American Vanguard Corporation

Information Technology Security Policies

PASSWORD POLICY

Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of AMVAC's entire company network. As such, all AMVAC employees (including contractors and vendors with access to AMVAC) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

General Password Construction Guidelines

Passwords are used for various purposes at AMVAC. Some of the more common uses include: user level accounts, email accounts, screen saver protection, voicemail password, and remote access logins. Every employee should be aware of how to select strong passwords.

Passwords must meet the following complexity requirements:

1. Not contain the user's account name or parts of the user's full name that exceed two consecutive characters
2. Be at least six characters in length
3. Contain English uppercase characters (A through Z)
4. Contain English lowercase characters (a through z)
5. Contain base 10 digits (0 through 9)

Password Protection Standards

Do not use the same password for AMVAC accounts as for other non-AMVAC access (e.g., personal ISP account, option trading, benefits, etc.). Do not share AMVAC passwords with anyone, including administrative assistants or secretaries.
All passwords are to be treated as sensitive, Confidential AMVAC information.

List of "dont's":

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't reveal a password to the boss
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation

If someone demands a password, refer them to this document or have them call someone in the IT department.

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Smartphones or similar handheld devices) without encryption.

All default system and equipment passwords must be changed. It is highly recommended that all passwords not controlled by the IT network infrastructure, be changed at least once every year. The AMVAC security system makes it mandatory that an employee changes his/her Network access **password every 90 days.** Reuse of network passwords is prevented. Password history is enforced to remember last **5 passwords**. Account lockout is enforced after **5 bad attempts**. Users may change their Network password at any time. The password must be changed immediately if it is suspected that the password has been compromised. The QAD passwords are changed every 90 days.

Administrative rights for Network and QAD are assigned only to AMVAC IT support personnel.

If an account or password is suspected to have been compromised, report the incident to IT support personnel and change all passwords.

COMPUTER, E-MAIL, INTERNET AND INTRANET USAGE POLICY

Overview

This policy sets forth AMVAC's policy with regard to computer, e-mail, Internet and Intranet usage, including access to, review or disclosure of e-mail messages sent or received by AMVAC employees, Internet and Intranet access and usage. AMVAC reserves the right to modify or update this policy at any time. Use of the computer system, e-mail system, Internet or the Intranet in violation of this policy can result in disciplinary action, including termination of employment.

AMVAC Computer Systems

AMVAC computer system, e-mail system, Internet and Intranet access (which are collectively called the "Computer System") are provided to employees at AMVAC's expense to assist them in carrying out AMVAC business and performing their job responsibilities.

AMVAC owns, maintains and is responsible for the Computer System. In the course of their employment, employees may use the Computer System to communicate internally with coworkers or externally with clients, consultants, vendors, and other business acquaintances. AMVAC provides its employees with the Computer System to facilitate business communications and to enhance their productivity. As with the telephone, there may be occasion to use the Computer System for personal purposes. Personal use is permitted so long as it does not interfere with job performance, consume significant resources, give rise to more than nominal additional costs, or interfere with the activities of other employees. Under no circumstances shall the Computer System be used for personal financial gain, or to solicit other for activities unrelated to AMVAC's business, or in connection with political campaigns or lobbying.

Access and Review of E-mail Communications, Internet and Intranet Usage

AMVAC treats all messages sent, received, or stored in the e-mail system as business messages.

AMVAC has the capability to access, review, copy and delete any messages sent, received or stored on the e-mail system. AMVAC also has the ability to access deleted messages in certain circumstances. AMVAC reserves the right to access, review, copy or delete all e-mail on the Computer System for any purpose and to disclose it to any party (inside or outside AMVAC). AMVAC reserves the right to review all computer files and communications to maintain system integrity and ensure that users are using the system appropriately, responsibly and in accordance with AMVAC policy and procedures.

Personal e-mail messages will be treated in the same way as business-related messages. AMVAC reserves the right to access, review, copy, delete, or disclose personal messages for any purpose. Accordingly, employees should not use the e-mail system to send, receive or store any messages that they wish to keep private. Employees should treat the e-mail system like a shared file system, and expect that any messages sent, received or stored in the system (or on hard drives) will be available to review by any authorized representative of AMVAC for any purpose.

When making use of the computer system, whether for business or personal use, employees and others should have no expectation that any communication or information transmitted over Amvac facilities or stored on company owned computers is or will remain private.

