



Data Security Policy

Revision: 02

21 March 2010

**Omni Air Group
6421 South Dorset Road
Spokane, WA 99224
USA
Tel. 509-838-8121**

This Plan is the property of Omni Air Group, and contains proprietary information. It may not be copied, printed or reproduced in any manner without the express written consent of Omni. The person to whom this Plan has been assigned is responsible for the safekeeping of this Plan and the timely insertion of all revisions in accordance with the procedures contained herein.

Record of Revisions

PLAN SERIAL NUMBER: _____

Insert all revisions immediately.

Record revision highlights, revision effective date and the initials of the person inserting the revision.

Revision	Description of Change (highlights)	Revision Effective Date	Revision Inserted By
Original	N/A - Original	22 May 2009	N/A
1	Addition of description of security measures for hosted IR databases	19 Sept. 2009	PMS
2	Updated FileMaker references	21 March 2010	PMS
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			

Data Security Policy

Table of Contents

RECORD OF REVISIONS	1
TABLE OF CONTENTS	2
1. GENERAL INFORMATION	3
A. Introduction	3
B. Terminology	3
2. SCOPE OF POLICY	3
A. Security Defined	3
B. Purpose	3
C. Responsibility	3
3. GENERAL POLICY	4
A. Required Policies	4
B. Best Practices	4
C. Errors and Violations	4
4. DATA CLASSIFICATION	4
A. General	4
B. High Risk	4
C. Confidential	4
D. Public	4
5. METHODS OF PROTECTION	5
A. Live Data	5
B. Backups	5
6. ACCESS CONTROL	5
A. Network and Servers	5
B. Usernames and Passwords	5
C. Authentication Devices	6
D. Logon Activities	6
7. ACCEPTABLE USE	6
8. VIRUS PREVENTION	6
A. Network and System Components	6
B. Email	6
9. INTRUSION DETECTION	7
A. System / Network	7
B. Reviews and Alerts	7
10. INTERNET SECURITY	7
A. High Risk Data	7
B. Confidential Data	7
11. SYSTEM SECURITY	7
12. EXCEPTIONS	7
13. SECURITY OF HOSTED DATABASES	7
A. General Information	7
B. Servers	8
C. Information Security Technologies	8
D. Data at Rest	8
E. Data in Motion	8
F. Data Backups	8
G. Support Services	8
H. Error Correction	8

Data Security Policy

1. GENERAL INFORMATION

A. Introduction

Storage of OAG information and client data on our computer systems, and transfer of this data across the OAG network and the internet, demands the need for appropriate security measures. Security measures include preservation of data as well as physical and virtual protection from unauthorized access. Security is not distinct from the functionality of our systems, and must be integrated at all levels.

This Policy is written to disseminate and clearly communicate to all OAG personnel, the company's policies regarding data security and the security of information in general. The policies contained herein are intended to incorporate current technological advances. Inaccurate information, inconsistencies, out-of-date information, and all instances of non-compliance must be reported to OAG using the company's internal Incident Reporter database.

B. Terminology

Throughout this document the terms "shall", "must", "will" and "should" are used carefully. "Shalls", "musts" and "wills" are to be considered directive in nature; "shoulds" represent best practices and goals. The terms "data" and "information" are used interchangeably.

The terms "system" and "network administrator" are also used within this document. These terms are generic and pertain to any person who performs those duties, not just those with that title or primary job duty.

2. SCOPE OF POLICY

A. Security Defined

Data security refers to protection of our clients' data and the company's data, applications, networks, and computer systems from unauthorized access, alteration, or destruction.

B. Purpose

The purpose of Omni Air Group's data security policy is:

- To establish a company-wide approach to information security.
- To prescribe mechanisms that help identify and prevent the compromise of information security and the misuse of OAG data, applications, networks and computer systems.
- To define methods and processes that allow OAG to satisfy its legal and ethical responsibilities regarding protection of sensitive information, and network / computer system connectivity to worldwide networks.
- To prescribe an effective mechanism for responding to external complaints and queries about real or perceived non-compliance with this policy, in order to effect risk controls and corrective actions.

