



---

# Stenson Tamaddon Privacy and Data Policy

---

February 2, 2024

## I. Introduction

1. Policy Statement. StenTam is firmly committed to respecting and protecting the privacy of our employees, clients, and business partners and complying with all applicable laws, regulations, and policies related to privacy and data collection, use, security, and retention. This policy applies to all StenTam employees, agents, those who use StenTam's Computer and Computer Systems, and any data entrusted to the Company.

## II. Definitions

1. "Computer and Computer Systems" is defined in StenTam's Safeguarding Company Property & Use of Computers and Computer Systems Policy, Paragraph II, 2 (Definitions).

2. "Confidential Business Information" is defined in StenTam's Safeguarding Company Property & Use of Computers and Computer Systems Policy, Paragraph II, 2 (Definitions).

3. "Data" means any written or recorded material in StenTam's possession or control or its User's possession or control in the course of their duties and includes information in any medium, such as paper, recordings or electronic files (whether stored on a network server, individual computer hard disk or separate disk from which information can be obtained by any means).

4. "Property" is defined in StenTam's Safeguarding Company Property & Use of Computers and Computer Systems Policy, Paragraph II, 2 (Definitions).

5. "User" is defined in StenTam's Safeguarding Company Property & Use of Computers and Computer Systems Policy, Paragraph II, 2 (Definitions).

## III. Policy

### 1. Privacy.

a. In the course of conducting business, StenTam collects, processes, transfers, discloses, and stores information received from and/or concerning employees, clients, business partners, Users, and others. StenTam collects, processes, transfers, discloses, and stores such information only for lawful and legitimate, legal and business purposes consistent with all applicable laws, regulations, and Company policy.

b. Where appropriate and/or as required, notice will be provided to those individuals whose information is collected, processed, transferred, and/or stored.

c. StenTam may transfer or disclose information as permitted by law or contract or with consent or when required to do so by legal process (including to law

enforcement), in connection with an investigation of suspected or actual illegal activity, to prevent or respond to any physical harm, financial loss, fraud, or to protect StenTam's legal rights, or as part of any auditing, compliance, and corporate governance function.

d. While we respect the privacy of our employees, agents, and Users, StenTam retains the right to monitor and inspect Company Property and Computers and Computer Systems to the fullest extent permitted by applicable law. **Users do not have any legitimate expectation of privacy in regard to their use of Property and Computers and Computer Systems.** Users are on notice that their use of the Computers and Computer Systems is not private, not confidential, and not anonymous. StenTam may monitor, inspect, access, collect, and use any information created, transmitted, or stored on any Computer and Computer System (including but not limited to internet activity, e-mail, instant messaging, voice messages, and any other communications made, received, accessed), without notice, in the ordinary course of business when the Company deems it appropriate to do so including, but not limited to, any of the following purposes or reasons:

- (1) System maintenance;
- (2) Compliance and investigations, including internal investigations; preventing, responding to, or investigating allegations of system abuse or misuse; and ensuring compliance with other laws, including software copyright;
- (3) Responding to a cyber incident;
- (4) Complying with legal and regulatory requests for information;
- (5) Business continuity; and
- (6) Review of Internet usage.

e. StenTam reserves the right to request any User's password and other security features to gain access to any third-party application not managed by StenTam but used to conduct Company business. A User's refusal to provide such requested information may result in temporary or permanent suspension or termination of the User's access to Computers and Computer System and, if an employee, constitutes grounds for discipline, including termination.

## 2. Data Protection and Security.

a. StenTam endeavors to and will take and enforce all reasonable security measures, including cybersecurity, to protect StenTam's information and any information entrusted to StenTam.

b. All Users will complete annual cybersecurity training.

c. All Users are required to immediately report any security violation, any actual or attempted compromise or unauthorized access of any Computers or Computer Systems, or the loss of data or information.

d. This policy incorporates the Information Security and Privacy Standard Operating Procedure, including data classification and requirements.

3. Use of Personal Messaging Platforms for Business Reasons.

a. StenTam prohibits StenTam employees, agents, and Users from using personal devices, such as personal smartphones, to conduct Company business.

b. Further, employees may not use messaging platforms that allow messages and content to be automatically deleted (*i.e.*, after receipt or after a set period of time) on StenTam devices or to conduct business on behalf of the Company. These prohibited platforms include, but are not limited to, Snapchat, Telegram, Viber, Wickr, and Signal.

III. Violation of this Policy

Violation of this policy may result in disciplinary action, up to and including termination of employment.

StenTam reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Accordingly, to the extent permitted by law, StenTam reserves the right to decline to defend or pay any damages awarded against employees or partners that result from any violation of this policy or any policy.

In addition, StenTam may also temporarily or permanently suspend or terminate any User's access, with or without notice, to any Property or Computers and Computer System for any reason, including if StenTam believes that any part of this policy, including the Acceptable Use Policy, has been violated.

The StenTam Chief Legal Officer is the proponent of this policy. Any questions concerning this policy should be addressed to the Chief Legal Officer, or his designee.