ELECTRONIC DEVICE AND INFORMATION USE POLICY
Section: Privacy and Security
Effective: March 2012
Applies to: All Joint Commission Enterprise Personnel

PURPOSE

To provide direction regarding the safe and secure use of enterprise-related information on both personal and Joint Commission owned Devices.

POLICY

The Joint Commission permits the use of various Devices by Joint Commission personnel whose job responsibilities include creating, transmitting, or accessing Electronic Systems that may contain Confidential Information. Personnel are required to comply with this policy if they use personal or company-issued Devices to connect to Joint Commission enterprise Electronic Systems in any way to access, store, or transmit enterprise-related information, including Confidential Information. Use of personal Devices solely to connect to Joint Commission enterprise Electronic Systems for the purpose of listening to and recording voicemails, or making phone calls is not use subject to this policy.

What this means to Personnel

- Personnel are responsible for the secure and safe use of Devices.
- Personnel are responsible for maintaining and updating personal Devices (i.e., the Information Technology Department will not support personal Devices, except as provided for in the Joint Commission Personal Electronic Device Remote Wipe Waiver).
- **The Joint Commission respects the rights of its employees to maintain their privacy and is committed to not infringing on these rights. E-mail and user accounts and their contents that do not contain information belonging to the Enterprise are considered private by The Joint Commission. Employees who use their own electronic devices can expect that their personal information will remain private and will not be viewed by The Joint Commission. The Joint Commission has no intention of accessing employees' personal information on their personal devices. However, there may be rare and exceptional circumstances when The Joint Commission may need to access an employee's personal device in order to comply with court orders or other applicable law, or to recover or protect Joint Commission property and security. It is important to note that employee privacy would still be protected even in those rare, extreme circumstances. In any effort to recover Joint Commission files, recover property or protect security, no access to the substance of personal emails would be permitted, and access to the device will not occur without the most stringent procedural protections on behalf of employees.**
- All enterprise information – including Confidential Information – that is accessed or stored on personal Devices is Joint Commission property.

- Like any company-issued Device, all enterprise information, including Confidential Information, stored on Devices must be returned to The Joint Commission when employment is terminated, or at the request of the Human Resources Department or the Office of Corporate Compliance and Privacy.
- Failure to comply with this policy may result in disciplinary action (see the Employee Handbook). Legal action also may be taken for violations of applicable regulations and standards.
- Personnel must use the Electronic Systems in strict compliance with The Joint Commission Code of Conduct, and Firewall, Confidentiality of Protected Health Information, and Confidentiality policies.

The Joint Commission may

- Inspect company issued devices at any time.
- Monitor, intercept and review outgoing and incoming e-mail, telephone conversations, voice mail recordings, instant messages and Internet and social media postings and activities on any company issued Device.
- For personal Devices, monitor and review outgoing and incoming corporate email and corporate hosted instant messages, in accordance with applicable law.
- Access, record, disclose, intercept, inspect, review, retrieve and print transactions, messages, communications, postings, log-ins, recordings and capture keystrokes on any company issued Device.
- Delete data if a Device is lost, stolen, or if the Authorized User is no longer employed by The Joint Commission or for any other reason that The Joint Commission deems reasonable and appropriate. Pursuant to the remote device waiver policy for personal devices.
- Remove from company-owned Devices material it believes is offensive, a security threat or illegal.
- Store copies of data and communications for a period of time and delete copies without notice.

DEFINITIONS

Authorized User – Any person authorized by the Information Technology Department to create, transmit, or access Confidential Information or Electronic Systems.

Confidential Information – Information defined in the Confidentiality and Confidentiality of Protected Health Information policies.

Devices – Any personal or company-issued electronic equipment or communication technologies (including Removable Media) that creates, transmits, or accesses the Electronic Systems or Confidential Information. These include computers, laptops, tablets/iPads, e-readers, e-mail, voice mail, telephones, smart phones, personal digital assistants, fax, and any similar equipment or technologies not yet produced.

Electronic Systems – Networks, servers (including The Joint Commission Blackberry® Server), voice mail, e-mail and other communication systems that are owned, leased or operated by The Joint Commission.

Legal Hold – Instruction issued by the Office of General Counsel to suspend the routine retention, storage, management and destruction policies for paper documents, electronically stored information, backup tape recycling, and archived media, therefore preventing the destruction, alteration, or mutilation of the documents or information.

Personnel – Includes the terms "officer," "commissioner or director," "employee," designated "contractors"," student "interns", "fellows" and "agents."

