The IA System Security Appendix

Contents

1 Introduction

Afa Trygg tjänstepensionsaktiebolag company org. no. 516401–8615 (the Supplier) strives to maintain a high level of security for its own and its customers' (user organisations') data. In order to achieve this, all work is carried out in a structured and documented manner and is regularly evaluated with the aim of continuously improving security and quality.

This Security Appendix explains how the Supplier achieves a high level of security for its user organisations' data, which is processed in the "Work Environment Information System", hereinafter referred to as the IA-system.

The appendix also includes a section on requirements concerning the user organisation's responsibility in terms of contributing to data security work.

Questions concerning the Supplier's measures to ensure good data security can be directed to IA support at the following e-mail address: iasupport@afaforsakring.se.

2 Organisational protection measures

2.1 Leadership

Information and IT security are focus areas in development, operation and maintenance.

2.2 Organisation

The Supplier has a dedicated organisation, the IA unit, which is responsible for all aspects (e.g. development, operation, maintenance, security and support) of the IA system's applications and platforms.

2.2.1 The security function

The IA unit has a central security function that provides support in terms of expertise, assessments and guidelines for information and IT security. The security function also deals with issues relating to physical security and staff security.

2.2.2 Computer Emergency Response Team (CERT)

In addition to the central security function, an internal Computer Emergency Response Team (CERT) is provided as required, under the leadership of the data security manager, to prevent damage, assess damage that has occurred during an attack and manage the recovery of any affected data.

2.3 Staff

The Supplier uses its own and hired staff (hereinafter referred to as "all staff") to deliver the IA system.

2.3.1 Non-disclosure

All staff sign a non-disclosure agreement before being granted access to the IT system in accordance with the Swedish Non-Disclosure Act (2020:914) on the Outsourcing of Technological Processing or Data Storage.

2.3.2 Background checks

Basic background checks are carried out on new staff, including employees and consultants, who will be working with the IA system.

2.3.3 Training

All staff who start working with the IA system receive training on how to use the IA system and on any relevant restrictions. They are also briefed on relevant governing internal rules.

In addition, staff receive security training specifically relating to their professional role, such as secure software development, threat modelling, the

use of security tools.

The Supplier then works on an ongoing basis to keep staff updated on the above and to continuously provide further training to staff when relevant areas are added.

2.3.4 Follow-up

Regular conversations with all staff are used to ensure a good working environment and to detect and prevent improper behaviour.

2.4 Governing Internal Rules

The Supplier uses governing internal rules (administered as documents) to ensure that operational security is maintained within the organisation. There is an internal process for drawing up/amending rules and applicable rules are revised at least once a year. The governing internal rules are under the control of the compliance officer and the Supplier's internal audit.

2.5 Regulatory compliance:

The Supplier's internal audit works in accordance with an annual audit plan. Internal audit reports to the Board of Directors, the Audit Committee and the CEO. The audit plan is prepared based on an objective and independent assessment of materiality and risk to provide an overall view of the company's internal governance and control.

2.6 Working methods, principles and quality controls

The Supplier works on the basis of the life cycle phases:

- Development
-
- Maintenance

The working methods, principles and quality controls relevant from a security perspective are described below.

2.6.1 Development and management

2.6.1.1 Working methods

Important working methods are:

- Security & Privacy by Design
- Threat modelling
- Behaviour-driven development (BDD)
- Continuous Testing
    - Functional

  - Non-functional
  - Code Quality
  - Software Composition Analysis
- Reference reviews
  - Suggested Solution
  - Code Quality
- Retrospective
- Infrastructure as Code (IaC)

2.6.1.2 Principles when choosing technologies

General principles are:

- In order to achieve maximum experience, security and manageability, the most suitable technologies are selected on the basis of the characteristics that the IA system must deliver, which in practice means that the IA system is a heterogeneous system with many different technologies, including open source and proprietary technology.
- In order to run a cost-efficient business, technologies are selected on the basis of “Consume – Buy – Build”. This means that the Supplier primarily uses open source technology, followed by proprietary technology, and as a last resort develops its own solutions.
- The Supplier chooses established technologies that have a proven track record to ensure stable and predictable delivery.
- The Supplier also chooses de facto standards when available to make it easier for all parties involved and to conduct cost-effective operations.
- To avoid the risk of entrapment, the Supplier chooses technologies that have a large and active community, regardless of whether these technologies are open source or proprietary.
- In order to be able to ensure quick and secure development, the Supplier chooses technologies with built-in control mechanisms, such as type-reliable programming languages.

2.6.1.3 Quality control checks

All proprietary code is checked at each check-in with Static Application Security Testing (SAST) and there is a control function that prevents code from entering production if it does not meet all quality and security requirements.

All code from an open source project is checked at each check-in with

Software Composition Analysis (SCA).

