Solidatus

Solidatus information security policy

Version: 2.0

Date: 05 October 2020

Author: Philip A. S. Miller

Contents

1. Introduction

The confidentiality, integrity and availability of information, in all its forms, are critical to the ongoing functioning and good governance of Solidatus. Failure to adequately secure information increases the risk of financial and reputational losses from which it may be difficult for Solidatus to recover. This information security policy outlines Solidatus' approach to information security management. It provides the guiding principles and responsibilities necessary to safeguard the security of the Company's information systems. Supporting policies, codes of practice, procedures and guidelines provide further details.

Solidatus is committed to a robust implementation of Information Security Management. It aims to ensure the appropriate confidentiality, integrity and availability of its data. The principles defined in this policy will be applied to all of the physical and electronic information assets for which the Solidatus is responsible.

Solidatus is specifically committed to preserving the confidentiality, integrity and availability of documentation and data supplied by, generated by and held on behalf of third parties pursuant to the carrying out of work agreed by contract in accordance with the requirements of agreed security standards.

1.1 Objectives

The objectives of this policy are to:

1.1.1 Provide a framework for establishing suitable levels of information security for all Solidatus information systems (including but not limited to all Cloud environments commissioned or run by Solidatus, computers, storage, mobile devices, networking equipment, software and data) and to mitigate the risks associated with the theft, loss, misuse, damage or abuse of these systems.

- This explicitly includes any certified Information Security Management Systems the Company may run.
- The resources required to manage such systems will be made available.
- Continuous improvement of any ISMS will be undertaken in accordance with *Plan Do Check Act* principles.

1.1.2 Make certain that users are aware of and comply with all current and relevant UK and EU legislation.
1.1.3 Provide the principles by which a safe and secure information systems working environment can be established for staff and any other authorised users.
1.1.4 Ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the data that they handle.
1.1.5 Protect Solidatus from liability or damage through the misuse of its IT facilities.
1.1.6 Maintain data and other confidential information provided by suppliers at a level of security commensurate with its classification, including upholding any legal and contractual requirements around information security.
1.1.7 Respond to changes in the context of the organisation as appropriate, initiating a cycle of continuous improvement.

1.2 Scope

This policy is applicable to, and will be communicated to all staff and third parties who interact with information held by the Solidatus and the information systems used to store and process it. This includes, but is not limited to: Cloud systems developed or commissioned by Solidatus, any systems or data attached to the Solidatus data or telephone networks, systems managed by Solidatus, mobile devices used to connect to Solidatus networks or hold Solidatus data, data over which Solidatus holds the intellectual property rights, data over which Solidatus is the data controller or data processor, electronic communications sent from the Solidatus.

2. Policy

2.1 Information security principles

The following information security principles provide overarching governance for the security and management of information at Solidatus.

2.1.1 Information should be classified according to an appropriate level of confidentiality, integrity and availability (see Section 2.3. *Information classification*) and in accordance with relevant legislative, regulatory and contractual requirements (see Section 2.2. *Legal and regulatory obligations*).
2.1.2 Staff with particular responsibilities for information (see Section 3. *Responsibilities*) must ensure the classification of that information; must handle that information in accordance with its classification level; and must abide by any contractual requirements, policies, procedures or systems for meeting those responsibilities.
2.1.3 All users covered by the scope of this policy (see Section 1.2. *Scope*) must handle information appropriately and in accordance with its classification level.
2.1.4 Information should be both secure and available to those with a legitimate need for access in accordance with its classification level. On this basis, access to information will be on the basis of *least privilege* and *need to know*.
2.1.5 Information will be protected against unauthorized access and processing in accordance with its classification level.
2.1.6 Breaches of this policy must be reported (see Sections 2.6. *Compliance* and 2.7. *Incident handling*).
2.1.7 Information security provision and the policies that guide it will be regularly reviewed, including through the use of annual internal audits and penetration testing.
2.1.8 Any explicit Information Security Management Systems (ISMSs) run within the Company will be appraised and adjusted through the principles of continuous improvement.

2.2 Legal and regulatory obligations

Threadneedle Software Ltd. (Solidatus) has a responsibility to abide by and adhere to all current UK and EU legislation as well as a variety of regulatory and contractual requirements.

