**HIC, Inc. Information Security Policy**

Angelica Y. Meza

Department of Professional and Continuing Education, University of San Diego

CSOL 540: Cyber Security Operational Policy

Dr. Michelle Moore

April 19, 2021

 **Table of Contents**

1. Information Security Program Charter ……………………………………………….......4
	1. Scope ………………………………………………………………………………….4
	2. Mission ………………………………………………………………………………..4
	3. Ownership and Responsibilities ………………………………………………………5
	4. Coverage of the Policy ………………………………………………………………..5
2. Laws, Regulations and Standards ………………………………………………………...6
	1. HIPPA ………………………………………………………………………………...6
	2. The HITECH Act ……………………………………………………………………..7
	3. The Privacy Act ………………………………………………………………………7
	4. Federal Information Security Management (FISMA) ………………………………..7
	5. Payment Card Industry Data Security Standard (PCI DSS) ………………………….7
3. Mobility Policy …………………………………………………………………………...8
	1. Purpose ………………………………………………………………………………..8
	2. Background …………………………………………………………………………...8
	3. Scope ………………………………………………………………………………….9
	4. Operational Policy ……………………………………………………………………9
	5. Roles and Responsibilities …………………………………………………………..10
	6. Applicable Laws/ Guidance …………………………………………………………10
	7. Effective Dates ………………………………………………………………………10
	8. Information and Assistance ………………………………………………………….10
	9. Approved …………………………………………………………………………….10
	10. Associated Resources ……………………………………………………………11
4. Asset Protection Policy for HIC, Inc. …………………………………………………...11
	1. Anti-Malware Policy ………………………………………………………………...11
	2. Access Control ………………………………………………………………………12
	3. Remote Access ………………………………………………………………………12
	4. Encryption …………………………………………………………………………...13
	5. Physical Access ……………………………………………………………………...13
5. Information Classification Scheme for HIC, Inc. ……………………………………….14
	1. General Statement of Purpose ……………………………………………………….14
	2. Policy …………………………………………………………………………..……14
	3. Scope ………………………………………………………………………………...15
	4. Access Control Requirements for HIC, Inc. Employees ……………………………15
	5. Definitions …………………………………………………………………………...16
	6. Data Classification …………………………………………………………………..16
	7. Public Information …………………………………………………………………..17
	8. Confidential Information ……………………………………………………………17
	9. Implementation and Enforcement of Policy ………………………………………...17
6. Privacy Policy for HIC, Inc. …………………………………………………………….18
	1. Privacy Domains …………………………………………………………………….19
	2. Restricted Data ………………………………………………………………………19
	3. Sensitive Data ……………………………………………………………………….19
	4. Internal Data …………………………………………………………………………20
	5. Public Data …………………………………………………………………………..21
7. Information Security Policy ……………………………………………………………..21
	1. Implementation ……………………………………………………………………...21
	2. Awareness and Training …………………………………………………………….21
	3. Management Support ………………………………………………………………..21
	4. Budget ……………………………………………………………………………….22
	5. Information Security Enforcement ………………………………………………….22
	6. Organizational Mission ……………………………………………………………...22
	7. Enforcement …………………………………………………………………………22
	8. Compliance Plan …………………………………………………………………….23

Glossary ……………………………………………………………………………………...24-25

References …………………………………………………………………………………...26-31

**Executive Summary**

The contents of this document include an Information Security Policy, as well as procedures, guidelines and best practices for the protection of the information assets of HIC, Inc. The Policy, as well as the procedures, guidelines and best practices apply to all employees and departments that have access to HIC, Inc. It is vital that this policy, guidelines and best practices are communicated to all employees. In turn, employees must review and understand the policy so everyone is aware of their responsibility in protecting HIC, Inc. assets. This Security Policy governs all aspects of hardware, software, communications and information. It covers all employees or other entities who may be given permission to log in, view or access HIC Inc. data. This document serves as guidance for procedures and best practices required for creating and maintaining a secure environment for the storage and dissemination of information. This document establishes the purpose, scope, authority, and organizational responsibilities of the information security program for HIC, Inc.

