HIC, Inc.

Security Program Charter

Author: EVP/COO – Chad Nelley

Charter Mission

The purpose of this Information Security Program Charter is to provide an overview of the policies, standards and procedures that make up HIC's IT/Cyber Security Program. These policies, standards and procedures document the practices undertaken to protect information which falls under federal and state laws and regulations such as HIPPA and PCI-DSS. The intent of the Program is to provide effective security balanced with the need for maintaining the open and collaborative network and IT Infrastructure environment required for business continuity of the HIC operation. It is imperative that HIC staff, vendors and 3rd Party Contractors are all apprised and familiar with these policies and have signed off on their understanding and willingness to adhere to them in order to sustain and maintain an ongoing business relationship with HIC, Inc. HIC exercises independent authority for establishing and executing its information security program.

It is the collective responsibility of all users to ensure:

- Confidentiality of information which HIC must protect from unauthorized access
- Integrity and availability of information stored on or processed by HIC information systems
- Compliance with applicable laws, regulations, and HIC policies governing information security and privacy protection

The Information Technology Security Program establishes guidelines and principles for initiating, implementing, maintaining, and improving information security management for HIC. The program is intended to protect the confidentiality, integrity and availability of information resources and is not intended to prevent, prohibit, or inhibit the use of information technology resources as required to meet HIC's mission and Healthcare service delivery goals.

Scope

The program charter applies to all users, all information assets, facilities, applications, systems, infrastructure and network resources. Auxiliary organizations or any entity, including third parties, using HIC information technology resources must operate those assets in conformity with the HIC Information Technology Security Program.

Information Security Policy

Policy is developed and executed, and expectations are set for protecting HIC information assets. These are supported by related policies, standards, guidelines and practices to facilitate corporate compliance.

These are defined as follows for purposes of this document and all associated and sub-charter articles:

- Policies are high-level statements of principle that provide technology direction to the HIC community.
- Standards establish specific criteria and minimum baseline requirements or levels that must be met to comply with policy. They provide a basis for verifying compliance through audits and assessments.
- Guidelines are recommended or suggested actions that can supplement an existing standard or provide guidance where there is an absence of standard.

Policy development is driven by HIC IT management and executive directives, new legislation and regulations as they pertain to the healthcare industry, risk assessment, audit findings and HIC strategic

planning and initiatives. Key executive, board and management stakeholders are consulted early on and research is conducted to find potential models from industry best practice, published whitepapers and State, Local and Federal regulations changes that may have an impact to HIC's continuing operations.

As the designated official, the EVP/COO, formally proposes company-wide policies, standards and guidelines in coalition with the VP of HR, General Counsel, VP of IT and the CISO. Under the broad authority provided by the Organizational Policies, the CISO establishes specific requirements for all members of the HIC community as they pertain to Cyber and Infrastructure Information Security. The formulation and distribution of information technology policies, standards, procedures, and guidelines connect HIC's mission to individual conduct, institutionalize impartial expectations, support compliance with laws and regulation, mitigate institutional risk, and enhance productivity and efficiency in the company's IT and general operations.

Overarching policies governing information technology are in place as follows.

- IT-AUCR Policy – Policy on Acceptable Use of Computing Resources
- IT-AC Policy – Information Technology Access Control Policy
- IT-IAOO Policy – Information Technology Infrastructure, Architecture, and On-going Operations
- IT-DC Policy – Data Classification Policy
- IT-SP Policy – Information Technology Security Policy
- IT-EMP Policy - Electronic Messaging Policy for Company Communication
- IT-AP Policy - Information Technology Accessibility Policy
- IT-PM Policy - Information Technology Project Management Policy
- IT-DP Policy – Information Technology Data Protection Policy
- IT-SM Policy – Information Technology Social Media Policy
- IT-HIPPA Policy – Information Technology HIPPA Compliance Policy
- IT-SOX Policy – Information Technology Sarbanes-Oxley Policy

Security Policy Management

In collaboration with all appropriate company representatives, the Chief Information Security Officer (CISO) leads efforts to develop, approve, and launch a suite of information security policies and standards, based upon the industry's best practices in information security. These policies, standards and guidelines formally establish the HIC Technology Security Program and set forth employee responsibility for information protection. The security policy also incorporates security requirements of applicable regulations including, but not limited to, the Payment Card Industry Customer Information Security Program, and Health Insurance Portability and Accountability Act. Professional organizations and centers of excellence, such as ISACA, ISO, NIST and SANS, will also serve as resources for additional effective security practices.

Security Governance

Information security cannot be treated solely as a technology issue. Based on the company's growing dependence on information technology and information technology-based controls, information and information technology security risks increasingly contribute to operational and reputational risk. Information security is an intrinsic part of governance and consists of the leadership, organizational structures and processes that safeguard HIC's information, its operations, its market position, and its reputation.

Board Authority

The HIC Board of Directors, grants authority to the CEO to establish rules and regulations for the company. The CEO grants authority to the EVP/COO to implement the policies and procedures of the Board relating to Company operations.

EVP/COO Authority

The CEO grants s the EVP/COO responsibility for company policies and procedures for acquisition, implementation, documentation and use of information technology resources and for meeting its compliance obligations. Information Technology (IT) also provides and manages a variety of computing facilities and services for the Company. The CEO also delegates specific responsibilities to the CISO.

