Stenson Tamaddon
Safeguarding Company Property & Use of Computers and Computer Systems

February 2, 2024

I. Introduction

1. Policy Statement. Every employee has a responsibility to protect and efficiently and properly use StenTam's property and assets, including physical property, money and assets, intellectual property, and confidential business information. This policy applies to all StenTam employees, agents, and Users.

2. Definitions

a. "Confidential Business Information" includes, but is not limited to, all StenTam internal, non-public information concerning StenTam's operations and financial position (*e.g*. income, profits, losses, costs, expenditures, and pricing, etc.), annual and long-range business plans, contracts, product or service plan, marketing plans and methods, training, educational and administrative manuals, customer and supplier information and purchase histories, employee lists, proprietary information, and privileged information.

b. "Intellectual Property" means all StenTam copyrights, patents, trademarks, trade secrets, and includes brand names and logos, research and development, inventions, proprietary software and processes, domain names, and social media accounts.

c. "Computers and Computer Systems" includes, but is not limited to, all StenTam owned or leased computers, networks, infrastructure (including routers, switches, and firewalls), software (including security and virus protection), voice mail, email, internet systems, monitors, servers, hard drives, storage devices, including cloud storage, hardware and peripheral devices, printers, and phones, and any passwords or security features used to secure and access such devices, systems, and software. Computer and Computer Systems includes data entrusted to StenTam by legal agreement, contract, or in the ordinary course of business. All Computers and Computer Systems

d. "Physical Property" includes, but is not limited to, all StenTam leased or owned buildings, desks, storage areas, file cabinets, supplies, Computers and Computer Systems, copying machines, and all other real and tangible property.

e. "Property" means all StenTam owned (in whole or part), leased, or entrusted Physical Property, Computers and Computer Systems, Intellectual Property, Confidential Business Information, and money and financial assets.

f. "User" means any person, including employees, agents, and those given access to, any Property, including Computers and Computer Systems.

II. Policy

1. General

a. Everyone is responsible for safeguarding and protecting Property from theft, fraud, waste, abuse, and damage. Theft, embezzlement, misuse, or the intentional or negligent damage or loss of Property will not be tolerated and is grounds for disciplinary action, up to and including termination.

b. Everyone is responsible for ensuring that any Property is efficiently used and only used for legitimate, bona fide business purposes.

c. Unless expressly authorized, never use any Property for personal reasons or gain or to promote any business, product, or service not offered by the Company or that competes with StenTam.

d. Unless expressly authorized, never share, disclose, release, publish, or transmit any Intellectual Property or Confidential Business Information.

e. Users who leave StenTam's employment or who lose or relinquish access to any Property must immediately return all such property and preserve any information.

II. Use of StenTam's Computers and Computer Systems

1. General. The Computers and Computer Systems are intended primarily for conducting legitimate, bona fide business; however, as set forth below, limited personal usage is permitted if it does not hinder performance of job duties or violate any other Company policy.

2. Acceptable Use Policy. The following policies and principles apply to StenTam's Computers and Computer Systems:

a. Do not create, transmit, upload, download, or store any illegal, harmful, or objectionable content, communication, file, or code.

b. Do not share passwords or give any unauthorized person access to your account(s) or to any Computers and Computer Systems and only use authorized encryption tools (both software and hardware).

c. Do not create, transmit, or store any highly sensitive information without management approval.

d. Do not access or use any social media platforms or accounts using any Computers and Computer Systems, and do not register for any online social media account, platform, or application using your Company-issued email account.

f. Do not record audio or video communications, unless authorized to do so. This provision does not apply to Zoom or similar meetings where consent of the participants is obtained in advance.

g. The following conduct in strictly prohibited:

(1) Violating, or encouraging the violation of, any federal state law or any StenTam policy;

(2) Violating, or encouraging the violation of the legal rights of others or rights otherwise legally actionable between private parties;

(3) Inciting or encouraging violence or hatred against any individuals or groups;

(4) Violating, infringing on, or otherwise misappropriating any third party rights, including intellectual property rights (trademark, copyright, design or patent rights), and right of privacy of any third party;

(5) Creating, transmitting, uploading, downloading, or storing any content or communication that is:

(a) offensive, racist, sexist, or otherwise discriminatory;

(b) threatening, abusive, harassing, or constitutes stalking;

(c) vulgar, obscene, indecent or unlawful material, including pornographic material;

(d) defamatory, deceptive, false, misleading, or inaccurate (including representing yourself as another person—real or fictional);

(e) spam, including unsolicited, bulk emails and commercial emails (unrelated to StenTam's business) and solicitations for personal, political, or religious causes.

(6) Using the Computers and Computer Systems to conduct any commercial activity or business (other than StenTam), including the sale of merchandise on online marketplaces;

(7) Engaging in or promoting any gambling activity;

(8) Creating, transmitting, uploading, downloading, storing, or redirecting any code, script, file, or program that is or contains a virus, worm, malware, Trojan horse, corrupted file, hoax, or other item of a destructive or deceptive nature;

(9) Altering, bypassing, exploiting, disabling, interfering, tampering with, circumventing, or gaining unauthorized access to any Computer and Computer System, including any functionality, security software or feature, limitation, or restriction, or attempting to do any of the foregoing;

(10) Downloading unapproved and/or unlicensed software from the Internet or other source;

(11) Removing, wiping, reformatting, encrypting, downloading, performing a factory reset, or transferring any Computers or Computer Systems or data of such systems without prior approval from the IT Department.

3. Limited Personal Use. Limited personal use (*i.e.*, email, Internet, etc.) is permitted, provided it is reasonable in frequency and duration, does not hinder performance of job duties, or violate any other Company policy. Use of Computers and Computer Systems, however, does not render personal information private (see Paragraph II, 4 below). To the extent Users intend to have their personal activities remain private, they should not use the Computers and Computer Systems.

4. Retention of records. All electronic data created, received, or stored on any Computers and Computer Systems, including email, are considered permanent business records and the property of StenTam and must comply with StenTam's Privacy and Data Policy.

5. Privacy Expectations. Users do not have any legitimate expectation of privacy in regard to their use of the Computers and Computer Systems, as more fully set forth in StenTam's Privacy and Data Policy.

III. Violation of this Policy

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

In addition, StenTam may also temporarily or permanently suspend or terminate any employee's, agent's, User's, invitee's, or licensee'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, another StenTam policy, or any law has been violated.

The StenTam Chief Legal Officer and the IT Department are the proponents of this policy. Any questions concerning this policy should be addressed to the Chief Legal Officer, or his designee, or the IT Department.