|  |
| --- |
|  |



[Introduction et Avertissement 2](#_Toc23760941)

[Description 2](#_Toc23760942)

[Résultat 2](#_Toc23760943)

[Recommandations 4](#_Toc23760944)

[Règles/Chartes 4](#_Toc23760945)

[GDPR 4](#_Toc23760946)

[Formations 4](#_Toc23760947)

[Télétravail/Mobilité 5](#_Toc23760948)

[Contrats (SLA/NDA) 5](#_Toc23760949)

[Nettoyage des Locaux 5](#_Toc23760950)

[Mots de passe 5](#_Toc23760951)

[Antivirus 5](#_Toc23760952)

[Postes Utilisateurs/Mises à jour 5](#_Toc23760953)

[Sauvegardes 6](#_Toc23760954)

[BYOD 6](#_Toc23760955)

[Questions 7](#_Toc23760956)

[Résumé: 11](#_Toc23760957)

# Introduction et Avertissement

L'outil d'auto-évaluation **Fit4Cybersecurity** a pour objectif d’apprécier la maturité d’une organisation au regard des bonnes pratiques applicables en matière de sécurité de l'information.

Le présent document est le résultat de votre évaluation sur le **Fit4Cybersecurity**. Il vous est destiné exclusivement. Il est à ce titre confidentiel.

Eu égard à la méthodologie utilisée et du fait qu'il s'agit d'une auto-évaluation, il est entendu que les résultats ne peuvent en aucune manière être exhaustifs. 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.

L'outil, Fit4Cybersecurity peut éventuellement fournir des recommandations. Il est entendu par le client que les recommandations ne sont ni exclusives ni exhaustives.

Notez également que les informations que vous nous avez fournies seront enregistrés pour effectuer des statistiques. De part de la nature des données, nous ne pouvons vous identifier. Sauf si par la suite vous nous contactez pour réaliser un diagnostic CASES.

# Description

Cet outil d'auto-évaluation est nommé Fit4Cybersecurity pour souligner l'introduction à la sécurité de l'information. Il est aussi un prérequis pour faire un **Diagnostic CASES**: un score minimal de 80/100 est requis. Le but pour cette restriction nous donne la possibilité de mieux adapter les recommandations à votre organisation lors du Diagnostic.

Durant cette auto-évaluation, 13 questions à choix multiples vous ont été posées. Après avoir analysé vos réponses, des recommandations vous ont été fournies.

Finalement, vous pouvez télécharger ce document en français, anglais ou en allemand ce qui vous aidera pour communiquer les résultats à vos fournisseurs si besoin.

# Résultat

Vous avez atteint **49**/100 avec vos réponses. Vous devez obtenir au minimum 80/100 pour pouvoir faire un Diagnostic CASES. Nous vous invitons à suivre les conseils issus de votre diagnostic pour progresser afin d’atteindre le score voulu.



# Recommandations

Voici la liste des recommandations, selon vos réponses.

## Règles/Chartes

1. L'entreprise doit définir des règles écrites pour éviter toute incompréhension.

2. Les règles (qu'elles soient organisationnelles, métier, ou à l'usage de l'informatique) doivent être connues et expliquées à tous, au moins oralement.

3. Si une transmission orale suffit dans un cadre "familial", les règles devraient être mises dans une charte ou un règlement, écrites et signées par tous, particulièrement en cas de croissance.

4. Les règles écrites et signées ont l'avantage :
 - d'éviter les oublis.
 - d’obtenir une preuve légale que les règles sont connues et acceptées.

5. Dans la mesure du possible, ses dernières doivent être simples et concises, afin de rester compréhensibles pour chacun.

6. Si possible, il ne faut pas hésiter à donner des astuces pour aider au respect des règles, voire parfois, expliquer en quoi elles sont nécessaires.

