Information Security Policy

Owner: Chris Martin, Operations Director

Version: 3.1 April 2018

Content

Content 2

1 Introduction 3

2 Responsibilities for information security 5

3 Information classification and handling 7

4 System/FA Domain security 8

5 Electronic data transfers 10

6 Laptop users 12

7 Mobile phones, PDAs and tablets 13

8 Disposal of hardware 14

9 Paper based data 15

10 Information Security Breaches: General 17

11 Non-Personal Data Breaches 19

12 Personal Data Breaches - Notification Procedure 20

1 Introduction

Policy Statement

Information plays an essential role in the business of First Actuarial.

To fulfil our obligations to the data subjects and owners of information, we will ensure the security of this information and the systems on which it is stored, and protect the information and systems from accidental or deliberate damage, loss or corruption.

Objectives

The objectives of First Actuarial's Information Security Policy are to preserve:

- Confidentiality - Access to information shall be confined to those with appropriate authority.
- Integrity – Information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specification.
- Availability - Information shall be available and delivered to the right person, at the time when it is needed.

Policy aim

The aim of this policy is to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by First Actuarial by:

- Ensuring that all members of staff are aware of, and fully comply with, the relevant legislation as described in this and other policies.
- Describing the principles of security and explaining how they shall be implemented within First Actuarial.
- Introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities.
- Creating and maintaining within the organisation a level of awareness of the need for Information Security as an integral part of the day to day business.
- Protecting information assets under the control of the organisation.

Scope

This policy applies to all full and part time employees, founders, partners, directors and officers, and all consultants and sub-contractors (hereafter collectively referred to as "Staff") working within First Actuarial. All staff are required to ensure that they understand and adhere to this policy and all relevant business procedures.

Failure to follow this policy is a disciplinary offence.

Related Information

The Information Security Policy must be viewed in the context of First Actuarial's overall governance structure; in particular the principles, standards and compliance requirements set out in the First Actuarial Compliance Manual and the Employee Handbook.

Version

Version	Date	Description	By	Reviewer
3.0	Mar 2018	Original version (2.3) separated into 2 documents, reformatted, and inclusion of more detailed data breach policy	M Sadler	C Martin
3.1	Apr 2018	Updated to reflect comments from the Board	Board	C Martin

2 Responsibilities for information security

Staff

All Staff have a responsibility to be aware of and to fulfil the relevant security arrangements for their role. We all need to:

- comply with Information Security procedures including the maintenance of data confidentiality and data integrity
- comply with the operational security of the information systems we use
- ensure that the confidentiality, integrity and availability of the information we use is maintained to the highest standard
- report breaches without delay (see Sections 10 to 12).

Failure to comply with the above may result in disciplinary action.

All Staff should inform the Operations Director if they see ways to improve the Information Security arrangements.

Information Security is managed within First Actuarial by the following:

Board of First Actuarial

The Board of First Actuarial has ultimate responsibility for Information Security including approval of the Information Security Policy.

Operations Director

Responsible for:

- the continuing development and improvement of Information Security;
- ensuring that First Actuarial policies and procedures comply with the ISO27001 standard;
- ensuring that applicable requirements related to Information Security are satisfied;
- driving the review and updating of the Information Security Policy for subsequent approval by the Board. This review shall take place at least annually;
- determining Information Security objectives and appropriate monitoring and measurement arrangements to be able to demonstrate how well those objectives are being met;
- managing Information Security communications and training.

Director of IT Services

Responsible for:

- managing and implementing the IT aspects of this policy in accordance with any IT policies on a day to day basis;
- leading the Systems - Technology Support Strategy Group which has a remit for operational matters including Information Security.

Office Information Security Representatives

Responsible for:

- acting as a sounding board on Information Security matters for their local office;
- raising awareness in their local office; for example by running training courses;
- obtaining local feedback, views and suggestions for improvements;
- identifying information security weaknesses and events;
- providing guidance to local employees to help with adherence to respective policies;
- liaising (with other representatives) to discuss Information Security matters, with the aim of identifying changes/improvements.

Line Managers

Responsible for ensuring that the staff under their management are aware of:

- the Information Security policies applicable in their work areas;
- their personal responsibilities for Information Security;
- how to access advice on Information Security matters.

Contracts with external suppliers

Where external suppliers require access to First Actuarial's systems, terms of access will be covered by a contract that must be in place before such access is allowed. These contracts shall ensure that the staff or sub-contractors of the external organisation shall comply with all appropriate security policies.

3 Information classification and handling

Types of information

First Actuarial handles the following types of information:

Public - Information intended for public use, eg external website and marketing material.

Internal Firm Information - Internal information that does not contain any client information or personal data. This may include draft 'Public' information that has not yet been published.