Chief Information Security Officer

As the overall IT security responsibilities are assigned to the EVP/COO as Operational leader, the EVP/COO designates the Chief Information Security Officer (CISO) the responsibility to develop and manage HIC's IT security program and to coordinate and provide IT security information to the EVP/COO. The CISO oversees an annual review of the security program and communicates any changes or additions to the appropriate stakeholders. In addition, the program is updated regularly to reflect changes in HIC policy, medical, administrative, or technical environments, or applicable laws and regulations. The CISO reports to the EVP/COO on the current state of company security relative to protecting HIC information assets as needed.

Roles and Responsibilities

For clarity within the HIC Organization, the EVP/COO is designated as the individual with ultimate responsibility for the security of HIC's IT systems and data. The EVP/COO designates the Chief Information Security Officer (CISO) to develop, implement and maintain a program of IT safeguards. The responsibilities of the CISO and other positions with security duties are described in detail in IT Roles and Responsibilities Handbook that serves as a supplement to this and all other security policy documents. Personnel identified there-in perform their assigned responsibilities in support of the IT Security Program. This Standard details the internal organization of information security and allocation of security responsibilities. Further, the IT Policy Library establishes management controls, the dedicated roles of individuals, review, approval and compliance processes and the plans to coordinate controls across the organization. Other Standards further elaborate on the defined roles. Technical support staff and individual users are expected to follow established standards and practices and to report potential security violations. Managers across the company are responsible for ensuring information security policies, standards and practices are followed by employees in their respective areas.

Privacy of Personal Information

All users of information technology resources are advised of the open nature of information disseminated electronically, and must not assume any degree of privacy or restricted access to

information they create or store on company systems. HIC information systems may be subject to disclosure under local, state and Federal law. The Company will disclose information about individuals only to comply with applicable laws or regulations, to comply with or enforce applicable policy, to ensure the confidentiality, integrity, or availability of company information, and to respond to valid legal requests or demands for access to company information. User access to IT systems is based on the principle of least privilege. Proper authorization and approval by the IT system user's supervisor and the System Owner is required for access.

Security Awareness and Training

The focus of security awareness at HIC is aimed at creating an attitude and commitment to strong, fundamentally sound and credible security practices and facilitating a climate that sees security rules as beneficial to the protection of the Company and its customers. Users must formally acknowledge their responsibilities through the acceptance of a statement on the terms of use of information technology resources. Training is required on an annual basis. Security awareness information is provided to new employees, vendors and 3rd party contractors at the time of orientation or commencement of a new contract. Online resources are provided to educate users on best computing practices and the importance of reporting security incidents. Security tools are provided at no charge. News of email scams, phishing attempts and other malicious actions will be posted via the CISO Blog to inform users of possible threats. HIC's IT Security operatives will, from time-to-time conduct active Phishing attempts against internal users with the intent of identifying and isolating "teachable moments" with an immediate training and education action associated when employees, vendors or independent contractors behave in ways that jeopardize the HIC business.

Security Policy Implementation Items (Charter Supplement)

Other specific policy areas can be found in the IT Policy Library and are supplemental to this primary Security Charter document. Some areas include but are not limited to:

- Identity Management
- Incident Management
- Operational Security
    - *Risk Management*
    - *Physical Security*
    - *Access Control*
    - *Systems Security*
    - *Personnel Security*
- Contingency Planning
- Security Assessments and Reviews
    - *Annual Security Plan*
- Compliance
- Policy Enforcement

HIC Core Business Drivers (The "why" for how we implement this Charter)

Everything that we do here at HIC revolves around business drivers. These policies are developed and defined to uphold and promote the attainment of the following key business drivers as defined by the Board and Sr. Executive Leadership:

- Market Share & Revenue Growth
- Profitability
- Customer Experience

- Data Integrity
- Brand Advancement
- Efficiency & Operational Excellence

Review and Revision

This document along with all sub-charter documents and policy documents will be subject to annual review and update. Every year as part of our review of all policies germane to the ongoing HIC Business, Management, employees, contractors and vendors will be subject to review and re-sign this and all affected policies that have changed over the course of the previous year. This review will be conducted between December 15th and January 3rd each year and renewed signatures will be due to the office of HR no later than January 31st. Where possible, electronic signatures will be collected and their records maintained in the HRIS system.

Conclusion

It is the expectation of management at HIC that every employee will adhere to and uphold the security principles outlined in this charter document. HIC's business continuity and ongoing success in a competitive market relies on our employees, vendors and contractors putting security and privacy ahead of convenience. The nature of our business makes us a primary target for bad actors who wish to harm our brand at the expense of our customer's critical data and information. We all must be vigilant in the protection of our data. All HIC Employees, vendors and contractors are reminded that the HIC core business drivers are the reason we exist. Without these policies, our business drivers would be placed at significant risk and our business therefore, in great jeopardy. We are passionate about these 6 objectives and dereliction or neglect of these policies will result in a breach of our corporate integrity. This integrity is paramount to our existence and commitment to our global community.

Signatures

HIC EVP/COO
Printed Name: Chad Nelley

Signature:_____

Date Signed:_____

HIC CISO
Printed Name: Gerald Elverson

Signature:_____

Date Signed:_____

HIC Employee/Contractor/Vendor

Printed Name:

Signature:_____

Date Signed:_____

Cc: HR Employee File, Contractor Agreement File, Vendor Agreement File, HIC Legal Dept