ADDITIONAL PROTECTION REQUIREMENTS UNDER CMG CYBER LIABILITY PROGRAM

Catholic Mutual has partnered with NAS to provide Cyber Liability coverage to all our members with a $250,000 limit. However, quotes can be obtained for additional limits up to $10 million. To help enhance your ability to obtain higher limits, your (Arch) Diocese should implement the following policies/procedures:

- Secured configured firewall protection throughout your (Arch) Diocese. See enclosed:
  - Sample Data Security Policy

- Anti-virus software updated on a monthly basis on all desktops, portable devices and mission critical servers. See enclosed:
  - Sample Protection against Malicious Programs Policy

- Privacy and security policies in place that addresses mandatory training that is followed by employees, contractors and other individuals with access to private medical or financial information. See enclosed:
  - Sample Information Security Policy
  - Organization Acceptable Use Policy

- All stored personal and/or confidential data on portable devices, including laptops, PDAs, back-up tapes, USB thumb drivers and external hard drives must be encrypted to industry standards. See enclosed:
  - Sample Removable Media Policy

- HIPAA program must be in place for any organization required to follow HIPAA compliance. See enclosed:
  - Information Access Management Policy

In addition, the following security needs to be in place to order to be considered for the PCI – DSS Assessment Coverage Endorsement (Coverage for fines and penalties levied by the Payment Card Industry Data Security Standards against merchants due to PCI DSS non-compliance) and Cyber Crime Coverage Endorsement (financial fraud, telecommunications fraud and phishing attacks):

- All processing, storing, transmitting or handling of credit or debit card data must have data security controls that are compliant with the Payment Card Industry Data Security Standards. See enclosed:
  - Sample Payment Card Information Security Policy

- Wire transfer protocols must prohibit one employee from controlling a transaction from beginning to end.

For additional information, please see the Cyber Liability Risk Management section on your Member Home page.

Sample Data Security Policy

Introduction

This Data Security Policy must be understood and followed by all Company employees.

Company data (including data collected or stored relating to clients, customers, patients, employees, etc.) is a valuable Company asset and must be protected. The Company depends on its information systems and, thus, data security is critical.

Data security flows from controlling unauthorized access to data. Breaches in data security poses risk (1) to the Company's ability to service its customers [clients or patients]; (2) of lost revenue through fraud or destruction of proprietary or confidential data; (3) of violation of business contracts, trade secrets, and customer [or patient] privacy; (4) of reduced credibility and reputation with its customers [clients or patients], shareholders and partners.

The goal is to ensure that data is protected in all of its forms, on all media, during all phases of its life cycle, from unauthorized or inappropriate access, use, modification, disclosure, or destruction.

This policy applies to all of our electronic data and all customer electronic data collected, stored or processed by the Company.

This policy will better define the overall objective which is to make all data and data processing resources accessible only on a need to know basis to specifically identified, authenticated, and authorized users or entities. Of course, public data is outside the scope of this policy.

Compliance with this policy is a condition of employment for employees. [Compliance with this policy may also be a contractual agreement for vendors, suppliers, and third party processor or agents, (collectively, "vendors". But, consider the use of a "Data Privacy & Security Agreement" with vendors.] All employees must read the policy completely, and confirm that they understand the contents of the policy and agree to abide by it.

Breach of Policy and Enforcement

Violation of this policy will result in disciplinary action up to and including termination. All employees are bound by this policy and are responsible for its enforcement.

Scope of the Policy

This policy applies to all Company and customer data that is collected or stored on any IT Asset owned by the Company, or its employees, or a third party on behalf of the company (sometimes referred to as "covered data"). IT Assets include computer hardware (e.g., sub-networks, application servers, file servers, workstations, data, etc.) and application software configured for the purpose of processing, handling, storing, transmitting, and receiving data.

This policy applies to any person or entity that collects or stores covered data related to the Company or its customers [client or patients], current or former employees, and any personal or medical information concerning any person, including full-time or part-time employees, vendors or processors who have access to such data, and other persons, entities, or organizations that have access to such data.

Data Transmission

Employees who access covered data must transmit such data in compliance with this policy. As necessary, communications included covered data must be encrypted during transmission.

Other countries (e.g. the European Union) have different, and often more stringent, privacy laws that apply to information related to individuals ("personal information"). Employees that plan to communicate personal information outside the United States must comply with the laws of the jurisdiction in which recipient of the communication resides.

Data Storage

Employees are responsible for the secure storage of covered data, including customer data, and must do so in compliance with this policy. As necessary, data stored must be secured with encryption. Access control mechanisms must be used to limit access only to authorized users.

Data Disposal

Access control mechanisms must be used to ensure that only authorized users can access covered data during the disposal process. Employees must follow the Company's procedures for the proper disposal of various types of data.

Data Security Policy Statement

This policy is designed to educate Company users [and vendors] about their obligation for protection all covered data; to ensure the security, integrity, and availability of all covered data; and to establish the Company's baseline data security stance and classification system.