**1. Information Security Program Charter**

HIC, Inc. is a leading health insurance company in the United States. It collects several types of identifiable health and personal information data. HIC, Inc. is committed to maintain and protect their member’s identifiable data as required by the Federal, State laws, and industry standards to safeguard the integrity, confidentiality, and availability of their member’s information.

This Information Security Program Charter created by HIC, Inc. defines its principles and responsibilities to protect all identifiable health information data of our valued members.

**1.1 Scope**

This Information Security Program Charter and its associated policies apply to all employees, independent contractors, affiliates, part-time and temporary workers, and anyone contracted to work in HIC, Inc. premises or anyone with access to HIC, Inc. information systems.

**1.2 Mission**

The Information Security Plan Charter aims to bridge the gap between regulatory compliance and security. HIC, Inc. ultimate goal is to mitigate any security risk to the company’s assets. Implementing security within this organization requires placing a set of policies, standards, guidelines, and procedures that address security objectives by bringing together the right people to provide appropriate direction on successfully implementing a security plan tailored to satisfy each member's job function mitigating any security threats.

This information Security Program will counter threats by developing a Network Security Policy to help develop the known risks and create the computer network access rules. A Security Awareness program will be put in place to implement continuous monitoring successfully.

**1.3 Ownership and Responsibilities**

Once the HIC, Inc. Information Security Program has been approved, the Chief Executive Officer (CEO) and the Chief Information Officer (CIO) will work together to appoint a Chief Information Security Officer (CISO) to collaborate in building security policies specifically tailored to suit the security needs of HIC, Inc. The Security Plan Charter will include the following phases:

* Preliminary evaluation
* Management sensitization
* Needs analysis
* Policies and procedures
* Implementation
* Maintenance

It is crucial to implement policies that protect confidentiality, integrity, and availability. The CISO will work closely with the CEO to implement a Role-Based Access Control (RBAC) policy to restrict network access based on the user’s role to preserve security. Any employee should have access to the information only needed to perform their jobs. Understanding how security policy, incident response, and documentation works can lead to well-informed decisions without violating its policies. Non-compliance protocols could potentially jeopardize HIC, Inc information by making it vulnerable to potential threats.

**1.4 Coverage of the Policy**

Reinforcing policy is vital in order to preserve security within this company. Creating positive security habits such as employee awareness through continuous training, audit assessments, and incident management is a good practice. Sometimes employees may sign off on receipt of the policy handbook upon hire, but the number who actually read it is debatable. Security teams must assure that policies are adequately communicated and understood. Top management must identify the most powerful messaging techniques for sharing policies so employees understand their roles and importance of maintaining safety (Monan, 2018).

**2. Laws, Regulations, and Standards**

HIC, Inc. is committed to protecting its members’ personal health information (PHI) and other types of personally identifiable information (PII). HIC, Inc. will implement the following industry laws to comply with Federal and State regulations and protect the integrity, confidentiality, and availability of the company’s assets.

**2.1 HIPPA**

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is a federal law that was initially created to protect the health coverage of any worker who lost or changed jobs. However, HIPPA now aims to protect the patient’s health information from being disclosed without previous authorization. Under the HIPPA law, the Department of Health and Human Services (HHS) establishes guidelines on how and when to release health records and determines the penalties and fines if these parameters are violated. HIPPA applies to verbal, written, and electronic patient records. HIPPA encompasses privacy, security, and breach rules that ensure privacy and reduce fraud. Some of the technical requirements to the HIPPA Security rule include:

* Access controls
* Audit controls
* Integrity
* Person or entity authentication
* Transmission security

**2.2** **The HITECH Act**

The Health Information Technology for Economic and Clinical Health Act was enacted in 2009 to promote health information technology. It requires audits of healthcare providers to ensure they are compliant with HIPPA’S privacy rules. It is considered an enhancement to the HIPPA security, privacy, and breach law. Under this law, patients must be notified if their personal health information was access without prior authorization. HITECH increased the response to PHI breaches and the reinforcement of those requirements.

**2.3 The Privacy Act**

This law was enacted in 1974 and aimed to protect personally identifiable information (PII) stored in any Federal government database. This law aims to address the intricacies of privacy requirements regarding personal health information collected under any federal agency such as Medicare. Since the Privacy Act was enacted, several healthcare information policies have surged to protect the health system infrastructure (Bosworth, 2014).

