CI-7 Hurricane Model Security

The modeling organization shall have implemented and fully documented security procedures for: (1) secure access to individual computers where the software components or data can be created or modified, (2) secure operation of the hurricane model by clients, if relevant, to ensure that the correct software operation cannot be compromised, (3) anti-virus software installation for all machines where all components and data are being accessed, and (4) secure access to documentation, software, and data in the event of a catastrophe.

AIR employs a number of physical and electronic security measures to protect all code, data, and documentation against both internal and external potential sources of damage, and against deliberate and inadvertent, unauthorized changes.

Electronic Security

The AIR network is made up of shared Windows and Linux servers along with a variety of desktop workstations and laptops used by individual employees. Within each department there may also be some workstations that contain applications or resources that are shared within the department. These machines may also be used to execute long running jobs.

Microsoft Windows servers are the foundation of the network. There are file, print, and Exchange mail servers. The network is connected with 1000/10,000 Mbps Ethernet switches for fast throughput. AIR also has Linux servers, which are primarily used for research and development of AIR models. They are also used for running these models for client services. Email is hosted at our parent company, Verisk's, New Jersey data center, but it is actively being migrated to Office 365. The AIR network also has a separate sub-network that contains classroom workstations. Students in classes see only what is available to that sub-network, not the servers and workstations of AIR employees.

As a directive from Verisk, every employee at AIR is required to complete the online Information Security Awareness with Privacy Principles program during the month of January. The program discusses key security elements that all employees must understand. To successfully complete the course, employees must review and accept the policies stated and score 80 percent or better on the assessment provided at the end of the course. Compliance with applicable regulations mandates that all employees be fully trained in security awareness.

Network Access Management

Access to the network is managed using:

- **Firewall**—The first stage of network protection is the use of firewalls. AIR policy is to maintain the minimum number of open ports necessary.
- **Network logon (internal)—**Access to the network via workstations at AIR's main office is restricted to AIR-approved Windows®-authenticated accounts with a valid user name and password. Passwords must be a minimum of eight characters in length and must contain a combination of alphabetic and numeric characters, including upper case letters. The Windows' login account password expires every 90 days. Use of personal computers is restricted without AIR network access approval. IS ensures that personal computers have functional anti-virus and Malware protection software, as well as relevant Microsoft patches.
- **Network logon (external)—**Access to the network from a workstation outside AIR's main office is subject to the internal network logon restrictions mentioned above, as well as access via the VPN gateway. VPN accounts are granted with management approval only.
- **Branch offices and remote users**—Access to the network from AIR's branch offices is subject to the internal network logon restrictions mentioned above, and can only be accessed via an encrypted link.

Data Servers Management

Access to the files and folders on AIR's data servers is regulated by permissions (read-only, read/write, etc.) assigned by management. In general, a member of one department has read/write access to that department's files and folders, and read-only access to the files and folders of other departments. Access to and permissions for specific folders are determined by the senior team leader and incorporated into each user's account profile.

The data servers are located in a secure server room located in New Jersey.

All model and software development is done within AIR's secure network. In general, developers have read-only access to the entire database, and read/write access to the product on which they are working.

Access to AIR's Internal Source Code present in TFS, GIT Enterprise, Bit Bucket and VSS is limited to the AD accounts /AD Groups, approved and created by IT Database Team. We have Certain AD Groups that are predefined as MSDN Groups, which automatically assumes access to source code when new employees are added in certain departments like SDG and QA.

The ability to delete any source control source code from these source control systems is hierarchal to the department leads and/or through a help desk request.

Access to AIRPort—All AIR employees have access to AIRPort. Access is granted using the employee's Windows®-authenticated user name and password. When a site is created, the administrator determines who has access to the site and each member receives an invitation to join the site. The site administrator also assigns rights to team members.

FTP Server Management

The AIR Worldwide FTP Servers are contained within the DMZ zone and are accessed in a secure manner. In computer networks, a DMZ (demilitarized zone) is a computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network. It prevents outside users from getting direct access to a server that has company data.