7. Les règles peuvent être adaptées à la fonction ou au type de contrat du collaborateur.

## GDPR

1. Le cycle de vie des données personnelles doit être accessible à tous (registre de traitement) ;
 - Comment sont-elles obtenues ?
 - Comment sont-elles traitées ?
 - Comment sont-elles accessibles et par qui, sous quelles clauses ?
 - Comment sont-elles modifiables ?
 - Combien de temps sont-elles conservées ?
 - Comment sont-elles détruites ?
Ce cycle devrait être décrit quelque part et accessible à tous (contrat de vente, site web, fichier présentable en cas d'interrogation ...).

2. En cas de prises de vues lors d’événements, une autorisation préalable doit être demandée aux intéressés. Cette autorisation peut être demandée lors de l’inscription à l’événement ou être indiquée de manière visible lors de l’événement. Plus d’information sur le site de la CNPD : [https://cnpd.public.lu/content/dam/cnpd/fr/dossiers-thematiques/droit-image/CNPD-Lignes-directrices-droit-a-l-image-protection-donnees-personnelles.pdf`](https://cnpd.public.lu/content/dam/cnpd/fr/dossiers-thematiques/droit-image/CNPD-Lignes-directrices-droit-a-l-image-protection-donnees-personnelles.pdf%60)

3. La vidéosurveillance doit être réalisée selon les [règles en vigueur](https://cnpd.public.lu/fr/dossiers-thematiques/videosurveillance/article2611.html), et les personnes qui y sont soumises doivent être avisées. Plus d’informations sur le site de la CNPD : <https://cnpd.public.lu/fr/dossiers-thematiques/videosurveillance/article2611.html>

## Formations

1. Les formations métier sont importantes et doivent être mises régulièrement à jour pour s'assurer de suivre les évolutions du métier et son notamment son adaptation aux nouvelles technologies.

2. Des formations sur les outils informatiques utilisés quotidiennement permettront de d’améliorer l’efficacité du personnel et d’éviter les erreurs.

3. Des formations faites en interne n'ont parfois pas le même impact que celles faites en externe, mais sont tout aussi valables, et parfois même plus appropriées pour la maîtrise du sujet et de la bonne orientation du discours.

4. Sensibiliser les utilisateurs à l’importance des informations traitées pour attirer leur attention sur les protections à mettre en œuvre.

## Télétravail/Mobilité

1. Une attention particulière doit être apportée à l'environnement visuel des télétravailleurs pour leur éviter d’être épiés.

2. Le matériel doit être chiffré s'il contient des données confidentielles pour éviter toute perte de confidentialité.

3. Les travailleurs « nomades » doivent faire l’objet d’une attention particulière notamment s’ils se connectent via des canaux non protégés (wifi publics…).

## Contrats (SLA/NDA)

1. Si les moyens et le contexte le permettent ou le nécessitent, un contrat doit être mis en place concernant la disponibilité, tant des informations nécessaires, que du matériel pour les manipuler. Ces contrat sont baptisés « SLA » (Service Level Agreement).

2. Il faut régulièrement revoir les contrats de SLA pour s'assurer:
 - qu’une interruption de service d’une durée trop longue ne puisse survenir sans être indemnisée;
 - de ne pas devoir payer des interventions d’une durée illimitée;
 - que la qualité des services rendus corresponde aux attentes.

## Nettoyage des Locaux

1. Des règles doivent être établies, spécifiant notamment les surfaces et mobiliers à nettoyer, et les éléments qui ne doivent pas être nettoyés ou déplacés durant le nettoyage.

2. Un contrat de confidentialité sera utile pour éviter la divulgation d’informations ou de conversations qui auraient « interceptées » de manière fortuite par le personnel de nettoyage.

3. Dans le même ordre d’idée, les documents confidentiels ne doivent pas être visibles ni accessibles par le personnel extérieur.

4. Le personnel d'entretien (comme toute personne non habilitée) ne doit pas intervenir dans un local à accès restreint, comme une salle d'archive ou une salle serveur.