As mentioned before, HIC, Inc. is committed to protecting its members’ personal health information. In addition to this, HIC, Inc. is aware of the importance of implementing standards and regulations that protect confidentiality, integrity, and availability by safeguarding the member's information while complying with Federal and State laws.

**2.4 Federal Information Security Management Act (FISMA)**

FISMA requires government agencies to adopt a common set of information security standards. It creates mandatory requirements to ensure the integrity, confidentiality and availability of HIC, Inc. data (Johnson, 2015).

**2.5 Payment Card Industry Data Security Standard (PCI DSS)**

PCI DSS is a worldwide information security standard that describes how to protect credit card information. HIC, Inc. stores, processes and exchanges cardholders’ information for Visa, MasterCard and American Express cards in order to collect the user’s payments. HIC, Inc. will enforce the following objectives:

* Build and maintain a secure network
* Protect cardholder data
* Maintain a vulnerability management program
* Implement strong access control measures
* Regularly monitor and test networks
* Maintain an information security policy

**3. Mobility Policy for HIC, Inc.**

**3.1 Purpose**

HIC, Inc. recognizes that modern telecommunications have many benefits for this company and its employees. Therefore, access to the Internet, email, and network is a privilege and carries responsibilities. This policy aims to define the company standards, procedures, and restrictions for users who have legitimate business requirements to use HIC, Inc. network and electronic resources by using any electronic device capable of storing data and connecting to the company's network.

* 1. **Background**

This policy aims to protect the confidentiality, integrity, and availability of HIC, Inc. technology infrastructure. The company's goal is to prevent data from being insecurely stored on a mobile device or network where data could be compromised. HIC, Inc. has designed specific policies to prevent any damage or loss of information. Employees that fail to adhere to these policies will be subject to disciplinary actions, up to and including termination.

* 1. **Scope**

This policy applies to all employees using HIC, Inc. mobile devices. Employees are only allowed to use HIC, Inc. devices such as laptops, tablets, smartphones, or any mobile device capable of storing data and connect to an unmanaged network supported and approved only by the company’s information security team.

* 1. **Operational Policy**

**Section I**

When HIC provides employees access to the Internet, email, or network with a supported device, it is intended that those technologies are only used for professional use and work-related purposes. Use of personal electronic devices to store or transfer data is prohibited. Failure to adhere to this policy will result in disciplinary actions, including termination.

**Section II**

All usage and electronically stored data on any HIC, Inc. network or IT equipment, regardless of the format in which it was stored, is considered the property of HIC, Inc. Therefore, any data stored in the company's network and equipment is not considered confidential or private. HIC reserves the right to closely monitor emails, files, Internet usage, and other forms of electronic communication.

**Section III**

Employees must abide by all software licenses and intellectual property policies according to Federal and State laws. Employees are responsible for safeguarding their user identification and passwords to ensure the confidentiality of any information stored on the electronic device.

**Section IV**

Employees that maintain a clean record and help enforce HIC, Inc. mobility policies are eligible to participate every month in a gift card give away and

**3.5 Roles and Responsibilities**

This policy applies to all HIC, Inc. employees, including full and part-time staff, contractors, and other users who utilize HIC, Inc. mobile devices to access, store, back up HIC, Inc. data, and network. Employment at HIC, Inc. does not immediately guarantee the ability to access the company’s network. Furthermore, it is the responsibility of any HIC, Inc. employee to ensure that all security protocols are being used and implemented. Failure to adhere to HIC, Inc. policies will result in the immediate suspension of the user’s account. Supervisors and managers are responsible for conducting training and performance evaluations under the Information Technology Department’s supervision to ensure users adhere to the HIC, Inc. mobility policy.

**3.6 Applicable Laws/Guidance**

HIC, Inc. reserves the right to refuse, by physical and non-physical means, the ability to connect to the company’s infrastructure network if the Information Technology department feels that such equipment is being used to put HIC, Inc. data at risk.

* 1. **Effective Dates**

This mobility policy is in effect as of January 1, 2021, and it is subject to change or to be modified at any time by the CIO.

* 1. **Information and Assistance**

Contact the IT department for more information regarding this policy.

