TECHNICAL AND ORGANIZATIONAL MEASURES

Confidential - 2018

This document is provided for information purposes only.
The information contained in this document can be modified at any time and is subject to potential technical and legislative developments.

1. Physical access control of premises and facilities

Appropriate measures to control and prevent the physical access of unauthorized persons to premises and facilities.

- Alarm system
- Security staff, concierges
- Video surveillance system
- Automated access control system / Risk assessment and mapping of the premises
- Identification reader, badges, chip cards, magnetic cards, transponder locking system
- Security locks
- Identity control
- Visitors record / All visitors are accompanied

Various items in the above list might be combined depending on the location and facilities. Not all items in the list are required and necessary on all premises and facilities.

2. Access control to data and systems

Technical measures (ID / security password) and appropriate processes (data from the user) to identify and authenticate users.

- Allocation of user rights on a need to know basis, these rights being revised or retired when any employee changes job or leaves the company
- Creation of user profiles including:
  - differential access rights (profiles, roles, transactions and features)
  - rights are administered by system administrators
- Password procedures (including special characters, minimum password length, password modification, etc.)
- Authentication using ID/password
- Using a secure password management tool
- Automatic session lock in the event of inactivity
- Disk encryption for laptops
- Exchange encryption
- Using the VPN technology
- Using intrusion detection systems
- Using an antivirus software / firewalls / limitation of unnecessary services and flows
- Automatic update of operating systems and apps
- Compartmentalization of networks / administration systems
- History of administration actions (bash_history), saving system and application logs in particular when this leads to data access, entry, modification or deletion.
- Using paper shredders

Various items in the above list might be combined depending on the role, type of software, specific requirements from customers and needs.

3. Availability controls

Measures for the availability and protection of data against accidental destruction or loss.

- Safeguard processes; data backup
- Remote storage
- Business Continuity Plan
- Fire and smoke alarm systems
- Antivirus/firewall systems
- Automatic fire detection (Certification APSAD R7)
- Automatic gas extinction (Certification APSAD R13)
- Intrusion detection (Certification APSAD R81)
- Portable and mobile fire extinguishers (Certification APSAD R4)
- Emergency power supply in case of a breakdown
- Backup Internet provider in case of a breakdown
- Preventive maintenance plan and tests based on manufacturers' recommendations

Various items in the above list might be combined depending on the location and facilities. Not all items in the list are required and necessary on all premises and facilities.

4. Segregation of duties

Measures foreseeing separate data management (storage, modification, deletion, transfer) with different objectives

- Keeping test and production systems apart
- Keeping development and production systems apart
- Keeping customer data logically apart

5. In-house measures and awareness raising

Measures to inform the staff and raise their awareness about data security. In-house, general processes.

- Regular assessment of the measures in place
- Confidentiality clause to the work contract
- Charter about the use of technology and communications means annexed to the company rules and regulations
- Raising staff awareness on protection- and security-related topics
- A member of the Association Française des Correspondants à la protection des Données à Caractère Personnel (AFCDP, French Association of Personal Data Protection Correspondents)
- A member of the Syndicat National de la Communication Directe (SNCD, National Syndicate for Direct Communication)