Data Security Responsibilities

All managers and supervisors must strive to ensure compliance with this policy by (1) helping each other understand and comply with the requirements herein, and (2) overseeing staff to ensure Company employees understand and comply with the requirements herein.

The Company may establish a Data Security Team that is responsible for:

- Defining the security requirements, controls and mechanisms applicable to all covered data.
- Defining the methods and guidelines used to identify and classify all covered data.
- Defining the procedures for identifying data owners for all covered data.
- Defining the labeling requirements for all covered data.
- Defining all other data security usage, processing, transmission, storage and disposal processes and procedures.
- Defining the procedures necessary to ensure compliance to this policy by all Company users [and vendors].
- Facilitating the evaluation of new regulatory, legal, and also best practice requirements as they are mandated or become recognized in industry.

Documentation

This policy requires procedures be developed, managed and performed. Thus, written documentation must be developed for all procedures necessary to comply with this policy including:

- The management of all userids and passwords on IT Assets;

- The management of all access control lists on all IT Assets;
- The execution and review of all audit trails;
- All incident response and reporting; and
- All other tasks necessary to support this policy.

Policy Review

This policy should be reviewed on a regular basis because of the dynamic nature of the Internet and data security threats. Accordingly, the Company's CEO [or insert CFO, COO, or other senior management officer] shall determine reasonable schedule for review of this policy and include other senior management, systems administration, and legal counsel in the review process.

Data Classification

Data classification is necessary to enable the allocation of resources to the protection of covered data, as well as determining the potential loss or damage from the corruption, loss or disclosure of data.

To ensure the security and integrity of all data the default data classification for any covered data is either "Sensitive Personal Information" or "Proprietary Company Data".

The Data Security organization is responsible for evaluating the data classification system and reconciling it with new data types as they enter usage. It may be necessary, as we enter new business endeavors, to develop additional data classifications. All covered data must fall into one of the following categories:

Public Company Data – Public company data is defined as data that any entity either internal or external to the Company can access. The disclosure, use or destruction of Public company data will have limited or no adverse affects on the Company nor carry any significant liability. (Examples of Public company data include readily available news, stock quotes, or sporting information.)

Proprietary Company Data – Proprietary company data is any information that derives its economic value from not being publicly disclosed. It includes information that the company is under legal or contractual obligation to protect.

The value of Proprietary Company Data to the Company would be destroyed or diminished if such information were disclosed to others. Most of the Company's sensitive information should fall into this category. Proprietary Company Data may be copied and distributed within the Company only to authorized users. Proprietary Company Data disclosed to authorized external users must be done so under a non-disclosure agreement. (Examples of Proprietary Company Data include company policies, sales plans, and application source code.)

Confidential Company Data – Confidential Company Data is information that is not to be publicly disclosed, regardless of its economic value. The disclosure, use, or destruction of Confidential Company Data can have adverse affects on the Company and possibly carry significant civil, fiscal, or criminal liability. This designation is used much less frequently. It is used for highly sensitive information whose access is restricted to selected, authorized employees. The recipients of confidential information have an obligation not to reveal the contents to another individual unless that person has a valid need to know for the information. Confidential Company Data must not be copied without authorization from the identified owner. (Examples of Confidential Company Data include company strategic plans or cryptographic keys.)

Sensitive Personal Information – Sensitive Personal Information is defined as data that only authorized internal Company entities or specific authorized external entities can access. The disclosure, use, or destruction of Sensitive Personal Information can have adverse affects on the Company and its relationship with its customers, and possibly carry significant liability for both. Sensitive Personal

Information is entrusted to and may transit or is stored by the Company (and others) over which they have custodial responsibility but do not have ownership. (Examples of Sensitive Personal Information include customer bank or brokerage account information, cryptographic keys, or other data considered private.)

Public Customer Data – Public customer data is defined as data that any entity either internal or external to the Company can access. The disclosure, use, or destruction of Public customer data will have limited or no adverse affects on the Company or its customer, and carry no significant liability. Public customer data is entrusted to, and may transit or be stored by the Company (and others) over which they have custodial responsibility but do not have ownership. (Examples of Public customer data include emails, public key certificates or other customer data that is readily available through other public channels or records.)

Data Ownership— In order to classify data, identify the owner of all covered data. The owner of data is responsible for classifying their data according to the classification system noted in this policy. If an owner cannot be determined for covered data, the Data Security organization must act as its custodian.

The default classification for all data not classified by its owner must be either "Sensitive Personal Information" or "Proprietary Company Data". The Data Security organization is responsible for developing, implementing, and maintaining procedures for identifying all data assets and associated owners.

The owner of all Sensitive Personal Information is the individual owner who generates or is assigned ownership of that data. (Data such as public key certificates generated by an external Certificate Authority but assigned to a specific customer are considered owned by that customer.)

Non-disclosure Agreements

If covered data needs to be released to entities outside of the Company, and a legitimate business reason exists for releasing the information, a written Non-Disclosure Agreement (NDA), requiring the data recipient's agreement to maintain that data in confidence and restrict its use and dissemination, must be obtained before disclosing the data.