* 1. **Approved**

Angelica Meza 1/1/2021

**3.10 Associated Resources**

This policy could be access at [www.hic.com/employeeshandbook](http://www.hic.com/employeeshandbook). Employees will be provided with training every month regarding the users responsibilities and opportunities to advance the user’s knowledge regarding HIC, Inc. policies and services.

**4. Asset Protection Policy for HIC, Inc.**

**4.1 Anti-Malware Policy**

HIC, Inc. is mandated to ensure its systems and facilities are secured and not subject to improper use. A malware infection would be devastating to our organization. A malware infection could cause temporary or permanent data loss, unauthorized access to HIC, Inc.'s network, delay of work, and more. Therefore, HIC, Inc. designed and implemented an anti-malware policy for all users concerning malicious actors. These measures will significantly reduce the risk of widespread malware infections amongst HIC, Inc.'s network. All employees, and anyone that connects to HIC, Inc. must read, understand and comply with the following:

* All electronic devices and servers connected to HIC, Inc. network must run an approved and up-to-date anti-virus product supported by the Information Technology Department to monitor any malicious software.
* All electronic devices and servers connected to HIC, Inc. network must run the latest Operating System and install applications supported by the Information Technology Department with the latest available patches applied.
* Employees must not attempt to uninstall or disable the anti-malware software. Users must request technical support if experiencing issues with the anti-malware software. Any messages requesting to disable the anti-malware software should be immediately reported to the help desk at servicedesk@hic.com
* Employees are prohibited from creating or distributing malicious code (viruses, worms, etc.) on HIC, Inc. network and facilities.
* HIC, Inc. reserves the right to disconnect any device from the network if an infection is found or suspected. If an employee suspects a device is infected with a virus, the employee must report this incident to the help desk at servicedesk@hic.com at soon as possible.
* Employees must report any suspicious emails to the help desk at servicedesk@hic.com. The anti-malware software must scan email attachments before delivery.
	1. **Access Control**

It refers to a set of conditions that, after review, determine access decisions.The conditions are a combination of attributes, obligations, authentication policies, and a risk profile (IBM, 2021).

HIC, Inc. will use the following key points to determine data access control:

* A unique username will be created for each employee. Therefore, each employee must identify themselves with the computers and networks. This unique username cannot be shared with anyone else.
* Each user must have a password or personal identification number (PIN) when logging into the network.
* Data access is determined and granted based on the employee’s role and job description with limitations to see, modify, add or delete data.

**4.3 Remote Access**

HIC, Inc. is aware that employees need to remote access the network to complete their job tasks. Since most employees using remote access will be connecting from a public unsecured network into HIC, Inc.'s private network, employees must authenticate their remote access (remote authentication) by using two-factor authentication. Employees must adhere to the two-factor authentication policies by:

* Employees must only use HIC, Inc. electronic devices supported and approved by the Information Technology department. Employees can only connect to HIC, Inc network with the electronic device (laptop, tablet, or cellphone) provided by your supervisor when hired.
* Employees must use their unique login credentials (username and password) to access HIC, Inc. network. In addition to this, HIC, Inc. will issue a smart card for each employee to authenticate remote access.
* HIC, Inc. will configure a client-to-site VPN connection to secure communication via the Internet.

**4.4 Encryption**

Data encryption is vital because even with the best practices, data could fall into the wrong hands. Employees at HIC, Inc. must always encrypt sensitive data as encrypted data could only be read when the user has the proper decryption key. As encrypting data provides an additional security layer, HIC, Inc. employees must ensure that laptops, backup files, stored data, emails, and transmitted PII data are encrypted.

**4.5 Physical Access**

As the digital realm matters to keep data safe, physical security controls cannot be neglected. HIC, Inc. employees, must be aware of the following:

* To preserve a perimeter of security, security guards will check employees' ID cards before entering the building. Visitors must wear a visitor badge and a formal appointment letter (email) stating which floor they are visiting and whom they are meeting with.
* Video surveillance will ensure security guards' visibility into the areas that need to be protected.

Only authorized employees could enter the server room. This room should be locked at all times, and authorized employees entering the room must not hold the door to allow other employees in after the server room is opened.

**5. Information Classification Scheme for HIC, Inc.**

**5.1 General Statement of Purpose**

This information classification scheme aims to provide a mandatory policy framework for classifying data. This policy provides information on how to determine the privacy category of the information and assign proper security guidelines to ensure confidentiality, integrity, and availability to meet the industry standards and federal and state laws.

