Global Information Assurance Certification Paper

Password Management

GIAC HIPAA Security Certificate
GHSC Practical Assignment Version 1.0

Julie L Baumler, CISSP, GSEC, GCUX

June 2004

Abstract -

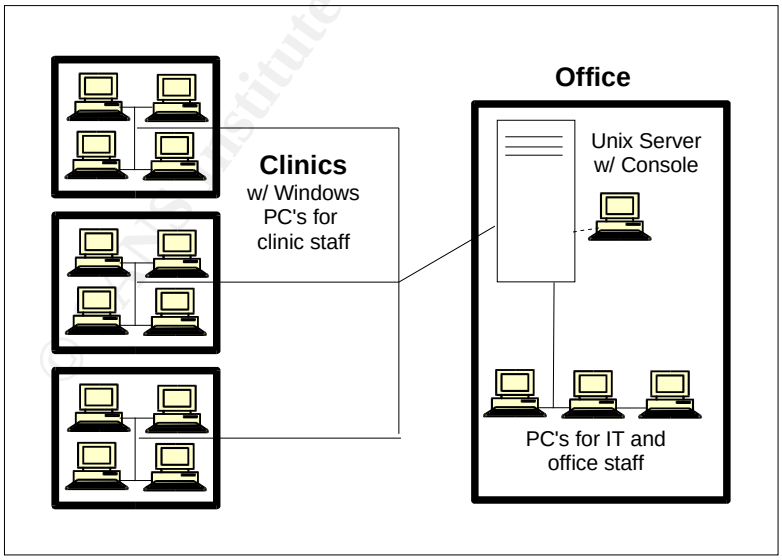
This paper discusses the HIPPA Security Rule 164.308(1)(5)(ii)(D) Administrative Safeguard Security Awareness and Training – Password Management. A sample policy and procedures to meet the requirements of this implementation specification in a community health care clinic setting using Unix and Windows is provided.

Assignment 1 – Define the Environment

GIAC Health provides community-based health care in a small metropolitan area. They have their own in-house electronic medical records system to access and track health records for patients in their clinics.

The records system is a client-server program with both graphical Windows and command-line Unix clients. The records system server runs on a small Sun server running Solaris 9. Clinics have PC's running Windows 2000 Professional for health care staff to access the records system. These PC's are part of a single Windows 2000 Active Directory domain (Windows 2000 Server - Service Pack 4.) The command-line client has additional reporting features and is used by clinic managers via SSH connections (using PuTTY) to the Solaris server. The records system uses the underlying client OS for authentication. The Solaris system has been configured to use MD5 passwords allowing for passwords over 8 characters in length.[1]

The following diagram show a logical view of the systems in GIAC Health as they apply to this paper. Note that supporting infrastructure such as Windows Domain Controllers, network equipment, firewalls, etc are omitted from this diagram.



1 Bruno Saverio Delbono, "Extending Solaris 8 char Password Limit," 27 May 2004, <http://www.mail.ac/users/bruno/solarispasswords.html>.

Assignment 2 – Explanation

Security Awareness and Training – Password Management

Password Management is part of the Security Awareness and Training Standard in 164.308(1):

> (5)(i) Standard: Security awareness and training. Implement a security awareness and training program for all members of its workforce (including management).
>
> (ii) Implementation specifications. Implement:
>
> (D) Password management *(Addressable)*. Procedures for creating, changing, and safeguarding passwords.

The Security Awareness and Training Standard details items that should be part of an employee security awareness and training program. This is an administrative safeguard, this means that it is most likely to be met through human factors, not technical ones, in this case by implementing a training program. The act specifies that the security awareness and training program should include security reminders and information on procedures regarding protection from viruses, worms, trojans and other malicious software; monitoring log-in attempts; and password management. The type of program required is open-ended, it could be anything from a formal training program to a check-off of information to be covered during informal training by knowledgeable co-workers.

The password management portion of the security information and training program should include information for users on how to create passwords, how to change passwords, and how to keep passwords safe. Password creation could be interpreted two ways, as setting a password as a part of initial account setup and as choosing an appropriate password. Both meanings are important in this context and should be addressed. Walsh identifies best practices in this area as including training on good passwords as well as how to remember passwords.