I HAVE READ THIS DATA SECURITY POLICY CAREFULLY, AND UNDERSTAND AND ACCEPT THE OBLIGATIONS THAT IT IMPOSES UPON ME, WITHOUT RESERVATION. I UNDERSTAND THAT VIOLATION OF THIS POLICY WILL RESULT IN DISCIPLINARY ACTION UP TO AND INCLUDING TERMINATION.

Employee Signature: _____ Date: ___ / ___ / _____

Print Name: _____

Sample Protection against Malicious Programs Policy

Establishment date, effective date, and revision procedure

This policy was established and approved by [Organization Name] on mm,dd,yyyy. The [Organization Name] Information Security department shall review this policy at least once a year, and at any additional time when there are changes that may affect corporate management with respect to Information Security. In the event that amendment or repeal of this policy becomes necessary as a result of such review, the [Organization Name] Information Security department shall prepare a draft and apply for authorization, and with prior confirmation of the Executive(s) in charge of the area(s) that will be affected by amendment or repeal, the [Organization Name] CISO/Security Director will authorize the amendment or repeal.

Table of revision history

Version	Date	Details of change	Issued by	Approved by

Overview

Effective protection against malware is critical to protecting [Organization Name]'s sensitive information and information assets. The introduction of malicious software into the organization's system could result in significant losses including loss of sensitive information, inoperability, reputational harm, and potential legal exposures. A such, it is critical to persevere the integrity of organizational systems.

Purpose

The purpose of this policy is to establish the requirements for anti-malware and spyware protection on [Organization Name] Personal Computers (PCs) and servers.

Scope

This policy applies to employees, contractors, consultants, volunteers, temporary and other workers at [Organization Name], and all personnel affiliated with company subsidiaries or third parties. This policy applies to all equipment that is owned or leased by, or otherwise in the custody or control of, [Organization Name].

Policy

Malicious Software

Malicious software is defined as all software that has been deliberately designed to harm or abuse the resources of computing systems. It is frequently concealed within, or masquerades as, legitimate software.

Malicious software includes, but is not limited to, viruses, Trojan horses, worms, logic bombs, file infectors, malicious macros, malicious scripts (e.g. Java, ActiveX), malicious cookies, key loggers, and hidden software for launching denial-of-service attacks.

Protection of PCs and Portable Devices

The organization's IT Department shall take appropriate measures to protect computers and portable devices against malicious software. Appropriate measures include the following:

- All information systems should have an anti-virus application installed that offers real-time scanning protection to files and applications running on the target system. All anti-virus software must be approved by the Chief Information Officer [*or person of similar role within the organization*].
- Where operationally possible, organizational PCs should be protected by an automated process that maintains the latest versions of approved anti-virus software.
- DAT files should be automatically updated with the latest virus definitions immediately after their release.
- Organizational PCs should be scanned at least once a week.
- Users should report any suspected infection that has not been cleaned or quarantined to their IT Helpdesk and follow the instructions received.
- Antivirus administrators should verify that all organizational PCs have been updated with the latest version of DATs.

- Virus scanning software should be set to automatically clean or delete infected files. If the virus scanning program is unable to clean/delete an infected file, the file that is infected should be quarantined for further review by the administrators.
- All incoming and outgoing email and attachments should be scanned for infections prior to being received by the user or being sent from the organization's system.
- Personal firewalls and anti-spyware should be implemented where network firewalls or an Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) are not implemented.

Under no circumstances may any user disable anti-virus software or any of its processes without the express authorization of [Organization Name]'s IT department. IT personnel should supervise any disablement of anti-virus protection and such disablement should be for the shortest time possible in order to accomplish the needed objective.

Protection of Servers

[*Organization Name's*] IT Departments shall take appropriate measures to protect servers against malicious software. Appropriate measures include the following:

- All servers should have an anti-virus application installed that offers real-time scanning protection to files and applications running on the target system. All anti-virus software must be approved by the Chief Information Officer [*or person of similar role within the organization*].
- Servers should be protected by an automated process that maintains the latest versions of approved anti-virus software.
- Severs should be equipped with an IDS or IPS, where possible.
- The DAT file should be distributed immediately upon release by the antivirus vendor.
- Antivirus administrators should verify that all servers have been updated with the latest version of DATs.
- Virus scanning software should be set to automatically clean or delete infected files. If the virus scanning program is unable to clean/delete an infected file, the file that is infected should be quarantined for further review by the administrators.
- Mail servers should have either an external or internal anti-virus scanning application that scans all mail going to or coming from the mail server.
- Local anti-virus applications may be disabled during backups only where an external anti-virus application continues to scan inbound emails and network traffic while the backup is being performed.

Non-Compliance

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

Sample Information Security Policy

Establishment date, effective date, and revision procedure

This policy was established and approved by [Organization Name] on mm,dd,yyyy. The [Organization Name] Information Security department shall review this policy at least once a year, and at any additional time when there are changes that may affect corporate management with respect to Information Security. In the event that amendment or repeal of this policy becomes necessary as a result of such review, the [Organization Name] Information Security department shall prepare a draft and apply for authorization, and with prior confirmation of the Executive(s) in charge of the area(s) that will be affected by amendment or repeal, the [Organization Name] CISO/Security Director will authorize the amendment or repeal.

