HIC Asset ID and Classification Policy

Overview

The purpose of this policy is to provide guidelines for acceptable use and protection measures for information asset identification, protection and classifications. Users are required to agree and comply by signing the separate Policy supplement found attached to this document.

Scope

This mandatory policy applies to all employees, volunteers, interns, 3rd party contractors and vendors who maintain a working relationship with HIC Inc., and who are accessing information assets of any kind in conducting business with or on behalf of HIC Inc.

Integrity

This policy has been designed to maintain the integrity of all of HIC's PHI Data as it pertains to our customers, 3rd party entities and minimum compliance standards set forth by our governing agencies and our Board of Directors and shareholders. HIC will maintain a zero tolerance enforcement of this policy.

Policy Objectives

HIC Inc defines information classifications based on the sensitivity, criticality, confidentiality/privacy requirements, and value of the information. All information assets, whether generated internally or externally, must be categorized into one of these information classifications: Restricted, Confidential, Internal Use Only, or Public. When information of various classifications is combined, the resulting collection of information or new information must be classified at the most restrictive level among the sources. Below is the table that outlines how HIC classifies data by category. It provides descriptions of the data classifications as well as specific examples to help provide additional context.

Responsibilities

The EVP/COO is the approval authority for the Asset Identification and Classification Standard.

The VP of IT is responsible for the development, implementation, and maintenance of the Asset Identification and Classification Policy and associated standards and guidelines.

The individuals, groups, or organizations identified in the scope of this policy are accountable for one or more of the following levels of responsibility when using HIC information assets:

Owners are managers of organizational units that have primary responsibility for information assets associated with their functional authority. When Owners are not clearly implied by organizational design, the EVP/COO will make the designation. Owners are responsible for: identifying information assets; assigning the proper information classification; ensuring the proper labeling for sensitive information; designating the Custodian in possession of the information; ensuring the information classifications are properly communicated and understood by the Custodians; and reviewing information assets periodically to determine if their classifications should be changed.

Custodians are the managers, administrators, service providers, and those designated by the Owner to manage, process, or store information assets. Custodians are responsible for understanding the information classifications, and applying the necessary controls to maintain and conserve the information classifications and labeling established by the Owners.

Users are the individuals, groups, or organizations authorized by the Owner to access information assets. Users are responsible for understanding the information classifications, abiding by the controls defined by the Owner and implemented by Custodians; maintaining and conserving the information classification and labeling established by the Owners; and contacting the Owner when information is unmarked or the classification is unknown.

Enforcement

Failure to comply with the Asset Identification and Classification Policy and associated standards, guidelines, and procedures can result in disciplinary actions up to and including termination of employment for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws.

Requests for exceptions to the Asset Identification and Classification Policy should be submitted to the EVP/COO along with a proper business justification and financial ROI presentation that outlines the positive financial impact vs. the risk associated with the potential exception. Exceptions shall be permitted only on receipt of written approval from the EVP/COO.

Information Asset Classification Table

Information Category	**Description**	**Examples**
Unclassified Public	Information is not confidential and can be made public without any implications for Company. Loss of availability due to system downtime is an acceptable risk. Integrity is important but not vital.	• Product brochures widely distributed • Information widely available in the public domain, including publicly available Company web site areas • Sample downloads of Company software that is for sale or distribution • Financial reports required by regulatory authorities • Newsletters for external transmission
Proprietary	Information is restricted to management approved internal access and protected from external access. Unauthorized access could influence Company's operational effectiveness, cause an important financial loss, provide a significant gain to a competitor, or cause a major drop in customer confidence. Information integrity is vital.	• Passwords and information on corporate security procedures • Know-how used to process client information • Standard Operating Procedures used in all parts of Company's business • All Company-developed software code, whether used internally or sold to clients
Client & 3rd Party Confidential Data	Information received from clients in any form for processing in production by Company. The original copy of such information must not be changed in any way without written permission from the client. The highest possible levels of integrity, confidentiality, and restricted availability are vital.	• Client Healthcare information/PHI • Electronic transmissions from clients • Product information generated for the client by Company production activities as specified by the client • 3rd Party Patient Health Information

Company Confidential Data	Information collected and used by Company in the conduct of its business to employ people, to log and fulfill client orders, and to manage all aspects of corporate finance. Access to this information is very restricted within the company. The highest possible levels of integrity, confidentiality, and restricted availability are vital.	• Salaries and other personnel data • Accounting data and internal financial reports • Confidential customer business data, records and confidential contracts • HIC Developed PHI – Patient Health Information • Non disclosure agreements with clients\vendors • Company business plans

***This policy conforms to and is based on the ISO27001 Standards as set forth by the International Organization of Standards.*

HIC Information Asset and Classification Supplement

As an HIC employee, I acknowledge and agree:

1. That I have read and understand the HIC Information Asset and Classification Policy.

2. Any violations of this policy will result in corrective action up to and including immediate termination of employment.

I_____, have read and accept the terms and conditions of the HIC Mobile Device Policy listed above.

Employee Signature: _____

Date: _____