Appendix 3

IA System Security

Appendix 3

Table of Contents

1 Introduction

AFA Insurance is committed to maintaining a high level of security for internal data and our customers' data. We have a structured process in place to enable us to achieve this and we regularly evaluate its performance to continuously improve data security.

This Security Appendix explains how AFA Insurance works to achieve a high level of security for its customers' data, which are processed in the "Occupational Health and Safety Information System", hereafter referred to as the IA System.

The Appendix also contains a chapter on the requirements that AFA Insurance places on its user companies, and the opportunities and obligations of the user companies to help ensure that security procedures and practices are upheld.

Any questions relating to AFA Insurance's data protection practices can be sent to AFA Insurance's Head of Security via IA Support.

2 Regulatory documents

AFA Insurance has its own set of regulatory documents covering system development, incident management, etc. to ensure that operational security is maintained in the operation and administration of the IA System.

3 Organisation

Security function

An in-house security function works in an integrated way with the business operations and provides the line organisation with expertise, evaluations and guidelines for data and IT security. The security function deals with a range of issues covering IT security, physical security and personnel security.

CERT (Computer Emergency Response Team)

The company has a team to manage cyber attacks, with specialist expertise in communications security, client protection, data centres, and Microsoft's and Unix' infrastructures. Other specialist expertise can be drawn upon if necessary.

4 Personnel security

All personnel, both our own staff and consultants, sign a confidentiality and non-disclosure agreement before they are given access to IT systems. Employees who work with the IA System receive training in how the IA System is used and what restrictions apply. We hold regular meetings with our own staff to detect and prevent improper conduct.

5 Asset management

The personal data processed in the IA System is classified as confidential. AFA Insurance therefore works actively with allocation of needs-based access rights via roles. Access rights are only granted to personnel to the extent necessary for them to perform their duties.

6 Access control

6.1 Within AFA Insurance

Only a few people in AFA Insurance's Operations Department have full access rights to databases and discs. The team from AFA Insurance's Systems Development Department, which is responsible for developing the IA System, has read access rights to the database, but no rights to discs. All logins to the IA System are made via personal accounts and are logged into the central log management system.

AFA Insurance's IA System support staff can connect to the user company and thus gain access to the user company's data linked to incoming support questions. Written permission to do so must first be obtained from the user company. All readings of data in the IA System are logged for each individual case. These logs can be accessed in the IA System by authorised staff at the user company.

6.2 For user companies

AFA Insurance establishes and allocates access rights only for administrators at the user companies. Thereafter, the user companies are themselves responsible for administration of users of the IA System within their own organisation. Access rights are granted via roles, assigned to users via the administrators. The user companies' users, administrators and other users are able to specify a temporary substitute for their access rights.

User companies are responsible themselves for their login method, e.g. user name/password, SSO via SAML 2.0, or a combination of these. AFA Insurance recommends SSO via SAML 2.0

7 Encryption

The system uses SSL encryption with publicly signed certificates. There are documented procedures in place for managing and updating cryptographic material such as keys for certificates.

The production database is encrypted.

8 Physical and environmental security

In our data centres, physical security comprises intruder alarms, fire protection systems, entry systems and CCTV surveillance.

The intruder alarm system is connected to a security company with short response times. The operations areas are patrolled by security guards at irregular times and at least twice every 24 hours.

Fire protection consists of smoke detectors connected to the fire services, and automatic extinguishing systems.

There is a power protection system installed in case of a power outage.

Only authorised personnel have physical access to the data centres. Access to the data centres is permission-based. The entry system logs successful and unsuccessful attempts at physical entry.

9 Equipment

The secure disposal of digital media requires all data on the media to be deleted and the digital media then to be destroyed. This is carried out at a secure facility by approved personnel.

10 Operational reliability

10.1 Communication

The data centres that are used are connected to the Internet via two separate providers. Automatic failover between the providers is used to ensure high availability.

The IA System is separated from other IT systems within AFA Insurance via firewalls. Only communication with explicit permission is allowed to pass through the firewalls

For sabotage attempts through so-called denial of service, AFA Insurance protects its environment through built-in firewall technology as well as through the Internet operator's care. Limited or unavailable service at such an opportunity is an accepted risk.

10.2 Traceability and monitoring

Centralised log management is used for the IA System and for related network communications. Designated personnel actively work to detect high-risk activities via rules-based alarms and tools for analysis of non-conformities. Where necessary, relevant components of the logs can be made available to customer companies.

Data is protected using access rights that are controlled at all levels in the IA System. Data processing, reading, editing and logins are all logged. Failed attempts to log in are also logged.

The IA System’s time is taken from the System’s servers. Logged times are presented in the user browser’s time zone and the format is taken from the user’s language settings.