It also includes internal processes and procedures.

Client Information - This includes most normal client work, that does not contain personal data.

Personal Data - This is information that contains personal data.

Security Classification

Information is classified to one of three security levels:

Public

Public information is not confidential and does not need to be protected.

This includes all public information. It may include internal firm information that has been explicitly marked as something we are willing to share.,

Internal

Information that needs to be protected against external disclosure.

This includes all non-restricted client information and internal firm information.

Information classified as "internal" may be subject to specific additional security measures.

Restricted

Information in this category is subject to the highest security measures.

All Personal Data will fall within this classification.

Client information on particularly sensitive or confidential matters (eg changes to scheme design, advice on redundancy exercises and any mergers & acquisition work) will be classified as restricted. Other client work may be classified as restricted at the discretion of the client manager.

4 System/FA Domain security

Locking computers

- All computers (laptops and desktops) should be password locked when unattended (eg at lunch-breaks, comfort breaks and similar).
- Staff must log out and shut down their computer when leaving work for the evening/over the weekend.
- Staff working remotely who access the network via LogMeIn must sign out when they have finished working for the day.

Windows Password Policy

- Passwords expire and must be changed at least every 42 days. Automatic reminders are issued as expiry approaches.
- Passwords may not be reused.
- Passwords must be meet complexity requirements:
  - Must be at least 8 characters long.
  - Must contain at least one English uppercase character (A-Z).
  - Must contain at least one English lowercase character (a-z).
  - Must contain at least one digit (0-9 or punctuation mark/symbol).
  - Should not be commonly used and obvious passwords (ie not to be based on easily discoverable information).
- Users are responsible for the security and confidentiality of their password. Passwords are:
  - Not to be disclosed or shared with others.
  - Not to be written down.

Account Lockout policy

- Accounts will be locked after multiple (10 in any 30 minute period) unsuccessful logon attempts.
- Accounts can only be unlocked by the IT Department.

Password Resets

- Expired or forgotten passwords can only be reset by the IT Department.
- Any such reset must be authorised by a First Actuarial Founder or Partner before the IT Department implements the request.

Software Installs and updates

- Most staff are prevented from installing software or updates to software which require administration rights. Any such updates will normally be done by the IT Department.
- Staff should not download or install any software even if they are able to do so eg where administration rights are not required

- In specific circumstances, some users may for operational reasons have administration rights to install software. If a user has such rights, how they are used must be agreed with, and permission to install any software sought from, the IT Department in advance.
- Non-business related software must not be installed or downloaded on First Actuarial hardware.

Use of Peripheral Equipment

- Peripheral equipment (eg a powerpoint clicker or mouse) should not be plugged into First Actuarial hardware unless supplied and/or approved by the IT Department.
- In particular, non-First Actuarial supplied USB devices must not be plugged into USB ports on First Actuarial hardware.

5 Electronic data transfers

Physical movement or transmission of electronic data outside of the First Actuarial network, particularly over the public internet or other external networks, is vulnerable to loss, theft or unauthorised access.

Sending Information by Email

All 'Restricted' information that is sent by email, outside of the First Actuarial domain, must be contained in a password protected or encrypted attached file (eg Word or Excel).

More specifically:

- Personal member data should not be sent in the open text of an email.
- Member data should be contained in a file of a suitable software package.
- Files containing sensitive and/or personal member data should routinely be zipped and encrypted using WinZip. WinZip is installed on every user's PC. The latest version of WinZip installed will directly zip and encrypt files added into an email as an attachment, when those options are selected by the user.
- Where recipients (outside of First Actuarial) do not have WinZip (and hence are unable to unzip and open password protected files), the native files (eg Excel files/Word documents) should be password protected using the inbuilt security of the relevant software package
- Passwords should not be contained in the same email as that which attaches the file containing the data. Passwords should be notified to the recipient by another method (eg verbally by telephone).
- The format of passwords for encrypting should be client specific and contain, as a minimum, a combination of letters and numbers. If an agreed password is reused for client communications it must be updated when a member of staff who knows the password leaves.

Data on DVD, CD or USB sticks

DVDs / CDs

- 'Restricted' information that is stored/saved to portable media must be encrypted.
- Encryption should be undertaken using WinZip or native document encryption (Word/Excel).

USB Memory Sticks

- All First Actuarial laptops and desktops are configured so that the USB sockets will not write to unencrypted datapens (although data can be read from unencrypted datapens).
- Portable media storage containing 'Restricted' information should not be left unattended.

When sending portable media storage through the post:

- Recorded Delivery, by an approved supplier or Royal Mail, must be used so delivery can be tracked.
- The password must not be posted within the same package containing the portable media storage.
- The recipient of the data must be contacted separately to confirm receipt and to be provided with the password to decrypt the encrypted files.

