[redacted]

Internal Procedure
IT.906P

Server Room Access

Purpose:

Describes access procedures for the [redacted] server and network communications room.

Definitions:

Server Room: The controlled environment which houses the GHS production servers, network equipment, telecommunications equipment, and associated peripherals.

Procedure:

Authorized Access

There are two entry/exit doors into the server room, both with the same entry mechanics. Entry to the server room may be obtained via any of the following methods:

1. Swipe of the user's magnetic identification badge
2. Entry of a combination on the door's keypad
3. Door key

All staff at GHS have a magnetic identification badge; however only authorized, approved individuals at GHS have their badges coded to permit entry to the server room. Only a subset of those authorized, approved staff know the combination to the door's keypad, or have a physical key. The physical key and keypad are used only during times of power outage which would preclude the use of the magnetic door swipe. The building management company maintains a log of magnetic door swipes for a period in excess of 3 years.

The [redacted] building management company and office cleaning staff has access via physical keys and magnetic cards. They do not have the combination to the keypad on the door.

All trash is placed outside the door of the server room so that the cleaning staff does not routinely need to enter the server room. If/when periodic cleaning of the server room is needed, the cleaning staff is accompanied by an authorized staff member and would sign the visitor log.

Visitor Access

An authorized staff member must escort any non-authorized employee or visitor in the server room. This includes: employees with no ID badge access, vendors, contractors, building maintenance personnel. Upon entry, a visitor's log must be completed that indicates:

i. Date and time of entry.
ii. Visitor's name
iii. Purpose of visit.
iv. Company Name
v. Date and time of exit.

The Visitor's log is kept consecutively, with a new sheet started each year. As a sheet is filled, it is filed in the Network Operations Manager's files. The file cabinet or Manager's office is locked when not in use. These records are kept for current year plus three (3) years.

[redacted]

Requests for Access

Request for access is made to one of three individuals: the Infrastructure Manager, the Network Operations Manager, and the VP of Enterprise Systems. If approved, one of these individuals will notify the [redacted] Facilities Coordinator, who will in turn notify [redacted] Building Management to implement the identification badge access to the server room for the new user. [redacted] Facilities Coordinator notifies the requesting authorized manager that the update is made for the new user access.

Audit Process:

1. One of the three authorized managers may request a list of swipe card entries into server room from the Facilities Coordinator, who then requests it from [redacted] Building Management.
2. Verify that authorized and non-authorized magnetic identification badges provide access or restrict access as intended.
3. Track all available keys to the server room. Only the Infrastructure Manager and the Network Operations Manager have keys.
4. Check both doors to ensure consistency of magnetic badge and physical key access.
5. Observe if users are routinely entering without swiping their authorized magnetic badge.
6. Observe if doors are being propped open or have been tampered with to prevent door closing/locking.
7. Review visitor's log to ensure entries are being made.
8. Verify that non-authorized individuals cannot request access logs or new user access from the [redacted] Facilities Coordinator.
9. Verify this procedure has been reviewed annually.

Related Policies and Procedures:

IT.031 Physical and Environmental Security

Revision History

Revision#	Team Lead	Approval Date	Department Manager	Approval Date	Effective Date
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

When printed, this document is uncontrolled. Please verify that you are using the most current policy or procedure based upon the controlled document on the [redacted] Intranet.