Removable Media – Any portable or removable data storage medium to which digital information can be written or exported, includes, magnetic tape, memory or flash drives (e.g., USB, SD, MS), floppy disks, zip disks, CD's and DVD's.

PROCEDURES **PERSONNEL**

1. Are only permitted to use the Electronic Systems, in a manner or for any purpose in strict compliance with The Joint Commission Code of Conduct, and Firewall, Confidentiality of Protected Health Information, and Confidentiality policies.
2. Should conduct all communications and transmissions of data over the Electronic Systems or using company issued Devices in strict compliance with all applicable policies, procedures, and guidelines. (See Electronic Communications, Intranet Use, and External Website Links.)
3. Should follow the retention guidelines, as set forth in the Records Retention policy, and retain pertinent electronic enterprise information if notified by the Office of General Counsel of a Legal Hold.
4. If accessing the Electronic Systems using a personal Device, must agree to this Policy and submit the Joint Commission Personal Electronic Device

Remote Wipe Waiver, before connecting any such Device to the Electronic Systems.

5. If accessing the Electronic Systems using a personal Device move the enterprise information to an Electronic System and delete it from their personal Device when the work is completed.
6. Removable Media and local C:\ drives are to be used for temporary storage only. Working storage or official documents should reside on Joint Commission Provided Systems.
7. Must not access or store Protected Health Information on a personal Device without the written consent of the Corporate Compliance Officer and Privacy Officer or Chief Information and Enterprise Security Officer.
8. Should not install any software on any company owned or issued Device for which the employee or enterprise does not hold a valid software license. The Joint Commission strongly supports adherence to software vendors' license agreements and copyright holders' notices.
9. Must not "auto forward" any Joint Commission e-mail or electronic data to systems outside the control of The Joint Commission (excludes telephones; telephones may be auto forwarded when personnel are working off-site).
10. Confidential Information may not be forwarded to any personal non-work related systems outside of the control of the Joint Commission.
11. Must follow the Reporting an Information Privacy or Security Incident policy to report any damage to or loss of a Device (including those personal Devices within the scope of this policy) or Confidential Information.
12. Should follow all minimum physical security procedures for Devices:
    - Do not leave Devices containing Confidential Information unattended, unless the Devices have been secured with locks or by the supervision of a responsible third party.
    - Do not check Devices as baggage when traveling; instead keep the Devices in their possession as carry-on luggage.
    - Position all Devices with visual displays so that the display and keyboard cannot be seen by others, or use a protective screen to prevent access to information by unauthorized individuals.
13. Should follow all minimum technical security procedures for Devices:
    - **Passwords:** Establish passwords, and follow all applicable security measures as outlined in the User Passwords policy.

- **Security timeout:** Enable the Device to go into a locked state after 30 minutes of inactivity. Enable the required use of a power-on password, following inactivity, to return the Device to its active state.
  - Do not allow a Device out of their possession without first placing them in a status requiring a log-in.
- **Failed login attempts:** The Joint Commission reserves the right to lock the Device after five failed attempts to log in to the Device.
- **Encryption:** Activate the encryption feature on all Devices, for all data stored on the Device, according to the Encryption policy.
- **Backups:** Make backups of all company-related information to Joint Commission Electronic Systems as soon as reasonably possible. The Joint Commission strongly recommends that personnel backup personal information. [Note: Some data is already backed up on enterprise systems; e.g., company e-mails do not need to be backed up because they are already backed up.]
- **Remote wipe**: Immediately notify IT in the event any Device is lost or stolen. The Device must be remotely wiped of all data and locked to prevent access by anyone other than IT or user. If the Device is recovered, it can be submitted to IT for resetting. [Note: The remote wipe will destroy all data on the Device, whether personal or business related.]
- **Device security modifications**: Do not modify any security measures put in place by The Joint Commission or native to the Device unless specifically authorized by the Chief Information and Enterprise Security Officer.

14. **Applicability of other policies:** Authorized Users must adhere to all applicable Joint Commission IT security policies, procedures, and security measures.

MANAGERS

1. For any reported loss or damage to a Device, (including those personal Devices within the scope of this policy) or Confidential Information, follow all procedures applicable to managers in the Reporting an Information Privacy or Security Incident policy.

COMPLIANCE

Failure to comply with this or any other security policy may result in disciplinary action (see the Employee Handbook). Legal actions also may be taken for violations of applicable regulations and standards such as ISO 17799:2005, HIPAA, HITECH, and others.