A non-exhaustive summary of the legislation and regulatory and contractual obligations that contribute to the form and content of this policy is provided in *Appendix A*.

Related policies will detail other applicable legislative requirements or provide further detail on the obligations arising from the legislation summarised below.

2.3 Information classification

The following table provides a summary of the information classification levels that have been adopted by Solidatus and which underpin the eight principles of information security defined in this policy.

These classification levels explicitly incorporate the General Data Protection Regulation's definitions of *Personal Data* and *Special Categories of Personal Data*, as laid out in *Solidatus' Data Protection Policy*, and are designed to cover both primary and secondary research data.

Detailed information on defining information classification levels and providing appropriate levels of security and access is provided in the *Information Classification Standard*. Information on appropriate encryption techniques for securing Confidential data can be found on the Solidatus website.

Information may change classification levels over its lifetime, or due to its volume.

Examples:

Security level	Definition	Examples	FOIA2000 status
Confidential	Normally accessible only to specified members of Solidatus staff. Should be held in an encrypted state outside Solidatus systems; may have encryption at rest requirements from providers.	See *Information Classification Standard*	Subject to significant scrutiny in relation to appropriate exemptions/ public interest and legal considerations.
Restricted	Normally accessible only to specified and/or relevant members of Solidatus staff.	See *Information Classification Standard*	Subject to significant scrutiny in relation to appropriate exemptions/ public interest and legal considerations.
Public	Accessible to all members of the public.	See *Information Classification Standard*	Freely available on the web.

2.4 Suppliers

All Solidatus' suppliers will abide by Solidatus' Information Security Policy, or otherwise be able to demonstrate corporate security policies providing equivalent assurance. This includes:

- when accessing or processing Solidatus assets, whether on site or remotely
- when subcontracting to other suppliers.

2.5 Cloud providers

Under the GDPR, a breach of personal data can lead to a fine of up to 4% of global turnover. Where Solidatus user Cloud services, Solidatus retains responsibility as the data controller for any data it puts into the service, and can consequently be fined for any data breach, even if this is the fault of the Cloud service provider. Solidatus will also bear the responsibility for contacting Information Commissioner's Office concerning the breach, as well as any affected individual. It will also be exposed to any lawsuits for damages as a result of the breach. It is extremely important, as a consequence, that Solidatus is able to

judge the appropriateness of a Cloud service provider's information security provision. This leads to the following stipulations:

2.5.1 All providers of Cloud services to Solidatus must respond to Solidatus' Cloud Assurance Questionnaire prior to a service being commissioned, in order for Solidatus to understand the provider's information security provision.

2.5.2 Cloud services used to process personal data will be expected to have ISO27001 certification or equivalent, with adherence to the standard considered the best way of a supplier proving that it has met the GDPR principle of privacy by design, and that it has considered information security throughout its service model.

2.5.3 Any request for exceptions will be considered by the Risk Manager and the Chief Operating Officer.

2.6 Compliance, policy awareness and disciplinary procedures

Any security breach of Solidatus' information systems could lead to the possible loss of confidentiality, integrity and availability of personal or other confidential data stored on these information systems. The loss or breach of confidentiality of personal data is an infringement of the General Data Protection Regulation, contravenes Solidatus' Data Protection Policy, and may result in criminal or civil action against Solidatus.

The loss or breach of confidentiality of contractually assured information may result in the loss of business, financial penalties or criminal or civil action against Solidatus. Therefore, it is crucial that all users of the Company's information systems adhere to the Information Security Policy and its supporting policies as well as the Information Classification Standards.

All current staff and other authorised users will be informed of the existence of this policy and the availability of supporting policies, codes of practice and guidelines.

Any security breach will be handled in accordance with all relevant Company policies, including the *Acceptable Use Policy at Solidatus* and the appropriate disciplinary policies.

2.7 Incident handling

If a member of staff is aware of an information security incident, they must report it to the Data and Technology Services Service Desk at admin@Solidatus.com or telephone their manager or a director.

Breaches of personal data will be reported to the Information Commissioner's Office by Solidatus' Data Manager. Incident handling is further outlined in Solidatus' *Incident Management and Data Breech Policy and Procedure*.

