Dwyer's Accounting

Cyber Security Policy

Samantha Sheehan

Computer Forensics and Security Year One

Security Policy

1. Overview

Employee misuse of resources is considered a major threat to any business. Management of this issue requires persistent monitoring, limited access and employee security awareness. Administrators responsibilities include software management, privilege level information sharing, limiting access to non-essential resources and careful monitoring to ensure compliance. Unsecured and vulnerable servers continue to be a major entry point for malicious threat actors. Consistent Server installation policies, ownership and configuration management are all about doing the basics well.

2. Purpose

The purpose of this policy is to establish standards for the use and maintenance of all equipment including internal server equipment that is owned and/or operated by Dwyer's Accounting. Effective implementation of this policy will minimize unauthorized access to proprietary information and technology.

3. Scope

All employees, contractors, consultants, temporary and other workers at Dwyer's Accounting and its subsidiaries must adhere to this policy. This policy applies to equipment that is owned, operated, or leased by Dwyer's Accounting or registered under a Dwyer's Accounting -owned internal network domain. This policy specifies requirements for equipment on the internal Dwyer's Accounting network.

4. Policy

4.1 Employee Hazards

4.1.1 Password Protection

4.1.1.1 All passwords MUST
•Contain at least 12 alphanumeric characters.
• Contain both upper and lower case letters.
• Contain at least one number (for example, 0-9).
• Contain at least one special character (for example, !$%^&*()_+|~-=\`{}[]:";'<>?,/).
4.1.1.2 All passwords MUST Not
• Contain personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
• Contain work-related information such as building names, system commands, sites, companies, hardware, or software.
• Contain number patterns such as aaabbb, qwerty, zyxwvuts, or 123321.
• Contain common words spelled backward, or preceded or followed by a number (for example, terces, secret1 or 1secret).
• Are some version of "Welcome123" "Password123" "Changeme123"
4.1.1.3 Users must not use the same password for company accounts as for other non- access (for example, personal ISP account, option trading, benefits, and so on).
4.1.1.4 User accounts that have system-level privileges granted through group memberships or programs such as sudo must have a unique password from all other accounts held by that user to access system-level privileges.
4.1.1.5 All user-level passwords (for example, email, web, desktop computer, and so on) must be changed at least every six months. The recommended change interval is every four months.
4.1.1.6 All system-level passwords (for example administration accounts, and so on) must be changed on at least a quarterly basis.

4.1.1.7 Passwords must not be shared with anyone. All passwords are to be treated as sensitive, Dwyer's Accounting Confidential information. This means passwords must not be inserted into email messages, text messages phone or face to face conversations.
4.1.1.8 Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.

4.1.2 Personal Equipment

4.1.2.1 The use of personal laptops to carry out tasks relating to Dwyer's Accounting is strictly prohibited.
4.1.2.2 Do not use personal storage devices such as hard drives, pen drives, usb sticks etc. with Dwyer's Accounting-owned equipment.
4.1.2.3 Do not access sensitive Dwyer's Accounting databases or client information using personal devices.
4.1.2.4 If employee e-mail, or other resources are being accessed with personal devices ensure appropriate security measures are taken (anti-virus/malware programmes such as MacAfee, encryption of sensitive information, regular updates etc.).
4.1.2.5 If employee e-mail, or other resources are being accessed with personal devices ensure network connection is private and secure. Do not access Dwyer's Accounting resources through open public access points under any circumstances.

4.1.3 Access restriction

4.1.3.1 Employee's internet access should be restricted to essential, productive, secure web browsing. Access to social media websites, message forums, media pages (YouTube etc.) will be denied.
4.1.3.2 Personal e-mail accounts should not be accessed through company equipment or network.
4.1.3.3 Employee's do not have access to install personal software on company equipment.
4.1.3.4 Personal cloud storage access will be denied. Sensitive client information, and/or information relevant to must not be stored in personal accounts.
4.1.3.5 Access to personal I.M. accounts will be denied.
4.1.3.6 Access to sites with public message boards, blog posts or any other forum type discussion will be denied.

