



Sandberg's Information Security Policy

Document control	1
Version control.....	1
Purpose	2
Scope.....	2
Outline	2
Compliance Measurement.....	6
Review & Update	7

Document control

Version number:	2.2
Policy owner:	Adam Dahlström, IT Manager
Effective date:	24 May 2017
Last review date	23 Jan 2024
Next review by date:	23 Jan 2025

Version control

Ver	Date	Changes
2.2	23 Jan 2024	Reviewed; no edits
2.1	12 Dec 2022	Content revised; minor format/spelling updates
2.0	15 Feb 2022	Content revised; data breach guidelines implemented
1.1	16 Nov 2021	Content revised, updated to follow a new policy template
1.0	24 May 2017	First version

Purpose

The services Sandberg provides to its clients are often subject to confidentiality or non-disclosure agreements. These generally require Sandberg to ensure that all Sandberg employees and subcontractors accept to be bound by an obligation of professional secrecy. Employees, subcontractors, and suppliers working for Sandberg may be required to undertake work covered by such agreements or work of a highly sensitive nature. It is, therefore, vitally important that employees, subcontractors, and suppliers understand the need for strict confidentiality in all aspects of work carried out for Sandberg.

As technology progresses, so the threat of unintended disclosure of confidential information increases. As Sandberg's clients seek to minimise the risk of unintended disclosure of confidential information by implementing Information Security standards (often aligned to the ISO27001 Standard for Information Security), they must ensure there are no weaknesses in their supply chain. The ISO27001 standard requires all suppliers to adhere to basic security policies, thus Sandberg has defined the Information Security Policy to ensure that Sandberg client data retains:

- **Confidentiality** – Data remains confidential to Sandberg employees and authorised parties only
- **Integrity** – Data is protected against accidental loss or corruption
- **Availability** – Data remains available for use by authorised parties as much as can be reasonably expected

Scope

This policy applies to:

- all employees of Sandberg Translation Partners in all regions
- any PCs, laptops or other mobile devices that are used for processing Sandberg's data (including client data of Sandberg), whether owned by the company or by employees of the company.

Managers are responsible for ensuring that all staff are fully trained regarding information and data security and for ensuring that all staff are fully compliant with the policies.

Outline

In complying with the policy, the following standards for secure working must be applied by all employees of Sandberg Translation Partners.

Secure Working Environment

Sandberg employees must work in a secure working environment, e.g. an Sandberg office or home, where unauthorised individuals cannot access Sandberg client data. Handling Sandberg client data in a public place is not condoned, with the exception of shared-use offices or similar spaces detailed below.

Working in a public office is acceptable as long as access to the office is restricted to authorised users. In these offices, Sandberg client data must never be left unattended, and care should be taken to ensure that other people cannot see the data being worked on, either by using a privacy screen on the laptop (see http://www.3m.co.uk/3M/en_GB/privacy-protection-UK/ for more information) or sitting where you cannot be overlooked.

Wi-Fi

PCs and laptops should not be connected to the internet over public Wi-Fi services as these are less secure than home or office Wi-Fi, even if a password has to be entered to use them.


Firewalls

PCs and laptops must have a hardware firewall to protect them from unauthorised remote intrusion via the internet. Hardware firewalls (in a domestic environment typically routers) should have their default password changed so that they cannot be remotely accessed.

PCs and laptops

All Sandberg employees have access to an Azure Virtual Desktop (AVD) profile hosted in a Microsoft data centre. These should be used as the primary working environment when processing and accessing Sandberg data.

Any PC or laptop used to access AVD or Sandberg networks must be configured with a password to restrict unauthorised access. Sandberg data should not be stored on local units, regardless of whether the unit is owned by Sandberg or not. If Sandberg data is temporarily stored locally on a personal unit, the user is responsible for ensuring this data is deleted after use.

PCs should be locked using the  + L keys (Windows) whenever left unattended in the office. All computers used to access Sandberg data must also be set up to lock automatically after 15 minutes of inactivity.

Operating System Updates

PCs and laptops used to access Azure Virtual Desktop or other Sandberg systems must be updated on a monthly basis with the latest Windows or Mac operating system security updates. These security updates fix vulnerabilities that have been identified as being publicly known to hackers. The Sandberg Tech team will advise when these patches have been released by Microsoft and will request all staff to run the updates on their local devices. The Sandberg Tech team will update and deploy updated Azure Virtual Desktop hosts monthly.

Operating systems and other software used to access Sandberg infrastructure must be properly licenced, up to date and of supported versions.