Table of revision history

Version	Date	Details of change	Issued by	Approved by

Overview

Purpose

The purpose of this policy is to describe [*Organization Name*]'s commitment, and the commitment of its management, to preserving the confidentiality, integrity, authenticity, and reliability of business-related information in the possession or control of the company and/or any of its employees, agents, contractors, subsidiaries, or affiliates, through the establishment of a comprehensive information security program.

Scope

This policy applies to employees, contractors, consultants, volunteers, temporary and other workers at [*Organization Name*], and all personnel affiliated with company subsidiaries or third parties. This policy applies to all equipment that is owned or leased by, or otherwise in the custody or control of, [*Organization Name*].

This policy applies to the use of all information, electronic and computing devices, and network resources used by [*Organization Name*] to conduct business or interact with internal networks and business systems, whether owned or leased by, or otherwise in the custody or control of, [*Organization Name*], the employee, a company subsidiary, or a third party.

Definitions

Information Security: As used in this Policy, *information security* means the preservation of the confidentiality, integrity, authenticity, and reliability of information through safeguards designed to protect against any unauthorized access, use, modification, or disclosure.

Executive Management: As used in this Policy, *executive management* means all directors and officers of the organization.

Policy

[*Organization Name*] and its executive management recognize the importance of managing information security risk across all levels of the organization in a manner that aligns with organizational principles, goals, and business continuity and processes. Executive management will set the organization's risk tolerance and implement policies and procedures that effectuate the organization's information security interests and align with its risk appetite. Accordingly, policies and procedures will be enacted that address the following:

1. Management of all user IDs and passwords on IT Assets;
2. Management of all access control lists on all IT Assets;
3. Execution and review of all audit trails;
4. Incident response and reporting; and
5. All other tasks necessary to support this Policy.

[*If the organization handles protected heath information and is covered by HIPAA and its regulations, the following policies and procures should be included: Workforce Security and Information Access Management Policy; Sanction Policy; Information System Activities Review Procedures; Data Backup Plan; Disaster Recovery Plan; Emergency Mode Operations Plan; HIPAA Physical Safeguards Policy; and HIPAA Technical Safeguards Policy.*]

Executive management may enact additional policies and procedures in its discretion in order to provide the appropriate level of protection to business-related information in the possession or control of the company and/or any of its employees, agents, contractors, subsidiaries, or affiliates.

Framework of [*Organization Name*]'s Information Security Program

In order to effectively manage risk to information security, [*Organization* Name] will provide for the following safeguards:

1. *Access control and user authentication management.* Physical and technological access control will be implemented to provide only authorized users with access to sensitive business information, systems, and networks for legitimate business purposes.

2. *System and network monitoring*. All systems and networks will be monitored through review of access logs, activity logs, fault logs, and privileged operations in order to detect any suspicious activity that could signal internal abuse of access rights or the presence of an intruder.

3. *Ongoing assessment of information security risk*. Risk assessments will be conducted to identify newly developed or developing vulnerabilities in systems and networks and to determine what modifications if any should be made to existing information security safeguards. As part of such assessments, information classifications shall be reviewed to ensure such classes are appropriate for the level of risk associated with the information.

4. *Employee training and awareness*. All employees will be trained on basic information security such as recognition of social engineering schemes (e.g., phishing and spear phishing), authorized uses and disclosures of information, and proper transmission, storage, and disposal/destruction of data. Employees will be responsible to secure transmission and storage of sensitive data through encryption or other appropriate means where required by data class or law.

5. *Compliance with legal obligations*. The information security program will provide an awareness of and take into consideration federal and state laws and contractual obligations.

6. *Vendor Management.* Whenever confidential or sensitive data is released to entities outside of the organization, and a legitimate business reason exists for releasing the information, a written Non-Disclosure Agreement (NDA), requiring the data recipient's agreement to maintain that data in confidence and restrict its use and dissemination, will be obtained before disclosing the data. Ongoing assessment of vendor relationships and vendor compliance with existing NDA's and other agreements will be conducted by the relevant vendor owners.

7. *Information security incident preparedness.* Detailed procedures will be in place to manage and direct the organization's response to an information security incident including designation of an Incident Response Team and the role of each team member.

8. *Business Continuity Plan*. Information security will be coordinated to effectuate and further the goals of the organization's business continuity plan.

9. *Sanctions for violations*. Appropriate disciplinary action will be brought against any employee, agent, contractor, or affiliate of the organization who violates the terms of any of the organizations information security policies, including possible termination of employment or expulsion from the organization's premises.

Additional safeguards may be necessary to protect assets of greater criticality, or where, after conducting a risk assessment, it is determined that the current information security program is insufficient to protect the organization's information, systems, and/or networks commensurate with the organization's risk tolerance.