2.8 Supporting policies, codes of practice, procedures and guidelines

Supporting policies have been developed to strengthen and reinforce this policy statement. These, along with associated codes of practice, procedures and guidelines are published together and are available on *Solidatus' website*.

Specific reference is made to:

2.8.1 The use of administrator privilege accounts – Solidatus Acceptable Use Policy

2.8.2 Network & Server passwords – Network Equipment Guidelines

2.8.3 Malware and other breaches - Incident Management and Data Breech Policy and Procedure

2.8.4 Workstation and BYOD Guidelines

All staff and any third parties authorised to access Solidatus' network or computing facilities are required to familiarise themselves with the company's privacy policy and non-disclosure agreement.

2.9 Review and development

This policy, and its subsidiaries, shall be reviewed by the Information Security Advisory Board (ISAB) and updated regularly to ensure that they remain appropriate in the light of any relevant changes to the law, organisational policies or contractual obligations. Additional regulations may be created to cover specific areas.

ISAB comprises representatives from all relevant parts of the organisation. It shall oversee the creation of information security and subsidiary policies.

The Information Security Manager will determine the appropriate levels of security measures applied to all new information systems.

3. Responsibilities

3.1 Members of Solidatus:

All members of Solidatus, Solidatus associates, agency staff working for Solidatus, third parties and collaborators on Solidatus projects will be users of Solidatus information. This carries with it the responsibility to abide by this policy and its principles and relevant legislation, supporting policies, procedures and guidance. No individual should be able to access information to which they do not have a legitimate access right. Notwithstanding systems in place to prevent this, no individual should knowingly contravene this policy, nor allow others to do so. To report policy contraventions, please see Section 2.7: *Incident handling*.

3.2 Data controllers:

Many members of Solidatus will have specific or overarching responsibilities for preserving the confidentiality, integrity and availability of information. These include:

3.2.1 Project Administrators:
Responsible for the security of information produced, provided or held in the course of carrying out research and development, consultancy or knowledge transfer activities. This includes ensuring that data is appropriately stored, that the risks to data are appropriately understood and either mitigated or explicitly accepted, that the correct access rights have been put in place, with data only accessible to the right people, and ensuring there are appropriate backup, retention, disaster recovery and disposal mechanisms in place.

3.2.2 Heads of Departments, Divisions, Centres:
Responsible for the information systems (e.g. HR/Registry/Finance) both manual and electronic that support Solidatus' work. Responsibilities as above (for *Principal Investigators/Project Administrators*).

3.2.3 Departmental Managers/Line Managers:
Responsible for specific area of Solidatus work, including all the supporting information and documentation that may include working documents/contracts/staff information.

3.3 Data Protection Officer:

Responsible for Solidatus compliance with the general Data Protection regulation.

Responsible for Solidatus' Data Protection Policy, data protection and records retention issues. Breach reporting to ICO.

3.4 IT Support Team:

Responsible for ensuring that the provision of Solidatus' IT infrastructure is consistent with the demands of this policy and current good practice.

3.5 Head of Software:

Responsible for physical aspects of security and will provide specialist advice throughout the Solidatus on physical security issues.

Responsible for this and subsequent information security policies and will provide specialist advice throughout the Company on information security issues.

3.6 Information Government Management Board:

Responsible for approving information security policies.

Solidatus

Document control

External document references

Title	Version	Date	Author
Data protection policy	1.0	28/05/2018	Philip Miller
ISO/IEC 27001:2013			EU

Version history

Version	Date	Approved by	Notes
V1	28/05/2018	Board	Initial document release
V2	05/10/2020	Board	Pre CE+ Audit

Distribution list

Name	Title	Department
Daniel Waddington	Head of Software	Engineering
Solidatus Board		

Contacts

Position	Name	Email	Notes
Director	Philip Miller	philip.miller@Solidatus.com	

Communications and training

Action	Response
Will this document be publicised through Internal Communications?	Yes
Will training needs arise from this policy?	Yes

If 'Yes', please give details:
Annual awareness-raising activities from comms – eg via newsletters, maildrops, posters. Principles incorporated into Solidatus' user awareness training.