[redacted]

Standard

Passwords

Department	IT
Date	05-04-2009
Policy Number	IT.003S

Replaces	
Policy Number	HRC.006 & IT.001.002
Date	05-04-2009

Review Frequency	Annual
Next Scheduled Review	05-2010
Page Number	Page 1 of 3

Purpose:

Establishes standards for implementation of passwords for user authentication to GHS' network and systems.

Related Policies & Procedures:

IT.023 User Access Policy
IT.001P Granting and Revoking Access Privileges

Replaces:

HRC.006 Password Policy
IT.001.002 Domain Access Passwords

Standard:

GHS' information systems and network have access and authentication controls which employ user ID and passwords unique to each individual user. User IDs and passwords, as a means of authentication, restrict user privileges on the system to only those files, applications, data and system resources needed for that user's job.

The display and printing of passwords shall be masked, suppressed, or otherwise blocked/obscured, to prevent unauthorized parties from discovering them.

Passwords, along with their corresponding user IDs, must <u>not</u> be inserted into email messages or other forms of electronic communication.

All vendor-defined or system default passwords shall be changed or deleted before the system is attached to the GHS network. No user shall log into the GHS network or system(s) anonymously (for example, by using a "guest" account). Every user login must employ a user ID and password that clearly indicates their identity.

Initial passwords issued for new users by the IT Department shall be valid only for the new user's first log-in session. At that time, the user shall be forced to choose another password. This process also applies to resetting a user's password, in the event that a user has forgotten their password.

All passwords (e.g., email, web, desktop computer, system administrator, root-level, etc.) must be changed every 60 days. Users will receive system generated reminders to change passwords in advance of their expiration date. If warranted due to security concerns, the IT Department may force password changes immediately (upon next log in).

All system administrator passwords on production systems shall be administered via the IT global password management database. User accounts that have system-level privileges granted through group memberships must have a unique password from all other accounts held by that user.

[redacted]

Department
IT
Date
05-04-2009
Policy Number
IT.003S

Replaces
Policy Number
HRC.006 & IT.001.002
Date
05-04-2009

Review Frequency
Annual

Next Scheduled Review
05-2010

To prevent password guessing attacks, where systems software permits, GHS shall limit the number of consecutive attempts to enter an incorrect password to not greater than five (5) attempts. Once the limit is reached, the user's ID will be locked out for a period of not greater than 30 minutes. The user may contact the IT HelpDesk to reset a forgotten password.

Password Construction

Users must choose passwords which are difficult to guess, are not based on personal information (such as a SSN, name, or address, for example), and are not words found in the dictionary (nor slang or jargon words). In addition, passwords must meet the following guidelines:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Be at least eight characters long.
- Can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" (*Do not use this example as a password).*

Password Use and Protection

All passwords shall be treated as sensitive and confidential information. In addition, the following guidelines must be observed:

- Passwords should never be written down or stored on-line.
- Do not share passwords with anyone, including administrative assistants, supervisors, or family members.
- Do not use the same password for Company accounts as for other non-Company access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various Company access needs (for example, the same password for voicemail as for email).
- Do not reveal passwords over the phone.
- Do not reveal passwords in an email message.
- Do not talk about passwords in front of others.
- Do not hint at the format of a password (e.g., "my family name").
- Do not reveal passwords on questionnaires or security forms.
- Do not reveal passwords to co-workers while on vacation.
- If someone demands a password, refer them to this document or have them call the IT HelpDesk.
- Do not use the "Remember Password" feature of applications (e.g., Outlook, Internet Explorer, etc.).
- Do not store passwords in a file on ANY computer system (including PDAs or similar devices) without encryption.

If an account or password is suspected to have been compromised, report the incident immediately to the IT HelpDesk and immediately change the password(s).

Application Development

Application developers shall ensure their programs contain the following security precautions:

- Authentication of individual users, not groups.
- Do not store or display passwords in clear text or in any easily transferrable form.
- Role management, such that one user can take over the functions of another without having to know the other's password.
- Support for TACACS+, RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

[redacted]

Notice

[redacted] reserves the right to interpret, change, amend, extend and audit compliance with this standard as needed to maintain a secure computing environment for the company.

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.

Department
IT
Date
05-04-2009
Policy Number
IT.003S

Replaces
Policy Number
HRC.006 & IT.001.002
Date
05-04-2009

Review Frequency
Annual

Next Scheduled Review
05-2010

Page Number
Page 3 of 3