**5.2 Policy**

* HIC, Inc. data must be categorized into two primary classifications. HIC, Inc. will classify its data into Public or Confidential. Confidential data will have subcategories to help better categorize confidential information.
* Data classification covers all electronically stored information (ESI), and non-electronic information (paper files and hard-copy data).
* HIC, Inc. data could be found in computers, laptops, smartphones, and storage media such as memory cards, flash drivers, and other storage devices. Any data found in any storage media must be analyzed and addressed before sharing, archiving, deleting, storing, or receiving data to protect data privacy.
* Appropriate access controls must be in place to protect data privacy from accidental disclosure, destruction, or modification. Any system that process, store or forward HIC, Inc. data must comply with all security policies.

**5.3 Scope**

This policy framework applies to all HIC, Inc.’s workforce, including but not limited to:

* *Executive and department heads:* The executive level will have full access to read, write and execute data. Department heads will be granted access with the inability to write or modify data without previous authorization.
* *Team members, volunteers, students, private contractors, and anyone who has access to HIC, Inc. data:* This tear has restricted network access. Employees can read data that the head department has previously authorized and strictly belongs to their job role.

HIC, Inc. policies apply to all employees, including full and part-time staff, contractors, and other users who have access to HIC, Inc. data, and network. Employment at HIC, Inc. does not immediately guarantee the ability to access the company's network. It is every employee's responsibility to ensure that all security protocols are being implemented and used. Failure to comply with HIC, Inc. privacy policies and security protocols will result in disciplinary actions, including job termination.

**5.4 Access Control Requirements for HIC, Inc. employees**

* A unique username will be created for each employee.
* Each employee must identify themselves with the computers and networks. This unique username cannot be shared with anyone else.
* Each user must have a password or personal identification number (PIN) when logging into the network.
* Data access is determined and granted based on the employee’s role and job description with limitations to see, modify, add or delete data.
* Employees must authenticate their remote access (remote authentication) by using two-factor authentication.
* Employees must only use HIC, Inc. electronic devices supported and approved by the Information Technology department.

**5.5 Definitions**

* *Protected Health Information (PHI):*PHI is defined as any oral, written or electronic individually identifiable health information collected or stored by HIC, Inc. Individually identifiable health information includes demographic information and anything related to the physical or mental condition of an individual. PHI is classified as highly sensitive confidential data and subject to HIPPA and HITECH Act (Northwell Health, 2016).
* *Personally Identifiable Information (PII):*PII is defined as any oral, written or electronic individually identifiable personal information collected or stored by HIC, Inc. All PII is subject to all applicable laws, including the New York State Social Security Number Protection Law, New York State Labor Law, and Fair Credit Reporting Act (Northwell Health, 2016).

**5.6 Data Classification**

HIC, Inc. has classified its data based on its sensitivity, context, and business value to determine the security level applied to the information. HIC, Inc. will classify its data into public or confidential. Confidential information will be subcategorized into highly sensitive, sensitive, or internal information.

**5.7 Public Information**

HIC, Inc. public information data may be released with previous HIC, Inc. authorization to the general public, competitors, and the press. Public information includes press announcements, regulatory filings, general sales, business contact information, and certification labels.

**5.8 Confidential Information**

HIC, Inc. considers all information that is not public confidential. Confidential information is classified as Highly Sensitive, Sensitive, or Internal.

* Highly sensitive data refers to any PHI or any information that would violate federal/ state law and cause any harm or financial loss to another person if lost, corrupted, or disclosed to an unauthorized person. It includes social security numbers, credit card data, and driver's license information.
* Sensitive data is any information that, if lost, corrupted, or disclosed to an unauthorized person, would cause any harm or injury to another person. It includes PII data elements.
* Internal refers to any confidential information that does not fall into any highly sensitive or sensitive information data.

**5.9 Implementation and enforcement of Policy**

This policy applies to all HIC, Inc. employees, including full and part-time staff. This mandatory policy is effective as of the first of next month.

* All employees will be subject to attend mandatory training.
* Job permanency is dependent upon completing training and adhering to the data policy.
* Supervisors and managers are responsible for conducting training and performance evaluations under the Information Technology Department's supervision.