This implementation specification is addressable, not required, likely because you could use other methods of authentication, such as various token or biometric authentication schemes, rather than passwords. If an alternate authentication scheme is used, there is no need to do training regarding passwords, but this fact must be documented. Although not explicitly required by the act, the training and awareness program in a biometric or token authentication environment should include equivalent topics for your authentication scheme such as getting your token, what to do if your token is lost, enrolling in the biometric system, and what to do if the biometric being used changes.

Assignment 3 – Policy

GIAC Health's Password Policy is written to ensure compliance with the HIPAA implementation specification 164.308(1)(5)(ii)(D) Password Management. It should be noted that the act specifies that employees should be trained on password management and this policy addresses mainly the actions that should be taken in this area; however, following this policy will ensure both that users are trained in password management and are managing passwords appropriately. It may be appropriate to have a more technically focused policy that addresses auditing to ensure that the password policy is being met and installing technical controls to enforce these policies, these were left out of this policy to simplify understanding for the many line employees who merely need to know about password management.

Password Policy

1. Overview
   Passwords are often the last line of defense for access to important GIAC Health resources and client data. Passwords are used to prove that the user is authorized to use a computer account and gain the privileges and access that accompanies that account. All GIAC Health employees with computer accounts are responsible for taking the following steps to ensure the security of passwords for their accounts on the GIAC Health systems.
2. Purpose
   The purpose of this policy is to establish a standard for password creation, password life, and password protection.
3. Scope
   This policy applies to all personnel and contractors of GIAC Health who have a computer account.
4. Policy
   4.1Password Construction
   - Passwords should contain at least 6 characters, 10 to 14 is better.
   - Passwords should consist of a mix of at least 3 of the four following groups:
     - Lowercase letters (a-z)
     - Uppercase letters (A-Z)
     - Digits (0-9)
     - Other printable characters (i.e. !@#$%^&*)
   - Passwords used on GIAC Health systems should be unique and not used for any other purpose. The same password may be used on the GIAC Health Windows and Unix systems.
   - Passwords should not contain the account name or any personal or identifying information about you, such as hobbies, family names, important personal dates, etc.

4.2 Password Management

4.2.1 Password Reset and Initial Password Assignment

- Asking to have a password reset when needed shows your concern for GIAC Health security[2].
- The help desk can create accounts and reset passwords on request of a supervisor for one of his or her underlings, supervisors will pass the password on to the user.
- To the extent possible, someone in each building and each shift will be trained and given access to reset passwords for their co-workers in their building.
- When passwords are reset or initially assigned, the passwords will be set so that they must be changed by the user upon login.

4.2.2 Changing Passwords

- Passwords should be changed every six months at minimum, every 90 days is recommended.
- Passwords should be changed immediately and the help desk notified if you have any reason to believe your password has been guessed or you have lost control of a written password or hint.
- Passwords should not be reused and new passwords should be significantly different from your previous password.

4.2.3 Password Safekeeping

- Passwords or password hints may not be placed or displayed on your desk or work area.
- If you have difficulty remembering your password, you may keep the password, or ideally a hint, to remind yourself of your password, in an unlabeled manner securely in your possession or locked in your locker or file cabinet. Ideally, this would only be used for the first day or so after changing your password.
- Passwords should never be emailed or placed in any electronic document. New/reset passwords may be given over the telephone only by Help Desk staff and others whose jobs include password reset responsibilities only to the authorized (and known) supervisors or from a supervisor to a staff member.
- You will never be asked for your password by any GIAC Health Staff member and should never give your password to anyone else.

4.3 Shared Accounts and Application Administration Accounts

- Passwords for shared accounts (such as Unix root accounts, network equipment management accounts, or administrative accounts for applications) will only be shared as directed by your supervisor or manager. The supervisor or manager is responsible for notifying the Security Officer of each shared account and who has access when it is created and each addition or removal of access to a shared account.

2 Rick Vanover, "Lock IT Down: Make a Password Policy Part of Your Security Plan," 1 June 2004, <http://techrepublic.com.com/5100-6264_11-1039746-1.html,> 19 February 2002, p. 2.

