Sample Aviation
Information Security Policy

Table of Contents

Goal of this Policy

The goal of this policy is to ensure the confidentiality and integrity of each piece of personal information owned by or entrusted to Sample Aviation. Personal information includes but is not limited to:

- Social Security Number
- Date of Birth
- Place of Birth
- Mother’s Maiden Name
- Cardholder Data, especially Credit Card Numbers
- Bank Account Numbers
- Income Tax Records
- Drivers License Number

Purpose of this Policy

The purpose of this policy is to define the principles that all officers, management, employees, and customers must follow when handling information.

With identity theft, fraud, and other information crimes on the rise it is essential that all of us at Sample Aviation strive to protect information, particularly our customer’s personal information. Not doing so can result in lawsuits, loss of business, and hefty fines.

Compliance

While this policy outlines procedures for handling information it can not cover every possible situation and is not a replacement for common sense. Also, this document was written in accordance with regulations. However, if any discrepancies arise between this document and appropriate regulations, the regulations should be followed and the discrepancy reported to your supervisor immediately.

Personal Responsibilities

All personal information gathered by Sample Aviation for the purpose of conducting business if considered confidential. Each employee or contractor whohandles this information is responsible for its appropriate use.

- You are responsible for your use or misuse of confidential information.
- You must not in any way divulge, copy, release, transmit, sell, loan, review, alter, or destroy any information except as properly authorized within the scope of your work assignment.

- You must take appropriate measures to protect confidential information wherever it is located.
- You must safeguard any physical key, ID card, or computer/network account that allows you to access confidential information. This includes creating computer passwords that are difficult to guess. Passwords must never be divulged to anyone.
- You must render confidential information held on any physical document or computer storage medium that is being discarded unreadable and unusable.
- You must report any activities that you suspect may compromise confidential information to your supervisor.
- You must not install any software on any company computers without the written permission of your supervisor. This includes offline and online software, toolbars, chat programs, plug-ins, and remote access applications.
- You must never use, save, store, record, copy, or transmit credit card information except as provided in this document.
- You must not allow customers or visitors to use company computers except any computers provided specifically for that purpose.
- You must not allow customer or visitors to connect to the company network except through ports or wireless access points provided specifically for that purpose.
- You must not add or install wireless access points to the company network.
- You must not connect company computers to any unsecured wireless access point whether provided by the company or by others.
- You must not access the company network remotely except as specifically instructed.

Protecting Information Wherever It Is Located

Each individual who has access to personal information must understand its security requirements and to take measures to protect the information wherever it is located, including:

- Printed Forms
- Computers
- Networks
- Storage Media (CD, diskette, USB Flash Drive, etc.)
- Filing Cabinets

If an authorized user is not aware of the security requirements for information to which he or she has access, he or she must provide that information with maximum protection until its requirements can be ascertained.

Any individual who has been given a physical key, ID card, or computer or network account that enables him or her to access information is responsible for all activities performed by anyone using that key or identifier. Therefore, each individual must be diligent in protecting his or her physical keys and ID cards against theft, and his or her computer and network accounts against unauthorized use. Passwords created for computer and network accounts must be difficult to guess. Furthermore, passwords should never be shared, or recorded and stored in a location that is easily accessible.

Special Requirements for Credit Card Holder Data

Cardholder Data is defined as the primary account number (credit card number or "PAN") along with other data obtained as a part of a card storage or payment transactions. Cardholder name and expiration date are also cardholder data when stored with the PAN.

Magnetic stripe data and the card verification code must never be stored or retained.

Cardholder data may only be processed and stored through the Sample Aviation Online System provided MyFBO.com and AHT Services. Cardholder data of any kind must never be recorded or transmitted outside of this channel.

Sharing Information

All personal information owned by or entrusted to Sample Aviation is considered confidential. This information may only be shared with:

- The individual for whom the information is maintained.
- Persons designated in writing by that individual.
- Government agencies that Sample Aviation has a legal obligation to provide such information.

The use of personal information in any manner, other than conducting business is strictly prohibited. Any employee of Sample Aviation that violates this principle will be terminated and prosecuted to the full extent of the law.

Exchanging Information

Information may only be exchanged between appropriate users within Sample Aviation’s Aviation Management Software, in written form, or verbally. Other methods including e-mail, ftp, chat, and instant messaging are not secure and should not be used to exchange information.

Discarding Information

Physical documents containing personal information should be cross-cut shredded prior to discarding.

Any computer hard drive or removable magnetic medium, such as a diskette, magnetic tape, Zip disk, etc., that has been used to hold any personal information must be electronically "scrubbed". Note that on such media, the mere deletion of confidential data is not sufficient.

Any non-erasable medium, such as a CD, optical disk, etc., that has been used to hold any personal information must be physically destroyed before being discarded.

Subpoenas

Individuals who receive investigative subpoenas, court orders and other compulsory requests from law enforcement should contact their supervisor before taking any action.

Reporting Breaches and Suspicious Activities

Any person who suspects that personal information has been breached must report it to their supervisor or the technology manager immediately. In addition, any suspicious activities that could lead to a breach, exposure, or corruption of personal information must also be reported.

Requirements for Technology Managers

Technology managers are those individuals who manage computing and network environments where personal information is stored, transmitted or processed, including:

- Computer operating environments (UNIX, Windows, Macintosh, etc.)
- Database management environments (SQL Server, Access, etc.)
- Application environments
- Network environments (wired and wireless networks, routers, switches, etc.)
- Physical storage facilities (CD and tape libraries, filing cabinets, USB keys, etc.)

Technology mangers must ensure that:

- All computers have up-to-date operating system software. Automatic updates should be used wherever possible.
- All computers have anti-virus and anti-spyware programs installed and operating with up-to-date virus signatures.
- Networks where personal information is stored or transmitted must be segregated from unsecured networks. This includes the separation of internal networks from the Internet through use of a firewall or appropriately configured router.
- Public portions of the network such as courtesy computers in the lobby and open WiFi access must also be segregated from the secured network. This me be accomplished either through multiple Internet connections (which has the benefit of adding redundancy), firewalls, or other appropriate hardware.

- WiFi for internal use must be secured using the latest available technology, presently WPA2 with strong passwords.
- Quarterly wireless access scanning must be conducted to assure no open access points to the secure network.
- Quarterly external network scans must be performed and documentation provided by a PCI-approved scanning vendor (ASV).
- A list of service providers must be maintained. Any remote access by service providers must be documented and secure technologies used to provide such access.
- For any service provider with access to cardholder data, their PCC compliance must be monitored.
- To the extent possible, staff users should not have administrative access to any computer.
- All use of secured computers and the secured network must be protected by strong passwords.
- This document must be reviewed annually and updated as needed.
- All employees and contractors are briefed at least annually on the content of this policy and its goal and intent.