6 Laptop users

Laptop users present a greater risk to data integrity as a result of the hardware, potentially containing sensitive data, being physically moved outside of First Actuarial's offices.

Laptops must not be left unattended in public places (eg coffee shops, restaurants etc). Kensington locks are available for each laptop user as additional theft protection (eg for when laptops are taken outside of First Actuarial offices).

Laptops left in First Actuarial offices overnight must be put away in locked drawers/cupboards or secured to the desk/docking station using a Kensington lock.

Shutting Down/Stand by ("Sleep" mode)

Laptops should be regularly shut down before leaving the office, instead of continually being placed into stand-by/sleep mode.

Use of Public WiFi

Encrypted WiFi or the tethering facility on smartphones must be used.

7 Mobile phones, PDAs and tablets

Company provided devices

First Actuarial provides mobile phones to Founders, Partners and some senior staff which synchronise with the First Actuarial network; particularly in relation to emails, contacts and calendars.

All such devices must use a password/PIN number to protect against unauthorised access to the phone/PDA/tablet and/or SIM card.

Own devices

Staff may synchronise their own devices (eg mobile phones, PDAs or tablets) with the network if they agree to comply with any security policy that the Board requires.

This will include:

- Use of password/PIN numbers to protect against unauthorised access to the phone/PDA/tablet and/or SIM card.
- The ability for the IT Department to remote wipe the device in the event of the device being lost.

Use of Public WiFi

Encrypted WiFi must be used if this is available.

If only open WiFi is available, then the IT Department can provide a VPN facility.

8 Disposal of hardware

All First Actuarial hardware must be returned to the IT Department for secure disposal.

Where multi-functional photocopiers (which have an internal hard-drive) are replaced, instruction should be given and confirmation sought that the hard-drive has been wiped/destroyed.

9 Paper based data

Clear desk policy

Non-First Actuarial staff may enter the offices outside of normal office hours; these individuals may include, for example, employees of contracted cleaning firms.

To limit the opportunity of personal information being readily accessible, staff must operate a clear desk policy as described below.

During the day

- When away from your desk ensure that 'Restricted' information cannot be accidentally read by others, by closing the file or placing the paperwork face down.

At the end of the day

- All 'Restricted' information must be removed from desks and stored out of sight in locked cupboards and drawers, or locked filing rooms/racks, with keys then being securely located (ie not left in the locks).
- 'Internal' information may remain on the desk but should be in a closed file or face down to prevent accidental reading.

Offsite storage and scanning

Any offsite storage/archive/scanning must be carried out by a supplier from First Actuarial's Preferred Suppliers List.

Sending files externally

Where files (or other paper based data) are being transported externally, a courier firm from First Actuarial's Preferred Suppliers List must be used.

Recipients of information sent by this distribution method must be asked to acknowledge receipt.

Taking files offsite

'Restricted' information should not, in the normal course of events, be taken offsite, but should be kept in the relevant office.

Where staff need access to paper-based 'Restricted' information, such as member data, photocopies of the relevant pages should be taken and these copies can then be taken offsite, provided that they are returned or disposed of after use in the confidential waste bins kept onsite.

Such 'Restricted' papers must not be left unattended in public places.

Using paper files at home/offsite

Staff who have a business need to take 'Restricted' information offsite must ensure that such information is not left in plain view. Any such papers should be stored out of sight when not in use.

Any such papers should be returned to the office at the earliest opportunity.

Disposing of data

Any papers containing 'Internal' or 'Restricted' information which are no longer required should be returned to the office for shredding or disposed of in the confidential waste bins provided, to then be shredded by the relevant external company.

Expression of wish forms

Where First Actuarial holds paper-based expression of wish forms (on individual member files), if these are not contained in sealed envelopes then a scanned electronic copy should be taken as additional back up.

10 Information Security Breaches: General

An information security breach includes:

- Disclosure to the wrong people (internal or external). This includes both actual disclosure and potential disclosure (ie. lost data which may or may not have been seen)
- Integrity: Where data is incorrect (either due to a deliberate change or failure to raise knowingly incorrect data)
- Availability: Where data is unexpectedly unavailable

Breaches apply for both paper and electronic records.

Reporting Breaches

Any staff member who becomes aware of an actual or potential Personal Data security breach must immediately notify the known circumstances to the information security representative for their office. If the information security representative is not available they should notify a local founder or partner; or, if necessary, any founder or partner within the firm. Outside of normal hours contact details of founders and partners may be found on the company website.

Where the breach includes the loss or compromise of IT equipment, the loss must also be notified to the IT Department immediately on 0330 363 8000. This number is manned 8am-6pm Monday to Friday. Outside of those hours a message should be left on the IT Department's voicemail. The voicemail system includes an automatic alert to members of the IT Department on the out of hours support rota.

