



Sandberg's Vendor Information Security Policy

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

Document control

Version number:	2.1
Policy owner:	Adam Dahlström, IT Manager
Effective date:	25 May 2018
Last review date:	9 Feb 2024
Next review by date:	9 Feb 2025

Version control

Ver	Date	Changes
2.1	9 Feb 2024	Reviewed; wording updated to cover processing of data in non-translation services
2.0	6 Feb 2023	Content reviewed and updated; updated to follow a new policy template; updated password management guidelines; guidelines for screen locking added; policy moved to the website.
1.0	25 May 2018	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.

Acceptance of each order confirmation sent to you as a subcontractor by Sandberg means that you undertake not to disclose to any person, nor to copy or use for any purpose whatsoever, any confidential information relating to the business affairs or trade secrets of Sandberg, its clients, subcontractors or suppliers, including but not limited to information about Sandberg's clients, employees and subcontractors, prices or any other matter or information about Sandberg and its business or the business of Sandberg's clients that is not freely available to the public. Your undertaking of professional secrecy as outlined above shall last indefinitely.

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 ISO 27001 Standard for Information Security), they must ensure there are no weaknesses in their supply chain. The ISO 27001 standard requires all suppliers to adhere to basic security policies, thus Sandberg has defined the Vendor 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.

If you have any questions about this policy, please email our vendor management team at vendor.management@stptrans.com.

Scope

This policy applies to:

- all subcontractors and suppliers to 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).

Outline

Sandberg requires that all client and company data remain confidential and secure at all times. To uphold this policy, subcontractors and suppliers must ensure they do not create an information security weakness in the supply chain. All subcontractors and suppliers are required to implement procedures and standards to ensure they do not breach the Sandberg Information Security Policy.

In complying with the policy, the following standards for secure working must be applied by all subcontractors and suppliers to Sandberg Translation Partners.

Secure Working Environment

Services undertaken for Sandberg must be performed in a secure working environment 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

PCs and laptops should be configured with a password to restrict unauthorised access. Any Sandberg content stored locally on the hard drives of laptops or other mobile devices should be further protected using one of the following methods, so that even if a hard drive is transferred to another PC the data cannot be accessed, or the data not retained for any longer than is required for the purpose of processing it:

- Encrypted with software such as BitLocker in Windows 10 Pro/Enterprise;
- In a password-protected .zip file using AES-256 encryption (7zip recommended).

Laptops or electronic devices (including backup drives, CD, DVDs, memory sticks) containing Sandberg client data must never be left unattended in public places. These items should not be transported in checked-in hold baggage when travelling by air. Laptops should not be left visible in the passenger compartment of a vehicle, but should be stored in a locked glovebox or luggage compartment instead.

PCs should be locked using the  + L keys (Windows) or the  + Lock screen (Mac) whenever left unattended. 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 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.

Password Management

Subcontractors and suppliers of Sandberg must:

- Set secure and unique passwords for any computer used to perform any services undertaken for Sandberg. Using different passwords avoids the risk that one password compromise will allow access to all systems;
- 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 containing Sandberg client data are lost, stolen or compromised;
- Never store passwords used to connect to Sandberg's or Sandberg's clients' 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 your password if it is suspected to have been identified by an unauthorised individual, as well as report the security breach to your Sandberg contact, 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

Data files should be password protected to avoid them being opened if the file is obtained by an unauthorised individual. Data files on a password-protected device do not need to be individually password protected.

Data theft must be reported to your Sandberg contact, even if the data files were password protected.

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 you.

Information about Sandberg, its clients, employees, suppliers, projects or data must never be posted to social networking sites.

Online security

Software should only be downloaded from reputable websites, such as the original manufacturers' websites. 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).

Cloud data storage services (e.g. Google drive, Dropbox, etc.) should be used with caution, as they may be hacked, resulting in unauthorised access to Sandberg client data.

Online tools must not be used to translate or process 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 when it has been applied already by Sandberg or its client on machine translation post-editing projects.

Transferring content

Content for translation or any other type of processing should be secured during transfer from Sandberg to you as subcontractor, and when you return it back to Sandberg, either via:

- Password-protected zip file, when transferring content via email (Sandberg will provide you with a password, used both in outgoing and incoming transfers); or
- A secure file transfer system such as OneDrive or a client portal, if requested.