## Mots de passe

1. Les mots de passe ne doivent pas former des mots ou des dates cohérentes pour qu'ils ne soient pas facilement devinables.

2. Des phrases complètes peuvent être utilisées comme mot de passe, même s'ils forment des mots complets.

3. Les mots de passe doivent être changés de temps à autre pour prévenir une possible fuite de ses dernières.

4. Les mots de passe réutilisés dans d'autres sites offrent plus de chance de divulgation. De plus, une seule perte de mot de passe suffit à compromettre la totalité des accès.

5. En cas d’alerte concernant la divulgation de données provenant d’un service en ligne, le mot de passe servant à accéder à ce service doit être immédiatement modifié, le cas échéant, également sur tous les comptes dans lesquels ce mot de passe était utilisé.

## Antivirus

1. Ce dernier doit être mis à jour, au moins de façon automatique pour couvrir le plus de menaces possibles.

2. Il doit être également activé en permanence pour protéger en continu la machine.

3. Tout appareil, y compris des appareils plus nomades comme les ordinateurs portables, les téléphones et les tablettes doivent avoir un antivirus, même ceux proposés par défaut dans les systèmes d'exploitation.

4. Dans l'idéal, il ne faut pas hésiter à faire des tests de temps à autre.

## Postes Utilisateurs/Mises à jour

1. Une machine doit être le plus à jour possible pour éviter le plus de failles, et ainsi éviter au possible les attaques par intrusion dans le réseau. Si beaucoup de systèmes d'exploitation se mettent à jour sans aide particulière, les logiciels doivent recevoir une attention particulière.

2. Les droits d'administration peuvent être laissés à des utilisateurs avertis et informés des consignes pour utiliser leur machine, mais nécessitent des règles précises.

## Sauvegardes

1. Toutes les données de l’entreprise doivent être sauvegardées au minimum pour leur durée légale de conservation. Les collaborateurs doivent être clairement informés des règles et du fonctionnement des sauvegardes afin qu’ils puissent y enregistrer leurs données.

## BYOD

1. Tous les appareils privés emmenés par les collaborateurs sur le lieu de travail doivent être soumis à un contrôle antiviral au minimum, afin d'éviter un maximum d'infection sur le réseau. L’accès aux données de l’entreprise doit être conditionné à une sécurisation haute des appareils (verrouillage automatique, chiffrement des données, contrôle à distance…).

# Questions

|  |  |
| --- | --- |
| **1** | **Dans l'entreprise, les procédures sont**  |
| **X** | **non écrites** |
|   | transmises oralement à toutes et tous |
|   | écrites et transmises par mail |
|   | lues et signées par tous, et inscrites dans une charte |
|   | écrites/expliquées avec du vocabulaire simple, non spécifique à un métier |
|   | assez longues, mais très précises |
|   | transmises avec des conseils et des bonnes pratiques pour aider les employés à les appliquer |
|   | adaptées selon la personne la personne et/ou son rôle |

|  |  |
| --- | --- |
| **2** | **Dans l'entreprise** |
|   | aucune autre donnée personnelle que celles des employés, ou aucune gestion concernant les données personnelles |
| **X** | **une personne responsable de toutes les actions liées aux données personnelles est désignée** |
|   | Le cycle de vie des données internes (comment elles sont récupérées, comment elles sont stockées, où et quand elles sont détruites...) est consigné dans un registre |
| **X** | **Les employés reçoivent une explication orale ou écrite sur le comportement à adopter lors du traitement de données personnelles**  |
|   |  |

|  |  |
| --- | --- |
| **3** | **Les employés sont formés régulièrement** |
|   | aux évolutions de leur métier |
|   | aux logiciels qu'ils utilisent quotidiennement |
| **X** | **à la sécurité de l'information** |
|   | en interne ou en externe par des spécialistes |
|   | à la conservation confidentielle des données, particulièrement si elles sont personnelles |