- In addition to regularly scheduled password changes, shared account passwords will be changed any time anyone who has the password leaves or changes duties so that the existing access is no longer needed.
- Whenever possible, alternate mechanisms, such as sudo, will be used to to allow Application Administration Accounts to not be used as login accounts.

4.4 On-Going Training

- The Security Officer is responsible for updating and distributing a document describing methods for creating compliant, memorable passwords to all users on a biannual basis.

5. Enforcement
   Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.
6. Definitions
7. Revision History
   1 June 2004 – original document

Assignment 4 – Option B – Procedures

The following procedures must be performed in order to comply with the GIAC Health Password Policy:

- Choosing a Good Password
- Random Password Generation
- Password Change and Initial Logon Procedures – Windows
- Password Reset / Initial Password Setting – Windows
- Password Change and Initial Logon Procedures – Unix System
- Password Reset / Initial Password Setting – Unix System
- Shared Account Management

CHOOSING A GOOD PASSWORD

Intended Audience: All GIAC Health Staff

PURPOSE: This document is intended to assist GIAC Health staff in choosing a password that meets the requirements of the GIAC Health Password Policy and is easy to remember.

ASSUMPTIONS: This document assumes the following:
- readers have read the GIAC Health Password Policy

DISCUSSION:
Your password protects our patients personal information and the company's data. It is important to to pick a strong password and protect it well to protect this crucial information. It is significantly easier to come up with a good password when some forethought is put into it, rather than when you are sitting at the password change prompt.

The password policy requires that users pick passwords which are at least 6 characters, ideally 10 to 14, and consist of a mix of upper and lower case letters, digits, and other printable characters (at least three of these elements must be present in a password.) The password should be unique to the GIAC Health systems and should not be easy for others to guess – for instance it should not contain the account name or personal information. However, the policy also discourages and limits writing down passwords to avoid password theft, this requires a memorable password, rather than one that is simply random.

A good password:

- is not guessable by any program in a reasonable time (less than one week)
- is easily remembered (so there is no need to write it down)
- is private (it is used and known by one person only)
- is secret (it does not appear in clear text in any file or program or on a piece of paper pinned to the terminal).[3]

AVOID common password guesses, such as:
- names (personal, family members, pets, fantasy characters,...)
- important dates (public or personal)
- words from the dictionary or popular slang (there are a number of automated "dictionary attack" tools to guess passwords)
- things easily known about you – your hobbies and interests, your favorite color, your car, your address

3 Lionel Cons, "Suggestions for Selecting Good Passwords," 1 June 2004, <http://www.slac.stanford.edu/comp/security/password.html>.

Some ways to find a memorable but secure password:
NOTE: examples here will specifically be oversimplified and inappropriate for our environment; do not use an example password from this or any password building tutorial.

- Pick a random password and then build a mnemonic .
  Example: eru)*>ER – even really ugly smiles star in the ER
- Pick a line from a song or a poem and use the first letters of each word for your password.
  Example: Happy Birthday To You - Hb2U
- Use something that reminds you of a piece of information so personal that you would not want anyone else to know it.
- Form a nonsense word by alternating between a consonant and one or two vowels[4] Add digits or other printable characters in the middle or at the end.
  Example: dioBa2Qo
- Use a word game similar to that featured in William Steig's children's book “CDB?” - using letters that are homonyms for words or syllables to create phrases.
  Example: See the bee? - CDB?

If you forget your password, ask your building's reset person to reset your password or have your supervisor call the help desk. Remember that “asking to have a password reset when needed shows your concern for GIAC Health security.”

If you must write down your password:
- It is better to write down something that will remind you of the password than the password itself.
- Keep your password reminder on your person or locked in your file cabinet or locker at all times. Do not leave a password or reminder in your workspace.
- Do not label your password or reminder as your password and do not write your username on the same piece of paper.
- Destroy your reminder when you memorize your password.

REVISION HISTORY: 1 June 2004 – original document
1 December 2004 and each six months thereafter - revised edition with changed password creation suggestions to be issued to all staff.

