



**GUIDE SDI TRS  
N°2351**

**RÉFÉRENTIEL DE SÛRETÉ NIVEAU « FONDAMENTAL »**

**2<sup>ème</sup> édition**

*(Les dates précises d'approbation et de publication sont accessibles dans SysMan)*

**Document entretenu par DGA/SSDI**



**L'édition en vigueur de ce document est celle accessible dans SysMan, avec les informations complémentaires de sa fiche documentaire dématérialisée. S'assurer de la validité et de la complétude de toute copie avant usage.**

<b>Rédaction</b>	DGA/SSDI/DPAR	Chargée de réglementation et officier contrôleur
<b>Vérification</b>	DGA/SSDI/DPAR	Chef du département de la protection, des audits et de la réglementation
<b>Vérification</b>	DGA/SSDI/AD	Animatrice et Responsable déléguée du domaine SDI
<b>Approbation</b>	DGA/SSDI/D	Responsable du domaine SDI

## POSITIONNEMENT DANS L'ENVIRONNEMENT DGA

Directions (entités) d'application :	Industriels de Défense
Activité du domaine de performance :	SDI
Pôles/métiers :	Maitrise des risques courants/Sécurité de défense et de l'information (MRC / SDI)
Systemes de management :	ISO 9001

## ÉVOLUTIONS

Nature des évolutions :	Mise sous la charte DGA actualisée et enregistrement qualité
Documents abrogés par cette édition :	/

## DÉCLINAISON

Autorisation de déclinaison :	<input type="checkbox"/>	Le cas échéant, précisions du périmètre de déclinaison :
		/

## TABLE DES MATIÈRES

<b>1. OBJET DU DOCUMENT .....</b>	<b>4</b>
<b>2. CHAMP D'APPLICATION .....</b>	<b>4</b>
<b>SIGLES ET ABRÉVIATIONS .....</b>	<b>4</b>
<b>3. UTILISATION DU RÉFÉRENTIEL.....</b>	<b>4</b>
3.1 EXIGENCES .....	4
3.2 EVALUATION .....	5
3.3 TRAITEMENT DES ECARTS.....	5
3.4 MISE A JOUR DE L'ÉVALUATION DU NIVEAU DE SURETE .....	5
<b>4. EXIGENCES .....</b>	<b>6</b>

# GUIDE

Objet : Référentiel de sûreté niveau « fondamental »

## 1. OBJET DU DOCUMENT

Ce référentiel de sûreté a été conjointement élaboré au sein d'un groupe de travail, piloté par la direction générale de l'armement (DGA) et réunissant des grands maîtres d'œuvres industriels (MOI) de la défense ainsi que le conseil des industries de défense françaises (CIDEF).

Il vise à assurer aux entreprises, par la mise en œuvre de treize mesures, un niveau minimal de sûreté, leur permettant ainsi de mieux se protéger contre l'ensemble des actes de malveillance qui peuvent survenir à l'encontre de leur personnel, de leurs actifs ou encore de leurs activités.

Ce guide se concentre uniquement sur les aspects relatifs au domaine de la protection physique et les mesures organisationnelles associées. Il ne traite pas des dispositions liées à la cyber sécurité qui font l'objet d'un référentiel dédié<sup>1</sup>.

## 2. CHAMP D'APPLICATION

Les exigences de ce référentiel s'adressent avant tout aux sociétés réalisant des prestations dans le cadre de contrats en lien avec la défense. Il est particulièrement recommandé de les appliquer pour les contrats qui ne sont soumis à aucune réglementation en matière de sûreté.

## SIGLES ET ABRÉVIATIONS

<b>CIDEF</b>	Conseil des industries de défense françaises
<b>DGA</b>	Direction générale de l'armement
<b>MOI</b>	Maître d'oeuvre industriel

## 3. UTILISATION DU RÉFÉRENTIEL

Ce référentiel doit être considéré comme un socle de base, permettant aux entreprises de progresser en matière de sûreté en mettant en place un niveau de protection minimal de leurs actifs et activités. Dans un contexte de concurrence économique exacerbée où les menaces et actes de malveillance sont significatives, la montée en maturité en matière de sûreté apparaît comme importante.

