Perform Air International Inc.
Quality System Manual
Policy QSM.22: Secure Computing Policy

Revision	Revision Date	Revision Change
N/I	02/08/2010	Initial Release/Re-release
1	09/16/2011	Revision to policy name and to policy to remove "PAI" references and correction of titles. Removal of Revision Bar from subsequent pages.
2	07/01/13	Extensive revision throughout.
3	03/31/2014	Revision for title change of Director of Information Technology. Revision of grammar / wording for clarity.
4	03/31/2021	Revision for title change to VP of Information Technology, end of p.4

Perform Air International Inc. is dedicated to providing a safe and secure computing environment to protect its employees, contractors, and patrons from illegal or damaging actions by individuals, either knowingly or unknowingly.

It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly. This policy applies to employees, contractors, consultants, temporary workers, and any personnel affiliated with third parties that utilize Perform Air International Inc.'s systems.

Any violation of this policy may be grounds for disciplinary action up to and including termination and, if found to be in violation of the law, may be subject to prosecution and criminal liability.

Computer and Network Resources

Perform Air International Inc. uses computers and network devices for the purpose of conducting company business only. These resources are provided at Perform Air International Inc. expense and therefore are to be considered company property.

All employees are responsible and accountable for the protection and appropriate use of company assets. They must adhere to the spirit as well as the letter of this policy as well as all applicable laws, regulations, contracts, licenses, procedures, practices, guidelines, and security rules. Employees, interns, and contractors may only access the information for which they have a valid business need and proper authorization. Actions of employees who knowingly bypass security settings or circumvent job specific authority through theft of passwords, accessing of privileged information, or utilizing the resources of users with higher privilege are to be considered subversive and are subject to immediate action per this policy.

Additionally, all information, files and messages created, stored, sent, received, or accessed on these systems are to be considered company property and as such should hold no expectation of privacy.

Hardware, Removable Media, and Peripherals

Any hardware, media, or peripherals not purchased by Perform Air International Inc. for business use is to be considered personal property until connected to company computer systems. Upon connection of said devices to a company computer system, they are subject to all of Perform Air International Inc.'s policies and procedures.

Installation of hardware and / or software for company use must be performed or supervised by authorized Information Technology staff to ensure compatibility with existing hardware and software. Any unauthorized additions or installations of hardware and/or software which cause loss

of productivity due to incompatibility are not the responsibility of the Information Technology Department and will be fixed on a time available basis only.

Fixes shall include, but are not limited to:

- Reverting to an earlier installation
- Reinstallation of the operating system
- Reformatting the hard drive and complete reinstallation

Laptops, PDA's, Smartphone's, and Personal Property

The Perform Air International Inc. networked computer system is a private network for the use of business functions only. Any device connected to the network (whether wired or wireless) is subject to all policies and procedures. All personal property systems used for business (whether by employee or contractor) are required to have current anti-virus software installed before connecting to the network. If a virus, Trojan horse program, internet worm, or any other malware program is found to have been released from a noncompliant personal computer, the employee or contractor may be subject to appropriate disciplinary action per this policy. Assistance with PDA's and Smartphone's is provided as a courtesy on a time available basis, but the Information Technology Department is not responsible for supporting personal devices. Any support for such devices is limited to restoring connectivity with Exchange / Outlook. The Information Technology Department is not responsible for incompatible software or loss of data.

Personal Use

Incidental, occasional, but brief personal use of computer systems is understandable and may be permitted with manager approval, provided the use does not violate company policies or laws and does not negatively affect the system's use for business purposes. Use of company computer systems will only be allowed on personal time and must not disrupt the operation of the network or the productivity of other users. Employees are expected to demonstrate a sense of responsibility and not abuse this privilege.

Prohibited Activities

In accordance with company policy, electronic communications may not contain content that may be offensive or derogatory on the basis of race, gender, sexual explicitness, religion, national origin, political beliefs, disability, or veteran status. Employees may not upload, download, copy, or otherwise transmit copyrighted, trademarked, or patented materials, trade secrets, or other proprietary information, software, or materials. Only software registered through the Information Technology Department may be installed on the computer systems. Employees may not install personal software (via download or removable media) on the systems.