4 Cons.

RANDOM PASSWORD GENERATION

Intended Audience: Help desk staff and others who reset passwords.

PURPOSE: This document shows a simple way to gain a random password.

ASSUMPTIONS: This document assumes the following:
- You are logged in at the command prompt of Blossom – the GIAC Health Solaris/Unix system, for instance via PuTTY.

SKILLS NEEDED: Unix command-line

PERMISSIONS NEEDED: account on Blossom

If you are authorized to reset passwords and do not have an account on blossom, contact your supervisor to have an account created for you.

TASKS:
The following task takes place on the Unix server.

1) Generate some random strings.
   Command: `head /dev/urandom | strings`

   This command gathers some random data from the Unix system and displays the sets of printable characters.

   Example:

```
242) Blossom % head /dev/urandom | strings
r\eT
-j-3
qcAN
;x"Q
vx7D
K`(?
```

2) Use one or more of the sets of characters as needed to create an appropriate length password.

REVISION HISTORY: 1 June 2004 – original document

PASSWORD CHANGE AND INITIAL LOGIN PROCEDURES – WINDOWS

Intended Audience: Users of GIAC Health's Windows Systems

PURPOSE: This document shows how to login to the GIAC Health Windows System and change your password initially and in the future.

ASSUMPTIONS: This document assumes the following:
- You are using a standard GIAC Health Windows System

PERMISSIONS NEEDED: - GIAC Health Windows account. Your supervisor will give you your username and initial password.

TASKS:
1) Pick a new password. See the document "Choosing a Good Password" for help.
2) Get the login screen.

GIAC Health systems require you to press the <CTRL>, <ALT>, and <DELETE> keys simultaneously in order to login.

Example:

[5]

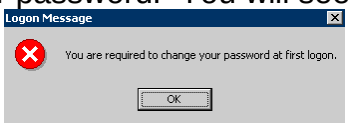
Ctrl + Alt + Delete

3) Enter your username and password in the spaces provided and click "OK".

Leave the "Log on to:" field set to GIAC.

4) Change your password.

The first time you login and whenever you have your password reset, you are required to change your password. You will see the following message:

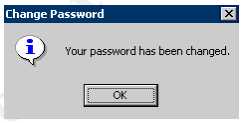


Click "OK".

5 Windows screen shots in this section are sanitized versions of those from Lamar State College "Changing Password on Windows 2000." See the Acknowledgments for further details.

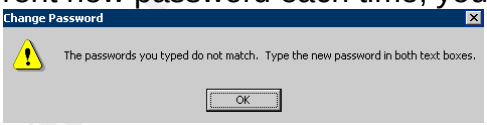
5) The “Change Password Screen” will appear:

- If you just logged in, your existing password will have been entered for you in the “Old Password” field; otherwise enter your current password in this field. All characters in passwords will be displayed as a set of asterisks (*).
- In the “New Password:” field, enter your new password.
- In the “Confirm New Password:” field, enter your new password again – this is to ensure that you typed it correctly.
- If you typed the new password the same both times, you will see the following message:



Click “OK” and the login process will continue.

- If you typed a different new password each time, you will see message:



Click “OK” and get another opportunity to type it in correctly twice.

6) Change your password every 3 to 6 months.

GIAC Health's password policy calls for changing your password a minimum of once every six months and ideally at least every three months.

To go back to the change password window in the future, press <Ctrl><Alt><Delete> when logged in to Windows. You will see the following window:

Click the “Change Password” button and the change password window will appear.

7) Contact the help desk if you have any further problems or your building's authorized password reset person if you forget your password.

REVISION HISTORY: 1 June 2004 – original document

PASSWORD RESET / INITIAL PASSWORD SETTING – WINDOWS

Intended Audience: Help Desk staff and others who reset passwords

PURPOSE: This document explains how to reset a Windows 2000 password. The same procedure can be used to set an initial password for a new Windows account.

ASSUMPTIONS: This document assumes the following:
- you are currently logged onto the GIAC domain and at the Windows 2000 command line.

SKILLS NEEDED: Windows 2000 command line

PERMISSIONS NEEDED:
- at minimum "Reset passwords on user accounts" permissions for the OU (Organizational Unit) the user belongs to.