Events data can be extracted from the IA System into Excel or PDF files.

Risk management data are extracted into PDF as protocols.

Manipulation of the logs is not possible from inside the IA System. The logs are saved without changes unless the case is removed, or the user is deleted or inactivated.

The system logs any changes to and readings of events data. Both successful and unsuccessful logins are logged. Changes to access rights are also logged.

Access to logs is dependent on access rights of the roles.

10.3 Backups

Databases and transaction logs are routinely backed up and recovery of backups is tested regularly. The system is adapted for a maximum data loss of 1 hour (ie RPO = 1), but backup is done on the transaction log every 15 minutes 24/7/365.

AFA Insurance focuses on high redundancy and accessibility in the architecture. Disaster recovery personnel and troubleshooting out of office hours are done by the staff in accordance with the emergency response routine. Backups of servers in both of the data centres are stored separately from the original.

10.4 Malware protection

The following protection is available from the Internet to the IA system:

- Antivirus
- Antispyware
- Vulnerability protection (CVE vulnerabilities)
- File block (Execute files checked in Sandbox)

Only http and https traffic are approved by default.The IA System is separated from other IT systems within AFA Insurance via firewalls.

Clients that are used to connect to the servers have anti-virus software enabled. Both servers and clients are hardened prior to deployment.

10.5 Vulnerability management

A team of dedicated staff is responsible for monitoring information from suppliers about products and components concerning security deficiencies and available updates. A risk analysis is performed, after which serious security deficiencies and important updates are addressed immediately. Other issues are addressed in line with documented procedures for routine version management. All changes to software used and to constituent third-party components in the IA System are documented.

11 Communications security

The solution is protected by a firewall so that only pre-defined traffic is allowed network access to the solution. This means that web servers and da-

tabase servers are in AFA Insurance's DMZ, which is separate from internal networks and the Internet.

All traffic that passes the firewall is logged. The logs are saved for a period of 12 months. All entries are saved for the same period of time.

12 Acquisition, development and maintenance of systems

12.1 Testing and development

Development team

Systems are developed using an agile approach, based on proactive quality assurance with continuous testing and feedback of performance. The agile approach to system development includes a requirement process and testing.

The development team is responsible for all activities needed to assure the quality of each product backlog item (PBI) in each sprint. The team is also responsible for assuring the quality of the IA System and the product over the long term.

Reference group

Any requests for new features are dealt with via a reference group. The reference group comprises company representatives, appointed by the sectors, and sector representatives. The reference group convenes twice a year to prioritise these requests. Different committees prepare the cases and present concrete proposals for new solutions for the various areas. The committees comprise users from different companies and sectors with interests in specific issues. The committees also serve as sounding boards during the development process to enable AFA Insurance to ascertain that the solution will provide what the reference group is requesting.

One week before the start of production, information about the content of future releases is sent to the chief administrative officers at each company.

IT environments

Separate IT environments are used for production and for testing and developing the IA System.

12.2 Browsers

The IA System is designed to work with XHTML-compatible browsers. The IA System generates reports in PDF, TIFF and Excel formats and its map feature uses Google Maps.

12.3 Penetration testing

External parties conduct thorough penetration tests at least once a year to

evaluate the system's security. User companies may not conduct security audits or penetration tests on the IA System without prior permission of AFA Insurance. Contact AFA Insurance's IA Support for further information.

12.4 End of contract

At the end of the contract, and in compliance with the general terms, all personal data will be deleted from reported work-related injury risks and work-related injuries. Other events are deleted.

Should the user company request its data to be migrated, reported events data can be exported to Excel and reported risk management data to PDF as protocols.

13 Managing data security incidents

The Application Manager is responsible for the operative management of serious IT incidents. This involves communication, investigation and reporting of incidents.

The Application Manager analyses the IT incidents to ensure that adequate action has been taken to manage the incident and that the experience gained from the incident can be used in the organisation's operative risk management processes.

A solutions team is appointed to solve the incident and assist the Application Manager with the investigation.

In the event of a cyber attack on AFA Insurance, CERT is enabled.

AFA Insurance's Crisis Management Team can be activated if warranted by the seriousness of the incident.

Incidents relating to personal data are managed in accordance with the Personal Data Processor Agreement.

14 Business continuity management

The IA System is mirrored in two separate data centres in the Stockholm area. Each data centre has the capacity to maintain system availability should one of the data centres go down.

15 Compliance

AFA Insurance's Internal Audit operates to an annual audit plan. Internal Audit reports to the Board of Directors, the Audit Committee and the CEO. The Audit Plan is prepared through an objective and independent assessment of materiality and risk to provide an overall opinion on the adequacy of internal governance and control.