${DOCUMENT}

|  |  |
| --- | --- |
| Version : | ${VERSION} |
| État document : | ${STATE} |
| Classification : | ${CLASSIFICATION} |
| Société : | ${COMPANY} |
| Document : | ${DOCUMENT} |
| Date : | ${DATE} |
| Consultant(s) : | ${CONSULTANT} |
| Représentant(s) client : | ${CLIENT} |

${COMPANY}

Sécurité de l'information

**Informations générales :**

Table des matières

1 Introduction 3

1.1 Avertissement 3

1.2 Interprétation des chiffres et « sensation » de sécurité 3

1.3 Contenu du document 4

1.4 Répartition sectorielle des contrôles 4

1.5 Glossaire 4

2 Synthèse du Diagnostic CASES 5

2.1 Résumé 5

2.2 Tableau des recommandations 6

ANNEXE A : Prise de notes 7

ANNEXE B : Légendes 8

Légende pour l’appréciation des recommandations 8

Légende du tableau d’évaluation détaillé 8

# 1 Introduction

## 1.1 Avertissement

Le Diagnostic CASES, réalisé à la demande du Client, a pour objectif d’apprécier la maturité d’une organisation eu regard aux bonnes pratiques applicables en matière de la sécurité de l'information. Les trois critères pris en compte dans le cadre du Diagnostic sont la confidentialité, l’intégrité et la disponibilité.

Le présent document, basé sur le Diagnostic CASES, est destiné à l’usage exclusif du client. Il est à ce titre confidentiel.

Au vu de la méthodologie employée et de la durée très limitée de l’entretien (2h) tenu pour le Diagnostic, il est entendu par les Parties que l’ensemble des résultats ne peut en aucune manière être exhaustif. À ce titre, l’appréciation du risque réel ou la liste des risques et vulnérabilités détectés sont basées sur les informations fournies par le Client et/ou ses représentants. L’analyse issue de cette appréciation ne peut engager SMILE GIE pour toute omission ou erreur qui seraient due à des tiers ou non.

Le Diagnostic CASES peut éventuellement fournir des recommandations (voir Annexe B, pour explications). Il est entendu par les parties que les recommandations ne sont ni exclusives, ni exhaustives.

## 1.2 Interprétation des chiffres et « sensation » de sécurité

La qualification de la maturité est un exercice qui permet d’apprécier si les mesures de sécurité en place sont à la hauteur du niveau de sécurité à obtenir en fonction des actifs à protéger. Par exemple, un résultat d’appréciation de 100% signifie que des moyens de protection jugés adéquats sont mis en œuvre. Par contre, comme aucune recherche exhaustive de failles n’est effectuée, rien n’affirme que ces moyens de protection soient efficaces et correctement implémentés.

Exemple : Un organisme a mis en place un contrôle d’accès par badge et un gardien à l’entrée de ses bureaux. Toutes les entrées et sorties sont consignées, les visiteurs portent un badge et sont toujours accompagnés.

Cette constatation peut atteindre la note maximum de mise en place de bonnes pratiques de 100%. Ce qui signifie que l’organisme a mis en place un contrôle d’accès en adéquation avec ce qu’il veut protéger. Il est sensible et conscient de son importance. Par contre, cela ne veut pas dire que la sécurité est correctement gérée, car les mesures de sécurité peuvent avoir des failles ou ne traitent pas tous les cas possibles.

**Exemples :**

* Y a-t-il une entrée de service, un fumoir externe ou d’autres accès aux bâtiments (quai de chargement) ?
* Qui autorise les accès, est-il facile de se procurer un badge ?
* Est-ce que les personnes qui quittent la société ont bien leurs accès supprimés ?
* Comment réagit le personnel en présence d’un inconnu seul dans les locaux ?
* Les consignes de sécurité sont-elles connues par l’ensemble du personnel ?
* Les exceptions sont-elles bien gérées ? (ouverture et fermeture des locaux, maladies, congés, pauses du gardien, etc.).
* Seule une analyse des risques permet d’apprécier plus exhaustivement les risques réellement encourus.

## 1.3 Contenu du document

Le chapitre 2 contient la synthèse du Diagnostic.

L’Annexe A contient les notes prises lors de l’interview. Elles permettent, si ce n’est pas le cas de comprendre pourquoi certaines recommandations sont faites.

L’annexe B, contient les légendes nécessaires à la compréhension de ce document.

## 1.4 Répartition sectorielle des contrôles

Le schéma ci-dessous présente les différents secteurs faisant l’objet de l’évaluation. Il faut noter que l’IT « pure » (Système d’information) ne représente qu’un tiers des contrôles.



