Solidatus information classification standard

Version: 1.1

Date: 7 September 2020

Author: Philip A. S. Miller

Contents

1. Introduction

1.1 Purpose

In order to preserve the appropriate confidentiality, integrity and availability of Solidatus' information assets, the Company must make sure they are protected against unauthorized access, disclosure or modification. This is not just critical for assets covered by the General Data Protection Regulation, and the primary and secondary data used for research purposes, but also for all business conducted across the company.

Different types of information require different security measures depending upon their sensitivity. Solidatus' information classification standards are designed to provide information owners with guidance on how to classify information assets properly and then use them accordingly.

This guidance — developed in accordance with the Solidatus' Information Security and Data Protection Policies — includes classification criteria and categories.

1.2 Scope

This standard applies to all Solidatus information, irrespective of the location or the type of service or device it resides on. It should consequently be used by all staff, and other members of the company and third parties who interact with information held by and on behalf of the Solidatus.

Any legal or contractual stipulations over information classification take precedence over this standard.

1.3 Assumptions

The definitions of personal data and protected characteristics laid out in the General Data Protection Regulation continue to be relevant and require the currently understood levels of protection.

The mechanisms offered as recommendations in this proposal continue to exist and are available to those that need them.

The reader has sufficient technical knowledge to implement the controls as laid out.

Solidatus is a registered trademark of Threadneedle Software Holdings Limited
Registered in England. Company No: 07485799. Registered office: 34 Copse Wood Way, England, HA6 2UA

2. Information classification

2.1 Information classification definitions

The following table provides a summary of the information classification levels that have been adopted by Solidatus and which underpin the principles of information security defined in the Information Security Policy. These classification levels explicitly incorporate the General Data Protection.

Regulation's (GDPR) definitions of *Personal Data* and *Special Categories*, as laid out in Solidatus' Data Protection Policy. Examples are provided in Section 2.2 below.

2.1.1 Confidential

- 'Confidential' information has significant value for Solidatus, and unauthorized disclosure or dissemination could result in severe financial or reputational damage to Solidatus, including fines of up to 4% global turnover from the Information Commissioner's Office.
- Data defined by the GDPR as *Special Categories* of Personal Data falls into this category.
- Only those who explicitly need access must be granted it, and only to the least degree in order to do their work (the 'need to know' and 'least privilege' principles).
- When held outside Solidatus, on mobile devices such as laptops, tablets or phones, or in transit, 'Confidential' information must be protected behind an explicit logon and by AES 256-bit encryption at the device, drive or file level, or by other controls that provide equivalent protection.

2.1.2 Restricted

- 'Restricted' information is open to groups of people within the company. It is subject to controls on access, such as only allowing valid logons from groups of staff, but it does not have the stricter controls required by 'Confidential' information.
- 'Restricted' information must be held in such a manner that prevents unauthorised access i.e. on a system that requires a valid and appropriate user to log in before access is granted.
- Information defined as *Personal Data* by the GDPR falls into this category, such as names, email addresses, phone numbers, photos. Information you may want to share with the company community, but not the general public at large, would fall into this category, such as the location of refuge points within the company. If information does not fit into the 'Confidential' or 'Public' categories, then it is 'Restricted' information.
- Public disclosure or dissemination of this information is not intended and may incur fines from the ICO and negative publicity for Solidatus.

2.1.3 Public

- 'Public' information can be disclosed or disseminated without any restrictions on content, audience or time of publication. Disclosure or dissemination of the information must not violate any applicable laws or regulations, such as privacy rules. Modification must be restricted to individuals who have been explicitly approved by information owners to modify that information, and who have successfully authenticated themselves to the appropriate computer system.

2.2 Examples

Security level	Definition	Examples	FOIA2000 status
Confidential	Normally accessible only to specified and/or relevant members of Solidatus staff.	1. GDPR-defined Special Categories of personal data: • racial/ethnic origin • political opinion • religious beliefs • trade union membership • physical/mental health condition • sexual life • criminal record. 2. Salary information. 3. Individuals' bank details. 4. Draft/final reports of controversial and/or financially significant subjects. 5. Passwords. 6. Large aggregates of GDPR-defined Personal Data (>1000 records) including elements such as name, address, telephone number. 7. HR system data, SITS data, Solidatus Central data. 8. Interview transcripts, databases or other records involving individually identifiable Special Categories of personal data.	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 or others.	1. GDPR-defined Personal Data (information that identifies living individuals, contained in databases, transcripts or other records e.g. name, email, work location, work telephone number and photographs. 2. Other information: a Reserved committee business. b Draft reports, papers and minutes. c Systems. d Internal correspondence. e Final working group papers and minutes. f Information held under license; company policy and procedures (as appropriate to the subject matter).	Subject to significant scrutiny in relation to appropriate exemptions/ public interest and legal considerations.
Public	Accessible to all members of the public.	1. Annual account. 2. Minutes of statutory or formal committees. 3. Pay scales. 4. Experts' Directory. 5. Information available on the Solidatus website or through the Solidatus' Publications Scheme programme. 6. Training information. 7. Company policy and procedures (as appropriate to the subject matter).	Freely available on the website or through the Solidatus' Publication Scheme.

2.3 Granularity of classification

The sets of information being classified should, in general, be large rather than small. Smaller units require more administrative effort, involve more decisions and add to complexity, thus decreasing the overall security.

2.4 Information retention

There may be minimum or maximum timescales for which information has to be kept. These may be mandated in a research or commercial contract. Other forms of information retention may be covered by environmental or financial regulations.

2.5 Data breaches

Any data breach must be immediately reported to Solidatus' Data Protection Officer or Information Security Team. See Incident Management and Data Breech Policy and Procedure.

3. Responsibilities

3.1 Data controllers, processors and information asset owners

For Solidatus-owned data, the company is defined as the Data Controller, whereas individuals are Information Asset Owners, and must record the personal information under their responsibility in the Information Asset Register.

If information is transferred outside the company – for example, to be processed in a software as a service application, or to be translated or transcribed by a third party – a data processing agreement must be established with this third party. Please contact Solidatus' Legal Team for further information.

Data Processors are responsible for ensuring the right controls are maintained, in order to ensure data can be stored and used appropriately. There must be a contract between Solidatus as the data controller and any data processors.

3.2 Members of Solidatus

All members of the Solidatus community, Solidatus associates, agency staff working for Solidatus, third parties and collaborators on Solidatus projects are users of Solidatus information. They are responsible for assessing and classifying the information they work with and applying the appropriate controls.

Solidatus community members must respect the security classification of any information as defined and must report any data breaches to the Information Security Manager or Data Protection Officer as quickly as possible.

3.3 Information Asset Owners

Information Asset Owners within the company are responsible for assessing information, classifying its sensitivity and stipulating how it can be used. They should then specify the appropriate controls to protect that information. They must record the information classification in the Information Asset Register.

3.4 Records Manager/Data Protection Officer

Responsible for reporting any breaches to the Information Commissioner's Office.

3.5 Information Governance Committee

Responsible for approving information security and governance policies.

Document control

External document references

Title	Version	Date	Author
Data Protection Policy	1.0	28/05/2018	Philip Miller
Information Security Policy	1.0	28/05/2018	Philip Miller
General Data Protection Regulation		2016	EU

Version history

Version	Date	Approved by	Notes
V1	28/05/2018	Board	Initial version
V1.1	7/09/2020	Board	Updated prior to CE+ Audit

Contacts

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

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:
Change in the levels at which information can be classified. Solidatus' information security awareness training course, plus other materials (such as the Cloud Assurance Questionnaire) will be updated to reflect the new classification levels.