**ITD\_0151A Compliance with Legal Requirements Policy Summary**

**Contractors and Vendors**

1. **PURPOSE:**

The purpose of this policy is to avoid breaches of legal, statutory, regulatory or contractual obligations, and of any security requirements, by establishing controls and individual responsibilities to ensure compliance with legal and regulatory requirements.

This policy is intended to supplement HHSC existing policies and, except to the extent specifically specified in this policy, does not replace or supersede any existing policy.

1. **DEFINITIONS:**

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Forensic Analysis Process | Process used to collect or safeguard information that may be used in a legal proceeding. Care must be taken to preserve a "chain of custody" to ensure the integrity of the information or data collected. |
| Intellectual Property Rights | Property in the form of patents, trademarks, service marks, trade names, trade secrets and copyrights. |
| Security Incident | Events that take place on any HHSC electronic information system that violate the confidentiality, integrity, or availability of the system and/or its data. |
| Stakeholder | Any person who uses HHSC Information Assets, including, but not limited to HHSC facility and corporate office employees, board members, volunteers, students, physicians, vendors, contractors, and other external parties. |

1. **POLICY:**

**1. Identification of Applicable Legislation**

HHSC Management shall keep abreast of changes to statutory, regulatory, and contractual requirements impacting HHSC Information Assets.

HHSC General Counsel, Corporate and Regional Compliance, and the Chief Information Security Officer (CISO) shall monitor all applicable sources, such as public announcements, professional organizations, etc. for news of proposed or pending statutory and/or regulatory changes that will require changes in the business processes used to safeguard and protect HHSC Information and Information Assets, including electronic protected health information (ePHI).

As information is received about proposed or pending changes in statutory and/or regulatory requirements, the Privacy and Security Council will recommend any necessary changes to current security policies, standards, and procedures.

All new contractual requirements that pertain to safeguarding HHSC Information Assets must be brought to the attention of the CISO who will evaluate the requirements and if needed or appropriate, bring them to the Privacy and Security Council for action.

**2. Intellectual Property Rights**

**2.1. Software Licenses**

Installation of unlicensed commercial (off-the-shelf) or proprietary software on servers, personal computers, laptops, appliances, or other computing devices owned by HHSC is a violation of HHSC policy and, possibly, copyright law and is subject to disciplinary action up to and including termination, subject to applicable collective bargaining agreements.

Proof of the license status for software installed on issued HHSC Information Assets assigned for individual use may be requested to validate the legal use of the software. Such proof may be demonstrated by copies of the original purchase orders, receipts, license keys, labeled and serialized distribution media, or other appropriate means.

Downloaded software must come from a known, reputable source and the user must retain evidence that the software is properly licensed or obtained under a legitimate open-source license agreement.

License documentation for shared computing devices in public areas with a standardized configuration will be maintained by ITD.

**2.2. Other Downloaded Materials**

Commercial recordings (video, audio) or other copyrighted material must be:

* Obtained legally with proof of ownership available on request.
* Used in compliance with the license agreement associated with the materials. This includes applicable limits on making copies and restricting the use to specific devices, workstations, etc.

**2.3. Education and Enforcement**

The CISO will include Intellectual Property Rights awareness in the Information Security Training Program.

The Chief Information Officer (CIO) will have a procedure for carrying out checks to ensure compliance with this policy. This may include, but is not limited to:

* Use of automated inventory tools.
* Random spot checks will be performed as part of a periodic security assessment by the HHSC Information Security Team.
* Random checks of devices under repair by the HHSC Corporate and Regional Technical Teams.
1. **Protection of Organizational Records**

In cases where there are varying retention periods or where it is technically or economically not feasible to separate information with different retention periods, the one with the longest retention period will take precedence.

When the retention period is not specified, or where it is not clear, the Information Owner will specify the retention period. This will be documented in the Responsibility for Assets Policy.