2.6.2 Operations

2.6.2.1 Working methods

- Least privileage
- Continuous Security Scanning
  - Software Composition Analysis (SCA)
  - Dynamic Application Security Testing (DAST)
- Continuous Testing in Production
  - Synthetic monitoring rolls every minute, around the clock, to ensure that the WEI system is available and qualitative
- Continuous Patching
  - Applications always use supported versions of e.g. frameworks
  - Normal behaviour is to address identified vulnerabilities as soon as possible, with the exception of vulnerabilities that we consider to be very minor and do not jeopardise security.

2.6.2.2 Quality control checks

All applications are monitored around the clock using automated synthetic monitoring.

All environments (see below) are checked weekly with Dynamic Application Security Testing (DAST).

2.6.3 Incident management

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

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

It is primarily theSupplier’s Developer teams and Platform team that performs the operational work, but the Incident Manager can call in all available staff as required.

In the event that the Supplier is exposed to a cyber attack, the Supplier’s own CERT is activated.

The Supplier'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.

3 Technological protection measures

3.1 Introduction

3.1.1 Technological layers

Areas of application

- The applications that IA users use directly or indirectly
- The IA system's applications are categorised into three types:
  - Mobile applications
  - Web applications
  - APIs

Platforms

- The platforms needed to be able to develop and operate the above applications, e.g. container cluster, application and database servers
- Platforms that are assembled into environments for applications to be deployed in, for example, the production environment, acceptance test environment and development environment

Infrastructure

- The underlying infrastructure needed to be able to develop and operate the above platforms such as data centres and virtualisation of its resources

3.2 Confidentiality

3.2.1 Control of access

3.2.1.1 General information

In view of the fact that sensitive personal data can be handled in the IA system, data is classified as confidential. The Supplier uses attribute-based access control containing roles, etc., to work actively with needs-based allocation of access rights.

3.2.1.2 For the Supplier

The Supplier's support staff for the IA system may need to connect to the user organisation and thereby access the organisation's data in order to provide correct answers 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.

Only a very limited number of (named) administrators have full rights to storage, backups and directory services. All logins to the IA system are made using personal accounts and are logged.

3.2.1.3 For user organisations

The supplier only creates and assigns authorisations for a first administrative account at the user organisation. The user organisation is then responsible for administration of users of the IA System within their own organisation. Access rights are granted via roles which the administrators assign to users. The user companies' users, administrators and other users are able to specify a temporary substitute for their access rights.

The user organisation is responsible for the login method.

3.2.2 Encryption

All communication uses encryption in transit with an encryption algorithm in accordance with 188 Scheme Crypto Policy (Swedish Certification Body for IT Security), the most common encryption being Transport Layer Security (TLS) version 1.2.

The storage (for example, database) of sensitive data always uses encryption at rest with the encryption algorithm in accordance with 188 Scheme Crypto Policy (Swedish Certification Body for IT Security), the most common being The Advanced Encryption Standard (AES), 128 bits.

There are documented procedures in place for managing and updating cryptographic material such as keys for certificates.

3.2.3 Separation

The IA system has fully dedicated platforms. These are separated from other systems and applications at the Supplier through network segmentation (firewall rules).

The IA system's production environments (production, training and reference) are completely separated from other environments, such as acceptance testing environments through network segmentation (firewall rules).

The IA system is a so-called multi-tenant system, which means that all user organisations' data is stored in the same database in the respective

environment and separated by means of logical separation.

3.2.4 Perimeter protection, enhanced security and maintenance

All environments are protected by firewalls with built in redundancy.

Servers used for the IA system have antivirus, anti-spyware and anti-ransomware installed and activated.

All equipment and software in the IA system is continuously maintained and largely automated with regard to patching of applications and platforms.

3.3 Accuracy

The IA system's time is retrieved from the system's servers, and underlying services. Logged times are presented in the user browser’s time zone and the format is taken from the user’s language settings.

The logs cannot be manipulated from within the IA system. The logs are saved as is.

3.3.1 Traceability

Centralised log management is used for the IA system and for related network communication. Designated staff actively work to detect high-risk activities using rules-based alarms and deviation analysis tools. Where necessary, relevant components of the logs can be made available to the user organisation.

Data is protected using authorisations that are controlled at all levels in the IA system. Data processing, reading, editing and logins are all logged. Failed attempts to log in and any changes to authorisations are also logged.