TASKS:
The following tasks take place on any Windows 2000 workstation in our domain.

1) Ensure that you are authorized to reset the users password.
   Help desk staff are authorized to reset passwords in person for any employee with current GIAC Health ID and an existing account and over the phone for a supervisor for their employee or themselves. Employees assigned as the building password reset person can reset passwords for any employee known to them or identified by a supervisor as in need of a reset.
2) Determine the new password that you will use.
   GIAC Health policy requires using a random password. See the document "Random Password Generation" for a method of generating a random password.
3) Reset the password and force change for next login.

   Command: `dsquery user -samid username | dsmod user -pwd password -mustchpwd yes`

   - This command is all one line.
   - Replace "username" with the login name of the user whose password is being changed.
   - Replace "password" with the new random password.
   - You will get a reply that starts with "dsmon succeeded:" followed by the user's Distinguished Name (CN=...,CN=...,DC=giac,DC=org).

   Explanation: The "dsquery user" with the "-samid" flag finds the user's Distinguished Name (DN) in Active Directory, this is passed via the pipe to the "dsmod user" command. The "-pwd" flag to dsmod user changes the password to the next string provided. "-mustchpwd yes" forces a password change on next login.

REVISION HISTORY: 1 June 2004 – original document

PASSWORD CHANGE AND INITIAL LOGIN PROCEDURES – UNIX SYSTEM

Intended Audience: Users of GIAC Health's Unix System

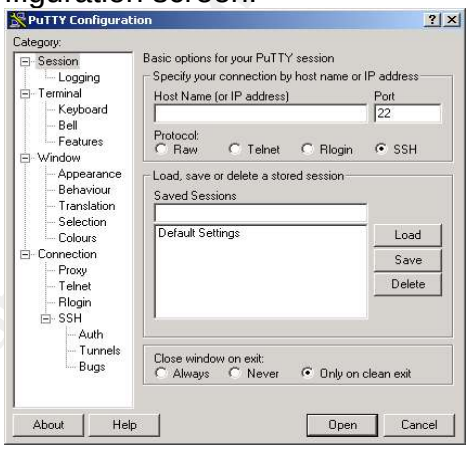
PURPOSE: This document shows how to login to the GIAC Health Unix System and change your password initially and in the future.

ASSUMPTIONS: This document assumes the following:
- You are logged in to a standard GIAC Health Windows System.

PERMISSIONS NEEDED: account on Blossom. Your supervisor will give you your username and initial password for Blossom.

TASKS:

1) Pick a new password. See the document "Choosing a Good Password" for help.
2) Start PuTTY from the Windows workstation.
   PuTTY is the terminal emulation program used at GIAC Health to connect to blossom.
   Command: Left click on the "Start" button.
   Pick "Programs->PuTTY->PuTTY"
   This opens the PuTTY configuration screen.



3) Connect to Blossom.
   Putty on the GIAC Health Systems has the default configuration set to our standards (an ssh connection) and will open with your cursor in the "Host Name (or IP Address)" box, all you need to do is type in the name of the host - "blossom" and press Enter.
   Command: Type "blossom", press the Enter key.
   This opens a new window with a connection to blossom and a request for your user name ("login as:")
4) Enter your username and password.
   Enter your username at the "login as:" prompt.
   Enter your current password when asked for you@blossom's password.

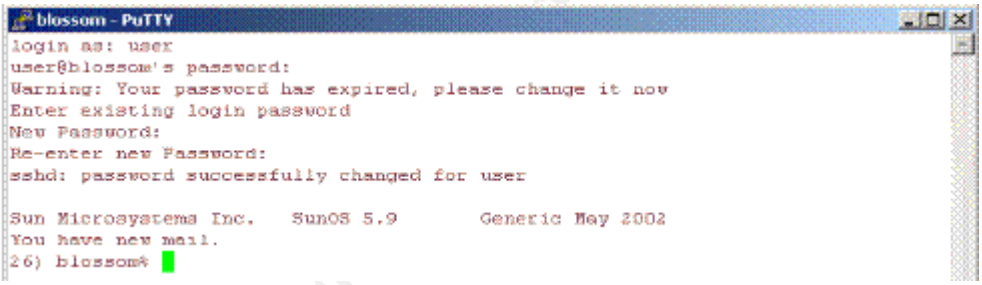
5) Change your password.
The first time you login and whenever you have your password reset, you are required to change your password. The system will say “Warning: Your password has expired, please change it now.”