Information that is essential for normal HHSC operations must be backed up per the requirements defined by the Information Owner and any removable media must be stored in accordance with the manufacturer's recommendations. Additionally, information must be preserved as future technology changes and applications are upgraded, and consideration given to the possibility of media deterioration.

1. **Data Protection and Privacy of Personal Information**

**4.1. Disclosure of Confidential-Reportable Information**

Any personally identifiable information is classified as Confidential-Reportable must be secured per Information Classification Policy. This includes, but is not limited to, information that is protected by various federal and state statutes.

See HIPAA and other related privacy policies on the HHSC intranet under Corporate Compliance. These policies address special requirements concerning the release of certain alcohol and drug abuse treatment records and psychotherapy notes, among others.

**4.2. Privacy Expectations of Information Stored On HHSC Information Assets** HHSC-issued laptops, personal computers, "smart phones", or other computing devices, along with the programs and files that they contain, and the networks and systems (i.e. file, e-mail, database servers, etc.) to which they connect to or use for storage, are the property of HHSC.

HHSC reserves and may exercise the right, at any time, to review, audit, intercept, copy and disclose any files, activity logs, or programs contained on any HHSC Information Asset, including HHSC issued personal computers, laptops, file server, e-mail server, etc. without notification or requesting permission from the creator or user of the information or files.

* Such access may take place in the course of performing corrective or preventative maintenance.
* For investigative or business continuity purposes, access shall be initiated by a written request up through the relevant chain of command to the CISO, and should, to the extent deemed necessary, involve the HR representative for the HHSC Staff member's department.
* Access to an individual's e-mail without their consent is granted only after written approval by their manager or designee is submitted to the CISO. Requests for such access are granted for investigational or business continuity purposes and the mail should be submitted directly to HHSC facilities or HHSC Corporate Office Human Resources where it can be examined and shared with General Counsel, Internal Audit, Corporate Compliance, or Physical Security, as dictated by circumstances.

**4.3. Privacy of Personal Information**

Disclosure of personal information that is not classified as Confidential-Reportable about HHSC personnel to external parties should not occur unless permitted or required by law, or unless permitted by clearly documented and explicit consent of the employee whose information is being disclosed.

**4.4. Electronic Monitoring Areas**

Personnel may be subject to electronic monitoring while in HHSC Secure Areas, including data centers, communication rooms, and other areas where critical HHSC Information Assets have been deployed.

**5. Prevention of Misuse of Information Processing Facilities**

**5.1. Use of HHSC Equipment**

Computers, networks and software purchased by HHSC are the property of HHSC. Although HHSC may assign one or more HHSC personal computer, laptop, tablet, cellular phone, "smart phone" or similar personal computing devices for an individual's use, no presumption of exclusivity or entitlement should be inferred from such an assignment. Any such HHSC device may be reclaimed for other purposes, reassigned to another HHSC stakeholder, or retired at any time based on operational needs.

Any unauthorized activities, including those addressed by the Stakeholder Accountability and Responsibility in ITD 0051 Information Security Policy, will be subject to corrective action, including up to termination of employment in accordance with applicable collective bargaining agreements, and/or termination of business relationship with HHSC as appropriate.

**5.2. Internet Use**

HHSC provides access to the Internet for the sole purpose of supporting HHSC business processes, mission and goals.

The following provisions shall apply to HHSC Internet use:

* Access to the Internet must be in compliance with applicable statutes, regulations and HHSC policies, including those that prohibit harassment and discrimination in the workplace. In addition, users are expected to use common sense and judgment to avoid any communication that is disrespectful, offensive or illegal.
* Access to the Internet from workstations within the HHSC network shall be allowed only through a firewall.
* Monitoring and filtering of Internet activity shall be conducted to protect the security and availability of Internet services within the HHSC network. Monitoring of Internet usage may performed at any time and without prior announcement.
* The reproduction, forwarding, or in any other way republishing or redistribution of words, graphics or other materials obtained from the Internet shall be done only with the permission of their authors/owners. It shall be assumed that all materials on the Internet are copyrighted unless specific stated otherwise

**5.3. E-mail Use**

HHSC provides access to the e-mail for the sole purpose of supporting HHSC business processes, mission and goals. E-mail is to be used as a business tool to facilitate communication and information exchange required by users of the HHSC e-mail system.