C. Responsibility

Omni Air Group's President is responsible for implementing this policy. The President shall ensure that:

- The policy is updated on a regular basis and published as appropriate.
- Appropriate training is provided to OAG's Manager of IT Services, network / system administrators, data owners, custodians, and users.
- Compliance is monitored on a continuous basis.

3. GENERAL POLICY

A. Required Policies

OAG uses a layered approach of overlapping controls, monitoring and authentication to ensure overall security of the company's data, network and system resources. Security reviews of servers, firewalls, routers and monitoring platforms are conducted on a regular basis. These reviews must include monitoring access logs and results of intrusion detection software, where it has been installed.

B. Best Practices

Vulnerability and risk assessment tests of external network connections should be conducted on a regular basis. At a minimum, testing should be performed annually, but the sensitivity of the information secured may require that these tests be done more often.

Education should be implemented to ensure that users understand data sensitivity issues, levels of confidentiality, and the mechanisms to protect the data. This education should be tailored to the role of the individual, network administrator, system administrator, data custodian, and users.

C. Errors and Violations

In accordance with OAG's positive no-blame safety culture, unintentional errors and "honest mistakes" which are reported promptly will NOT result in disciplinary action, and will help the company implement risk-mitigating strategies to preclude reoccurrence.

Violations of this Data Security Policy which are the result of malevolence or willful disregard for policy may result in disciplinary actions.

4. DATA CLASSIFICATION

A. General

It is essential that all company data be protected. There are however gradations that require different levels of security. All data should be reviewed on a periodic basis and classified according to its use, sensitivity, and importance. OAG has defined and specified three classes of information and data as follows.

B. High Risk

This includes information and data for which there are legal requirements for preventing disclosure, or financial penalties for disclosure. Data covered by federal and state legislation, such as FERPA, HIPAA or the Data Protection Act, are in this class. Payroll, personnel, and financial information are also in this class due to privacy requirements. Sensitive safety data of our clients as recorded in each of our client's IR databases is also in this class. Trade secrets, including usernames and passwords used to protect such secrets from unauthorized access, also fall in this class.

C. Confidential

This includes data and information that would not expose the company to loss if disclosed, but that the data owner feels should be protected to prevent unauthorized disclosure. In these cases, it is the data owner's responsibility to implement necessary security requirements.

D. Public

Information and data classified as Public may be freely disseminated.

NOTE:

Data or Information that is not classified shall be treated as HIGH RISK until a determination is made by the appropriate risk-decision authority.

5. METHODS OF PROTECTION

A. Live Data

All information resources should be categorized and protected according to the requirements set for each classification. The data classification and its corresponding level of protection should be consistent when the data is replicated and as it flows through the Company.

- Data owners must determine the data classification and must ensure that the data custodian is protecting the data in a manner appropriate to its classification.
- No Company-owned system or network subnet shall be permitted a connection to the Internet without the means to protect the information on those systems consistent with its confidentiality classification.
- Data custodians are responsible for creating data repositories and data transfer procedures which protect data in the manner appropriate to its classification.
- High risk data must be encrypted during transmission over insecure channels.
- Confidential data should be encrypted during transmission over insecure channels.

B. Backups

All appropriate data should be backed up, and backups tested periodically, as part of a documented, regular process. Backups of data must be handled with the same security precautions as the data itself. When systems are disposed of, or repurposed, data must be certified deleted or disks / drives destroyed consistent with industry best practices for the security level of the data. Systems, hard drives and media that contain (or previously contained) data classified as HIGH RISK shall be disposed of by physical destruction of the system, drive or media.

6. ACCESS CONTROL

A. Network and Servers

Where possible, more than one person must have full rights to any company owned server storing or transmitting high risk data. Data owners or custodians may enact more restrictive policies for end-user access to their data.

Access to the network, servers and systems should be achieved by individual and unique logins, and should require authentication. Authentication includes the use of passwords, smart cards, biometrics, or other recognized forms of authentication.