Information Security Roles and Responsibilities

Information Security will be primarily managed by [*Organization Name*]'s Chief Information Officer, Chief Information Security Officer, and Information Technology personnel [*or other persons with similar roles*]. Individual department managers will be responsible for ensuring that employees within their departments are complying with [*Organization Name*] information security policies and procedures. Responsibilities of those in information security roles will include:

1. Fostering an organizational climate where information security is prioritized and considered in the context of business continuity and objectives.

2. Defining the security requirements, controls and mechanisms applicable to all covered data.

3. Defining the methods and guidelines used to identify and classify all covered data.

4. Defining the procedures for identifying data owners for all covered data.

5. Defining the labeling requirements for all covered data.

6. Defining all other data security usage, processing, transmission, storage and disposal processes and procedures.

7. Assisting department managers and supervisors to better understand how information security risks associated with their systems translate to organization-wide risk.

8. Providing ongoing assessment of the risk to the organization's information, systems, and networks.

9. Monitoring the organization's systems and networks for questionable activity.

10. Defining the procedures necessary to ensure compliance to this policy by all organization users and vendors.

11. Ensuring all members of executive member remain apprised of the organization's information security posture and any developing risks.

12. Assisting in the organization's ongoing compliance with state and federal law and other legal obligations.

13. Working with other Incident Response Team members to respond to, contain, and eradicate information security incidents.

Policy Compliance

Compliance Measurement

Compliance with this policy will be verified by the [*Organization Name*] through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the [Policy Owner].

Exceptions

Any exception to the policy must be approved by the [Policy Owner] in advance.

Non-Compliance

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

By signing below, I acknowledge that I have read and fully understand my obligations under this Policy and hereby agree to abide by its terms.

_____ _____

Name Date

Important Note to User: This is a sample agreement is not a "one-size-fits-all" and should not be used by any organization without review and modification to fit the needs of such organization. Organizations should cross-reference with relevant existing policies where appropriate, comparing against relevant policies (e.g. mobile device and acceptable use policies), ensuring terms are defined consistently across policies. Additional changes to this agreement may be necessary to account for varying individual organizational security needs and user privacy expectations. In addition, while efforts have been made to ensure that the terms of this policy comply with employee rights under the National Labor Relations Act, this is a contentious and ever changing area of the law, and therefore total compliance cannot be guaranteed. **Delete this note before publishing.**

Sample Organization Acceptable Use Policy

Establishment date, effective date, and revision procedure

This policy was established and approved by [Organization Name] on mm,dd,yyyy. The [Organization Name] Information Security department shall review this policy at least once a year, and at any additional time when there are changes that may affect corporate management with respect to Information Security. In the event that amendment or repeal of this policy becomes necessary as a result of such review, the [Organization Name] Information Security department shall prepare a draft and apply for authorization, and with prior confirmation of the Executive(s) in charge of the area(s) that will be affected by amendment or repeal, the [Organization Name] CISO/Security Director will authorize the amendment or repeal.

Table of revision history

Version	Date	Details of change	Issued by	Approved by

Overview

Effective information security requires the support and participation of all employees and affiliates of [Organization Name] who deal with company information and/or information systems. All computer users within the company are responsible for reading and following the guidelines set forth below. Pease review your Employee Handbook for further details.

Purpose

This policy describes the acceptable use of [Organization Name]'s computer equipment. By complying with the directives set forth below, employees help to protect [Organization Name] from risk of malware attacks, compromise of network systems and services, and legal liability.

Scope

This policy applies to employees, contractors, consultants, volunteers, temporary and other workers at [Organization Name], and all personnel affiliated with company subsidiaries or third parties. This policy applies to all equipment that is owned or leased by, or otherwise in the custody or control of, [Organization Name].

This policy applies to the use of all information, electronic and computing devices, and network resources used by [Organization Name] to conduct business or interact with internal networks and business systems, whether owned or leased by, or otherwise in the custody or control of, [Organization Name], the employee, a company subsidiary, or a third party.

Policy

All employees, contractors, consultants, volunteers, temporary and other workers at [Organization Name], and all personnel at company subsidiaries and third-parties are responsible for exercising good judgment regarding appropriate and reasonable use of information, electronic devices, and network resources in a manner that complies with [Organization Name]'s policies and procedures, and local laws and regulations.

General Use and Ownership

1. [Organization Name]'s proprietary information created and/or stored on electronic and computing devices whether owned or leased by, or otherwise in the custody or control of, [Organization Name], the employee, or a third party, remains the sole property of [Organization Name].

2. Employees have a responsibility to promptly report the theft, loss or unauthorized disclosure of [Organization Name] trade secrets, or proprietary or confidential information such as information relating to product development, organizational security measures, and business, financial, or marketing strategies.

3. Employees may access, use or share [Organization Name]'s trade secrets and proprietary information such as customer lists and contact information, development of systems, processes, products, know-how, technology and internal reports and procedures, only to the extent it is authorized and necessary to fulfill their assigned job duties or in limited circumstances where such access, use, or disclosure is protected under the National Labor Relations Act and is compliant with applicable laws.