The following provisions shall apply to e-mail use. This list is not exhaustive, and other provisions may be applied in accordance with future business use or statutory requirements:

* The enterprise e-mail system is owned by and maintained by HHSC to satisfy its business needs. Therefore all e-mail messages stored on the HHSC e-mail system is the property of HHSC.
* To maintain security of the HHSC computer network, only the following types of e-mail accounts are approved for use:
* HHSC e-mail system accounts
* Business related external web-based e-mail accounts approved by department managers and ITD management
* Web-based and third-party ISP e-mail accounts may not be accessed through the HHSC network, except where approved by the CISO for business purposes, and documented as a security exception.
* Automatic forwarding of HHSC e-mail system account messages to any external e-mail account is prohibited.
* HHSC e-mail system accounts may be accessed by system administrators to maintain the integrity and security of the HHSC e-mail system.
* E-mail messages that contain ePHI must not be sent to recipients outside of the HHSC e-mail system unless encrypted by HHSC approved encryption methods.
* Prohibited e-mail content practices include, but are not limited to:
* The sending of any chain-letter messages, discriminatory, obscene, derogatory, defamatory or any other types of inappropriate messages that may contain sexually explicit material, ethnic or racial slurs, or anything that could be interpreted as disparaging of others based on race, national origin, gender, sexual orientation, age, disability or religious or political beliefs.
* To enforce prohibited e-mail content compliance, HHSC Executive Leadership reserves the right to approve monitoring of user e-mail messages.

**5.4. Instant-Messaging Use**

Free instant-messaging services supplied by AOL, Yahoo, MSN, and other commercial carriers are not, as of the date of this policy, encrypted or secure, and must not be used to exchange any HHSC business- or patient related information, or messages that contain ePHI. Only instant-messaging software that is approved by ITD and that can provide encryption-in-transit, encryption-at-rest, and adequatelogging of instant-messages shall be used to exchange HHSC business- or patient related information.

**5.5. Text-Messaging Use**

Text-messaging services supplied by cellular phone carriers such as Verizon, AT&T, Sprint, and other commercial carriers are not, as of the date of this policy, encrypted or secure and must not be used to exchange any HHSC business- or patient related information, or messages that contain Protected Health Information (PHI). Only secure text-messaging services that are approved by ITD and that can provide encryption-in-transit, encryption-at-rest, and adequate logging of text-messages shall be used to exchange HHSC business- or patient related information.

1. **Regulation of Cryptographic Controls**

Any computer hardware or software that is produced by HHSC will comply with current federal statutes regulating the export of cryptographic technology.

1. **Protection of Information for Legal Processes**

When HHSC General Counsel presents the CISO with a request for a "litigation hold" on information, the CISO will notify the CIO or designee, who will then notify the appropriate System Administrators, Information Owners, and/or HHSC Information Security Team, and request they take necessary measures to preserve and collect the required data and information.

Whenever evidence clearly shows that HHSC has been victimized by a computer or communications crime, a thorough investigation must be performed by internal ITD Security Incident Response Team ("SIRT"). This investigation must provide sufficient information so that management can take steps to ensure that (1) such incidents will not be likely to take place again, and (2) effective security measures have been reestablished.

**7.1. Sources of Digital Evidence**

For every production computer system, the HHSC Information Security Team, SIRT, and/or System Administrators must identify the sources of digital evidence that reasonably could be expected to be used in a court case or requested by Legal Affairs for litigation holds. These sources of evidence must then be subject to a standardized capture, retention, and destruction process comparable to that used for vital records.