E-Mail Etiquette

Since e-mail messages may be read by someone other than the intended recipient and are corporate records that may be disclosed to outside parties or a court in connection with litigation, e-mail messages must be courteous, professional and businesslike. Remember that e-mail messages, once sent, are usually irretrievable. Be sensitive to the fact that, in the absence of explanation, e-mail messages may be ambiguous and convey the wrong impression. This is of specific concern when a message is being forwarded to multiple recipients. All e-mail messages should be carefully reviewed prior to sending and employees are advised to consider printing the messages and reading them first prior to distribution to ensure that their content is completely appropriate.

Storing and Deleting E-Mail Messages

AMVAC strongly discourages the storage of large numbers of e-mail messages for a number of reasons. First, because e-mail messages frequently contain confidential information, it is desirable to limit the number, distribution and availability of such messages. Second, retention of messages consumes storage space on the network server and

personal computer hard disks, and can slow down the performance of both the network and individual personal computers. Finally, in the event that AMVAC needs to search the network server, back-up tapes or individual hard disks for genuinely important documents, the fewer documents it has to search through, the faster the search can be done.

Accordingly, employees should promptly delete any e-mail messages they send or receive that no longer require action or are not necessary to an ongoing project. Employees should audit their stored e-mail messages periodically to identify messages that are no longer needed or should be deleted.

Subscriptions to Mailing Lists and Discussion Groups

No employee shall subscribe to any e-mail mailing list or discussion group, unless the subject and purpose of the list or group is directly related to the employee's job duties.

Confidentiality

Since e-mail is convenient to use, easy to send to multiple people and leaves a documentary record, employees must exercise a greater degree of caution in transmitting information via e-mail than they take with other means of communication (e.g., written memoranda, letters or phone calls). Employees are required to take particular care that confidential information of AMVAC or its customers is not transmitted or forwarded to outside individuals or companies not authorized to receive that information.

Permitted and Prohibited Uses

Use Primarily for Business Purposes

The use of AMVAC's Computer System is a privilege, not a right, and may be revoked.

Prohibited uses include, but are not limited to:

- Playing games on the computers;
- Intentionally wasting limited computer resources;
- Engaging in activities which disrupt the business environment of the workplace;
- Engaging in actions which damage computers, Computer Systems or computer networks;
- Using the Computer System for commercial purposes, for personal gain or profit, or to engage in illegal activity;
- Using the e-mail system to copy and/or transmit any documents, software or other information protected by the copyright laws; or
- Using the computer system in violation of AMVAC policies, including this Computer, E-mail, Internet and Intranet Usage Policy.

Additional Restrictions on E-mail Use

E-mail messages, whether created inside AMVAC or created outside AMVAC and transmitted within AMVAC, can generate claims or defamation, harassment and discrimination. Therefore, employees may not:

- Use the e-mail system to engage in any communications that are in violation of any policy, including AMVAC 's Equal Employment Opportunity or Sexual Harassment policies; or use the e-mail system to transmit or display defamatory, sexually explicit, obscene, offensive or harassing messages, images, cartoons, jokes or pictures.
- Messages that disclose personal information without authorization;
- Unwelcome propositions, requests for dates, or love letters;
- Profanity, obscenity, slander or libel;
- Ethnic, religious, or racial slurs; and
- Any other message that could be construed as harassment or disparagement of others based on their sex, race, sexual orientation, age, national origin, disability, or religious or political belief.

Internet and Intranet Use

An employee accessing the Internet and Intranet from an AMVAC site or remote site is responsible for all on-line activities which take place through the use of his or her login and password. When using another organization's networks or computing resources, employees must comply with the rules appropriate for that network.

Anti-Virus & Anti-Spyware

All systems are protected with Antivirus and Antispyware software. The two components of this software are the desktop client, and a central server, which checks for updated virus definitions daily, and updates the desktop clients on a daily basis. The anti-virus software provides protection from viruses or worms that attempt to control a system, and give a remote user unauthorized access to it.

Computer viruses can be injected into the Computer System through the receipt of e-mails, e-mail attachments, internet sites or files from other systems. Employees should exercise particular care when opening attached files and hyperlinks attached to e-mails. Employees must immediately inform IT support personnel of the presence of any virus or spyware on any AMVAC computer. Any computer that is infected or suspected of being infected must immediately be disconnected from the network to reduce the risk of spreading a virus. Employees are prohibited from disabling or interfering with any virus and spyware scanning software installed on their system.

Spam Filter

AMVAC scans all incoming e-mails and use a Spam filtering system before it reaches the AMVAC Email Servers.

Loading of Software at the Desktop

The loading of software at the desktop level is restricted to IT personnel or someone authorized by IT.

