Security measures: questions to ask yourself to ensure good IT hygiene

In order to answer these questions, you need to:

- **Identify and document the software used** (name of business software, Word, Excel, etc.) and their current versions.
- **Identify and assess potential threats** and their impact on the privacy of data subjects by carrying out an in-depth risk analysis.
- **Plan security measures adapted to these threats,** including back-up procedures and secure hosting locations. These measures must be regularly updated to remain effective in the face of new threats.

User authentication:

- **Have you defined a unique identifier (login)** for each user to guarantee precise traceability of actions?
- **Do you require users to use strong passwords** with a minimum of 12 characters, including uppercase and lowercase letters, numbers and special characters?
- **Have you set up a password renewal policy** requiring users to change their passwords after enrolment and at regular intervals (every 3 months, for example)?
- **Do you use two-factor authentication (2FA)** to reinforce user account security?
- **Have you established a procedure** for dealing with lost logins?
- **Do you ensure user awareness and training** in password management and account security best practices?

Managing access privileges:

- **Have you defined different authorization profiles** (based on the principle of « *least privilege* ») according to the roles and responsibilities of people with access to information?
- **Do you regularly remove obsolete access permissions** to prevent unauthorized access to information?
- **Have you drawn up and communicated an IT charter** to all users of the Information System (employees, trainees, service providers, etc.), detailing good practice and obligations in terms of data security?
- **Do you organize regular training sessions** to raise employee awareness of data security and the use of information systems?
- **Do you carry out periodic audits of access privileges** to ensure that they comply with your organization's security policy(ies)?

Securing user workstations :

- **Do you limit the number of attempts to access an account?**
- **Have you installed a software firewall?**
- **Do you use regularly updated antivirus software?**
- **Do you install critical updates (security patches) without delay** to correct operating system and software vulnerabilities?
- **Do you encrypt data** stored on workstations, including storage devices (external hard drives, USB, etc.)?
- **Do you use an automatic session lock** after a short period of inactivity to prevent unauthorized access?
- **Do you carry out regular audits** of workstations to check compliance with security policies and identify any vulnerabilities?
- **Have you introduced regular back-up procedures** for important data stored on workstations to prevent data loss in the event of a breakdown or attack?
- **Have you educated and trained users** on the importance of securing data on mobile devices and media?
- **Do you use mobile device management (MDM) solutions** to reinforce the security and compliance of mobile devices used by employees?

Continuity of your organization's activities:

- **Do you have security measures in place** for back-ups made on an external site, guaranteeing the availability of data in the event of a major disaster?
- **Have you put in place a business continuity plan** detailing the procedures to be followed in the event of a major disruption, in order to minimize interruptions and keep critical services running?
- **Have you drawn up a disaster recovery plan** to quickly restore information systems and data after an incident?
- **Do you regularly test these plans** to ensure they are effective and to identify any areas for improvement?
- **Do you organize exercises and simulations** to prepare your staff to react effectively in the event of a crisis?

Supervision of maintenance operations:

- **Do you record maintenance operations** in a logbook to ensure full traceability of actions carried out?
- **Do you accompany and supervise** all service provider interventions to ensure compliance with security and confidentiality procedures?
- **Do you erase data from all equipment** before scrapping it, to prevent any risk of data recovery?
- **Do you inform users** before any work is carried out on their workstations?
- **Do you require service providers to comply with current security standards** and data confidentiality clauses?

Managing access to your organization's Information System (IS) and incident management :

- **Have you set up an access logging system**?
- **Have you informed users** of the logging system?
- **Have you protected logging equipment and logged information** against unauthorized access and alteration?
- **Do you have a procedure for managing security incidents**, including detection, analysis and rapid resolution?

Access protection for servers, security equipment and other storage units:

- **Have you installed locked doors** to control physical access to servers, security equipment and other storage units?
- **Have you installed intruder alarms** to detect and prevent unauthorized access?
- **Do you periodically check security systems** to ensure that they are working properly and effectively?
- **Do you use video surveillance devices** to monitor and record sensitive areas (e.g. server rooms)?
- **Do you carry out regular security audits** to identify and correct any vulnerabilities in your protection systems?

Internal computer network protection:

- **Have you limited network flows to what is strictly necessary**?
- **Have you secured remote access to mobile computing devices via VPN** to guarantee the confidentiality and integrity of communications?
- **Do you use the TLS protocol with a key of at least 128 bits** to protect web services and guarantee secure connections?
- **Have you implemented security protocol(s)** (WEP2, WEP3, etc.) for Wifi networks?
- **Do you encrypt all your data** (at rest and in motion)?
- **Have you set up a Wifi access management policy**?
- **Do you use intrusion detection and prevention solutions** (IDS/IPS)?
- **Have you set up network segmentation policies** to isolate systems and limit the impact in the event of compromise of part of the network?

Securing servers and applications :

- **Have you adopted a rigorous administrator password policy**?
- **Have you installed a software firewall** on each server?
- **Do you use regularly updated antivirus software?**
- **Do you promptly install critical updates (security patches)** to correct operating system and software vulnerabilities?
- **Do you encrypt data** stored on servers and applications to protect confidentiality?
- **Do you carry out regular security audits** to identify and correct any vulnerabilities in your servers and applications?

- **Do you have policies in place for regularly updating and backing up** data stored on servers and applications to prevent loss in the event of failure?
- **Do you regularly train your system administrators** in server and application security best practices?
- **Do you have policies for regularly updating and backing up** security equipment?

Archive management :

- **Have you implemented specific access procedures** (restricted access, separate databases, etc.) to protect archived data and guarantee their confidentiality?
- **Do you destroy archives securely**, following strict procedures to prevent any unauthorized retrieval of data?
- **Do you have an archive retention plan** detailing the retention periods for the different categories of data and the conditions for their destruction?
- **Do you have archive management policies in place** to guarantee the integrity, confidentiality and availability of archived data?

Exchanges with other organizations:

- **Do you encrypt sensitive data before they are sent over any communication channel** to guarantee their confidentiality and integrity during transit?
- **Do you transmit the secret decryption code** in a separate transmission and via a different channel to reinforce the security of exchanges?
- **Do you have data exchange management policies in place**?
- **Do you regularly educate and train employees** in good security practices for data exchanges with external organizations?
- **Have you drawn up confidentiality and data processing agreements** with partner organizations to ensure compliance with legal obligations and good practice in data protection?

Relations with IT providers (if applicable):

- **Have you included a specific confidentiality clause in all data processing agreements?**
- **Have you checked that the guarantees announced by service providers are effective** (security audits, site visits, regular checks, etc.)?
- **Have you included conditions for the return and/or destruction of data** in data processing agreements?
- **Do you establish regular reports** with service providers to monitor performance, security incidents and corrective measures implemented?