- At the “Enter existing login password” prompt, enter your current password. You will not see any of the characters you type when entering passwords.
- At the “New Password:” prompt, enter your new password.
- At the “Re-enter new Password:” prompt, enter your new password again – this is to ensure that you typed it correctly.
- If you typed the new password the same both times, you will see the message “sshd: password successfully changed for your_name” and you are now done and at the blossom command prompt.
- If you typed a different new password each time, you will get the message: `passwd(SYSTEM): They don't match.`

  `Please try again`

  and get another opportunity to type it in correctly twice.

Example:



6) Change your password every 3 to 6 months.
GIAC Health's password policy calls for changing your password a minimum of once every six months and ideally at least every three months.

To change your password in the future, type the command “passwd” from the blossom command prompt.

Command: `passwd`

Example:

```
258) blossom% passwd
Enter existing login password:
New Password:
Re-enter new Password:
passwd: password successfully changed for user
```

7) Contact the help desk if you have any further problems or your building's authorized password reset person if you forget your password.

REVISION HISTORY: 1 June 2004 – original document

PASSWORD RESET / INITIAL PASSWORD SETTING – UNIX SYSTEM

Intended Audience: Help desk staff and others who reset passwords

PURPOSE: This document explains how to reset a Unix password. The same procedure can be used to set an initial password for a new Unix account.

ASSUMPTIONS: This document assumes the following:
- you are currently logged into blossom the GIAC Health Unix server.
- You are familiar with the Unix password command to the extent of being able to change your own password. (See the document "Password Change and Initial Login Procedures – Unix System", if needed.)

SKILLS NEEDED: Unix command line, using sudo

PERMISSIONS NEEDED:
account on blossom, member of the RESET sudo User_Alias.
You can check this by running "sudo -l", which will show at least the following information:

```
blossom % sudo -l
You may run the following commands on this host:
                (root) /bin/passwd
```

If you are trained in this procedure and do not have this access, email the help desk supervisor asking for this access.

TASKS: The following tasks take place on the Unix server.

1) Ensure that you are authorized to reset the users password.
   Help desk staff are authorized to reset passwords in person for any employee with current GIAC Health ID and an existing account and over the phone for a supervisor for their employee or themselves. Employees assigned as the building password reset person can reset passwords for any employee known to them or identified by a supervisor as in need of a reset.
2) Determine the new password that you will use.
   GIAC Health policy requires using a random password. See the document "Random Password Generation" for a method of generating a random password.
3) Reset the password.
   Command: `sudo /bin/passwd username`
   Replace "username" with the login name of the user whose password is being changed. The dialog will look very similar to when you change your own password using the password command. You will receive a number of prompts:
   - You may see the sudo "Password:" prompt – enter your password.
   - You will see the "New Password:" prompt from the passwd command, enter a random new password.
   - You will see the "Re-enter New Password:" prompt – enter the new password again.

4) Force the password to be changed at the next login.

Command: `sudo /bin/passwd -f username`

Replace “username” with the login name of the user whose password is being changed.

Example:

```
264) blossom% sudo /bin/passwd -f user
Password:
passwd: password information changed for user
```

REVISION HISTORY: 1 June 2004 – original document

SHARED ACCOUNT MANAGEMENT

Intended Audience: System, Application, and Network Administrators, their Supervisors, Security Officer

PURPOSE: This document describes the management of application and shared accounts.