4.1.4 Download restrictions

4.1.4.1 Do not download or install software on company equipment.
4.1.4.2 Do not download music, movies or any other media on company equipment.
4.1.4.3 P2P file sharing, file sync or any other file sharing service is strictly prohibited.

4.1.5 Misuse of Company Resources

All resources provided by the Dwyer's Accounting are to be used in the manner intended by management. Business e-mail is to be used strictly for company business. Software provided on company pc's is provided for Dwyer's Accounting related purposes only. Dwyer's accounting retains the right to monitor and access company accounts at any time to ensure the security and privacy of our company and our clients.

4.2 Administrative Duties
(In this instance, as there is no I.T. department, the administrator is the owner/manager, unless otherwise directly appointed by Dwyer's Accounting)

4.2.1 Password Management

4.2.1.1 Administrators are also expected to follow the password policy section 4.1.1 in this document.
In addition:
4.2.1.2 All system-level passwords (for example, root, enable, NT admin, application administration accounts, and so on) must be changed on at least a quarterly basis.
4.2.1.3 Applications installed by administrators must support authentication of individual users, not groups.
4.2.1.4 Applications installed by administrators must not store passwords in clear text or in any easily reversible form.
4.2.1.5 Applications installed by administrators must not transmit passwords in clear text over the network.
4.2.1.6 Applications installed by administrators must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

4.2.2 Software Installations

4.2.2.1 All software installations must be limited to the administrator. A request system will be available to employee's if they wish to use software other than what is available.
4.2.2.2 The administrator will obtain and track the licenses and test new software for conflict and compatibility.
4.2.2.3 The administrator will inspect and research rigorously any software request before an approval is made.
4.2.2.4 The administrator will research and inspect rigorously upcoming software, and maintain a list of approved software installations.
4.2.2.5 Operating system and software updates must be pre-approved and installed by the administrator.

4.2.3 Access Restriction

4.2.3.1 The administrator is responsible for restricting employee access to all non-essential resources mentioned above in section 4.1.3.
In addition:
4.2.3.2 Access to sensitive information will be implemented using the principal of least privilege. Sensitive company information is limited on a need to know basis, employee's having access only to what they need.
4.2.3.3 Web services available to employee's will be investigated and tested before approval.
4.2.3.3 Hyper-links listed on these services must also be investigated and either approve or disabled.
4.2.3.4 Internal resources must only be accessed by employees, controlled by the principal of least privilege, whereby access and file permissions are granted on a need to know basis.
4.2.3.5 External resources must be limited to essential, productive and secure web services or software which has been previously approved.

4.2.4 Hardware

4.2.4.1 An inventory must be maintained of computers, servers, terminals, modems and other access devices that are attached to the network.
4.2.4.2 Routine audits of hardware on the network must be carried out. Security gaps found must be resolved immediately.
4.2.4.1 External drives or other external hardware must be limited to or approved by the administrator before use on company equipment.

4.3 Server/Network Security

4.3.1 Server Configuration

4.3.1.1 Services and applications that will not be used must be disabled where practical.
4.3.1.2 Access to services should be logged and/or protected through access-control methods such as a web application firewall, if possible.
4.3.1.3 The most recent security patches must be installed on the system as soon as practical.
4.3.1.4 Always use standard security principles of least required access to perform a function.
4.3.1.5 Servers should be physically located in an access-controlled environment.
4.3.1.6 Servers are specifically prohibited from operating from uncontrolled cubicle areas.

4.3.2 Server Monitoring

4.3.2.1 All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
- All security related logs will be kept online for a minimum of 1 week.
- Daily incremental tape backups will be retained for at least 1 month.
- Weekly full tape backups of logs will be retained for at least 1 month.
- Monthly full backups will be retained for a minimum of 2 years.

4.3.2.2Security-related events will be reported to InfoSec, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security related events include, but are not limited to:
- Port-scan attacks.
- Evidence of unauthorized access to privileged accounts.
- Anomalous occurrences that are not related to specific applications on the host.