**7.2. Disclosure of Information to Law Enforcement**

By making use of HHSC systems, users consent to allow all information they store on HHSC systems to be divulged to law enforcement. HHSC Management shall reserve the right to determine what information will be divulged to law enforcement about users of HHSC systems. Information may be divulged if HHSC Management finds it reasonably necessary to (a) satisfy any applicable law, regulation, legal process or enforceable governmental request, (b) enforce security policies, including investigation of potential violations thereof, (c) detect, prevent, or otherwise address fraud, security or technical issues, or (d) protect against imminent harm to the rights, property or safety of HHSC, its users or the public as required or permitted by law.

All disclosure of information to law enforcement will be coordinated through HHSC General Counsel and HHSC Facilities' Security Departments.

**7.3. Internal Investigations**

Until charges are pressed or corrective action taken, all investigations of alleged criminal or abusive conduct must be kept strictly confidential to respect and preserve the reputation of the suspected party.

**7.4. Forensic Analysis Process**

Every analysis or investigation, using data storage media, that contains information that might at some point become important evidence to a computing crime or fraud and abuse trial, must be performed with a copy rather than the original version. This will help to prevent unexpected modification to the original information.

**7.5. Information Security Investigations**

All HHSC internal investigations of information security incidents, violations, and problems, must be conducted by trained staff authorized by the CISO.

1. **APPLICABILITY:**

This policy applies to all HHSC facilities and HHSC Corporate Office stakeholders. Compliance with this policy is mandatory. Compliance will include periodic reviews by the HHSC Information Security Team. Information Security Policy Exception Requests must be submitted in writing by relevant Management to the CISO, who will facilitate HHSC Leadership approval. Requests shall include justification and benefits attributed to such exception.

1. **RESPONSIBILITIES:**

The CISO is responsible for the oversight of compliance with legislative, regulatory and contractual obligations affecting protection of HHSC Information Assets; for approving investigations of HHSC Information Assets; and for providing leadership in the investigation and management of security events. The CISO is also responsible for reviewing changes in regulatory and statutory law that impacts information security, and updating organizational security policies to align with required security requirements.

The CIO is responsible for ensuring that all internally developed software applications comply with appropriate federal and state regulations and for ensuring that any HHSC developed program code and documentation include an HHSC copyright notice.

The HHSC Information Security Team is responsible for identification of digital sources of information and collection of electronic evidence to be used in court cases surrounding HHSC security events as outlined in ITD 132 Management of Information Security Incidents and Improvements Policy.

General Counsel is responsible for reviewing and communicating changes in applicable legislative laws impacting information security to relevant organizational areas; for providing guidance regarding monitoring of HHSC Users; and for maintaining and updating contracts to reflect changing and required legislative and regulatory language for security of information.

Corporate Compliance is responsible for reviewing and communicating impacts of Privacy legislation to relevant organizational areas; and for providing guidance to HHSC Users on their individual responsibilities and procedures to follow for safeguarding patient protected health information.

HHSC Management is responsible for educating staff so as to maintain awareness of policies to protect HHSC Information Assets, and giving notice of the intent to take corrective action against personnel for breach of security policies.

HHSC Stakeholders are responsible for giving credit to applicable parties for use of their respective intellectual property (IP) when used for HHSC business and to respect Copyright Laws; for using HHSC Information Assets in a manner that is in compliance with legislative, regulatory and contractual obligations; for protection and non-disclosure of protected health information in compliance with HIPAA Privacy and Security requirements.

**VI. REFERENCES:**

* ISO/IEC 27002:2005, an information security standard published by the International Organization for Standardization (ISO) and by the International Electrotechnical Commission (IEC), entitled Information technology - Security techniques - Code of practice for information security management:

o Section 15: Compliance Management Objectives

* 15.1 Comply with legal requirements
* Security Standards for the Protection of Electronic Protected Health Information 45 CFR Part 164 Subpart C; 45 CFR 164.308(a)(2);45 CFR 164.308(a)(3)(i); 45 CFR 164.310(b)