## 1.5 Glossaire

|  |  |
| --- | --- |
| Terme | Définition |
| Actif | Tout ce qui a de la valeur pour l’organisme (biens et information). |
| Sécurité de l'information | Protection de la confidentialité, de l’intégrité et de la disponibilité de l’information; en outre, d’autres propriétés, telles que l’authenticité, l’imputabilité, la non-répudiation et la fiabilité, peuvent également être concernées. |

# 2 Synthèse du Diagnostic CASES

## 2.1 Résumé

Le niveau de maturité calculé par le Diagnostic est calculé sur xxx points. Le niveau actuel est estimé à environ xxx points. Ce résultat montre que l’administration communale est déjà bien sensibilisée à la thématique de la sécurité de l’information, mais que quelques points peuvent être améliorés.

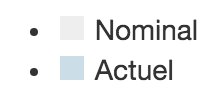
Par contre, l’évaluation décèle des recommandations du type « Risque très important » (●●●), sur-lesquels une attention toute particulière doit être portée. Nous y retrouvons notamment l’absence de mise à jour du système d’exploitation et des logiciels sur les postes locaux, ainsi que le non changement des mots de passe Windows après la première utilisation.

Une série de recommandations est axée sur la mise en place d’une charte de sécurité qui permet de rappeler aux utilisateurs les bonnes pratiques diverses concernant l’utilisation du système d’information, mais également sur une sensibilisation à la thématique désormais disponible dans le catalogue de formations officielles de l’INAP.

De façon globale, la plupart des mesures de sécurité sont faciles à implémenter et n’ont pas de coût direct.

Toutefois, au vu de la durée de l’évaluation (1,5 heure), celle-ci ne peut être exhaustive, et seule une analyse des risques peut déterminer plus en profondeur les risques auxquels l’administration est exposée.





**Vision de la conformité par domaine de la sécurité :**



## 2.2 Tableau des recommandations

La table suivante représente, la liste des recommandations formulées. Elle est ordonnée par gravité, puis par coût direct à prévoir, car certaines mesures organisationnelles ne coûtent que du temps interne de mise en œuvre.

La légende explicitant la lecture de ce tableau se trouve dans l'annexe B. Le détail des notes prises au regard des recommandations se trouve dans l'annexe A.

| **Nr** | **Recommandation** | **Domaine** | **Gravité** | **Maturité actuelle** | **Maturité visée** |
| --- | --- | --- | --- | --- | --- |
| ${RECOMM\_NUM} | ${RECOMM\_TEXT} | ${RECOMM\_DOM} | ${RECOMM\_GRAV} | ${RECOMM\_CURR\_MAT} | ${RECOMM\_TARG\_MAT} |

La légende explicitant la lecture de ce tableau se trouve au chapitre 4 « Légendes », le détail des notes prises au regard des recommandations se trouve au chapitre 3.