REFERENCES:

- International Standards Organization (ISO 27002 - Information Security Standard).
- HIPAA Final Security Rule, 45 CFR Parts 160, 162, and 164, Department of Health and Human Services, http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/default.asp, February 20, 2003.
- American Reinvestment and Recovery Act of 2009 (ARRA)/ (HITECH) http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_bills&docid=f:h1enr.pdf *(The HITECH Act begins at H.R. 1-112 through 1-165 (pp. 112 through 165 in the document). The security and privacy provisions are found at Subtitle D Privacy, beginning H.R. 1-144 (p. 144))*

APPROVALS

Policy Approval – This policy statement requires the approval of the Chief Information and Security Officer of The Joint Commission.

Procedure Approval – The initial procedure and any changes thereto require the approval of the Chief Information and Enterprise Security Officer.

♦ ♦ ♦

EFFECTIVE: March 2012
REVIEWED: March, 2012, December 2012, July 2013
MODIFIED: December 2012, July 2013

The Joint Commission

Personal Electronic Device Remote Wipe Waiver

Purpose

The purpose of this Waiver is to explain Remote Wipe Technology and to ensure that employees understand and agree to a Remote Wipe of their personal Devices when it is deemed necessary. Terms capitalized but not otherwise defined herein are to have the meanings given them under the enterprise's *Electronic Device and Information Use Policy.* Remote Wipe Technology is used to protect the integrity of Joint Commission enterprise information and Confidential Information (also referred to herein as "enterprise data"). Signing this Waiver is voluntary. However, all employees who use a personal Device to access, connect to, or use The Joint Commission's Electronic Systems are required to sign this Waiver after reading the enterprise's *Electronic Device and Information Use Policy*.

Definitions

Cloud Storage: A service provided to users of computers and electronic devices in which data is maintained, managed and backed up remotely through the Internet, or "Cloud."

Remote Wipe Technology: Technology that erases all data on a Device and resets the Device to the factory settings.

Remote Wipe: The remote removal of all Device-based data, such as mail, calendar, photos, and contacts from the Device. The Remote Wipe destroys all data on the Device, whether personal or business related. A user's data may also remain available through a web browser or cloud data storage.

Applicability

This Waiver applies to the same personal Devices and employees outlined in the *Electronic Device and Information Use Policy*.

Employees who do not connect their personal Devices to The Joint Commission enterprise's Electronic Systems are not required to sign the Waiver.

Employees who connect their personal Devices to The Joint Commission enterprise's Electronic Systems solely for the purpose of listening to and recording voicemails, or making phone calls are not required to sign this Waiver.

Employees that qualify as Non-exempt under the Employee Handbook, are not eligible to connect their personal Devices to The Joint Commission enterprise's Electronic Systems, and therefore are not required to sign the Waiver.

Remote Wipe

If a Device is lost or stolen, the employee should immediately notify the Information Technology Department. The Device must undergo a Remote Wipe of all enterprise data and be locked to prevent access by anyone other than IT or the user.

When a Remote Wipe is initiated by the IT Department, the user's Device is wiped of all data and restored to the factory default settings. **The Remote Wipe is not limited to enterprise data.** Data that the employee has added to the Device for personal use is also deleted. This data cannot be recovered on the Device itself, but can usually be restored if the data has been backed up on another Device such as a personal computer or on Cloud Storage, and **employees should back up personal data frequently to minimize loss if a Remote Wipe is necessary.** Employees should back up enterprise data as required under the *Electronic Device and Information Use Policy*.

A Remote Wipe is initiated only when the IT Department is instructed to do so by the HR Department, the Office of Corporate Compliance and Privacy, or as otherwise required. Examples of situations requiring Remote Wipe include:

- Theft of the Device
- Loss of the Device
- Termination of employment, when it cannot be verified that the employee had the Device reset to factory settings, wiped the Device of enterprise data, or used another acceptable method to remove enterprise data.

Employee Declaration

I, _____, hereby attest that I have read and understand the above *Personal Electronic Device Remote Wipe Waiver*.

I acknowledge and agree that The Joint Commission may Remotely Wipe any Device I use to receive company e-mails or access Joint Commission enterprise Electronic Systems. I acknowledge and accept that the Remote Wipe may be done at anytime without warning and would also include the erasure of any and all information, company or personal, residing on the Device that I am using to receive company e-mail or connect to Joint Commission enterprise Electronic Systems in any way (except as specifically excluded herein) to access, store, or transmit enterprise-related information, including Confidential Information. However, under normal circumstances, a Remote Wipe will only be initiated as provided for in this Waiver.

_____ _____

Employee Signature Date

_____ _____

Manager Signature Date

_____ _____

IT Administrator Signature Date