Personal Data in content

Sandberg places great importance on the correct, lawful and fair handling of all personal data, respecting the legal rights, privacy and trust of all individuals with whom it deals. This responsibility extends to the safe and secure handling of personal data in content for translation or any other type of processing, and Sandberg's employees, subcontractors and suppliers have a crucial role in safeguarding that data.

Sandberg's policies are based on the requirements of the EU General Data Protection Regulation (GDPR), which came into force on 25 May 2018, and affects the handling of all personal data for individuals within the European Union, as well as the export of personal data outside of the EU.

Sandberg handles content at the following three security levels:

- Content containing no personal data;
- Content containing non-sensitive personal data;
- Content containing sensitive personal data.

The security level of the content you will be translating or processing for any other type of service will be flagged up to you in the Purchase Order you receive for the work.

Content containing no personal data

Most of the content Sandberg handles contains no personal data, and as such does not come under GDPR requirements. However, as much of that content will be confidential to the companies who commission the work, the above information security standards still apply to it.

There are no restrictions in terms of data retention or in which country you work when processing content with no personal data.

Content containing non-sensitive personal data

Content containing personal data that is not categorised as sensitive and does not contain special categories of data may be content which refers to data subjects in their work capacity rather than as private individuals, for example the name and contact details of a manager in a company whose annual report you translate, which will be in the public domain after the annual report is published.

This type of personal data in content for translation or any other type of processing is considered low risk for the data subject, but must still be handled appropriately.

This means that we will:

- Restrict the processing of this content internally;
- Have no restriction on which country you work from;
- Ask you to delete all content after delivery and safe receipt by our Project Manager, if the content you handle is in a file-based format;
- Ask you not to retain personal data in TMs.

Content containing sensitive personal data

Certain types of content will be categorised as “sensitive”, and will have stricter controls to safeguard the personal data on the data subjects whose details appear in our projects.

Under the GDPR, special categories of personal data must be handled with the utmost care. These categories include, for example, information about an individual’s:

- race
- ethnic origin
- politics
- religion
- trade union membership
- genetics
- biometrics (where used for ID purposes)
- health
- sex life
- sexual orientation

The type of content which may contain this kind of sensitive data, is, for example, medical records.

This type of personal data in content is considered high risk for the data subject, and must be handled securely.

This means that we will:

- Heavily restrict the processing of this content internally;

- Not send the content for translation or other processing outside of the EU, EEA and approved countries without explicit agreement with the client;
- Ask you to delete all content after delivery and safe receipt by our Project Manager, if the content you handle is in file-based format;
- Ask you not to retain personal data in TMs.

Flagging up personal data in content

Under the GDPR, it is the responsibility of the data controller, that is, our client or the end-client, to inform us if there is personal data or sensitive personal data in the content for translation or other type of processing. However, as they do not always know the full extent of the content that files contain, you as the supplier translating or otherwise processing the file(s) have a significant responsibility in flagging up any personal data if it hasn't been specified at the start of the project already.

Sandberg will flag up content with personal data, and sensitive personal data, in the Purchase Order we send to you. If you do find personal data, especially any sensitive data in the special categories:

- Tell your Project Manager;
- Continue work as normal;
- Delete the files and, if applicable, translation memories generated in the translation process after delivery and safe receipt by your Project Manager, if the content you handle is in a file-based format.

For more information about Sandberg's commitment to data protection and information security, you can view our internal Data Security Policy [here](#).

Compliance Measurement

Sandberg actively promotes compliance with this Information Security Policy. All employees, subcontractors, and suppliers are encouraged to report any breaches or potential for a breach with regards to information security or handling of personal information promptly to the senior management of the company, via your Sandberg contact. For more information on the safeguarding of data security, see the Vendor Privacy Policy.

Breaches

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

Deliberate or unintentional breaches of this policy may lead to action up to and including immediate removal from Sandberg's database and termination of our relationship. Legal action may be sought in cases where the breach has harmed the business affairs or trade secrets of Sandberg, Sandberg's clients, working partners or suppliers.

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. When we update our Vendor Information Security Policy, we will take appropriate measures to inform you, depending on the significance of the changes made. We will obtain your consent to any material changes to the Vendor Information Security Policy if and where this is required by applicable laws and regulations. You can see when this Vendor Information Security Policy was last updated by checking the 'Last

For External & Internal Use

Review Date' displayed at the top. If you continue to use the functions on the Sandberg Passport vendor portal, you are deemed to have accepted the updated Vendor Information Security Policy.