Committee.

## Acronyms

None for this policy

## Policy

### Annual Training Requirement

All staff will complete an annual security awareness training.

The IT Team will establish a security awareness training program and will ensure all employees have access to the program using [PLACE HOLDER FOR SECURITY AWARENESS TOOL].

When applicable, training completion and results will be maintained in the individuals Human Resources personnel file, as part of the permanent record.

### Periodic reminders (HIPAA 1.5.1)

Once a month, the IT team will send reminders, updates, additional training, or simulations to all staff members to help staff maintain a high level of security awareness and sensitivity.

The IT team will use automated means to deliver reminders and confirm that each employee has received them via email and delivery receipts.

# Appendix E: Incident Response Policy and Plan

## Overview and Purpose

The Purpose of this policy is to ensure that information security increases our ability to win in the market and against our competition by effectively identifying, responding to, and managing information security incidents.

## Scope

This policy applies to entities outlines in the Cybersecurity and IT Policy base document/policy.

## Enforcement

See enforcement clause in the Cybersecurity and IT Policy.

## Roles and Responsibilities

**CISO** or equivalent person designated in writing:

1. Is responsible for proper implementation of the Incident Management Policy and Process.
2. Leads all aspects of response to an incident and is the primary source of truth and communication within the organization and coaches external communicators before breach disclosure to third parties. The CISO also leads incident response exercises and communicates the plan to senior leaders within the organization

**Office or Facilities Manager** – Keeps non-essential personnel from interfering with breach response. Contributes to physical security aspects of the response.

**IT Manager** – Keeps the CISO informed of Incidents.

## Acronyms

* IRT – Incident Response Team
* PACE Plan – A plan to cover the Primary, Alternate, Contingency, and Emergency modes of accomplishing a particular task or action. The purpose of the PACE Plan is to provide the means to contact the people needed during an emergency to take the appropriate immediate action to respond to an emergency.
* MTTR – Mean time to Resolution
* IRT – Incident Response Team
* CAL OES – California Governor’s Office of Emergency Services. Referenced in this plan.
* SUNY Broome – State University of New York’s public domain resources were referenced in this plan.

## Policy

### Incident Response Team

The following departments or sections will provide a point of contact who is available on a 24/7 basis to assist with any security incident that occurs:

1. Facilities Manager or Physical Security Office
2. Finance
3. Legal Counsel
4. Operations
5. Technology
6. Information Technology
7. CISO
8. Public Affairs, Marketing, or Communications
9. Internal Audit
10. Governance and Compliance
11. Other departments as required

If the appointed contact is not available, the department or section lead becomes the assisting party until another member of their department or section is replaced.

*A list of contact information is available here: [LINK\_TO\_IRT\_STAKEHOLDERS]*

### Incident Response Team Notification

In collaboration with other departments, the information security team will establish a PACE plan for notifying all members, participants, or stakeholders of an incident response team in case of a security incident. Stakeholders may include third parties such as an outsourced SOC, IR team, MSSP, etc.

All potential members, participants, or stakeholders of an IRT will be familiar with the notification PACE plan and have appropriate personnel prepared to utilize any applicable services indicated.

Each department contributing a member to the IRT will establish an alias, distribution list, or equivalent that complies with the PACE Plan and notifies the appropriate individual assigned to IRT duty in case of an IRT notification.

*The IRT Notification PACE Plan can be found here: [LINK\_TO\_PACE\_PLAN]*

### Incident Response Team Communications

According to a PACE Plan, the incident response team will establish an operations center and connect with communications tools.

A physical operations center will include ample seating, tools for collaboration and presentation, and at least one computer workstation with access to a high-speed internet connection to connect remote participants virtually.

A virtual operations center will enable remote participants to communicate, present information and multi-media, and form semi-private collaboration spaces such as breakout rooms.

*The IRT PACE Plan can be found here: [LINK\_TO\_PACE\_PLAN.]*

**External Points of Contact** - The information security department will maintain the following points of contact and make them available to the IRT:

1. MSP
2. MSSP
3. Internet Service Provider
4. Local FBI
5. Local Law Enforcement’s Computer Crime Department
6. Local CIRT or FIRST
7. Web Host
8. SaaS, IaaS, or other -aaS provider
9. Other Third-Party providers

### Events and Incidents (HIPAA 1.6.1)

The IT Team will respond to alerts and events identified by the end-point detection and response tool and will determine if any alert meets the threshold of a security incident as defined by this policy.