**6. Privacy Policy for HIC, Inc.**

* This privacy policy aims to provide guidelines for classifying and handling various data types according to the different privacy domains to establish the criticality of the information and the implementation of security guidelines. This policy was designed to protect the confidentiality, integrity, and availability of data required by HIC Inc. and applicable law. This data-handling privacy policy applies to all electronic data managed and owned by HIC, INC.
* Data might be stored in data centers, data accessed or stored remotely on any electronic device by employees, including and not limited to business associates, cloud service providers, vendors, contractors, and temporary staff. Systems that process, store or forward HIC, INC information must comply with all levels of security and must be handled according to this privacy policy to protect data from intentional or unintentional disclosure, modification, or destruction.
* This privacy policy will be used to determine HIC, INC data handling and classification for any electronic data created, maintained, processed, or transmitted utilizing electronic or physical resources. Data will be classified and handled according to HIC, INC data protection level, and data type to meeting external regulatory, internal regulatory, and other contractual requirements to avoid the adverse impact of loss, theft, or unavailability of the data. If a specific data is classified as within two or more data classifications, that data set must be managed according to the most restrictive applicable data classification. If a data set seems not to fit a specific data classification model, the Data Security Compliance Program (DSCP) must be contacted immediately. Losing or compromising data's confidentiality or availability due to non-compliance will significantly impact HIC, INC by negative financial impact, damage to HIC, INC’s reputation, regulatory or legal action potential, and violation of HIC INC’s missions, policies, or principles (Phelan, 2017).

**6.1 Privacy Domains**

**6.2 Restricted Data**

* Protection Level: P4-High
* Policy and Legal Requirements:This data must be protectedto comply with Federal or State law, regulations, or a contractual obligation.
* Access:Only authorized users with approved access, signed confidentiality, or other non-disclosure agreements permitted by law**.** Data must be handled with the approval of the Data Owner and for legitimate business purposes.
* Adverse Business Impact Statement: High adverse impact to regulatory or legal action, **v**iolations of HIC, INC policies and principles, HIC INC’s reputation, finances, and critical operations.
* Restricted Data Types:

Personally Identifiable Information (PII)

Protected Health Information (PHI)

Research Health Information

Payment Card Industry Data (PCI)

Confidential Security information

**6.3 Sensitive Data**

* Protection Level: P3-Moderate
* Policy and Legal Requirements:Protection of data is required by the data owner and might be required by Federal or State law as well.
* Access:Only authorized users (information custodians) with approved access, signed confidentiality, or other non-disclosure agreements permitted by law**.**
* Adverse Business Impact Statement:Moderate adverse impact to regulatory or legal action, violations to HIC, INC policies and principles, HIC, INC reputation, finances, and critical operations.
* Sensitive Data Types:

HIC, INC Intellectual Property

Employee Information

Litigation/Investigation Materials

Contracts

Physical Building Designs

Financial Information

* 1. **Internal Data**
* Protection Level: P2-Low
* Policy and Legal Requirements:Federal or State laws do not protect data. However, the protection of data is governed by HIC, INC policies.
* Access:The intended audience for data access under the design of the system (Phelan, 2017).
* Adverse Business Impact Statement:Low adverse impact.
* Internal Data Types:

Public Directory Information

Routine Business Records and Email

Research Using Publicly Available Data

* 1. **Public Data**
* Protection Level: P1-Minimal
* Policy and Legal Requirements:Protection of data is protected by HIC, INC policy. Minimum-security standards apply.
* Access:Data intended could be obtainable by the public.
* Adverse Business Impact Statement:Minimal adverse impact.
* Public Data Types:
* Public-facing Websites
* Published Research Maps
* Press Releases

**7.** **HIC, Inc. Information Security Policy**

**7.1 Implementation**

The adoption of an information security policy helps make an organization secure and minimize the risks of unacceptable use of any the HIC Inc.’s information resources. The following factors play an important role in improving an information security in organization.

**7.2 Awareness and Training**

Users will get training every six months to keep employees updated on any policy and protocol changes. Training aids to create security awareness, which help employees to be aware of potential threats and risks threatening the organizations information’s assets.