4. All employees are responsible for exercising good judgment regarding the reasonableness of their personal use. Individual departments are responsible for creating their own guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such guidelines, employees should consult their supervisor or manager.

5. All information considered sensitive or vulnerable must be encrypted. Such information includes but is not limited to employee personal information, customer lists and contact information, and [Organization Name] trade secrets and proprietary or confidential information.

6. In order to maintain the security and integrity of company systems and networks, authorized individuals within [Organization Name] may monitor electronic and computing equipment, systems, and network traffic at any time.

7. [Organization Name] reserves the right to audit all electronic and computing equipment, networks, and systems on a periodic basis to ensure compliance with this policy.

8. Employees and users of [Organization Name] equipment are expected to take charge of their own training by attending in-house classes provided by the IT department, and reviewing and becoming familiar with software documentation.

Security and Proprietary Information

1. Mobile and computing devices that connect to the internal network will be limited to the minimum access necessary to conduct business in order to protect [Organization Name]'s sensitive, proprietary, or confidential information from potential compromise. However, nothing in this paragraph shall be construed to interfere with or restrict employee rights under the National Labor Relations Act.

2. All system level and user level passwords must comply with the security requirements of the *Access Control Policy*. Employees are prohibited from providing any other individual access to company networks and systems, either intentionally or through failure to take reasonable steps to secure their access.

3. All computing devices must be secured with a password-protected screensaver that activates automatically after 10 minutes or less. Employees must manually lock the screen or log off when leaving their computing device unattended.

4. Employees must use extreme caution and comply with the safeguards in [Organization Name]'s *Email Policy* when opening e-mail attachments received from unknown senders, which may contain malware.

5. Employees must safeguard all [Organization Name] equipment assigned to their exclusive or shared use, and all [Organization Name] equipment within their work area.

6. Employees traveling with [Organization Name] laptop computers must always carry them in carry-on baggage and not in checked baggage.

Unacceptable Use

The following activities are prohibited. Employees may be exempted from certain restrictions where required to engage in legitimate job responsibilities (e.g., systems administration staff may need to engage in specified restricted activity in order to test company security vulnerabilities or to disable the network access of a host if that host is disrupting production services). Employees may also be exempted from specific restrictions in limited circumstances where activities are protected by the National Labor Relations Act.

Employees are prohibited from engaging in any activity that is illegal under local, state, federal or international law while utilizing [Organization Name]-owned resources.

The lists below are not exhaustive, but attempt to provide guidance on what activities fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited:

1. Violating the rights of any person or company protected by copyright, trade secret, patent or other intellectual property laws and regulations, including, but not limited to, installing or distributing "pirated" or other software products for which the [Organization Name] lacks an appropriate license.

2. Unauthorized and unlawful reproduction of materials protected by copyright including activities such as digitization and distribution of photographs from magazines, books, online databases, or other similar copyrighted sources, copyrighted music, and the installation of any copyright protected software for which [Organization Name] or other end user lacks a valid license.

3. Accessing data, a server or an account for any purpose other than conducting [Organization Name] business or for limited activities protected by the National Labor Relations Act, such as union organizing or other protected concerted activities.

4. Exporting technical information, software, or encryption software or technology, in a manner prohibited by international or regional export control laws. Employees should consult management prior to exporting any material that is in question.

5. Introducing malicious programs into company networks or servers (e.g., viruses, worms, Trojan horses, e-mail bombs, suspicious packers, etc.).

6. Disclosing account passwords to others or allowing others to access and use your account in any manner. This includes access or use by family and other household members when working from home.

7. Using a [Organization Name] computing device to procure or transmit material that is in violation of the organization’s anti-discrimination and harassment policies and state and federal laws.

8. Using any [Organization Name] account to make fraudulent offers of products, goods, or services.

9. Making statements about warranty, expressly or implied, of any product, good, or service unless such statements are part of legitimate job duties.

10. Effecting security breaches or disruptions of network communication or services. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless such activities are within the scope of regular business duties or otherwise permitted by law. For purposes of this section, "disruption" includes, but is not limited to, bulk email or spam, denial of service, packet spoofing, network sniffing, pinged floods, and forged routing information for malicious purposes.

11. Using any form of network monitoring that intercepts data not intended for the employee's host, unless this activity is a part of legitimate job duties.

12. Bypassing user authentication and/or security of any host electronic or computer device, network, or account owned by [Organization Name].

13. Disabling anti-virus software on workstations or devices.

14. Interfering with or denying service to another user's host (for example, denial of service attack).

15. Sending any messages such as programs, scripts, or commands with the intent to cause interference of, or disable, a user's terminal session, by any means, whether locally or via the Internet/Intranet/Extranet.

16. Disclosing information about, or lists of [Organization Name]'s employees to customers, competitors, or other similar parties outside of [Organization Name].

17. Hacking systems and databases or acting to disrupt systems or cause unnecessary network congestion or application delays.

18. Using remote control or remote access software on any internal or external host personal computers or systems not specifically set up by the IT staff.

