RÉPUBLIQUE
FRANÇAISE

Liberté
Égalité
Fraternité

BACK TO BASICS

SENSITIVE DATA AND PROCESSING

Data and processing are considered "sensitive" if their compromise, loss, or alteration could seriously hinder the entity's ability to achieve its objectives, or even to exist. Identifying these sensitive elements is crucial to the elaboration of an information security strategy which might ensure their protection.

This document provides a simple assessment method which can be applied to any type of entity - whether it be a small business, a multinational company, or a governmental organisation or association - to protect their data and processing at the right level.

It should be noted that security measures specific to classified information (Secret and Top Secret), as defined by the French legal framework IGI 1300, are not covered in the recommendations.

1/ DEFINE SENSITIVITY LEVELS

→ **Establish a homogeneous impact scale for the entire entity**, enabling the assessment of the likely consequences of a data compromise. This scale can be inspired by the model below, or based on security requirements (availability, integrity, confidentiality…) - although this alternative is less intuitive for business units.

→ **Define data sensitivity levels**, for instance:

- low sensitivity (level 1): minor impacts only;
- sensitive: at least one significant (level 2) or serious (level 3) impact;
- highly sensitive: likely to have a critical impact (level 4). This level includes information protected by the "*Diffusion Restreinte*" (DR) label, i.e. restricted circulation.

Impact	Human	Financial	Legal	Operational	Image
Minor	Minor physical or psychological damage	None	Warning	None	Limited local media coverage
Significant	Moderate physical or psychological damage	Losses below X	Out-of-court settlement	Disruption below T hours/day	Regional media coverage, impact on local reputation
Serious	Serious but reversible physical or psychological damage	Losses between X and Y	Civil liability of the entity	Disruption between T and U hours/day	National media coverage, loss of stakeholder confidence
Critical	Irreversible physical or psychological damage, including death	Losses greater than Y	Individual criminal liability of a corporate officer	Disruption greater than T hours/day	International media coverage, major loss of market share

V1.0 (03/25)

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

2/ IDENTIFY AND CATEGORISE

→ **Carry out a broad inventory of the entity's data and processing**, without limiting it to sensitive elements.

→ **Categorise sensitive data and processing by division/department and by context of use** (testing, production, regulatory internal control, etc.), for example:

> financial data;

> commercial data and intellectual property;

> data subject to regulations;

> data linked to the operation of the information system (logs, IP addressing, architecture models).

→ **Identify the source(s) and the person(s) responsible** for each category of data and processing.

→ **Assess the level of sensitivity of the data categories:**

> the CISO must question the needs expressed by the business to avoid under or over assessment;

> the assessment must be validated by decision-makers;

> this assessment by category is preferable to an assessment by data, due to the time constraints and availability of decision-makers.

→ **Raise the sensitivity level when accumulating or aggregating data,** if necessary (e.g.: a repository containing level 2 data could be re-evaluated as a level 3 repository).

→ **Include regular reviews in the assessment process**, as sensitivity evolves over time and according to context.

3/ ANTICIPATE AND PROTECT

→ **Define the security requirements to be applied to information systems**, depending on the sensitivity of the data they process:

> for each category and level, identify the security requirements (availability, integrity, confidentiality...) whose failure are most likely to be responsible for the feared impacts. For example, if a critical operational impact is mainly caused by the unavailability of a category of IS, the need for availability is paramount;

> based on the security needs thus defined, apply *ad hoc* measures. For instance, to meet the need for availability, a business continuity plan may be required;

> for certain levels (e.g. DR/restricted circulation data), regulatory requirements may apply.

→ **Frame the conditions of interconnection between sensitivity levels,** including non-sensitive one.

→ **Prioritize security efforts according to simple criteria** such as the sensitivity levels or the exposure, which can be assessed on the basis of :

> the number and type of people (internal, service provider, partner, public) who can access the data;

> the number and level of control of interfaces enabling access to data (physical access, logical access, third-party networks).