**7.3 Management support**

At HIC, Inc., top management support plays a crucial role in successful implementation of information security policies. Top management must understand the importance of information security; hence reassuring all employees is following security protocols.

**7.4 Budget**

The budget is crucial when implementing an information security policy in organizations. HIC, Inc. will designate a technical budget that covers all the necessary tools to ensure the network’s security.

**7.5 Information Security Policy Enforcement**

This security policy aids to identify HIC, Inc.’s important assets, and to achieve a successful performance. This information security policy can only be enforced by conscious implementation. Therefore, all employees must understand the policies, verify if the policies are being violated**,** and address incidents in case of policy violation.

**7.6 Organizational Mission**

It is important for HIC, Inc. to set goals and objectives as they help to the successful implementation of security policies.

**7.7 Enforcement**

All HIC, INC. employees, divisions and departments, must adhere to these policies.

Individual departments must follow all detailed procedures to handle department- specific cases In addition, this policy will guide annual security reviews by the Information Technology Department, as well as audits requested by the HIC, Inc. administration. Violators of these policies will be subject to employee disciplinary procedures including job termination. Departments and divisions may impose sanctions upon their employees, within these policy guidelines, for any violations of the security policy standards.

**7.8 Compliance plan**

All departments must ensure that all security procedures are documented and implemented. All areas within HIC, Inc. will be subject to regular audits to ensure compliance with security procedures and standards. These include the following:

Information systems

Systems providers

Owners of information and information assets

Hosting agencies of information and information assets

Users

HIC, Inc. policies apply to all employees, including full and part-time staff, contractors, and other users who have access to HIC, Inc. data and network. Employment at HIC, Inc. does not immediately guarantee the ability to access the company's network and its data. It is every employee's responsibility to ensure that all security protocols are being implemented and used. Failure to comply with HIC, Inc.'s privacy policies and security protocols will result in disciplinary actions, including job termination.

**Glossary**

**Backup:** A copy of files and programs made to facilitate recovery if necessary.

**Business Continuity:** Procedures that describe how an organization's business functions after a significant disruption of the normal business environment.

**Business Recovery Strategy:** The documentation of a set of instructions that describe how business processes will be restored after disruption.

**Contingency Plan:** Management policy designed to maintain or restore business operations.

**Data:** Information collected together for reference or analysis.

**Disaster Recovery Plan:** IT plan designed to restore operability of the target system after a major hardware or software failure.

**Disruption:** An event that causes the system to be inoperable for an unacceptable length of time.

**Facilities:** Interconnected information resources that share common functionality. They include hardware, software, information, information applications and communications.

**Information:** Any data or knowledge collected, processed, stored, managed, transferred or disseminated by any method.

**Owner:** State Agency responsible for producing, collecting and maintaining the authenticity, integrity and accuracy of information.

**Risk Management:** Risk management is the process of assessing, controlling and mitigating the risks to information systems and technologies.

**Server:** A server is a computer that runs software and provides access to a part of the network and network resources.

**Shared Network:** A network shared with third party or non-organizational users.

**System:** A term used to describe a major application or a general support system.

**Web Site:** Used for information dissemination on the Internet (published to the public) or an intranet (internal to an organization).

**References**

Aguiar, J. (2018). *Data Classification and Protecting Information | Journal Of AHIMA*. Journal

Of AHIMA. Retrieved 2 April 2021, from <https://journal.ahima.org/data-classification->and-protecting-information/.

Bosworth., S., Kabay, M., & Whyne, E. (2014). *Computer Security Handbook, Sixth Edition,*

*Volume 1 & 2* (6th ed.). Wiley.

Burde, H. (2021). *THE HITECH ACT: An Overview*. Journal of Ethics | American Medical

Association. Retrieved 17 March 2021, from <https://journalofethics.ama->assn.org/article/hitech-act-overview/2011-03.

Cornelius, B. (2021). *On Policies, Control Objectives, Standards, Guidelines & Procedures*. The

State of Security. Retrieved 6 March 2021, from <https://www.tripwire.com/state-of-security/regulatory-compliance/understanding-policies-control-objectives-standards-guidelines-procedures/>

Harvey, S. (2020). Kirkpatrickprice.com. Retrieved 3 April 2021, from

https://kirkpatrickprice.com/blog/classifying-data/.