19. Using [Organization Name] equipment for personal profit, political fundraising, gambling activity, non-business-related instant messaging or chat room discussions, or downloading or displaying of offensive material, unless such fundraising or messaging activity is for the limited purpose of exercising employee rights under the National Labor Relations Act, such as union organizing or other protected concerted activity.

20. Browsing pornographic, offensive, or otherwise undesired and questionable sites on the internet which may result in introduction of malicious programs into the company's network or server.

Email and Communication Activities

Employees are perceived to represent the company when they use company resources to access the Internet. To avoid confusion, during online communications unrelated to legitimate work responsibilities, whenever employees state an affiliation to the company, they are encouraged to clearly indicate the following: "I do not represent the company in any manner. Any opinions

expressed on this matter are my own and not necessarily those of the company". However, such disclosure is not required for limited communications protected by the National Labor Relations Act. Questions concerning such disclosures should be addressed to the IT or HR Departments.

The following email activities are strictly prohibited:

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam), except in limited circumstances where such communication is protected by the National Labor Relations Act, such as union organizing or other protected concerted activity.

2. Any form of unlawful harassment via email, telephone or paging, whether perceived as harassment through language, frequency, or size of messages.

3. Unauthorized use, misappropriation, or forging of information in email headers.

4. Solicitation of emails for another email address, other than that of the poster's account, with the intent to unlawfully harass or collect replies.

5. Creating or forwarding harassing and unwanted "chain letters", "Ponzi", or other "pyramid" schemes of any type regardless of content, sources, or destinations. Nothing in this paragraph will be construed to limit employees from engaging in legitimate protected concerted activity under the National Labor Relations Act.

6. Posting [Organization Name] proprietary or confidential information such as product development, organizational security measures, and business, financial or marketing strategies to external newsgroups, bulletin boards, or other public forums without authority.

7. Any use of unsolicited emails obtained from within [Organization Name]'s networks that were sent by other Internet/Intranet/Extranet service providers on behalf of, or to advertise, services hosted by [Organization Name] or connected via [Organization Name]'s network.

8. Posting non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam) or other similar abusive tactics.

Blogging and Social Media

1. Blogging by employees, whether using [Organization Name]’s property and systems or personal computer systems, when used to carry out job responsibilities, is also subject to the terms and restrictions set forth in this Policy. Limited and occasional use of [Organization Name]’s systems to engage in blogging related to legitimate job-related responsibilities is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate [Organization Name]’s policy, is not detrimental to [Organization Name]’s best interests or image, and does not interfere with an employee's regular work duties. However, nothing in this paragraph shall be construed to limit employees’ rights to discuss the terms and conditions of their employment or to engage in other legitimate protected concerted activities under the National Labor Relations Act. Employees should also note that blogging from [Organization Name]’s systems is subject to monitoring.

2. Employees shall not engage in any blogging whether during the course of business duties or after working hours that unlawfully defames or maligns the image, reputation and/or goodwill of [Organization Name] and/or any of its employees. Employees are also prohibited from making

any discriminatory, disparaging, defamatory, harassing, or otherwise unlawful comments when blogging, or otherwise engaging in any conduct prohibited by [Organization Name]'s *Anti-Discrimination and Harassment* policy.

3. Employees may not hold themselves out as representatives of the company or attribute personal statements, opinions or beliefs to [Organization Name] when engaged in blogging or posting to newsgroups, or other social media. If an employee expresses his or her beliefs and/or opinions in blogs or social media posts, the employee is encouraged to disclose the following: "I do not represent the company in any manner. Any opinions expressed on this matter are my own and not necessarily those of the company". However, where engaging in limited activity protected by the National Labor Relations Act, such as discussing terms and conditions of employment, employees need not provide such disclosure. Employees who engage in blogging outside the scope of their job duties assume any and all associated risk.

4. [Organization Name]'s Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any [Organization Name] confidential or proprietary information or trade secrets such as product development, organizational security measures, and business, financial or marketing strategies, or any other material designated as confidential when engaged in blogging.

5. In addition to following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, [Organization Name]'s trademarks, logos and any other [Organization Name] intellectual property may also not be used in connection with any blogging activity except in limited circumstances where such use is protected by the National Labor Relations Act. In all circumstances, employees must comply with all applicable copyright, trademark, and other similar intellectual property laws.

Policy Compliance

Compliance Measurement

Compliance with this policy will be verified by [Organization Name] through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the [Policy Owner].

Exceptions

Any exception to the policy must be approved by the [Policy Owner] in advance.

Non-Compliance

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

Information Access Management Policy

PURPOSE
In recognition of the critical role that information systems play in COMPANY Corporation ("COMPANY") business activities, this policy defines the Health Insurance Portability and Accountability Act (along with its subsequent amendments "HIPAA") Security Rules Administrative Safeguards (45 C.F.R.164.308) and other requirements necessary for the secure handling and storage of electronic protected health information ("ePHI"). This policy defines administrative safeguards that everyone at COMPANY is expected to be familiar with and to consistently follow.

