Sandberg's Security Training Policy

Document control

Version number:	1.3
Policy owner:	Adam Dahlström, IT Manager
Effective date:	2 Aug 2021
Last review date:	23 Jan 2024
Next review by date:	23 Jan 2025

Version control

Ver	Date	Changes
1.3	23 Jan 2024	Reviewed; no edits
1.2	21 Feb 2023	Reviewed; no edits
1.1	15 Feb 2022	Content revised, updated to follow a new policy template
1.0	2 Aug 2021	First version

Purpose

The purpose of this document is to provide a comprehensive summary of internal procedures related to the training of Sandberg Translation Partners (Sandberg) personnel and users on the security aspects of using information systems for the purpose of external reviews.

Access to Sandberg's information and systems is restricted only to authorised users. Newly authorised users must go through an onboarding training process which includes a security training program. Once passed, the new user is provided full access to Sandberg's systems as per their respective user access level.

Scope

The Security Training Policy applies to all users of information at Sandberg. Users of information comprise of Sandberg employees only: both office- and home-based, regardless of geographic locations. Access to systems may also be granted to third parties such as software developers and other service providers. Such third party organisations and their respective users to whom access has been granted are subject to non-disclosure agreements and they follow the same steps and procedures outlined in Sandberg's Security Training Policy and other relevant and related policies.

All Sandberg employees are required to read, understand, and comply with the Security Training Policy, as well as to go through the corresponding security training programme part of their individual onboarding process, and to present any questions to the policy owner or to HR.

Outline

This policy outlines how users with access to Sandberg's information and systems are trained on security-related aspects linked to the overall information security procedures established in the company, and what the separate training elements are. Failure to follow the established security principles by any user could expose Sandberg to various risks such as legal and compliance issues, malicious attacks, or compromise of network systems and services, and others.

Understanding the importance of information security and individual responsibilities and accountability of users – regardless of the access level each is granted – is instrumental in achieving compliance with national and international information security regulation. The established internal procedures are inspired and guided by the best practices and requirements set out in ISO 27001, the global standard for information security management.

Section A.8.2 of ISO 27001 states that "All employees of the organisation and, where relevant, contractors and third-party users shall receive appropriate awareness training and regular updates in organisational policies and procedures, as relevant for their job function." Sandberg has therefore implemented procedures that cover both an initial onboarding training session on security awareness-related aspects, as aforementioned, as well as structure for regular updates on security policies and procedures when updates are warranted.

Security training at Sandberg is organised in a systematic manner with assessment of requirements and pre-defined needs for knowledge and skills, execution of the training programme, and regular measurement of results all catered for. The required knowledge and skills are pre-defined, where users, based on their role and responsibilities, have different training needs and requirements. For example, staff members who implement or manage information security aspects such as access control and information classification, need to be trained in-depth on the company's information security policies within the context of ISO 27001, whereas other users do not need the in-depth

knowledge on information security in order to be fully compliant with established company, national and international information security regulations.

Training is followed by monitoring where managers and responsible personnel are monitoring user compliance and measuring the degree of understanding of security procedures as per each individual's required level of knowledge and skills. Where gaps are identified additional training sessions are scheduled for full compliance to be maintained.

Regular security breach training is conducted to prepare Sandberg staff on how to identify and deal with spam, phishing attempts and malware.

If changes to regulation take place, all relevant policies are updated with follow up training sessions taking place in order for all employees to be fully trained on all novelties.

Compliance measurement

Compliance with the Security Training Policy and undertaking any relevant training – be it introductory during the onboarding process or additional training due to changes in information security policies – is mandatory. Sandberg's team managers and management are required to ensure full and continuous compliance of the respective teams within the organisation. Unannounced security testing takes place regularly by the internally appointed person responsible for the company's compliance aspects, as well as by the IT Manager who oversees all aspects of the Information Security policies. Periodic reviews for information security quality assurance are also provisioned for.

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.