4.3.3 Network Security

4.3.3.1 Data encryption should be used on all files on the network and only the users authorised to view the data should have the decryption software.
4.3.3.2 Confidential files on the network should ask for a username and password then cross-match it with the access control list to see if the user should have access to the file. If someone who does not have access to the file tries to view the file, their username should be shown on the access control list log and flagged so that the network administrator can take action to stop the person attempting to access the file.
4.3.3.3 Use security cards to reduce the risk of unauthorised users accessing the server/network terminals and accessing restricted data.
4.3.3.4 A combination of firewall restriction and whitelisting should determine access to the network.
4.3.3.5 Administrative level privileges (the highest order privilege) determines access privilege for all other users on the network.

4.4 Physical Security

4.4.1 The non-public areas of the company premises are designated a secure area. Visitors are to be escorted at all times and a record of visitors kept in reception.
4.4.2 In order to prevent unauthorised access during silent hours an intruder alarm system must be installed.
4.4.3 All equipment owned by the company are to be inventoried regularly and be uniquely marked as being the property of Dwyer's Accounting.
4.4.4 All equipment storage areas are 'out of bounds' to visitors.
4.4.5 On-going maintenance arrangements are to be made for all essential equipment and installations and are to be reviewed at regular intervals by the administrator.
4.4.6 Equipment is not to be removed from the practice without the authority of the administrator.
4.4.7 At the end of each working day, all room occupants are to ensure that windows are fully closed and secured.
4.4.8 The last person to leave the building is responsible for:

- Ensuring that all security shutters are closed.
- Ensuring that the rear entrance door to the first floor is secured.
- Ensuring that the Intruder Alarm is set.
- Ensuring that the main door is secured.
- Ensuring that the side security gate is secured.

4.5 Malware Protection

4.5.1 Anti-Virus

4.5.1.1 All servers MUST have an anti-virus application installed that offers real-time scanning protection to files and applications running on the target system if they meet one or more of the following conditions:
• Non-administrative users have remote access capability
• NBT/Microsoft Share access is open to this server from systems used by non-administrative users
• HTTP/FTP access is open from the Internet
• Other "risky" protocols/applications are available to this system from the Internet at the discretion of the administrator
4.5.1.2 All servers SHOULD have an anti-virus application installed that offers real-time scanning protection to files and applications running on the target system if they meet one or more of the following conditions:
• Outbound web access is available from the system

4.5.2 Mail Server anti-virus
If the target system is a mail server, it MUST have either an external or internal anti-virus scanning application that scans all mail destined to and from the mail server. Local anti-virus scanning applications MAY be disabled during backups if an external anti-virus application still scans inbound emails while the backup is being performed.

4.5.3 Anti-Spyware
All servers MUST have an anti-spyware application installed that offers real-time protection to the target system if they meet one or more of the following conditions:
• Any system where non-technical or non-administrative users have remote access to the system and ANY outbound access is permitted to the Internet
• Any system where non-technical or non-administrative users have the ability to install software on their own

4.6 Encryption

Proven, standard algorithms such as DES, Blowfish, RSA, RC5 and IDEA should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. For example, Network Associate's Pretty Good Privacy (PGP) uses a combination of IDEA and RSA or DiffieHillman, while Secure Socket Layer (SSL) uses RSA encryption. Symmetric cryptosystem key lengths must be at least 56 bits. Asymmetric crypto-system keys must be of a length that yields equivalent strength. Key length requirements will be reviewed annually and upgraded as technology allows. The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by InfoSec. Be aware that the export of encryption technologies is restricted by the U.S. Government. Residents of countries other than the United States should make themselves aware of the encryption technology laws of the country in which they reside.

5. Compliance

5.1 Compliance Measurement

The administrator will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by the administrator in advance.

5.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Disclaimer

Sections of this policy have re-used some policy directives from various Sans policy templates, which carry the following free use disclaimer:

Free Use Disclaimer: This policy was created by or for the SANS Institute for the Internet community. All or parts of this policy can be freely used for your organization. There is no prior approval required.

More detailed explanations and a full glossary are available at their website:

https://www.sans.org/security-resources/glossary-of-terms/