TASKS:

- Shared accounts should be avoided and alternate mechanisms used whenever possible.
- Passwords to shared accounts should only be shared when ordered to do so by your supervisor.
- Whenever a new shared or application account is created, administrators need to notify their supervisor by the end of the business day. The supervisor must notify the Security Officer by the end of the week of the account name, purpose, and who has the password to the account.
- Supervisors must notify the Security Officer by the end of the week when the list of people with access to a shared account changes.
- The Security Officer will track shared accounts in the user management database and is responsible for reporting to supervisors on a quarterly basis which accounts they supervise and who has access.
- shared account passwords will be changed any time anyone who has the password leaves or changes duties so that the existing access is no longer needed.

REVISION HISTORY: 1 June 2004 – original document

Bibliography

Bain, Trevor. "Trevor's Command Line Notes." 3 June 2004. <http://ist.uwaterloo.ca/~etbain/CommandLine_Notes.html>.

Barnes, Vince. "A Password Policy Primer." 1 June 2004. <http://networking.earthweb.com/netsecur/article.php/10952_3076681_1>.

Cole, Eric, Jason Fossen, Stephen Northcutt, and Hal Pomeranz. SANS Security Essentials with CISSP CBK. Version 2.1. Vol. 2. GIAC Certification Series. The SANS Institute, 2003.

Cons, Lionel. "Suggestions for Selecting Good Passwords." 1 June 2004. <http://www.slac.stanford.edu/comp/security/password.html>.

Delbono, Bruno Saverio. "Extending Solaris 8 char Password Limit." 27 May 2004. <http://www.mail.ac/users/bruno/solarispasswords.html>.

Granier, T. Brian. "Unique User Identification." 11 April 2004. <http://www.giac.org/practical/GHSC/Brian_Granier_GHSC.pdf>.

Guel, Michelle D. "A Short Primer for Developing Security Policies." 28 May 2004. <http://www.sans.org/resources/policies/Policy_Primer.pdf>.

"JSI Tip 6820 What are the new Active Directory command-line tools in Windows Server 2003?" 3 June 2004. <http://www.jsiinc.com/subn/tip6800/rh6820.htm>.

"JSI Tip 7325 How do I reset most user's passwords, and/or force them to change the password at the next logon?" 3 June 2004. <http://www.jsiinc.com/subo/tip7300/rh7325.htm>.

Lamar State College – Port Arthur. "Changing Password on Windows 2000." 3 June 2004. <http://www.pa.lamar.edu/dept/cs/tutorials/2000passwd/prompted.html>.

Lamar State College – Port Arthur. "Changing Password on Windows 2000." 3 June 2004. <http://www.pa.lamar.edu/dept/cs/tutorials/2000passwd/user.html>.

Microsoft. "Dsmod user" 3 June 2004. <http://www.microsoft.com/windowsxp/home/using/productdoc/en/default.asp?url=/windowsxp/home/using/productdoc/en/dsmod_user.asp>.

Microsoft. "Dsquery user." 3 June 2004. <http://www.microsoft.com/windowsxp/home/using/productdoc/en/default.asp?url=/windowsxp/home/using/productdoc/en/dsquery_user.asp>.

Palmer, Michael J. MCSE Guide to Microsoft Windows 2000 Server. Cambridge, MA: Course Technology, 2000.

"Password Protection Policy." 28 May 2004. <http://www.sans.org/resources/policies/Password_Policy.pdf>.

Steig, William. CDB? Aladdin Paperbacks, 2003.

Tech Republic. "Sample Password Policy." 1 June 2004. <http://www.techrepublic.com/download_item.jhtml?id=r00220020214van01.htm>.

Vanover, Rick. "Lock IT Down: Make a Password Policy Part of Your Security Plan." 1 June 2004. <http://techrepublic.com.com/5100-6264_11-1039746-1.html.> 19 February 2002.

Walsh, Tom. "Best Practices for Helping to Comply with HIPAA Security Regulations." 25 May 2004. <http://www.rsasecurity.com/solutions/health/downloads/HIPAA_Best_Practices_1.pdf>.

ACKNOWLEDGEMENTS

The policy format is copied from T. Brian Granier's practical and the policies at http://sans.org/resources/policies. Granier's paper guided the format of this paper as well. The screen shots from Microsoft Windows used to document Windows password changes are sanitized versions of the ones from Lamar State College, as once sanitized they were identical in content to my own sanitized versions but displayed much more clearly.