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

The definitions apply as per Terms and Conditions of (Commissioned) Data Processing.

1 Organization

Measure	Description
Security responsibilities	• LucaNet has tasked a security officer with designing, coordinating, and monitoring this IT Security Guideline. • LucaNet'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	• LucaNet 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. • LucaNet retains records of its protocols after they are no longer in effect.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, LucaNet will carry out a risk assessment.
Confidentiality	• LucaNet employees who can access the Customer's data are obligated to maintain its confidentiality.

Training	• LucaNet 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	• LucaNet restricts access to facilities that house IT systems in which the Customer's data is processed to authorized personnel.
Protection against disruptions	• LucaNet uses industry-standard systems to prevent data from being lost due to power outages and line disruptions.
Emergency plans	• LucaNet maintains contingency plans for facilities that house IT systems in which the Customer's data is processed. • During restoration, LucaNet 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	• LucaNet employees must receive permission from LucaNet 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 LucaNet's facilities.

3 Access

Measure	Description
Authentication	• LucaNet employs industry-standard procedures to authenticate users who attempt to access its IT systems. • LucaNet ensures that passwords meet certain minimum requirements and must be changed on a regular basis (or enables the Customer to do so). • LucaNet uses industry-standard procedures to protect passwords. • LucaNet monitors repeated attempts to access its IT systems with invalid passwords (or enables the Customer to do so). • LucaNet ensures that blocked user accounts are not assigned to any other individual (or enables the Customer to do so). • LucaNet revokes the access rights of every employee who leaves the company.
Authorization	• LucaNet maintains up-to-date records on employees who are authorized to access IT systems that house the Customer's data. • LucaNet specifies which of its employees are authorized to grant, modify, and revoke permission to access data and other resources. • LucaNet only allows employees to access the Customer's data when doing so is required for their duties at work.
Locking computers	• LucaNet instructs its employees to lock their computers before leaving them unsupervised.

4 Operations

Measure	Description
Data restoration	• LucaNet creates backups from which the Customer's data can be restored on a regular basis (read: at least once per week) and stores them in a separate location. • LucaNet has procedures at its disposal that control access to backups of the Customer's data. • LucaNet reviews its data restoration procedures every 12 months (at minimum). • LucaNet logs its data restoration activities.
Malware	• LucaNet employs firewalls to protect its corporate network from the public Internet. • LucaNet uses up-to-date virus scanners at the access points to its corporate network (read: for e-mail accounts) and on all its file servers and individual workstation computers. • LucaNet does not permit the installation of software that it has not approved.
Encrypting the Customer's data	• LucaNet encrypts the Customer's data or enables the Customer to encrypt its data for transmission on public networks. • LucaNet encrypts media that contain the Customer's data and are designated for use outside of LucaNet's offices.

Measure	Description
Deletion of the Customer's data	• Based on a corresponding protocol, LucaNet 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, LucaNet 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, LucaNet must be notified immediately.
	• LucaNet 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 take