Software

Sandberg users may not pass on any installers for software to third parties that they have accessed through the company network unless such software is available on a freeware, shareware or open-source licence.

If a personal computer used to access Sandberg infrastructure is infected with a virus or other malware, or if the antivirus software reports that it is not functioning, the user must immediately notify Sandberg.

Password Management

Sandberg users must:

- Set secure and unique passwords for any computer used to access Sandberg infrastructure
- Never disclose their user IDs or passwords to anyone else
- Never write down or store a password in any way that can be interpreted by anyone else
- Immediately report to Sandberg if computers, laptops or units used for multi-factor authentication are lost, stolen or compromised

- Never store passwords used to connect to Sandberg systems directly on your PC, unless you have a personal user account on the computer to which no one else has access, and you protect your personal user account with a password at least equivalent to the minimum password requirements outlined below
- Immediately change their password if it is suspected to have been identified by an unauthorised individual, as well as report the security breach to the Sandberg Tech team, even if there is no suspicion of unauthorised access

Passwords should comply with the following guidelines to minimise the risk of a hacker identifying the password:

- Use at least 12 characters in length
- Use a combination of upper/lower case letters, numbers and symbols
- Do not use a password containing personal information or words found in a dictionary
- Do not use a password containing your birthday date
- Regularly change your password

Data Security

Users may not remove any data, information or files relating to Sandberg, its clients, suppliers, projects, translation memories, glossaries, reference material or any other document from the Sandberg network. Users may not make copies for use elsewhere such as on home computers or laptops.

Data theft must be reported to line managers and Sandberg's Tech team, even if the data files were password protected.

Users are responsible for any personal data (such as documents and photos) stored on Sandberg computers and understand that Sandberg provides no backup services for such data and cannot be held liable in the event of its loss. Users must not store data files for which they do not own the copyright (e.g. music or videos) on Sandberg computers.

Emails

Sandberg's computer systems are maintained solely for conducting Sandberg business. The use of the internet and email for any other purpose may be subject to action under the Sandberg disciplinary procedures.

Office computers, home equipment purchased by Sandberg, networks and email systems are the property of Sandberg. All copies of messages created, sent, received or stored on Sandberg's systems shall remain the property of Sandberg. Messages are not the private property of employees and as such there should be no expectation of privacy in any circumstances. If employees use Sandberg email addresses for communication that is not business related, they waive any privacy or any other rights in relation to such communications and consent to their being read, monitored, recorded and otherwise intercepted by Sandberg.

Sandberg reserves the right to access and monitor all messages created, sent, received or stored on Sandberg's systems. The contents of email messages may be disclosed internally and to third parties without further permission of the employee and at the discretion of the Managing Director or IT Manager. Staff must remember that even when an email message is deleted it is still possible for the message to be retrieved and read. The use of passwords does not assure confidentiality and the existence of a password does not restrict the company's right to access email messages.

Sandberg equipment should not be used to create, send, receive or retain material via emails or the internet that could be regarded as offensive, obscene, lewd, pornographic, illegal or that breach copyright. Use of Sandberg's computer network in such a way will amount to gross misconduct that can lead to disciplinary proceedings and possible dismissal.

Emails are subject to the same laws as other written documents; therefore emails that contain comments that could be regarded as defamatory, inaccurate or misleading must be avoided.

Regardless of the Managing Director/IT Manager's right to retrieve and read any email messages, non-project related emails should be treated as confidential by other employees and opened only by the intended addressee.

Staff should be mindful that all emails and downloads can contain viruses. Whilst all incoming emails are scanned for viruses and malware, staff should be cautious about opening all unsolicited emails containing unexpected content which encourages the recipient to open a file attachment or click on a link to a website (see next section for further guidance).

Email Security

Emails should not be trusted to have come from the person they say they are from. Faking sender details, and even the layout and colour scheme of an email, is easy.

Unexpected emails, appearing to come from legitimate organisations, should be treated with caution, especially if they motivate you to take action, e.g.

- they offer something unexpectedly pleasant, such as confirming an unexpected payment to you, a golden opportunity, or even a parcel for collection
- they report something unpleasant, such as attaching an unexpected bill, a payment demand, or a fine

Such emails are designed to trigger an immediate reaction, intended to trick users. Links in such emails are likely to lead to websites with malware and/or request that personal information is provided to access the detail.