The IT Team will resolve alerts and events, remediating any root causes and tuning tools such that they do not produce false positives.

<<COMPANY>> will use the following definitions of events and incidents following the definitions in NIST 800-61 rev 2:

* **Event** – Any observable occurrence in a system or network, such as a user requesting a web page or a firewall blocking a connection attempt.
* **Adverse event** – an event with a negative consequence like a system crash or unauthorized use of system privileges
* **Incident** – a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. This may include such actions as the threat of or actual use of a Denial of Service (DoS) attack or Distributed DoS (DDoS), or a user hosting illegal content on company resources.

### Triage and Escalation

Not every event turns into an incident. When an event is reported, the first person in the reporting chain with authority to determine if an event meets the threshold of an incident must triage the event (or attempt to correlate seemingly unconnected events) and make a judgment or seek additional information. That person must then document their decision in the appropriate register for tracking.

### Tracking and reports

When an incident occurs, <<COMPANY>> will assign the incident a category and track the incident in accordance with the process section of this appendix.

When tracking or reporting, maintain the following information based on NIST 800-61 rev two and US-CERT Guidelines:

1. The incident category and tracking number
2. The assessed functional impact
3. The assessed information impacts
4. The date and time that the activity was detected and the date and time the activity occurred
5. The number of systems, records, or users impacted.
6. The network and physical location or identification of systems, records, or users impacted.
7. The points of contact for additional follow-up
8. The attack vector or root cause (as known/available)
9. The associated indicators of compromise, including signatures or detection measures developed in relationship to the incident
10. The actions taken to mitigate the incident and recommended actions the client undertake
11. Tracking is essential for reasons such as conducting post-mortem analyses, contributing to a lessons learned repository, identifying attack patterns that can expose insights about the team and the adversary.

### Incident Categories

When categorizing incidents, use the following table:

|  |  |  |  |
| --- | --- | --- | --- |
| Category | Name | Description | MTTR Goal (time from categorization) |
| CAT A | Simulations | -Used to annotate incidents created to test systems and simulate attackers | Not applicable |
| CAT B | Unauthorized Access or Compromised Asset | -A person gains logical or physical access without permission to a client network, system, application, data, or other resource  -Attempted or successful destruction, corruption, or disclosure of sensitive information or intellectual property  -Compromised host, network device, application, user account. This includes malware-infected hosts where an attacker is actively controlling the host (e.g. RAT) | 1-3 Hours |
| CAT C | Denial of Service | -An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.  -Either as victim of or participating in the DoS/DDoS | 3 Hours |
| CAT D | Malware or Malicious Code | -A virus, worm, Trojan horse, or other code-based malicious entity that successfully infects a host.  -This does not include compromised hosts that are being actively controlled by an attacker via a backdoor or Trojan. (See CAT B) | 12 Hours |
| CAT E | Inappropriate Access, Unlawful Activity | -Theft/ Fraud/ Human Safety/ Child Porn. Computer-related incidents of a criminal nature, potentially involving law enforcement. \*NOTE | 24 Hours |
| CAT F | AUP Violation | -A person violates acceptable use of any network or computer use policies. | 24 Hours |
| CAT G | Reconnaissance, Scanning, or Attempted Access | -Any activity that seeks to access or identify a client computer, open ports, protocols, service, or any combination for later exploit.  -This activity does not directly result in a compromise or denial of service. | 72 Hours |
| CAT H | Uncategorized/Under Investigation | -Unconfirmed incidents that are potentially malicious or anomalous activity that warrants further review. | 72 Hours |

\*NOTE - Human safety and human dignity concerns should be reported to law enforcement ASAP: within minutes not hours.