B. Usernames and Passwords

Users shall not share usernames and passwords, nor should they be written down or recorded in unencrypted electronic files or documents. In addition,

- All users must secure their username or account, password, and system access from unauthorized use.
- All users of systems that contain high risk or confidential data must have a strong, alpha-numeric and case-sensitive password.
- Empowered accounts, such as administrator, root or supervisor accounts, must be changed frequently,
- Passwords must not be placed in emails unless they have been encrypted.
- Default passwords on all systems must be changed after installation.
- All administrator or root accounts must be given a password that conforms to the password selection criteria when a system is installed, rebuilt, or reconfigured.
- Logins and passwords should not be coded into programs or queries unless they are encrypted or otherwise secure.

C. Authentication Devices

Users are responsible for safe handling and storage of all Company authentication devices. Authentication tokens (such as a SecureID card) should not be stored with a computer that will be used to access the Company's network or system resources. If an authentication device is lost or stolen, the loss must be immediately reported to the OAG IT Manager so that the device can be disabled.

D. Logon Activities

The IT Manager will monitor all systems and periodically review all records of logon attempts and failures, successful logons and date and time of logon and logoff. In addition,

- Activities performed as administrator or superuser must be logged where it is feasible to do so.
- Personnel who have administrative system access should use other less powerful accounts for performing non-administrative tasks.
- Terminated / transferred employee access will be periodically reviewed and updated as necessary.
- Terminated employees should have their accounts disabled immediately upon transfer or termination.

7. ACCEPTABLE USE

Company computer resources shall be used in a manner that complies with Company policies and State and Federal laws and regulations. It is against Company policy to install or run software requiring a license on any Company computer without a valid license.

Use of the Company's computing and networking infrastructure by Company employees unrelated to their Company positions must be limited in both time and resources and must not interfere in any way with Company functions or the employee's duties. It is the responsibility of employees to consult their supervisors, if they have any questions in this respect.

Uses that interfere with the proper functioning or the ability of others to make use of the Company's networks, computer systems, applications and data resources are not permitted. Use of Company computer resources for personal profit is not permitted without specific written authorization.

Decryption of passwords is not permitted, except by authorized staff performing security reviews or investigations. Use of network sniffers shall be restricted to system administrators who must use such tools to solve network problems. However, sniffers shall not be used to monitor or track any individual's network activity except under special authorization by the Company President.

8. VIRUS PREVENTION

A. Network and System Components

All servers, workstations, and desktop systems that connect to the network must be protected with approved, licensed anti-virus software that it is kept updated according to the vendor's recommendations.

B. Email

Headers of all incoming data including electronic mail will be scanned for viruses by the email server where such products exist and are financially feasible to implement. Outgoing electronic mail should be scanned where such capabilities exist.

- Where feasible, system or network administrators should inform users when a virus has been detected.
- Virus scanning logs must be maintained whenever email is centrally scanned for viruses.

The willful introduction of computer viruses or disruptive/destructive programs into the Company environment is prohibited, and violators will be subject to prosecution.

9. INTRUSION DETECTION

A. System / Network

Intruder detection must be implemented on all servers and workstations containing data classified as high risk. Operating system and application software logging processes must be enabled on all host and server systems. Where possible, alarm and alert functions, as well as logging and monitoring systems must be enabled.

B. Reviews and Alerts

Server, firewall, and critical system logs should be reviewed frequently. Automated review should be enabled and alerts should be transmitted to the administrator when a serious security intrusion is detected.

10. INTERNET SECURITY

A. High Risk Data

All connections to the Internet must go through a properly secured connection point to ensure the network is protected when the data is classified as high risk.

B. Confidential Data

All connections to the Internet should go through a properly secured connection point to ensure the network is protected when the data is classified as confidential.

11. SYSTEM SECURITY

All systems connected to the Internet should have a vendor supported version of the operating system installed, and must remain current with security patches. System integrity checks of host and server systems which contain high risk Company data should be performed at regular intervals by the OAG IT Manager.

