RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

BACK TO BASICS

DATA LEAK PREVENTION

In eleven best practices, check out the French cybersecurity agency ANSSI's essential resources for protecting your organization against data leaks.

→ **Raise awareness among management and employees** of their role in protecting the data they handle, and of the potential impact of a compromise.

→ **Assess the risks involved in sharing data with subcontractors and service providers, and contractualize data security.**

→ **Develop, have developed, or choose applications based on the principle of data protection by design and by default** (see GDPR) right from the design stage, for instance by applying restrictive rules to the massive export of data. To go further, see CERT-FR's feedback (those recommendations – only available in French - are applicable beyond the social sector).

→ **Implement a data management policy aligned with the business lines:**

> identify sensitive data (personal or regulated data, intellectual property, etc.) and easily revocable data (user passwords, tokens, etc.), and only store data necessary for the proper functioning of the business and the IS;

> archive or delete obsolete data securely;

> define a secure backup policy – refer to ANSSI's "Back to Basics" The golden rules of backup or, for greater precision, the guide *Sauvegarde des systèmes d'information* (only available in French).

→ **Preparing for a crisis:**

> create and update crisis management procedures;

> identify the relevant contacts to notify (CNIL, ANSSI, gendarmerie, cyber-malveillance, service providers, customers, DPO, etc.);

> draw up a crisis communication plan in advance. – refer to ANSSI's guide *Anticiper et gérer sa communication de crise cyber* (only available in French).

→ **Ensure the security and confidentiality of data and processing carried out directly or by a subcontractor**, including:

> physical security measures: security of access to premises, etc.;

> IT security measures: in-depth defense, encryption of stored and in transit data, anti-virus, EDR, etc.;

> secure, dedicated administration access for subcontractors;

> maintenance in operational condition (MCO) and maintenance in security condition (MCS) of the information system.

→ **Design a strong access and privilege management policy :**

> carry out multifactor authentication and implement the password best practices listed in ANSSI's *Recommandations relatives à l'authentification multifacteur et aux mots de passe* (only available in French);

> prevent the pileup of roles;

V1.0 (01/25)

www.cyber.gouv.fr / conseil.technique@ssi.gouv.fr

- systematically minimize data access by role, IS area (development/production/pre-production) and time slot;
- supervise and log. Logs must be protected, as explained in ANSSI's *Recommandations de sécurité pour l'architecture d'un système de journalisation* and *Recommandations de sécurité pour la journalisation des systèmes Microsoft Windows en environnement Active Directory* (guides only available in French).

→ **Implement digital nomadism best practices,** as detailed in ANSSI's *Recommandations sur le nomadisme numérique* (only available in French), in particular by adopting privacy filters (R7) and setting up automatic session locking (R16).

→ **Deploy and supervise specialized tools tailored to the organization's needs**, such as DLP (Data Loss Protection) software or digital safes.

→ **Set up automatic tools for reactive monitoring** (e.g. haveibeenpwned.com) **and, if possible, foresighted monitoring** (sector monitoring, cyber threat intelligence (CTI)). These actions can be carried out in-house or by a service provider.

→ **Investigate the source of data leaks,** in the event of a proven incident, so as to adopt appropriate remediation measures and avoid further compromise by the same vector (e.g. infostealer).