### Categories of Functional Impact

The following define functional impact to <<COMPANY>>’s systems or environments

|  |  |
| --- | --- |
| Category | Definition |
| None | No impact on <<COMPANY>>’s ability to go to market and win |
| Low | Minimal effect: <<COMPANY>> can still go to market but has reduced its competitive edge |
| Medium | <<COMPANY>>’s ability to go to market and win is in question |
| High | <<COMPANY>> is no longer able to go to market and win |

Categories of Information Impact The following table establishes information impact to COMPANY’s systems or environments

|  |  |
| --- | --- |
| Category | Definition |
| None | No impact to CIA or the ability to go to market and win |
| Suspected but not identified | A data loss or impact to availability is suspected, but no direct confirmation exists |
| Privacy Breach | Sensitive personally identifiable information (PII) of employees, customers, clients, or other third party was either accessed or exfiltrated. If you’re unsure, ask your legal team! |
| Proprietary Breach | Proprietary information, such as intellectual property, was accessed or exfiltrated |
| Integrity loss | No longer able to trust either sensitive or proprietary information |

### Reporting Security Incidents (HIPAA 1.6.1)

Any staff member, regardless of department, who discovers a security incident must report it to the IT team.

The IT Team will maintain a telephonic and ticketed system for users to report security incidents. More details about the tools and systems established for reporting may be found here: [LINK\_TO\_REPORTING\_DOCS]

Employees who wish to report an observed incident can submit one by:

* + - 1. Calling (XXX)XXX-XXXX
      2. Emailing IRREPORTEMAIL@IT\_ACCOUNT\_COMPANY.COM
      3. Submitting a ticket at LINK\_TO\_TICKET\_PORTAL

The IRT will track the incident and provide periodic reports to <<COMPANY>> leadership.

### Evidence Retention and Chain of Custody

Evidence or information collected will be tracked by quantity and description. People who have custodial responsibility must execute proper due diligence by securing evidence, limiting access, reporting the evidence under their control when and to whom applicable, and documenting that evidence. If a physical device, description will include:

* + 1. Manufacturer
    2. Model
    3. Serial Number
    4. If evidence is digital or a file, include:
    5. Filename
    6. File hash
    7. Modified, created, and accessed times
    8. File Size

Physical media may also need to be protected with technology such as write-blockers

If evidence is a record of testimony or similar information, include:

1. Name of interviewee
2. Name of interviewer
3. Location obtained
4. Medium used
5. Time collected
6. Signature of both interviewee and interviewer
7. Records of testimony should only be used when legally required or advised by legal counsel.

When evidence is transferred from one party to another, chain-of-custody will be maintained regardless of the reason for transfer. A document must accompany the evidence that maintains the date and time of every transfer, who the evidence was transferred from, and who the evidence was transferred to. For each transfer, transferring and receiving parties will both record:

1. Date and time
2. Name
3. Organization/department
4. Signature
5. Purpose of custody change

### Reporting template

<<COMPANY>> will track all incidents using TICKETING\_SYSTEM\_NAME and will establish a ticket format to capture all the information required by this policy.

Incident Response Tickets will have a category and template that indicates its high priority and is distinct from routine IT support or IT helpdesk tickets.

Should the ticketing system be unavailable for any reason, the following reporting template is provided as an alternative

|  |  |  |
| --- | --- | --- |
| <<COMPANY>> SECURITY INCIDENT REPORT | | |
| Incident Tracking Number |  | |
| Incident Category |  | |
| Functional Impact |  | |
| Information Impact |  | |
| Dates and times | Local | UTC |
| Detected (Local and UTC) |  |  |
| Started (Local and UTC) |  |  |
| Stopped (Local and UTC) |  |  |
| Num. of affected systems, records, or users |  | |
| Summary/Narrative of Incident | | |
|  | | |
| Network location or identification of systems, records, or users impacted | | |
|  | | |
| Attack vector or root-cause analysis | | |
|  | | |
| Associated indicators of compromise | | |
|  | | |
| Actions taken | | |
|  | | |
| Recommended mitigations and/or follow-up actions | | |
|  | | |
| Points of contact for follow-up | | |
|  | | |

### Reporting Incidents to Legal Authority (HIPAA 4.2.4)

<<COMPANY>> will maintain points of contact to report confirmed cybersecurity incidents within 60 days of their discovery to the Federal Government in accordance with HIPAA.