A DMZ is an optional and more secure approach to a firewall and effectively acts as a proxy server as well.

In a typical DMZ configuration for a small company, a separate computer (or host in network terms) receives requests from users within the private network for access to websites or other companies accessible on the public network. The DMZ host then initiates sessions for these requests on the public network. However, the DMZ host is not able to initiate a session back into the private network. It can only forward packets that have already been requested. Users of the public network outside the company can access only the DMZ host. However, the DMZ provides access to no other company data.

Remote Access

AIR provides Virtual Private Network (VPN) service to give users access to the internal network while they are traveling or working at home. A VPN connection to the AIR network enables employees to work remotely. Users can connect to a server to share files, to share their desktop via Remote Desktop protocol, and use X windows/SSH to connect to Linux resources. Since the home PC is not part of the AIR Worldwide domain, the users cannot see all of the workstations and servers in the Network Neighborhood. However, they can search for a particular server or workstation. Once the user finds the appropriate system, the user will be asked to enter their AIR Windows user name and password.

Using the VPN gateway to access the workstation at AIR Worldwide requires manager's approval, as well as the following computer pre-requisites:

- Anti-virus must be installed on an employee's PC with signatures set to automatically update. AIR can provide Symantec AV or employee can provide their own.
- The built-in Windows firewall (Windows 7/8) must also be installed and configured.

Access for Remote Offices

AIR Worldwide has several offices outside the Boston headquarters. Our branch offices have their own networks and servers, and each office has the ability to access the Boston servers and our Intranet via the VPN gateway.

File Back-up

To provide a safety net to AIR's network, AIR maintains a thorough back-up policy covering select files, databases, and applications stored on the network, including all document, source and data files related to Touchstone and the AIR Atlantic Tropical Cyclone Model.

During the workweek, all critical servers are backed up in full to secondary storage using CommVault. Local backups are stored onsite and replicated offsite on a per-dataset basis. Daily sync operations are run for critical primary data sets to an offsite storage system for BCP purposes. The replication of our primary storage solutions is facilitated by EMC Isilon SyncIQ and EMC RecoverPoint.

Virus Protection

Virus protection software is installed on the AIR servers, desktops, and notebooks. The virus protection maintenance policy is set up to automatically download virus signature pattern files every morning. These files are then automatically sent to all servers and workstations within the network. This protection scans not only incoming email and email attachments, but also any files introduced through external media, such as USB drives.

The virus scanning software, Symantec, is always scanning files on our Windows desktops and servers. IS-installed Symantec always scans files as they are opened to ensure that no viruses have infected working files. Symantec is updated for new virus protection immediately upon release of an updated virus signature file.

AIR blocks spam using Proofpoint. All email is filtered through the spam servers before being passed to the mail server.

Symantec is also installed on the FTP server. All files that are uploaded and downloaded are scanned automatically.

Microsoft® Patches

Patches to Microsoft products (including security patches) are provided and deployed using BigFix. As Microsoft releases patches; the patch is deployed and installed automatically.

Laptops

In addition to the security software outlined in this document, all laptops are required to have BitLocker Full Disk Encryption software installed. BitLocker Full Disk Encryption provides the highest level of data security with multi-factor pre-boot authentication and the strongest encryption algorithms. The entire hard drive contents—including the operating system and even temporary files—are automatically encrypted for a completely transparent end-user experience.

Disaster Recovery

The Disaster Recovery (DR) Procedure should be executed when any automated or human-sourced information determines there is a service outage at AIR. The goal is to determine if an authorized entity from AIR can determine if DR failover should or should not take place.

An incident response consists of three distinct phases: Emergency Response, Recovery, and Restoration, each with its own set of objectives. The duration of each phase will depend on the nature of the event and its effect on AIR's critical business processes.