Any personal software found on Perform Air International Inc. systems will be removed and the violation reported. If non-standard software is required to fulfill job responsibilities, the employee must have their manager submit a written electronic request (e-mail or Tech Request) to the Information Technology Department. The software will be evaluated for usability vs. security/compatibility and, if determined safe, final approval will come from Executive Management. The software license will be added to the Technology Inventory database.

Employees may not use company systems to gain access to remote computers or systems outside the scope of their job function. This includes non-company chat rooms, and peer-to-peer file sharing (Kazaa, BitTorrent, Napster, etc.). Access to social networking sites (MySpace, Facebook, etc.) will be allowed only as required by the position. Web accessed personal e-mail (HotMail, MSN mail, AOL webmail, Gmail, etc.) may only be accessed per the Personal Use section above. Employees may not enable unauthorized third parties to have access to or use Perform Air International Inc. systems. Any other illegal activities, acts in violation of this policy, or abuse of the privilege of access to e-mail or the Internet may be subject to appropriate disciplinary action.

Monitoring

Perform Air International Inc. reserves the right to monitor, access, retrieve, read, and disclose the contents of any electronic communication to law enforcement officials or other third parties for business purposes or to comply with the law. This may be done with or without the prior notice to the recipients or originators of the information. All systems may be monitored by authorized personnel at any time.

If a monitored communication is found to be of a personal nature, monitoring will cease as soon as practical. However, excessive or inappropriate personal use of company systems may be subject to appropriate disciplinary action per company policy.

Storage for Files and E-mail

Network drives are provided for business related files, programs, and documents. They are NOT for personal use. Do not store non-business files on company computer equipment. Any files not of a business nature related to Perform Air International Inc. that are lost or corrupted are not the responsibility of the Information Technology Department and will not be restored.

All employees have a limit (disk quota) of the amount of space their files may occupy on the file server based on the type of work done. If the amount of space is exceeded, you will be unable to save any more files to your drive. It is the employee's responsibility to clean out old files that are no longer used. If an employee's work dictates that their disk quota needs to be increased, the employee must have their department manager submit a Tech request to the Information Technology Department.

Mailbox limits are the responsibility of the employee. All mailboxes have a size limit to prevent server overload. The server notifies an employee when they must clean out their mailbox (either by moving to their archive folders or deleting old messages) before this limit is reached. Once the limit is reached, the employee will be unable to send further e-mail until the mailbox is cleaned out and/or messages are archived.

Record Retention

Employees should use the utmost care and discretion in creating electronic communications. Even when a message has been deleted, it may still exist on a back-up system, be recreated, be printed, or may have been forwarded to someone else. As with paper documents created and received by an employee, it is the responsibility of the employee to ensure that electronic messages that should be retained are saved.

Viruses, Hoaxes, Chain Letters, and Tampering

To ensure the integrity of our systems, the following precautions should be taken by all employees:

- Do not open e-mail with an attachment from a sender that is unknown to you. Delete it immediately.

- Delete chain letters. Do not forward.

All messages regarding viruses received from sources that are not part of the Information Technology Department should be considered suspicious and probably a hoax. Either delete the message or forward to an Information Technology person for verification.

To prevent computer viruses from being transmitted through the company's computer system, unauthorized downloading of any software is strictly prohibited. Any files received via the internet or other online sources as well as computer disks (including removable, USB, Serial, CD, or DVD media) received from outside sources MUST be scanned by the Information Technology Department with virus protection software before opening.

The intentional introduction of viruses, attempts to breach or bypass system security, and other malicious tampering with any of Perform Air International Inc. systems is expressly prohibited. Employees must immediately report, via Tech Request, any viruses, tampering, or other system breaches to the *Vice President* of Information Technology.

Standards of Conduct

The following guidelines are provided to protect you and company information, files, and passwords:

- All software installed on Perform Air International Inc. systems is licensed and not to be copied.

- Change your password at least every 90 days. Save your work frequently at established intervals (Most office programs can do this automatically). This allows your work to be retrieved in the event that the network goes down unexpectedly.

- Lock your workstation before leaving your desk for more than 5 minutes.

- Choose a passphrase of at least 15 characters using capital letters, numbers, spaces, and special characters.

- Never put your password in a visible place.