Those with Internet access privileges may not:

- Access inappropriate websites, examples include those involving gambling, pornography or obscene materials; those that display defamatory, sexually explicit, obscene, offensive or harassing messages, images, cartoons, jokes or pictures; or those that display profane, obscene, libelous content, or ethnic, religious, or racial slurs;
- Obligate AMVAC financially to any commercial web-site;
- Use the Internet from an AMVAC site to engage in the practice of moonlighting or for any commercial purposes, advertising or other similar activities.
- Use the Internet from an AMVAC site to download movies, MP3, streaming video/audio for personal use.
- Use the Internet from an AMVAC site to access personal email accounts and instant messaging services.

Computer System Security

Importance of System Security

AMVAC has an obligation to maintain the confidentiality of its own information and of customer information. As a consequence, all users of the Computer System must take steps to ensure the security of the system and maintain the confidentiality of all information on the system or communicated through the use of the system.

System Access

Password and User Logon IDs are unique to each authorized user and will be assigned by the IT support personnel. Passwords must be kept private. They should not be shared, coded into programs or written down.

Employees who may be away from their computer for more than a brief period of time should lock the computer or log off the system. Computers should be shut down as often as possible.

Installing or Downloading Software

The IT support personnel must approve and install all software on any AMVAC computer. No employee may download software without the approval of the IT support. When and if authorized to download software, employees must comply with all restrictions and procedures for downloading software, including mandatory virus scanning and detection procedures. Employees must inform the IT department of any virus, configuration change or different behavior of a computer or application, especially after the addition of new software to the computer system.

All employees must obey and follow all licensing agreements and procedures with regard to the use and installation of all software. AMVAC retains the right to inspect computers periodically to verify that all software has been approved and licensed properly.

Remote Access

All remote access to the Computer System must use encryption services to protect confidentiality of the session. Information regarding access to the Computer System is confidential and must not be posted on electronic bulletin boards, listed in telephone directories, placed on business cards or made available to third-parties without express written authorization of the IT department.

Violations

Reporting Violations of Policy

Any employee who becomes aware that the use of the Computer System has resulted in a violation of this policy or other AMVAC policies should promptly report any such violations to the Human Resource Manager or other company supervisory personnel. Employees may also contact the IT department to report any violations.

Enforcement

Use of the Computer System in violation of this policy or other AMVAC policies may result in disciplinary action, including termination of employment.

Software Copyright Compliance Policy

It is the policy of the company to prohibit software piracy and copyright infringements throughout the corporation.

Software will be used only in accordance with its license agreement. Unless otherwise provided in the license, any duplication of copyrighted software, except for backup and archival purposes by the IT department or designated department, is a violation of copyright law. In addition to violating copyright law, unauthorized duplication of software is contrary to Amvac's standards of conduct. The following points are to be followed to comply with software license agreements:

1. Amvac employees must use all software in accordance with its license agreements. Employees do not own this software or its related documentation, and unless expressly authorized by the software publisher, may not make additional copies except for archival purposes.
2. Amvac will not tolerate the use of any unauthorized copies of software in the organization. Any person illegally reproducing software can be subject to civil and criminal penalties including fines and imprisonment. Amvac will not condone illegal copying of software under any circumstances and anyone who makes, uses, or otherwise acquires unauthorized software will be appropriately disciplined up to and including termination.
3. No employee shall give software licensed to the company to any outsider including clients, customers, or any other third party. No software shall be used within Amvac, or installed on company computers, that have been brought in from any unauthorized location, including but not limited to, the Internet, the home, friends and colleagues.
4. Any employee who determines that there may be a misuse of software within the company should notify his or her supervisor or the I.T. Department.
5. All software used by the company on company-owned computers will be purchased through appropriate procedures established by the individual operating company and consistent with this policy.

American Vanguard Corporation

Information Technology Security Policies

I, _____ hereby acknowledge that I have
(Print Name)
received a copy of the American Vanguard Policy titled "Electronic Communications and Software Policy" dated 4/18/2011 as approved by the Company's Information Technology Department. I further acknowledge that I have read, understand and will comply with all provisions of said policy that specifically covers: access to associate e-mail, Internet and Intranet systems, system/e-mail passwords, monitoring of electronic communication, personal use, prohibited communication, confidential information, electronic message storage, encryption policy violation and separation from the Company.

I also acknowledge that if I violate any or all provisions of the American Vanguard "Electronic Communications" policy I will be subject to disciplinary action up to and including termination of employment. In addition, I am aware that employees who, use the Company's electronic communication systems for defamatory, illegal or fraudulent purposes or who break- into unauthorized areas of the American Vanguard computer system will be subject to civil and criminal prosecution. This includes, but is not limited to, the changing, deletion or destruction of files or programs by employees not authorized to do so.

Employee Signature: _____

Date: _____