[redacted]

Internal Procedure
IT.912P

Self-Audit Procedures

Purpose:

To ensure all GHS IT policies, standards and procedures are being upheld; to provide a more secure computing environment; to comply with federally mandated rules and regulations regarding protection of health information and personal information; to aid in on-going process improvement in GHS' security compliance program.

Definitions:

NIST = National Institute of Standards and Technology

Procedure:

Overview

Quarterly, an internal self-audit is performed. This audit shall encompass the current written policies, standards and procedures that exist within the IT department at GHS. Each policy, procedure, or standard shall have written auditing procedures that can serve as proof that the policy, standard or procedure is being upheld. Although a subset of the total policies, standards and procedures is selected for each quarterly audit, every policy, standard and procedure shall be internally audited at least once per year. The GHS Systems Security Officer shall provide leadership and management of the self-audit process.

Methodology

A minimum of one-third of the total number of IT-related or security-related policies, standards and procedures shall be audited each quarter. All incomplete and failed items (see Scoring, below) shall be targeted for re-audit during the next quarterly self-audit.

The list of policies, standards, and procedures to be audited shall be made available to the IT department a minimum of 30 days in advance. For each policy, standard, or procedure, a list of self-audit procedures is documented, that when performed, shall serve as evidence of compliance with that policy, standard, or procedure.

Resources to conduct the self-audit may be comprised of existing staff and/or contract staff, as needed. Under no circumstances would a staff member be responsible for auditing items for which they are the primary source of implementation or compliance.

Scoring

A Self-Audit Worksheet is used to track the procedures being audited and the outcome. Each item being audited is worth 1 point. Outcomes for each item may be categorized as:

- Passed – (P) the procedure had the expected outcome; compliant. 1 point is awarded.
- Incomplete – (I) the outcome met the intent only partially; compliant with errors. 0.5 point is awarded.
- Failed – (F) the procedure did not meet the expected outcome; non-compliant. 0 point is awarded.

All incomplete (I) and failed (F) outcomes shall be accompanied by comments which detail the findings, including why a specific procedure failed or was only partially met. The scoring goal for each self-audit

[redacted]

shall be 100%. If the total score of a self-audit falls below 75%, the incomplete and failed items shall be re-audited within 45 days (rather than waiting until the next scheduled quarterly self-audit). This is done to speed up compliance on the non-compliant items, and to ensure that no more than one-third of the items on the following quarterly audit will consist of delinquent items from a previous audit. All items that fail on the re-audit must be included in the next quarterly self-audit, and shall be brought to the attention of the Systems Security Officer, the Sr. VP of IT, the VP of Enterprise Systems, and the Sr. Manager of Systems and Network Operations.

Reporting

At the conclusion of the self-audit, a written report shall be prepared containing:

- the Self-Audit Worksheets used,
- the scores on each item, total points, and score (expressed as a percentage),
- a summary of compliance by policy, standard or procedure,
- an explanation and recommendation for the most serious failures,
- the "lessons learned" and/or ways to improve the self-audit process going forward.

This report shall be presented to the GHS Systems Security Officer within 14 days of the conclusion of the self-audit, and shall be signed by the GHS Systems Security Officer, Sr. VP of IT, and the VP of Enterprise Systems. The GHS Systems Security Officer shall store this report in a secured location having limited, controlled access. These reports shall be considered proprietary and confidential materials of [redacted], and are for internal consumption only (within [redacted] and [redacted]). These reports shall be kept for a minimum of 3 years.

As a by-product of the "lessons learned," updates to the policies, standards and procedures shall be made, if appropriate, including updates to this Self-Audit Procedure.

Audit Process:

1. Ask the Systems Security Officer for the last two Self-Audit Worksheets and Reports. These shall be stored in a secure location (such as a locked drawer, cabinet, etc.).
2. Review the scoring, comments and point totals on two Self-Audit Worksheets selected at random over the past year. Verify that:
    a. comments are shown for each incomplete or failed item,
    b. the correct points were awarded,
    c. the total scores (percentages) were calculated appropriately.
3. If a total score of less than 75% was obtained during any self-audit during the past year, verify that a re-audit of incomplete and failed items was performed within 45 days.
4. Review the last two Self-Audit Worksheets. Look for failed and incomplete items on the older Self- Audit Worksheet, and verify that these were re-audited in the subsequent self-audit.
5. Verify that a minimum of 3 years worth of self-audit reports are being kept on-file.

Related Policies and Procedures:

IT.021 Security Assessment Policy
Self-Audit Worksheet

Revision History

Revision #	Team Lead (Systems Security Officer)	Approval Date	Department Manager (Sr. VP of IT)	Approval Date	Effective Date
[redacted]	[redacted]		[redacted]		