Ce référentiel peut être utilisé :

- De manière contractuelle, par un donneur d'ordre vers un de ses sous-traitants ou fournisseurs pour assurer un niveau minimal de sûreté.
- Dans le cadre d'un processus d'auto-évaluation par une entreprise souhaitant valoriser son niveau de sûreté auprès de ses donneurs d'ordres.

Le référentiel de niveau fondamental a été conçu avec un souci de pragmatisme en proposant des mesures simples et applicables par toute entreprise, quel que soit sa taille et la nature de ses activités.

### 3.1 Exigences

Chaque exigence se présente sous la forme d'un tableau comprenant les éléments suivants :

- La catégorie à laquelle l'exigence appartient ;
- Un libellé ;

---

<sup>1</sup> Le référentiel de maturité cyber est disponible sur le site de l'armement, [à l'adresse suivante](#).

- Un commentaire permettant de préciser les attendus et de définir les termes clefs ;
- Les éléments de preuve devant être apportés par l'industriel lorsque l'application du référentiel est rendue obligatoire dans le cadre d'un contrat ou dans le cadre d'un processus d'auto-évaluation.

Certaines exigences contiennent des recommandations qui ne sont pas obligatoires à mettre en œuvre mais conseillées.

### 3.2 Evaluation

L'entreprise doit réaliser une évaluation de son niveau de sûreté par rapport aux exigences du présent référentiel. Cette analyse devra identifier les écarts entre les mesures mises en œuvre et ces règles. Elle devra aussi s'assurer que les éléments de preuve demandés sont bien disponibles et accessibles.

Il n'y a pas de formalisme particulier imposé pour les éléments de preuve. L'entreprise peut cependant les rassembler dans un document unique, constituant ainsi une première version d'une politique de sûreté.

Pour faciliter l'évaluation et aider l'entreprise à se positionner vis-à-vis de chaque exigence, quatre niveaux de réponse gradués ont été définis :

1. Non conforme : l'entreprise ne met en œuvre aucune mesure permettant de respecter partiellement ou entièrement l'exigence.
2. Partiellement conforme : l'entreprise met en œuvre certaines mesures permettant de respecter partiellement l'exigence mais des actions supplémentaires doivent encore être conduites afin d'atteindre l'exigence.
3. Conforme : l'entreprise met en œuvre l'ensemble des mesures permettant d'atteindre l'exigence.
4. Conforme + : l'entreprise met en œuvre des mesures qui vont au-delà des attendus de l'exigence.

L'entreprise est conforme au référentiel de sûreté dès lors qu'elle respecte l'ensemble des treize exigences.

### 3.3 Traitement des écarts

En analysant ce référentiel, une entreprise peut identifier des écarts par rapport aux exigences. Dans ce cas, il est souhaitable que cette dernière produise un plan d'action listant les mesures proposées et les jalons calendaires associés pour atteindre le niveau demandé. La fourniture de ce plan d'action peut être rendue obligatoire par voie contractuelle.

L'évaluation du niveau de sûreté par rapport aux règles du présent référentiel comprend donc :

- L'ensemble des règles avec lesquelles l'entreprise est conforme.
- Le cas échéant, un plan d'action, où pour chaque écart qu'elle identifie l'entreprise indique les actions mises en place pour le corriger. Ce plan d'action prévoit, au minimum, l'échéance et le responsable de la mise en œuvre de chaque mesure.

Cette évaluation, une fois réalisée, comporte des informations sensibles et doit donc être protégée *via* un moyen de chiffrement<sup>2</sup> dès lors qu'elle est exportée vers l'extérieur.

Une attestation formelle est réalisée par le dirigeant exécutif de l'entreprise ou par toute personne qu'il désigne, à partir de ces éléments.

### 3.4 Mise à jour de l'évaluation du niveau de sûreté

Le réexamen de l'évaluation du niveau de sûreté peut être demandé contractuellement.

Dans tous les cas, l'entreprise réexamine son niveau de sûreté au moins tous les ans ou lorsqu'un événement est de nature à modifier le contexte dans lequel cette déclaration a été établie

<sup>2</sup> Si l'usage d'un moyen de chiffrement est impossible, l'évaluation réalisée peut être transmise par voie postale.

(changement d'organisation, délocalisation etc.). L'attestation formelle est alors mise à jour en précisant les éventuels changements. L'entreprise archive les versions successives des attestations.

#### **4. EXIGENCES**

Les exigences sont définies dans le document suivant disponible sur le site internet Armement/Rubrique sûreté physique.