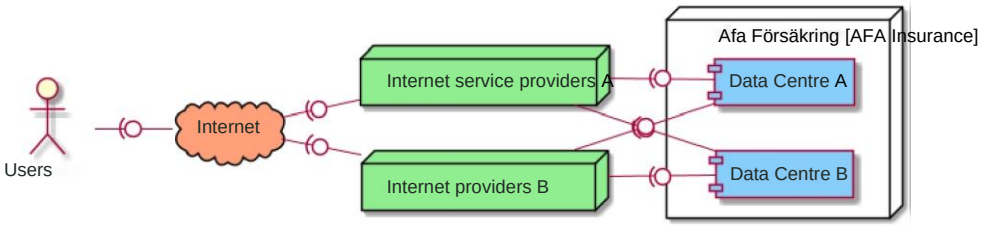
Access to logs is always based on authorisation.

3.4 Availability

3.4.1 Redundancy

3.4.1.1 Internet access

Two independent, external suppliers are used to ensure a redundant connection to the Internet.



3.4.1.2 Data centres

Both data centres are identical in terms of systems and mirrored in real time, in order to offer high availability without the need for downtime.

With regard to attempted sabotage through so-called denial of service, the environments are protected through built-in technology in the firewall and by the provision of the Internet operator.

3.4.1.2.1 Data Centre A

- Located in the Stockholm area
- Private data centre
- The data centre is used by the Supplier's insurance operations, asset management, preventive operations and support functions
- Internal evaluation for protection level 2 (MSB)

3.4.1.2.2 Data Centre B

- Located in the Stockholm area
- Colocation Centre
- The supplier has its own equipment, stored in locked racks, in a dedicated and access-controlled cage
- The data centre is used by the Supplier's insurance operations, asset management, preventive operations and support functions
- Other customers using the colocation centre are unknown
- Internal evaluation for protection level 3 (MSB)

3.4.1.2.3 Security specifically related to data centres

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

The intruder alarm is connected to a security company that responds to alarms around the clock. The operations areas are patrolled by security guards. This happens at irregular intervals 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 staff have physical access to the data centres. Access to the data centres is based on authorisation. The entry system logs successful and unsuccessful attempts at physical entry.

Any data on digital media that is disposed of is deleted. The digital media is then destroyed. This is done at a secure facility by security-approved staff.

3.4.2 Backup and recovery

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, but back-up takes place on the transaction log every 15 minutes 24/7/365.

- Recovery Point Objective/Data loss (RPO) in 1 hour
- RTO (Recovery Time Objective/Down time) in 8 hours

Backups of servers in both data centres are stored separately from the original for 60 days.

3.4.3 Monitoring

All applications, platforms and infrastructure are monitored around the clock using automated monitoring. Any deviations are alerted to authorised staff.

3.4.4 Exporting data

Event data can be downloaded from the IA system as Excel or PDF files. Risk management data is downloaded as a protocol to PDF.

3.4.5 End of contract

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

The user organisation can download its data from the system. Data on reported events is downloaded to Excel. Data on reported risk management is downloaded as a protocol to PDF.

4 User organisation's own responsibility

4.1 Web application

4.1.1 Updated browsers

IA is delivered as a SaaS service that is used via web interface. The web application is adapted for xhtml-compatible browsers and optimised for chromium-based browsers. Browsers are kept up to date.

4.1.2 Choice of login method

The IA system offers login via user name/password and/or Single Sign-On (SSO) via SAML 2.0.

Logging in using SSO enhances security when using the IA system. The user organisation itself can configure the system so that only login via SSO is accepted, in order to ensure that users of the IA system have authenticated themselves before logging into the IA system. However, SSO means that anonymous reporting of cases in the IA system cannot be done.

The level of authentication is set by the user organisation when configuring SSO in the user organisation's environment.

A log of SSO logins is available to authorised users in the system. The log shows any login problems for individual users.

4.1.3 Handling position data/coordinates

The IA system uses Google Maps as its map function.

Use of Google Maps constitutes acceptance of Google's terms of use: https://maps.google.com/help/terms_maps/and privacy policy https://www.google.com/policies/privacy/. When the map is opened, no data is transferred to Google from the IA system.

If the user organisation does not wish to use Google Maps, it can be switched off under General Settings on the Admin/Organisation page in the system.

4.2 Mobile app

The system has a mobile app for reporting, which is optional to use. The mobile app is developed for iOS and Android and can be downloaded on App Store and Google Play.

It is important to keep the app updated to the latest published version.

The app uses the phone's built-in camera and map function, which makes it possible to send pictures and/or position data. Both functions can be switched off using the system's administration function.

Communication between the mobile app and the system's backend is encrypted via https. Data is primarily sent from the app to the backend. Only the case

status is returned to the app.

Login to the app takes place via a group account via user name and password.

4.3 APIs

The IA system has APIs for automated administration of the organisation and users, as well as services for downloading data.

The APIs are version managed. Information about new versions of the APIs reaches the user organisation via the system's newsletter. Old APIs are removed about 6 months after the new ones are published.

Log of imports is shown in the system for authorised users- Ay error entries are shown in the log.