Also, files attached to these emails should never be opened as they may contain malware to infect PCs, either logging passwords or encrypting files that then require a ransom to be paid to (possibly) decrypt the files. Such malware can encrypt all the files on a PC in a matter of minutes.

Personal Information and Social Networking

Requests for personal information should be treated with suspicion. Personal information posted on social networking sites should be posted with caution, ensuring the correct privacy settings are applied. Fraudsters can use personal information for impersonation to trick a third-party into believing they are corresponding with a Sandberg employee.

Information about Sandberg, its clients, projects or data must never be posted to social networking sites. You must not disclose any aspect of Sandberg's computer systems to any third party without the prior approval of the IT Manager.

Staff should also be careful when communicating in a personal capacity by email or through social media. They should be particularly aware of the following and must not:

- send emails from personal equipment to work colleagues or Sandberg business contacts which could be regarded by the recipient as defamatory, discriminatory, bullying or causing harassment;
- breach company, client or business associate confidentiality;
- bring the company into disrepute by emailing or posting comments or images on websites or on social media networking sites which directly or indirectly reference the company, its employees or business contacts in a derogatory manner or in any way could be regarded as constituting harassment or bullying.

Online security

Software should only be installed after approval has been sought from the Tech team, who will confirm where software should be obtained from. Software downloaded from other sources may contain malware that can be used to obtain remote access to data on the PC, laptop or other device (e.g. smartphone). Installation of software on AVD hosts is limited to members of the Tech team.

Sandberg uses approved and monitored cloud data service integrated in the company infrastructure (OneDrive). Other cloud data storage services (e.g. Google drive, Dropbox, etc.) must not be used to store Sandberg data, as they may be hacked, resulting in unauthorised access to Sandberg client data. The only exception to this policy is where staff may need to understand how a cloud data storage service works in order to undertake a translation project for a client. In this case, approval must be sought from the Tech team and only test data used.

Online tools must not be used to translate any parts of a text. Source text in Sandberg projects must not be entered into any online or third-party tools or platforms, including but not limited to MT engines and text assessment tools. MT should only be used within the scope of Sandberg's internal MT workflows as determined and published by Sandberg's Tech team.

Data breaches

Data breaches will differ depending on the quantity, content, risk and impact of the data involved. Sandberg needs to be able to respond quickly and efficiently to any data breach and to identify the data classification.

In the event of a data breach or a suspected data breach, the IT manager should be informed promptly of the potential or confirmed breach. The notification should include details of the nature of the breach, what data is involved in the breach and the classification of the data that is involved.

Once a report has been made, an assessment will be carried out to establish the risk of the data that has been breached and the rights and freedoms of the data subject(s) affected by the breach.

If the breach has resulted in the rights and freedoms of the data subject(s) being affected, Sandberg will notify the ICO within 72 hours without delay. If Sandberg does not notify the ICO within 72 hours of the breach, the manager responsible will electronically notify the ICO to inform them of the reason for the delay. Sandberg will provide all the information that is available to the ICO and will continuously update them when more information is available without delay.

The following information must be provided to the ICO:

- A detailed account of the breach
- All categories of the affected personal data
- The number of data subject(s) and records which have been affected

- Contact information for the manager responsible for the notification
- Any steps that will be taken to manage the breach along with the consequences that the breach may have caused
- When the responsible manager contacts the ICO all records will be recorded in the company's GDPR folders

The Management team will respond to any breach with containment, recovery, assessment, consideration, evaluation, and response.

Data Security Reporting to the Data Subject(s)

If the breach is likely to be of a high risk to a data subject(s), Sandberg will notify the data subject(s) without delay.

Sandberg will notify the data subject(s) in a clear and concise manner and in accordance with ICO guidance.

Sandberg will take the necessary steps to ensure that the high risk that has affected the rights and freedoms of the data subject(s) will no longer affect them.

If the breach affects many data subjects and personal data records, Sandberg will take a decision as to whether it would be more appropriate and efficient to inform each data subject individually or collectively.

Sandberg will detail all information relating to the breach of personal data and any facts, communications or reports that result from the breach along with all the actions that have been taken and the effects of the actions.

Compliance Measurement

Deliberate or unintentional breaches of this policy will be considered a disciplinary matter. Such breaches under the disciplinary procedure may constitute gross misconduct and may lead to action up to and including dismissal.

Breaches of this policy must be notified to the policy owner for investigation.

Review & Update

This policy is reviewed and updated annually. In cases where changes to the organisation or changes to national, international, GDPR or otherwise information security-related regulations take place, additional and more frequent reviews of the policy will take place.