# ANNEXE A : Prise de notes

| Information à collecter | Information collectée | Évaluation de la maturité | | | | | Recommandation | Maturité visée |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | R | **½** | **** | Q |
| ${PRISE\_NOTE\_CATEG\_1} | | | | | | | | |
| ${PRISE\_NOTE\_TO\_COLLECT\_1} | ${PRISE\_NOTE\_COLLECT\_1} | ${PRISE\_NOTE\_QUEST\_1} | ${PRISE\_NOTE\_1\_1} | ${PRISE\_NOTE\_2\_1} | ${PRISE\_NOTE\_3\_1} | ${PRISE\_NOTE\_4\_1} | ${PRISE\_NOTE\_RECOMM\_1} | ${PRISE\_NOTE\_TARG\_MAT\_1} |
| ${PRISE\_NOTE\_CATEG\_2} | | | | | | | | |
| ${PRISE\_NOTE\_TO\_COLLECT\_2} | ${PRISE\_NOTE\_COLLECT\_2} | ${PRISE\_NOTE\_QUEST\_2} | ${PRISE\_NOTE\_1\_2} | ${PRISE\_NOTE\_2\_2} | ${PRISE\_NOTE\_3\_2} | ${PRISE\_NOTE\_4\_2} | ${PRISE\_NOTE\_RECOMM\_2} | ${PRISE\_NOTE\_TARG\_MAT\_2} |
| ${PRISE\_NOTE\_CATEG\_3} | | | | | | | | |
| ${PRISE\_NOTE\_TO\_COLLECT\_3} | ${PRISE\_NOTE\_COLLECT\_3} | ${PRISE\_NOTE\_QUEST\_3} | ${PRISE\_NOTE\_1\_3} | ${PRISE\_NOTE\_2\_3} | ${PRISE\_NOTE\_3\_3} | ${PRISE\_NOTE\_4\_3} | ${PRISE\_NOTE\_RECOMM\_3} | ${PRISE\_NOTE\_TARG\_MAT\_3} |
| ${PRISE\_NOTE\_CATEG\_4} | | | | | | | | |
| ${PRISE\_NOTE\_TO\_COLLECT\_4} | ${PRISE\_NOTE\_COLLECT\_4} | ${PRISE\_NOTE\_QUEST\_4} | ${PRISE\_NOTE\_1\_4} | ${PRISE\_NOTE\_2\_4} | ${PRISE\_NOTE\_3\_4} | ${PRISE\_NOTE\_4\_4} | ${PRISE\_NOTE\_RECOMM\_4} | ${PRISE\_NOTE\_TARG\_MAT\_4} |
| ${PRISE\_NOTE\_CATEG\_5} | | | | | | | | |
| ${PRISE\_NOTE\_TO\_COLLECT\_5} | ${PRISE\_NOTE\_COLLECT\_5} | ${PRISE\_NOTE\_QUEST\_5} | ${PRISE\_NOTE\_1\_5} | ${PRISE\_NOTE\_2\_5} | ${PRISE\_NOTE\_3\_5} | ${PRISE\_NOTE\_4\_5} | ${PRISE\_NOTE\_RECOMM\_5} | ${PRISE\_NOTE\_TARG\_MAT\_5} |
| ${PRISE\_NOTE\_CATEG\_6} | | | | | | | | |
| ${PRISE\_NOTE\_TO\_COLLECT\_6} | ${PRISE\_NOTE\_COLLECT\_6} | ${PRISE\_NOTE\_QUEST\_6} | ${PRISE\_NOTE\_1\_6} | ${PRISE\_NOTE\_2\_6} | ${PRISE\_NOTE\_3\_6} | ${PRISE\_NOTE\_4\_6} | ${PRISE\_NOTE\_RECOMM\_6} | ${PRISE\_NOTE\_TARG\_MAT\_6} |
| ${PRISE\_NOTE\_CATEG\_7} | | | | | | | | |
| ${PRISE\_NOTE\_TO\_COLLECT\_7} | ${PRISE\_NOTE\_COLLECT\_7} | ${PRISE\_NOTE\_QUEST\_7} | ${PRISE\_NOTE\_1\_7} | ${PRISE\_NOTE\_2\_7} | ${PRISE\_NOTE\_3\_7} | ${PRISE\_NOTE\_4\_7} | ${PRISE\_NOTE\_RECOMM\_7} | ${PRISE\_NOTE\_TARG\_MAT\_7} |
| ${PRISE\_NOTE\_CATEG\_8} | | | | | | | | |
| ${PRISE\_NOTE\_TO\_COLLECT\_8} | ${PRISE\_NOTE\_COLLECT\_8} | ${PRISE\_NOTE\_QUEST\_8} | ${PRISE\_NOTE\_1\_8} | ${PRISE\_NOTE\_2\_8} | ${PRISE\_NOTE\_3\_8} | ${PRISE\_NOTE\_4\_8} | ${PRISE\_NOTE\_RECOMM\_8} | ${PRISE\_NOTE\_TARG\_MAT\_8} |

# ANNEXE B : Légendes

## Légende pour l’appréciation des recommandations

Chaque recommandation comporte une indication du degré d'importance:

 : Risque très important qui doit être traité en urgence.

 : Risque important nécessitant une attention particulière.

 : Risque mineur/suggestion qui permettrait l’amélioration du niveau de la sécurité.

## Légende du tableau d’évaluation détaillé

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Information à collecter** | **Information collectée** | **Évaluation de la maturité** | | | | | **Recommandation** | **Maturité visée** |
| **Sujet** | **** | **½** | **** | **** |

**Information à collecter** : Question posée pendant l’interview, sujet à traiter.

**Information collectée** : Informations diverses collectées suite à la question posée.

**Évaluation de la maturité** :

**Sujet**  : Point de sécurité à évaluer

****: La (ou les) mesure de sécurité est correctement implémentée.

**½ **: La (ou les) mesure de sécurité est partiellement implémentée.

****: L’implémentation de la (ou les) mesure de sécurité est planifiée.

****: La (ou les) mesure de sécurité ne sont pas en place.

**Recommandation** : Formulation de ce qu’il faudrait idéalement faire pour contrer le risque.

**Mat visée** : Maturité visée après mise en place de la mesure.