Note: HIPAA Policies and supporting documents are supplemental to COMPANY's Employee Handbook, the terms of which are incorporated herein by reference, and is intended to be read in concert with the same. In the event any terms appear to conflict, please see your supervisor for clarification.

SCOPE
These policies apply to all COMPANY Personnel.

COMPANY's Information Security Officer ("ISO") owns and is responsible for updates, enforcement, and exceptions and may be appropriately delegated only to specified, qualified individuals. Department heads are responsible for ensuring their department Personnel are complying with all applicable policies and procedures, addressing non-compliance, and informing the ISO (or delegate) of issues when appropriate.

DEFINITIONS
COMPANY means COMPANY Corporation.

HIPAA means the Health Insurance Portability and Accountability Act, along with its subsequent amendments.

Personnel means all employees, consultants, contractors, and volunteers who perform work directly for COMPANY and not through an intermediary.

PHI means protected health information as defined under HIPAA.

POLICY
"Required" and "Addressable" are defined under HIPAA.

Company shall implement policies and procedures to prevent, detect, contain, and correct security violations. 45 C.F.R.164.308(a)(4).

COMPANY shall implement policies and procedures for authorizing access to ePHI that are consistent with the applicable requirements of the HIPAA Privacy Rule.

Specifically, COMPANY shall undertake the following activities and processes:

- Isolating health care clearinghouse functions (Required). If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the ePHI of the clearinghouse from unauthorized access by the larger organization.

- Access authorization (Addressable). Implement policies and procedures for granting access to ePHI, for example, through access to a workstation, transaction, program, process, or other mechanism.

- Access establishment and modification (Addressable). Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

VIOLATIONS

Any violation of this policy may result in disciplinary action, up to and including termination of employment. As applicable, COMPANY may notify law enforcement authorities of any suspected or actual unlawful activity and to cooperate in any investigation of such activity. Conduct in violation of this policy is not within the course and scope of employment. Therefore, COMPANY reserves the right not to defend or pay any damages awarded against Personnel that result from violation of this policy.

Any Personnel who is requested to undertake an activity which he or she believes is in violation of this policy or observes potential violations, must notify the ISO or the legal team immediately.

RELATED DOCUMENTS/ATTACHMENTS

COMPANY should list any related documents here or in a master document list.

HISTORY

Version	Description/Action	Date	Reviewer(s)
.00	All HIPAA policies reviewed and revised.		Executive Management General Counsel VP, AGC Privacy & Compliance Information Security Officer

Sample Payment Card Information Security Policy

Establishment date, effective date, and revision procedure

This policy was established and approved by [Organization Name] on mm,dd,yyyy. The [Organization Name] Information Security department shall review this policy at least once a year, and at any additional time when there are changes that may affect corporate management with respect to Information Security. In the event that amendment or repeal of this policy becomes necessary as a result of such review, the [Organization Name] Information Security department shall prepare a draft and apply for authorization, and with prior confirmation of the Executive(s) in charge of the area(s) that will be affected by amendment or repeal, the [Organization Name] CISO/Security Director will authorize the amendment or repeal.

Table of revision history

Version	Date	Details of change	Issued by	Approved by

Overview

[Organization Name] seeks to meet the data security expectations of customers and vendors with whom it has a business or professional relationship. As a processor of payment card information, the organization understands that it is responsible for highly sensitive information belonging to customers and/or vendors that must be appropriately safeguarded in accordance with the Payment Card Industry Data Security Standards (PCI-DSS). In order to provide adequate safeguards for this information, the organization will create and implement a PCI-DSS Compliance Plan.

Purpose

The purpose of this policy is to create and maintain a PCI-DSS Compliance Plan to ensure payment card and other sensitive information is adequately safeguarded against unauthorized access, acquisition, alteration, or disclosure.

Scope

This policy applies to employees, contractors, consultants, volunteers, temporary and other workers at [Organization Name], and all personnel affiliated with company subsidiaries or third parties. This policy applies to all equipment that is owned or leased by, or otherwise in the custody or control of [Organization Name].

Policy

Development of a PCI-DSS Compliance Plan

As a processor of payment card information, [Organization Name] understands its compliance obligations under the PCI-DSS and seeks to protect sensitive customer information in its possession or control. As such, the organization's executive management including the Chief Executive Officer, Chief Information Officer, and Chief Financial Officer, and a designated Information Technology Officer [*and anyone else within the organization deemed necessary*], will work together to develop an organization-wide PCI-DSS Compliance Plan (Plan). Such Plan will comply with the most up-to-date version of the PCI-DSS and will be reviewed for updates on at-least an annual basis. Additional review of the Plan shall be undertaken as soon as practicable after release of any new versions of the PCI-DSS to ensure the organization's continued compliance.

At all times data security standards implemented in the Plan shall meet the minimum requirements set forth in the latest version of the PCI-DSS. However, in their discretion, [Organization Name] executive management may require additional safeguards in the Plan than those required by the PCI-DSS in order to address evolving organizational needs.

[Organization Name] understands that it may have additional data security and privacy compliance obligations under federal and/or state law which shall be addressed through additional safeguards, as necessary.