IBM. (2021). *IBM Knowledge Center*. Ibm.com. Retrieved 29 March 2021, from

https://www.ibm.com/support/knowledgecenter/SSPREK\_9.0.7/com.ibm.isam.doc/admin/cpt/rbaAdminPolicyManagement.html.

Johnson, R. (2015). *Security policies and implementation issues*. Jones & Bartlett Learning.

Microsoft. (2021). *Endpoint Protection anti-malware policies - Configuration Manager*.

Docs.microsoft.com. Retrieved 28 March 2021, from <https://docs.microsoft.com/en->us/mem/configmgr/protect/deploy-use/endpoint-antimalware-policies.

Microsoft. (2021). *End point Protection anti-malware policies - Configuration Manager*.

Docs.microsoft.com. Retrieved 28 March 2021, from <https://docs.microsoft.com/en->us/mem/configmgr/protect/deploy-use/endpoint-antimalware-policies.

Monan, E. (2018). Securitymagazine.com. Retrieved 15 April 2021, from

<https://www.securitymagazine.com/articles/89271-the-importance-of-communication->for-security.

Mullahy, T. (2019). *5 Physical Security Controls Your Business Needs - Total Security Advisor*.

Total Security Advisor. Retrieved 27 March 2021, from https://totalsecurityadvisor.blr.com/facility-security/5-physical-security-controls-your-business-needs/.

New York Foundling. (2020). [Ebook]. Retrieved 22 March 2021, from

<https://nyfoundling.sharepoint.com/sites/HUB-HumanResources/SiteAssets/Forms/AllItems.aspx?id=%2Fsites%2FHUB%2DHumanResources%2FSiteAssets%2FSitePages%2FHUB%2DHumanResources%2F834268760New%20York%20Foundling%20Employee%20Handbook%20%2D%2012%2D18%2D2020%2Epdf&parent=%2Fsites%2FHUB%2DHumanResources%2FSiteAssets%2FSitePages%2FHUB%2DHumanResources>.

Northwell. (2016). Northwell.edu. Retrieved 2 April 2021, from

https://www.northwell.edu/sites/northwell.edu/files/d7/900.12%20Data%20Classification%20and%20Handling%20Policy%20Round%203.pdf.

Office of Management and Enterprise Services. (2017). Retrieved 15 April 2021, from

https://www.ok.gov/cio/documents/InfoSecPPG.pdf.

Palmer, M., Robinson, C., Patilla, J., & Moser, E. (2000). Horseproject.wiki. Retrieved 3 March

2021, from <http://horseproject.wiki/images/1/18/Information-Security-Policy-Framework-Research-Report.pdf>.

Pensacola. (2021). Cityofpensacola.com. Retrieved 15 April 2021, from

<https://www.cityofpensacola.com/DocumentCenter/View/1680/Information-Security->Policy-PDF.

Phelan, P. (2017). It.ucsf.edu. Retrieved 8 April 2021, from

https://it.ucsf.edu/sites/it.ucsf.edu/files/data\_classification\_standard\_v1\_final\_3.pdf.

Pourkhomami, P. (2018). *The Importance of IT Security Policies for Your Organization*.

Managed IT Services & Technology Consulting | OSIbeyond. Retrieved 7 March 2021, from <https://www.osibeyond.com/blog/it-security-policies-every-organization-must-have-them/>

University of Ghana. (2015). *Anti-Malware Policy | University of Ghana Computing Systems*.

Ugcs.ug.edu.gh. Retrieved 28 March 2021, from <https://ugcs.ug.edu.gh/policies/anti->malware-policy.

Wayne County Community College District. (2021). *Mobile Device Acceptable Use*

*Policy* [Ebook]. Retrieved 22 March 2021, from <http://www.wcccd.edu/dept/pdf/IT/mobile_policy.pdf.>

Wismen, M., & Keller, C. (2017). Diva-portal.org. Retrieved 15 April 2021, from

http://www.diva-portal.org/smash/get/diva2:1154975/FULLTEXT01.pdf.

*5 Important Regulations In United States Healthcare | Maryville Online*. Maryville Online. ( 2021). Retrieved 18 March 2021, from <https://online.maryville.edu/blog/5-important-> regulations-in-united-states-healthcare/.