*A list of contact information is available here: [LINK\_TO\_IRT\_STAKEHOLDERS]*

### IR Retainer (HIPAA 1.6.1)

<<COMPANY>> will maintain and outside digital forensics and incident response team on retainer. The IT team and CISO will maintain contact information for the IR team on retainer in the Incident Response Contact Roster

*The Incident Response Contact Roster can be found here: [LINK\_TO\_INCIDENT\_RESPONSE\_CONTACT\_ROSTER]*

## Process

1. When an incident is discovered, the individual who discovers it will report it to the appropriate entity such as the Security team, IT Committee, or CISO via phone, email, or trouble ticket.
2. The notification will immediately alert the information security team or security watch personnel, who will collect the following information and contact the reporter as needed: When notified of a security incident, immediately log the following:
   1. The caller/notifier’s name
   2. Time of notification
   3. The notifier’s contact information
   4. The nature of the incident (collect who, what, when, where, why)
   5. Equipment or persons involved
   6. Location of equipment or persons involved
   7. How the incident was detected
   8. When an event was first noticed indicating that an incident occurred
3. Make an initial determination of the following or add details as appropriate:
   1. Is the equipment, system, or information impacted business critical?
   2. What is the severity of impact or potential category of incident?
   3. Name of the system being targeted, along with the operating system, IP address, and location
   4. Information about the origin of the attack, if possible, including but not limited to IP Address, domain name, or any other information about the origin of the attack.
4. Refer to the IT emergency contact list (Located here: [LINK]) or affected department contact list and call the designated numbers in order on the list.
   1. Use the contact lists to determine both management personnel to be contacted and incident response personnel.
   2. Contact the appropriate incident response personnel using both email and phone messages.
   3. Note the time and manner of each contact
5. The staff member receiving notification will then list all additional parties who may discover the incident and collect their contact information. Parties to contact may include:
   1. Helpdesk
   2. The CISO
   3. Intrusion Detection monitoring personnel
   4. A system administrator
   5. A firewall administrator
   6. A business partner
   7. A manager
   8. The security department or a security person
   9. An outside source

List all parties to contact and determine the contact information for each. Each party should have at least one 24/7 point of contact identified. People outside the IT department likely have different contact procedures than those inside IT.

1. If the event meets the standard of “Incident,” the authority triaging will use the PACE plan to contact appropriate members of the Incident Response Team (IRT) who will convene. Contacted members of the response team will meet physically or virtually via a secure, out of band system, and determine a strategy:
   1. Is the incident real or perceived?
   2. Is the incident still in progress/
   3. What data or property is threatened and how critical is it?
   4. What is the business impact should the attack succeed? See Incident Categories and Categories of Information Impact tables to understand impact. Contact relevant people that may provide more information to severity.
   5. What systems or systems are targeted, where are they physically or on the network?
   6. Is the incident inside a trusted or sensitive network?
   7. Is the response urgent?
   8. Can the incident be quickly contained?
   9. Will the response alert the attacker and do we care?
   10. What type of incident is this?
   11. Who else needs to know?
2. The IRT will create an incident ticket and the incident will be categorized into the highest applicable level as established in the policy section of this appendix.
3. The IRT will begin taking time-stamped notes on the ticket itself (technology permitting).
4. Select the appropriate plan or playbook based on the initial assessment of the incident. If an appropriate plan does not exist, create an initial plan.
   1. New plans created must be documented so that they can be encapsulated after recovery is complete.
5. Notify any additional personnel as appropriate or indicated by the playbook.
6. All incident response team members begin work to contain the incident and gather additional information.
   1. Team members will use forensic techniques, including reviewing system logs, looking for gaps in logs, review intrusion detection systems, and interviewing witnesses and the victim of the incident to determine how the incident occurred.  
        
