Security Policy

Focus on the essential

Security: a DIMO Software's commitment

Computer data are a **particularly valuable and sensitive asset** for all companies.

DIMO Software is therefore committed to protecting and securing its customers' production computer data (databases, files, etc.)

DIMO Software's approach to information security management thus enables to prevent **loss, theft, or damage to computer data** and **prevent any intrusion into the computer systems** concerned.

In accordance with the principle of continuous improvement (Deming cycle), DIMO Software consolidates its information security management system to identify threats and implement appropriate controls **so as to preserve the confidentiality, integrity, and availability of computer data belonging to its customers.**

1 Security within DIMO Software

DIMO Software operates an architecture allowing for **data security** and **high availability** of the virtual machines.

The active hardware around our data centre is duplicated to ensure the **continuity of service** (switches, power supplies, high availability firewall, air-conditioning in the servers room).

▸ Management of access controls

Management of access controls to the Information System

Thanks to our Active Directory (authentication and user accounts management server), a detailed security management is applied to the various services of the information system. In addition, a secure outside access allows employees to **connect remotely** to the information system.
DIMO Software's **data network** is monitored and partitioned (monitoring solution, anti-virus, and anti-spam) to avoid any security flaw and interaction. Moreover, for visitors' convenience and security, DIMO Software offers a **guest Wi-Fi network**, separated from of all the networks of the information system.

Physical access control

Access to the building and the various sensitive areas is controlled by a biometric system and a video monitoring of sensitive areas.

A **reception service** is open all day long to welcome the public and direct the people to the relevant departments.

An **intruder alarm** monitors the building on a 24 hour/7 day basis, and ensures rapid intervention by the security officers in the event of breaking and entering.

Monitoring

To ensure the daily operation of the information system, **all activity is recorded** (access, changes, errors).

In parallel, the resources dedicated to the proper operation of the information system are **monitored in real time** (bandwidth of networks, CPU power, availability rate, capacity of the data centre).

DRP (Disaster Recovery Plan)

The data centre is replicated on a daily basis on the remote site at a hoster; this allows a **disaster recovery of the mission-critical applications** in case of failure or total loss of the building.

Annual tests are carried out to check the proper operation of replications. **Procedures for initiating the DRP** (documentation, decision makers, scope) are developed and made available to the DIMO Software's and the hoster's technicians.

Backup

The information system is backed up on a daily basis according to **the backups management procedure** of virtual machines and physical servers. The restore can be completed at file, hard drive, or full virtual machine level.

The data from the non-sensitive servers is saved for one week, up to several months.

Electrical security

DIMO Software ensures **electrical compliance** through an annual audit carried out by an authorized external company.

The electrical circuits of the switches (network endpoint and core) **are uninterruptible,** allowing for the continuity of activity and more particularly the supply of the telephony system.

Fire protection system

The data centre is monitored on a 24 hour/7 day basis by a **fire protection system** connected to the SECURITAS' central monitoring unit. A building-evacuation procedure (fire drill) is carried out each year by the Health and Safety Committee. In parallel is performed an annual check of the fire-fighting facilities (ventilation, fire extinguishers).

Maintenance & support (hardware)

All DIMO Software's active hardware is on **maintenance contract.** According to the importance of the hardware, the time needed to resolve a failure can range from 4 to 24 hours.

DIMO Software follows up the **failures and enhancement requests** through a tool aimed at requesting internal and external service.

2 Security of computer data

▸ Access to the data of hosted customers

Access rights are limited and traced.
Customer data are compartmentalized.
Our hoster partner is ISO 27001 certified.

▸ Data of non-hosted customers

The data are transferred via secure tools and deleted after processing.

3 Security management

▸ HR management

Throughout his collaboration with the company, the DIMO Software's employee is monitored by the management and Human Resources teams. This monitoring involves a detailed work contract, which includes confidentiality clauses, information meetings on the rules of procedure, annual interviews on the skills and goals to achieve.

▸ Executive committe

DIMO Software's Executive Committee meets every month to validate the different work to be done for the maintenance and the development of the information system.