This IT Security Guideline defines the technical and organizational measures currently undertaken by Sponsorvista.

1 Organization

Measure	Description
Security responsibilities	Sponsorvista has tasked a security officer with designing, coordinating, and monitoring this IT Security Guideline. Sponsorvista's security officer reviews this IT Security Guideline and all the technical and organizational measures undertaken at the company every 12 months (at minimum) in order to propose improvements when necessary.
Guidelines	Sponsorvista has established protocols that describe the measures specified in this IT Security Guideline and the relevant procedures and responsibilities pertaining to individuals who have access to the Customer's data. Sponsorvista retains records of its protocols after they are no longer in effect.
Risk Management	Prior to rendering its services and processing the Customer's data, Sponsorvista will carry out a risk assessment.
Confidentiality	Sponsorvista employees who can access the Customer's data are obliged to maintain its confidentiality.
Training	Sponsorvista informs its employees of the following: • Basic principles of data protection • Technical and organizational measures in this IT Security Guideline • Their respective tasks with regard to IT Security • The personal consequences they will face should they violate the privacy of data and/or this IT Security Guideline

2 Physical security

Measure	Description
Facility access	Sponsorvista restricts access to facilities that house IT systems in which the Customer's data is processed to authorized personnel.
Protection against disruptions	Sponsorvista uses industry-standard systems to prevent data from being lost due to power outages and line disruptions.
Emergency plans	Sponsorvista maintains contingency plans for facilities that house IT systems in which the Customer's data is processed. During restoration, Sponsorvista reconstructs the Customer's data in its original state or the most recent state in which it was backed up before it was lost or destroyed.
Mobile work	Sponsorvista employees must receive permission from Sponsorvista before storing the Customer's data on portable devices, accessing the Customer's data from remote locations, or processing the Customer's data outside of Sponsorvista's facilities.

3 Access

Measure	Description
Authentication	Sponsorvista employes industry-standard procedures to authenticate users who attempt to access its IT systems Sponsorvista ensures that passwords meet certain minimum requirements and must be changed on a regular basis (or enables the Customer to do so) Sponsorvista uses industry-standard procedures to protects passwords. Sponsorvista revokes the access rights of every employee who leaves the company.
Authorization	Sponsorvista maintains up-to-date records on employees who are authorized to access IT systems that house the Customer's data. Sponsorvista specifies which of its employees are authorized to grant, modify, and revoke permission to access data and other resources. Sponsorvista only allows employees to access the Customer's data when doing so is required for their duties at work.
Locking computers	Sponsorvista instructs its employees to lock their computers before leaving them unsupervised.

4 Operations

Measure	Description
Data restoration	Sponsorvista creates backups on a regular basis and stores them in a separate location. Sponsorvista has procedures at its disposal that control access to backups of the Customer's data. Sponsorvista reviews its data restoration procedures every 12 months (at minimum). Sponsorvista logs its data restoration activities.
Malware	Sponsorvista employes firewalls to protect its corporate network from the public internet. Sponsorvista uses up to date virus scanners at the access points to its corporate network and on all its file servers and individual workstation computers. Sponsorvista does not permit the installation of software that it has not approved.
Encrypting the Customer's data	Sponsorvista encrypts the Customer's data or enables the Customer to encrypt its data for transmission on public networks. Sponsorvista encrypts media that contain the Customer's data and are designated for use outside of Sponsorvista's offices.
Deletion of the Customer's data	Based on a corresponding protocol, Sponsorvista specifies how data and data media are to be deleted or destroyed when they are no longer needed.
Printing the Customer's data	Based on a corresponding protocol, Sponsorvista has set restrictions on printing the Customer's data and rules for the proper storage and disposal of printed materials containing said data.
Data protection violations	Whenever an incident occurs that is classified as a data protection violation, Sponsorvista must be notified immediately.

	Sponsorvista maintains records of data protection violations that contain the following details (at minimum): • A description of the incident • The period in which it occurred • The name of the person who reported the incident • The name of the person who received the incident report • The measures taken