      *Note: Only authorized personnel appropriate for the situation should perform interviews or examine evidence. If in doubt consult the CISO and legal counsel*.
   2. Forensics evidence and data will be gathered and maintained in accordance with the policy section of this appendix.
7. The incident response team will recommend changes to contain the incident, prevent the incident from impacting further systems, and to prevent the incident from recurring.
   1. All changes will be annotated in the incident response ticket
   2. Management will approve changes, potentially expediting or modifying normal change control processes to appropriately mitigate risks. Any change or departure from normal procedure will be documented in the ticket.
8. If the incident is a system compromise, team members will remediate the incident and restore the affected system(s) to an uncompromised state. They may do one or many of the following:
   1. Re-install and restore data from backups if necessary. Note: Verify if you are required to preserve evidence before executing!
   2. Rotate passwords if there is a reasonable possibility they have been disclosed.
   3. Be sure the system has been hardened by turning off or uninstalling unused services.
   4. Validate appropriate patching levels.
   5. Validate that intrusion detection/EDR/other protections are running.
   6. Validate appropriate logging and reporting.
9. If the incident is a DDoS:
   1. Determine if the Internet provider cut the circuit and why. If they turn the circuit back on and there’s still an ongoing DDoS, the circuit may flop again. This would require scrubbing prior to traffic landing on the circuit.
   2. Determine if the DDoS is a noisy feint designed to take your attention away from a more nefarious goal.
10. If the incident is ransomware, follow your ransomware playbook. This may require:
    1. Contacting outside counsel
    2. Implementing your external Communications Plan
    3. Validating backup integrity
    4. Identifying and remediating root cause
11. All the following will be documented:
    1. How the incident was discovered.
    2. The category of the incident.
    3. How the incident occurred, whether through email, firewall, etc.
    4. Where the attack came from, such as IP addresses and other related information about the attacker.
    5. What the response plan was.
    6. What was done in response?
    7. Whether the response was effective.
12. After documentation is compiled, notify proper external agencies:
    1. If prosecution of the intruder is possible, notify the police or other appropriate agency
    2. Compile a list of all agencies to contact, contact information, and the date/time they were contacted
13. Assess damage and cost to the organization and estimate both the damage cost and the cost of the containment efforts.
14. Review response and update policies. Plan and take preventative steps to prevent re-compromise or the intrusion from recurring.
    1. Consider whether an additional policy could have prevented the intrusion.
    2. Consider whether a procedure or policy was not followed which allowed the intrusion, and then consider what could be changed to ensure that the procedure or policy is followed in the future.
    3. Was the incident response appropriate? How could it be improved?
    4. Was every appropriate party informed in a timely manner?
    5. Were the incident-response procedures detailed and did they cover the entire situation? How can they be improved?
    6. Have changes been made to prevent a re-infection? Have all systems been patched, systems locked down, passwords changed, anti-virus updated, email policies set, etc.?
    7. Have changes been made to prevent a new and similar infection?
    8. Should any security policies be updated?
    9. What lessons have been learned from this experience?

# Appendix F: Disaster Recovery and Emergency Mode Operations Policy and Plan

## Overview and Purpose

The purpose of this policy is to establish necessary steps and mitigation plans in the event of a disaster. This policy will outline data recovery, loss mitigation, and a plan to return to full operating capacity.

## Scope

Employees – This policy applies to all doctors, technicians, managers, leaders, employees, contractors, and third parties who have access to <<COMPANY>>’s IT assets or information and may be bound by contracts or agreements including but not limited to BAAs.

IT Assets – This policy applies to all information assets owned, leased, or otherwise used by <<COMPANY>> or which store <<COMPANY>>’s information.

## Enforcement

Any employee or third-party found to have violated these policies may be subject to disciplinary action which may include termination of employment, contract, or other arrangement.

## Roles and Responsibilities

The CISO or equivalent person designated in writing is responsible for proper implementation of the Information Classification and Handling Policy.

## Acronyms

None for this policy

## Policy (HIPAA 3.1.2)

The meat of the policy

### Backups (1.7.1, HIPAA 1.7.2)

The IT Team will ensure that exact copies of all data on <<COMPANY>>’s systems are backed daily to off-site storage such as cloud storage.

When <<COMPANY>> leverages a cloud, SaaS, or other third-party service to generate, access, and utilize data, including PHI, <<COMPANY>> will rely on that service’s back-up procedures except when they reside on <<COMPANY>>’s premises or networks.

Accordingly, <<COMPANY>> will only select vendors or service providers which have full back ups of at least ePHI and will establish backups for vendor systems present on <<COMPANY>>’s networks.

*For more information on the tools used for backups and third-party services see the software and service inventory.*

### Data restoration (HIPAA 1.7.2, 1.7.4, 2.11)

The IT team will maintain the ability to restore data from back-up exact copies and will rehearse the ability to restore data on several test machines once a quarter.