Emergency Response

Once an incident is discovered and as it continues to unfold, the Emergency Response Team (ERT) is mobilized to determine the severity and extent of the incident. The ERT identifies what the situation is, how severe it is, what operations will be impacted if any, and what is the extent of the damage from the incident. This team reports all this information along with recommendations on how we should react to the Recovery Management Team (RMT). The RMT, headed by the company's president, decides whether the incident warrants a large-scale response by the company. Depending on the severity and impact of the incident, the RMT may activate all or a portion of the Business Continuity Plan.

Recovery

If the Business Continuity Plan is activated, it means that AIR’s headquarters is not operational (fully or partially) and may not be accessible resulting in a focus shift to the recovery phase. The recovery phase involves activating and mobilizing the BCP teams and expanding the level of communications to internal and external parties. Employees will support operations from their designated recovery locations as defined in the BCP.

Restoration

The restoration phase assumes that some or all of AIR’s headquarters was damaged, continuity plans were activated, and employees and operations were relocated. During the restoration phase, the ERT stays at the AIR Headquarters to assess the extent, impact, and damage of any incident. They communicate with the RMT who will decide whether/when AIR can re-occupy its headquarters. When that decision is made, the teams involved in the re-location back from the disaster site will be activated and involved.

Information Security Incident Response Plan

All Suspected Data Breaches should be immediately reported to Verisk Help Desk, whose employees have been trained in managing incident response. They review what is reported and, if they deem it necessary, they invoke the Security Response Team.

Members of the Security Response Team are immediately notified simultaneously until one of the senior staff responds to the Help Desk. Confidentiality is extremely important and everyone is on a need-to-know basis. The decision-making around who gets notified and what happens next is wholly the Security Response Team’s responsibility. The Response team will reach out to the person reporting the incident, get their business leaders involved, and start invoking.

Physical Security

AIR is located in a multi-story office building that contains multiple businesses. The building lobby is staffed by security guards 24 hours a day who verify the security badge of everyone who enters the building. Upon entering the building, the employee is required to swipe their badge by the elevator bank.

Employee Badges

Access to AIR's floor is restricted to current AIR employees and guests. All AIR Employees are issued an electronic security badge on the first day of their employment. All AIR employees (including employees visiting from other offices) should have their AIR security badges on their person at all times.

Employees who forget their badge must stop at the security desk and wait for clearance. In the event that a badge is lost, staff must notify the Office Manager *immediately* so that it can be deactivated and a new one can be issued.

The main entrances to the AIR offices are locked between 5:30 p.m. and 8:30 a.m. The use of the security badge is required to enter either of the doors on the north side of the building during those hours.

The data servers are located in a secure server room. Access to the server room is granted by electronic badge verification and is limited to essential personnel only.

Visitors

All visitors must be reported *in advance* to the Front Desk where they will be pre-cleared through our Visitor Clearance Program. Staff report the visitor's first and last name (spelled correctly), date(s) and time(s) of visit(s), and with whom they are meeting. Upon arrival, all guests must show photo ID at the security desk in the lobby to receive a 24-hour, self-invalidating badge indicating what floor and company they have clearance to visit. This badge cannot access any areas that require electronic badge verification. A new badge will be issued for each day of a guest's visit. All guests that are not pre-cleared will be announced via phone for approval before being given a badge.

During business hours, all guests must check in with the AIR receptionist and must be escorted by an AIR employee.

Emergency Evacuation Team

In the event of an emergency, announcements are made over the loud speaker instructing employees to remain or evacuate. Members of the AIR staff have been trained (Emergency Evacuation Team) to inform and guide employees in the event of an evacuation.

Relevant Form: *G-6, Computer/Information Standards Expert Certification*

Disclosure

1. ***Describe methods used to ensure the security and integrity of the code, data, and documentation.***

AIR employs a number of physical and electronic security measures to protect all code, data and documentation against both internal and external potential sources of damage, and against deliberate and inadvertent, unauthorized changes.

AIR's security policies, which are outlined above, are discussed in the *Verisk Information Security Policy Framework* document. An AIR custodian shall be available to further discuss the AIR security policies and procedures with the independent peer auditor and with the Professional Team.