Solidatus

Incident management and data breach policy and procedure

Version: 2.2

Date: 07 October 2020

Author: Philip A. S. Miller

Contents

1. Introduction

Information security is everyone's responsibility. All staff are required to take responsibility for the protection of personal and business sensitive information that they manage or access. It is therefore essential that all Threadneedle Software Ltd (Solidatus) staff and contractors are familiar with, and comply with, the organisation's information security policy.

1.1 Purpose

The purpose of this policy is twofold:

1.1.1 firstly, to ensure that all staff are fully aware and understand the process to be followed if an information security incident occurs;

1.1.2 secondly, to ensure that all information security incidents are thoroughly documented and recorded.

All information security incidents must be reported to minimise any potential risk and impact that may occur as a result of it. Failure to report an incident has the potential to result in disciplinary action.

All employees of Solidatus, temporary staff and service providers with access to Solidatus information/systems are subject to this policy.

1.2 Policy

1.2.1 The data policy of the Company is based on the information published by the ICO - https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/

1.2.2 Solidatus adopts a risk-based approach to the assessment of data risks. Solidatus' approach to risk management to the management of all business risks, including data breaches. Solidatus will ensure that there are adequate skilled resources in all lines of defence to manage risk within the Solidatus' 2LOD process (Staff – process owner, overseen by the Executive – business owner).

1.3 Framework

The framework of this policy is based upon the following statements:

1.3.1 We know how to recognise a personal data breach.
1.3.2 We understand that a personal data breach isn't only about loss or theft of personal data.
1.3.3 We have prepared a response plan for addressing any personal data breaches that occur.
1.3.4 We have allocated responsibility for managing breaches to a dedicated person or team.
1.3.5 Our staff know how to escalate a security incident to the appropriate person or team in our organisation to determine whether a breach has occurred.

2. Identifying incidents and personal data breaches

2.1 Incidents

An information security incident involves the loss or misuse of any personal or business sensitive data held by Threadneedle Software Ltd regardless of format. This includes electronic data held within Threadneedle Software Ltd ICT systems and physically held information.

An information security incident can happen for a number of reasons:

2.1.1 Failure to follow Threadneedle Software Ltd information security policies (and therefore place corporate information at risk).
2.1.2 Loss or theft of files or equipment on which data is stored.
2.1.3 Inappropriate access controls allowing unauthorized use.
2.1.4 Human error.
2.1.5 Hacking/virus attack.
2.1.6 Social engineering communications where information is obtained by deceit.

Some examples of Information Security incidents are as follows:

2.1.7 Theft or loss of IT equipment.
2.1.8 Accessing personal information about clients/staff inappropriately.
2.1.9 Leaving confidential/sensitive files unattended.
2.1.10 Disclosing your password to someone else.
2.1.11 Inadequate disposal of confidential material.
2.1.12 Unauthorized disclosure of sensitive client information.
2.1.13 Using client information for personal gain.
2.1.14 Sending a sensitive email to the wrong recipient by mistake.

An adverse impact of these can be defined for example as:

2.1.15 Threat to personal safety or privacy.
2.1.16 Legal obligation or regulatory penalty.
2.1.17 Financial Loss/Commercial Detriment.
2.1.18 Disruption to business.
2.1.19 Reputational loss.

These are not exhaustive lists but are representative of the circumstances which this policy seeks to cover.

2.2 Personal data breaches

The following is the trigger for this process:

2.2.1 Access by an unauthorised third party.
2.2.2 Deliberate or accidental action (or inaction) by a controller or processor.
2.2.3 Sending personal data to an incorrect recipient.
2.2.4 Computing devices containing personal data being lost or stolen.
2.2.5 Alteration of personal data without permission.
2.2.6 Loss of availability of personal data.

Solidatus

3. Responding incidents and personal data breaches

3.1 Provisions

Solidatus

3.1.1 Has in place a process to assess the likely risk to individuals as a result of a breach.
3.1.2 Knows who is the relevant supervisory authority for our processing activities.
3.1.3 Has a process to notify the ICO of a breach within 72 hours of becoming aware of it, even if we do not have all the details yet.
3.1.4 Knows what information we must give the ICO about a breach.
3.1.5 Has a process to inform affected individuals about a breach when it is likely to result in a high risk to their rights and freedoms.
3.1.6 Knows we must inform affected individuals without undue delay.
3.1.7 Knows what information about a breach we must provide to individuals, and that we should provide advice to help them protect themselves from its effects.
3.1.8 Documents all breaches, even if they don't all need to be reported.

3.2 Reporting an incident or personal data breach data breaches

All information security incidents should be reported immediately on being identified to the Information Management & Governance (IMG) team via admin@solidatus.com. The sooner an incident is reported the sooner the risks can be assessed and managed. Lost IT equipment should also be reported directly to the Operations Directors.

All incidents will need to be formally recorded on an incident report form (See Annex A) and investigated by the team involved in the incident.

The form should be completed as a formal record of the incident by the person responsible for the incident and emailed to their line manager and once fully completed finally emailed to the IMG team within ONE day of the incident being identified.