The same test machines may not be used for two tests in a row.

### Fail-over (HIPAA 1.7.2, 1.7.4)

The IT Team will ensure that <<COMPANY>> has backup internet connections that automatically fail-over in case of an outage.

Fail-over mechanisms will prioritize <<COMPANY>>’s ability to communicate with its cloud providers and then will prioritize the public’s ability to contact <<COMPANY>> such as by browsing <<COMPANY>>’s websites.

Fail-over mechanisms will be tested twice yearly.

### Emergency Communications (HIPAA 1.7.2, 1.7.4)

The IT Team will establish a secure Primary, Alternate, Contingency, and Emergency (PACE) plan for <<COMPANY>> communications during emergencies and ensure that all staff are contactable by all four means of the PACE plan.

The IT Team, in conjunction with the Facilities manager, will ensure that the Emergency Communications PACE Plan is rehearsed with the entire staff twice a year.

*The Emergency Communications PACE Plan can be found here: [LINK]*

### Emergency Operations (HIPAA 1.7.2, 1.7.4)

**Natural Disaster** - <<COMPANY>> designates that it will not provide services to customers during natural disasters including but not limited to weather emergencies. <<COMPANY>> will notify all employees when operations are suspended because of natural disaster or inclement weather using its emergency communications PACE Plan

**Power Outage** – The IT Team will establish a means to maintain power to all Essential and Critical computation equipment in case of a power outage to ensure data and connectivity are not lost for at least 2 hours.

**Cybersecurity Incident (HIPAA 3.1.2)** – During a cybersecurity emergency such as a major outage due to ransomware, <<COMPANY>> will activate incident response, utilize its emergency communication plan to notify employees, and the IT Team will establish a secure means to maintain or replicate the functions of all Essential and Critical Services and to sustain access to PHI.

**Testing and Rehearsal** – Emergency Operations will be rehearsed via tabletop exercise yearly and power outages and cybersecurity incidents will be rehearsed and tested physically yearly.

# Future Appendix’s

Acceptable Use Policy

Remote Working Policy/BYOD Policy

Change Management and Change Control Policy

Business Continuity Policy and Plan

Technical Security Policy

Reputation Management

System Lifecycle Management

# References

US-CERT Federal Incident Notification Guidelines, accessed 13 May 2021. https://us-cert.cisa.gov/incident-notification-guidelines#Standard\_Data\_Elements

CJCSM 6510.01B, 2012. Accessed May 2021. https://www.jcs.mil/Portals/36/Documents/Library/Manuals/m651001.pdf?ver=2016-02-05-175710-897

Cichonski, P., Millar, T., Grance, T. and Scarfone, K. (2012), Computer Security Incident Handling Guide, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.SP.800-61r2 (Accessed May 13, 2021)

Scarfone, K., Grance, T. and Masone, K. (2008), Computer Security Incident Handling Guide, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-61r1.pdf (Accessed May 13, 2021)

FIRST Case Classification Guidelines. Accessed May 2021. https://www.first.org/resources/guides/csirt\_case\_classification.html

fInfoSec Nirvana. Security Investigation Series: Part 2 – Incident Classification. Accessed May 13, 2021). https://infosecnirvana.com/part-2-incident-classification/

FIRST Acceptable Use Policy Template. Accessed 31 January 2022. https://www.first.org/resources/guides/#Acceptable-Use-Policy-Template

Incident Response Policy and Plan. The Department of Housing and Urban Development. Office of the Chief Information Officer. HUD Handbook July 2400.35 2016 REV 1. Accessed February 3, 2022.

California Joint Cyber Incident Response Guide - Cal OES, Incident Response Plan Example Accessed February 3, 2022.

Security Incident Response Plan. SUNY Broome. Accessed February 3, 2022.

Department of Transformation and Shared Services. State of Arkansas. Employee Handbook. Accessed February 3, 2022.

Santa Fe College. Appropriate Use Policy. Accessed February 3, 2022.

Oregon State University. Information Services Divisional Change Management Policy. Accessed Feb 3, 2022.

Albany State University. Information Security Awareness Training Policy. Accessed Feb 3, 2022.