Examples of breaches are given at the end of this section.

Handling Breaches

The information security representative (or their alternative if they are not available) will determine if the breach involves Personal Data. Where breaches involve Personal Data they must follow section 12, otherwise they must follow section 11.

Examples of breaches

- Device loss
  - Loss of any portable data storage device on which personal data is stored
- Data theft
  - Theft of data by any employee or contractor
  - Hacking attack
  - Malware
- System failure leading to loss or corruption of personal data
  - Virus or Trojan attack

- Compliance
  - Failure to put in place contracts with subcontractors
  - Data sharing outside of agreed terms in data sharing protocols

- Errors
  - Such as incomplete mail merging, or mis-matching names and addresses
  - Sending email to the wrong recipient
  - Attaching paperwork that is unrelated when picking up printed correspondence

- Unforeseen circumstances such as a fire or flood

11 Non-Personal Data Breaches

This section concerns data security breaches that do NOT include Personal Data.

Investigation and external reporting

The local information security representative shall be responsible for the following:

1. Recording the breach on the internal ISO Incidents and Events Log.
2. Investigating the breach.
3. Determining if the breach involved client data
   - Where the breach does involve client data the information security representative shall report the breach to the client manager. The client manager will then decide what information to report to the client.
4. Deciding what factors gave rise to the breach and recommending changes to processes or systems to prevent a similar breach in future.

Review of breaches

The Information Security Sub Group will review all breaches record on the ISO Incidents and Events Log (including any Personal Data breaches) to establish any changes to procedures that are required across the business.

12 Personal Data Breaches - Notification Procedure

About the obligation to report Personal Data security breaches

This section concerns data security breaches relating to Personal Data only.

Broadly, Personal Data means data relating to a living individual who can be identified from that data.

First Actuarial must investigate any potential Personal Data security breach and identify actual breaches.

In some circumstances where a breach is likely to have a significant impact, the breach must be reported to the Information Commissioner's Office (ICO) within 72 hours of our being reasonably sure that a breach has taken place.

When a Personal Data security breach presents a high risk to the rights and freedoms of data subjects there is an additional duty to communicate the details to the individuals concerned so that they can take steps to protect themselves.

Failing to notify a breach when required to do so can result in a significant fine (up to 10 million Euros for a firm of First Actuarial's size).

Investigation and external reporting

The operations director, the local information security representative and the client manager shall be responsible separately or jointly for the following:

1. Deciding if a Personal Data security breach has occurred
2. Reporting all breaches to the data controller.
   - Where the data controller is the client, this should follow any agreed reporting process. If there is no such agreement reporting should be done immediately.
3. Recording the breach on the internal ISO Incidents and Events Log.
4. Investigating the breach.
5. Where we are the data controller then if appropriate report to the ICO, after using the "Risk to individuals" Matrix to determine the significance of the security breach.
6. Liaising with external agencies and the press in connection with the incident.
7. Deciding what factors gave rise to the breach and recommending changes to processes or systems to prevent a similar breach in future.

Which breaches are reported to the Data Controller?

Unlike reporting to ICO (see below) there is no discretion in whether to report Personal Data breaches to the data controller. Therefore, all Personal Data breaches must be reported to the data controller (which is likely to be the client and the Scheme Actuary).

GDPR itself requires this to be done “without undue delay” and the associated guidance defines this as “promptly.”

On becoming aware of a breach, unless otherwise agreed, First Actuarial will report such breaches to the data controller within 24 hours.

Which breaches are reported to the ICO?

Decisions on reporting Personal Data breaches to the ICO must be made by the data controller. Depending on the appointment, the data controller may be the client, the Scheme Actuary, or First Actuarial. Our standard appointments allocate responsibility for reporting to ICO to the client.

Guidance from the Article 29 Working Party (advisory body on data protection to European Commission) in 2017 about Personal Data security breach reporting under GDPR is as follows:

“You only have to notify the relevant supervisory authority of a breach where it is likely to result in a risk to the rights and freedoms of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on individuals – for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

This has to be assessed on a case by case basis. For example, you will need to notify the relevant supervisory authority about a loss of customer details where the breach leaves individuals open to identity theft. On the other hand, the loss or inappropriate alteration of a staff telephone list, for example, would not normally meet this threshold.”

When to report to data subjects

Under GDPR there is a duty to report security breaches that are likely to result in a high risk to the rights and freedoms of individuals.

The term ‘high risk’ indicates that the threshold for notifying data subjects is higher than for notifying the ICO.

First Actuarial’s Information Asset Registers for each dataset contain a risk matrix to help determine the level of risk to a data subject in the event of a breach. This should be referred to when deciding whether to report to the ICO or the data subject.