If an information security incident is caused by an external contractor, this should be reported through their Threadneedle Software Ltd contact. The team responsible for the external contract should check whether contract terms were appropriate in respect of information security and had been complied with.

3.3 Organizational management of information security incidents

The IMG team will keep a log of all incidents reported and will produce a regular report on the number, type and originator of information security incidents for review by the Information Governance Group (IGG) to allow any trends to be identified and addressed.

In line with the Threadneedle Software Ltd Risk Management Policy, the IMG team will conduct a risk assessment for each incident, to gauge the impact and likelihood of realisation, in relation to data subjects, clients and also Threadneedle Software Ltd.

As required individual or company wide reset of passwords across all SaaS platforms will be determined, implemented and recorded in the Incident Log.

As required the ICO will be notified within 72 hrs and recorded in the incident log.

All incidents will be reported to the Director/Head of Division after the risk assessment is complete to address with the employee(s) involved and also, when the mitigated risk is rated at medium or above, to Human Resources.

Human Resources will assist with consideration as to whether disciplinary action needs to be taken in respect of employees who have not complied with information security policies and guidance.

A significant security breach, or repeated security breaches, by the same individual will result in disciplinary action. Breaches of a criminal or illegal nature will be, where appropriate, reported to the relevant authorities.

All incidents and significant risks related to Information Security Incidents are captured and reported on at Board level.

3.4 Notification of breach to authorities

Data breach notifications will be made within 72 hours of the breach being uncovered and will contain the following:

3.4.1 A description of the nature of the personal data breach including, where possible:
3.4.2 the categories and approximate number of individuals concerned;
3.4.3 the categories and approximate number of personal data records concerned.
3.4.4 The name and contact details of the data protection officer (if your organization has one) or other contact point where more information can be obtained.
3.4.5 A description of the likely consequences of the personal data breach.
3.4.6 A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

3.5 Notification of breach to affected persons/companies

Where necessary persons or companies may be notified about a data breach, the notification will take the form or a letter/email unless otherwise mandated by contract:

3.5.1 The name and contact details of your data protection officer (if your organization has one) or other contact point where more information can be obtained.
3.5.2 A description of the likely consequences of the personal data breach.
3.5.3 A description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

4. Governance

4.1 Company structure

4.1.1 Private Limited Company, registered in London and Singapore.
4.1.2 Principle Governance: Executive and Board of Directors.

4.2 Registered addresses

4.2.1 HQ: 34 Copse Wood Way, London, HA6 2UA, United Kingdom.
4.2.2 Singapore: 9 Raffles Place, #26-01 Republic Plaza, Singapore 048619.

4.3 Registered offices

4.3.1 London: 68 Lombard Street, London, EC3V 9LJ, United Kingdom.
4.3.2 Singapore: 138 Cecil Street, #08-01A Cecil Court, Singapore 069538.

4.4 Accountability officer

4.4.1 Philip Miller – Email: philip.miller@solidatus.com Mobile: +44 (0)7803 619445.
4.4.2 ICO organization name: Threadneedle Software Limited.
4.4.3 ICO registration reference: ZA347748.

Solidatus

Annex A

Information security incident report

[To be completed and returned within one working day]
[Complete electronically]

Report number	

Completed IMG.

1. Notification

Reported by	Division	Phone ext	Date Reported

2. Incident details

Type of incident [tick all that apply]:	
Equipment loss	
Data loss	
Unauthorized disclosure	
Unauthorized access	
Breach of policy	
Other (expand)	

Date incident occurred	
Date incident detected	
Incident location	
Person(s) responsible for incident (originator)	

Media/device type	
If portable storage device was this password protected in line with Invest NI policy?	
If portable storage device was this encrypted? *[Please note that all Invest NI issued mobile phones and laptops are encrypted]*	
Did the device have network connectivity?	
Was any personal or business information stored on the device?	
If answer to above was 'No' explain why:	

Please describe the incident in as much detail as possible:

Please describe the information/data type. For example: is it personal information (give specific examples). Is it business sensitive (give specific examples) – consider if the information is in the public domain/would it be disclosed under FOI/would the owner/subject be concerned at its disclosure. If possible attach the information:

Solidatus

Identify potential risks to the subject/owner of the information? Eg potential for identity theft/phishing aid/commercial detriment/reputational damage:

What steps have been taken to mitigate the risks associated with the incident? For example has the information been retrieved? Has it been returned or destroyed? Has the subject/owner been informed of the incident?

What remedial action has been taken to mitigate against future similar incidents occurring at an individual/team/organizational level?

Identify any potential impact this incident may have on Invest NI's reputation or relationship with customer/stakeholder:

I confirm that the above is a complete and accurate account of the incident, information involved and potential impact:

Title	Name	Date
Originator		
Line manager		

Solidatus

Document control

Version history

Version	Date	Approved by	Notes
V1.0	01/04/2017	Board	Initial version
V2.0	01/06/2019	Board	Updated post relocation
V2.1	02/02/2020	Board	Updated post relocation, added in accountability
V2.2	07/10/2020	Board	Merging of incident and breach management