Solidatus

Solidatus acceptable use policy

Version: 0.1

Date: 29 September 2020

Author: Philip A. S. Miller

Contents

1. Introduction

This Acceptable Usage Policy covers the security and use of all Threadneedle Software Ltd (Solidatus)'s information and IT equipment. It also includes the use of email, internet, voice and mobile IT equipment. This policy applies to all Solidatus' employees, contractors and agents (hereafter referred to as 'individuals').

This policy applies to all information, in whatever form, relating to Solidatus' business activities worldwide, and to all information handled by Solidatus relating to other organisations with whom it deals. It also covers all IT and information communications facilities operated by Solidatus or on its behalf.

2. Computer access control – individual's responsibility

Access to the Solidatus IT systems is controlled by the use of User IDs, passwords and/or tokens. All User IDs and passwords are to be uniquely assigned to named individuals and consequently, individuals are accountable for all actions on the Solidatus' IT systems. Staff are given an AD account on joining Solidatus.

2.1 General

Individuals must:

2.1.1 Ensure that their passwords are strong i.e. at least 8 characters and contain both cases, numerals and special characters without repeating patterns (this will be enforced by system level controls).
2.1.2 Change default passwords upon first use of all equipment and applications including Bring Your Own Device (BYOD) items.
2.1.3 Alert the Operations Directors to software or applications with are no longer required by yourself.
2.1.4 Ensure that applications on BYOD are licensed and still supported or removed from the device.
2.1.5 Change passwords if you believe that the account may have been compromised and inform the Operations Directors.
2.1.6 Accept security and critical updates to operating systems and applications
2.1.7 Ensure that Solidatus' corporate data is not downloaded and/or stored on BYOD devices
2.1.8 Be logged in via "user" accounts when browsing the internet and email and not logged int via "Administrator" accounts when performing these activities.

Individuals must not:

2.1.9 Allow anyone else to use their user ID/token and password on any Solidatus IT systems.
2.1.10 Leave their user accounts logged in at an unattended and unlocked computer.

2.1.11 Use someone else's user ID and password to access Solidatus' IT systems.
2.1.12 Leave their password unprotected (for example writing it down).
2.1.13 Perform any unauthorized changes to Solidatus' IT systems or information.
2.1.14 Attempt to access data that they are not authorized to use or access.
2.1.15 Exceed the limits of their authorization or specific business need to interrogate the system or data.
2.1.16 Connect any non-Solidatus authorized device to the Solidatus network or IT systems.
2.1.17 Store Solidatus data on any non-authorized Solidatus equipment.
2.1.18 Give or transfer Solidatus data or software to any person or organization outside Solidatus without the authority of Solidatus.

Line managers must ensure that individuals are given clear direction on the extent and limits of their authority with regard to IT systems and data.

2.2 Internet and email conditions of use

Use of Solidatus internet and email is intended for business use. Personal use is permitted where such use does not affect the individual's business performance, is not detrimental to Solidatus in any way, not in breach of any term and condition of employment and does not place the individual or Solidatus in breach of statutory or other legal obligations. All individuals are accountable for their actions on the internet and email systems.

Individuals must not:

2.2.1 Use the internet or email for the purposes of harassment or abuse.
2.2.2 Use profanity, obscenities, or derogatory remarks in communications.
2.2.3 Access, download, send or receive any data (including images), which Solidatus considers offensive in any way, including sexually explicit, discriminatory, defamatory or libelous material.
2.2.4 Use the internet or email to make personal gains or conduct a personal business.
2.2.5 Use the internet or email to gamble.
2.2.6 Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
2.2.7 Place any information on the Internet that relates to Solidatus, alter any information about it, or express any opinion about Solidatus, unless they are specifically authorized to do this.
2.2.8 Send unprotected sensitive or confidential information externally.
2.2.9 Forward Solidatus mail to personal (non- Solidatus) email accounts (for example a personal Hotmail account), except for legitimate business purposes.
2.2.10 Make official commitments through the internet or email on behalf of Solidatus unless authorized to do so.
2.2.11 Download unlicensed copyrighted material such as music media (MP3) files, film and video files (not an exhaustive list) without appropriate approval.
2.2.12 In any way infringe any copyright, database rights, trademarks or other intellectual property.
2.2.13 Download any software from the internet without prior approval of Senior Management.
2.2.14 Connect Solidatus devices to the internet using non-standard connections.

2.3 Clear desk and clear screen policy

In order to reduce the risk of unauthorised access or loss of information, Solidatus enforces a clear desk and screen policy as follows:

2.3.1 Personal or confidential business information must be protected using security features provided for example secure print on printers.
2.3.2 Computers must be logged off/locked or protected with a screen locking mechanism controlled by a password when unattended.
2.3.3 Care must be taken to not leave confidential material on printers or photocopiers.
2.3.4 All business-related printed matter must be disposed of using confidential waste bins or shredders.

2.4 Working off-site

It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:

2.4.1 Working away from the office must be in line with Solidatus remote working policy.
2.4.2 Equipment and media taken off-site must not be left unattended in public places and not left in sight in a car.
2.4.3 Laptops must be carried as hand luggage when travelling.
2.4.4 Information should be protected against loss or compromise when working remotely (for example at home or in public places). Laptop encryption must be used.
2.4.5 Particular care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones and tablets. They must be protected at least by a password or a PIN and, where available, encryption.

2.5 Mobile storage devices

Mobile devices such as memory sticks, CDs, DVDs and removable hard drives must be used only in situations when network connectivity is unavailable or there is no other secure method of transferring data. Only Solidatus authorised mobile storage devices with encryption enabled must be used, when transferring sensitive or confidential data.

2.6 Software

Employees must use only software that is authorised by Solidatus on Solidatus' computers. Authorised software must be used in accordance with the software supplier's licensing agreements.

2.7 Viruses

Solidatus has implemented centralised, automated virus detection and virus software updates within the Solidatus. All PCs have antivirus software installed to detect and remove any virus automatically.

Individuals must not:

2.7.1 Remove or disable anti-virus software.
2.7.2 Attempt to remove virus-infected files or clean up an infection, other than by the use of approved Solidatus anti-virus software and procedures.

2.8 Telephony (voice) equipment conditions of use

Use of Solidatus voice equipment is intended for business use. Individuals must not use Solidatus' voice facilities for sending or receiving private communications on personal matters, except in exceptional circumstances. All non-urgent personal communications should be made at an individual's own expense using alternative means of communications.

Individuals must not:

2.8.1 Use Solidatus' voice for conducting private business.
2.8.2 Make hoax or threatening calls to internal or external destinations.
2.8.3 Accept reverse charge calls from domestic or International operators, unless it is for business use.

2.9 Actions upon termination of contract

All Solidatus equipment and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned to Solidatus at termination of contract.

All Solidatus data or intellectual property developed or gained during the period of employment remains the property of Solidatus and must not be retained beyond termination or reused for any other purpose.

2.10 Monitoring and filtering

All data that is created and stored on Solidatus computers is the property of Solidatus and there is no official provision for individual data privacy, however wherever possible Solidatus will avoid opening personal emails.

IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy. Solidatus has the right (under certain conditions) to monitor activity on its systems, including internet and email use, in order to ensure systems security and effective operation, and to protect against misuse.

Any monitoring will be carried out in accordance with audited, controlled internal processes, and applicable legislation.

It is your responsibility to report suspected breaches of security policy without delay to your line management, or Senior Management.

All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with Solidatus disciplinary procedures.

Document control

Version history

Version	Date	Approved by	Notes
V0.1	29/09/2020	Board	Initial version