Sandberg's Access Control 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 control of access to information resources of Sandberg Translation Partners (Sandberg) for the purpose of external reviews.

Access to Sandberg's information and systems is restricted only to authorised users. An Access Control Policy is therefore necessary to ensure that only authorised users can obtain access to Sandberg's information and systems.

Scope

The Access Control 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 Access Control Policy and other relevant and related policies.

All Sandberg employees are required to read, understand, and comply with the Access Control Policy and to present any questions to the policy owner or to HR.

Outline

This policy outlines how access is managed, who may access Sandberg's information and systems, and under what circumstances. Unauthorised access could expose Sandberg to various risks such as legal and compliance issues, malicious attacks, or compromise of network systems and services, and others.

Therefore, a series of requirements apply to any authorised user or user authorised to grant access to Sandberg's systems, in order for Sandberg's systems to be properly protected against unauthorised access, while allowing business to be conducted normally.

Protecting access to IT systems and data is critical to maintain the integrity of Sandberg's data and to prevent unauthorised access to such resources, in full compliance with GDPR, national and international regulations. The established internal procedures are in accordance with the best practices and requirements according to ISO 27001, the global standard for information security management.

Section A.9 of Annex A of ISO 27001 lists a total of 14 required controls in relation to access control to be put in place in order for an organisation to be eligible to obtain the international standard. Sandberg strives to have controls and procedures inspired and guided by the 14 required controls listed in the aforementioned ISO certification requirements in the company's internal procedures and policies (although Sandberg is not formally certified to ISO 27001 yet), alongside a number of additional controls and procedures related to access control in order for full national and international regulation to be met.

Some of these controls include:

- Business requirements of access control are pre-determined before any users are granted access to information and systems, and before any additional controls are implemented.
- User access management is carefully defined with aspects such as:
    - User registration requirements and user IDs

    - Provisioning of access/revoking access
    - Management of authentication data
- User responsibilities and password protection
- Access rights and management of access rights
- System access control:
    - Secure log-on procedures
    - Password policy
    - Password management system
    - Access to source code for in-house built systems
    - System administrator access
- Periodic reviews
- Overall compliance with other overarching elements such as e.g. information classification

Compliance measurement

Compliance with the Access Control Policy is mandatory. Sandberg's team managers and management are required to ensure full and continuous compliance of the respective teams within the organisation. Unannounced audits may take place, organized by the policy owner. 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.