12. EXCEPTIONS

In certain cases, compliance with specific policy requirements may not be immediately possible. Reasons include, but are not limited to, the following:

- Required commercial or other software in use is not currently able to support the required features;
- Legacy systems are in use which do not comply, but near-term future systems will, and are planned for;
- Costs for reasonable compliance are disproportionate relative to the potential for damage.

All instances of non-compliance must be reported into the Company's IR database for investigation and review by the OAG QC Committee. A Corrective Action Plan will be developed in the IR database for coming into compliance with the Company's Information Security Policy within a reasonable amount of time, and responsibilities assigned to appropriate personnel.

13. SECURITY OF HOSTED DATABASES

A. General Information

OAG's Incident Reporter (IR) software programs are based on the FileMaker platform. Hosted client databases are served on FileMaker Server Advanced, a time-tested and stable platform. Through agreement with our trusted business partner TierPoint™, OAG's servers reside in a modern state-of-the-art facility that provides server co-location and data backup services for large financial institutions.

TierPoint's Liberty Lake, Washington facility is climate-controlled and finger-print secure with five internet pipelines, conditioned UPS power and backup generators. TierPoint also provides their Fortinet "Clean IP" firewall appliance to all OAG servers. Together, these partnerships and agreements result in the highest levels of security and integrity of data, with 99.96% uptime reliability.

B. Servers

OAG servers contain redundant power supplies and multiple redundant drives. A backup server is maintained in service-ready configuration, in the unlikely event of operating system or hardware failure. Servers are maintained and updated regularly by TierPoint.

C. Information Security Technologies

The Fortinet “Clean IP” firewall provides network intrusion detection / protection, and anti-virus software.

D. Data at Rest

In addition to password protection, stored data (data-at-rest) is protected from unauthorized access utilizing a Fortinet “Clean IP” firewall and RSA Keys encryption @ 128 bits.

E. Data in Motion

The FileMaker Pro client-server application is used by clients to communicate with their IR databases which reside on FileMaker Server Advanced, using SSL (Secure Socket Layer) security encryption. Client-assigned usernames are set up for access by client employees, and default passwords must be changed at first login. Passwords are alpha-numeric, and case-sensitive. Application / system activity and access are traced and logged at the user ID level.

FM Pro applications are also used by OAG support staff for client support, but only when necessary, and in accordance with the data security procedures set forth herein. OAG personnel do not have access to client employees’ passwords. Clients may also connect to their IR databases via supported web browser. Web connections are encrypted at 128 bit SSL and are logged at the user ID level.

F. Data Backups

Client databases are automatically backed up by FileMaker Server Advanced every three hours. Full system backups are performed nightly.

G. Support Services

OAG provides the following Support Services during the hours of 8:00 AM to 4:30 PM, M-F, Pacific time:

- Resolution of basic issues related to the installation, functionality, and usage of client databases;
- Troubleshooting and resolution of hardware and/or software problems reported by clients.

H. Error Correction

OAG addresses all reported errors in accordance with the following priority status:

- **Priority Errors** – are those which render a client’s database inaccessible, inoperative or severely functionally impaired. When a problem is classified as a Priority Error, OAG promptly assigns full time resources as needed to work on the problem until resolved. OAG responds to all Priority Errors within one (1) hour of notification (if notification is made during Support Hours) or by 9:00 AM the following business day (if notification is made after Support Hours). OAG will use its best efforts to provide an error correction or work around solution within 4 hours of a Priority Error notification;
- **Secondary Errors** – are those which substantially degrade performance or substantially restrict use of a client’s database. OAG responds to all Secondary Errors within four (4) hours of notification (if notification is made during Support Hours) or by 1:00 PM the following business day (if notification is made after Support Hours). OAG will use its best efforts to provide a work around solution as promptly as practicable, and an error correction within 48 hours of a Secondary Error notification;
- **Minor Errors** – are all other errors which require assistance or information from OAG. These problems should be resolved within a time-frame that is mutually agreed upon with the client.