|  |  |
| --- | --- |
| **4** | **Les responsabilités IT et Sécurité de l'Information** |
|   | sont assurées en interne par une personne responsable |
|   | sont assurées en interne par plusieurs personnes responsables |
| **X** | **sont sous-traités contractuellement** |
|   | sont sous-traité sans contrat  |
|   | ne sont pas attribuées; chacun résout son problème ou fait appel à un autre employé avec plus de compétence dans le domaine |

|  |  |
| --- | --- |
| **5** | **Lors d’un déplacement, les employés** |
|   | N’utilisent aucun appareil professionnel, car le télétravail n'est pas une pratique autorisée et la seule connexion possible au réseau d'entreprise est interne |
| **X** | **Se connectent via VPN (Virtual Private Network)**  |
|   | Se connectent via un WiFi public, une connexion ouverte, ou une connexion protégée par mot de passe d'un organisme ou d'une personne externe |
|   | Utilisent une connexion privée ou du partage de réseau d'un téléphone personnel ou professionnel |
|   | Utilisent un filtre à écran, ou portent une attention particulière à la vision possible sur les écrans au travers des fenêtres ou dans les transports publics |
|   | Utilisent un matériel avec un stockage de données chiffré ou sans données confidentielles pour éviter toute perte involontaire de données |

|  |  |
| --- | --- |
| **6** | **Des contrats avec les différents prestataires (informatique, comptabilité...)** |
|   | ne sont pas définis, et ces derniers n'interviennent uniquement en cas de besoin de façon ponctuelle |
| **X** | **définissent la confidentialité des données et la protection nécessaire de ces dernières** |
|   | définissent le temps maximum pour lequel ces derniers doivent intervenir |
|   | sont régulièrement revus pour s'assurer qu'ils correspondent toujours aux besoins |

|  |  |
| --- | --- |
| **7** | **Le nettoyage des locaux de travail se déroule** |
|   | en interne, par les employés, de façon ponctuelle |
| **X** | **pendant les heures de bureau** |
|   | sous couvert de règles données concernant ce qu'il faut éviter de faire, ou éviter de toucher |
|   | sous couvert d'un contrat spécifiant la confidentialité à respecter |
|   | alors que tous documents confidentiels sont stockés dans des armoires sous clé ou autre endroit verrouillé. |
|   | en évitant les salles ou les accès sont interdits, comme une salle d'archive ou une salle serveur |

|  |  |
| --- | --- |
| **8** | **Les mots de passe dans l'entreprise** |
|   | ne sont pas soumis à des consignes particulières, ou sont laissés à discrétion de chacun |
|   | sont centralisés dans un fichier, ou tous connus par une ou plusieurs personnes |
|   | sont partagés selon le besoin d'accéder à une machine |
| **X** | **font 12 caractères ou plus, et possèdent au moins une majuscule, une minuscule, un chiffre et un caractère spécial** |
|   | ne forment pas de mots ou de dates cohérentes |
|   | sont des phrases complètes |
|   | sont changés régulièrement, tous les ans ou tous les deux ans |
| **X** | **sont enregistrés dans un gestionnaire de mots de passe** |
|   | sont sauvegardés dans les navigateurs Web |
|   | sont différents pour chaque application, même pour un utilisateur |

|  |  |
| --- | --- |
| **9** | **Les réseaux sans fil** |
|   | ne sont pas activés dans l'organisme |
|   | sont utilisés sans distinction par les personnes externes et internes à l'entreprise |
|   | sont donnés sans distinction à des externes comme des personnes internes à l'organisme et sans récolte d'identité |
| **X** | **sont protégés par des mots de passe très longs (plus de 20 caractères)**  |
| **X** | **des imprimantes sont protégées par un mot de passe** |

|  |  |
| --- | --- |
| **10** | **Un logiciel antivirus** |
|   | n'est pas utilisé |
| **X** | **est installé sur toutes les machines de bureau et les ordinateurs portables** |
|   | est mis à jour sur toutes les machines, de façon automatique comme manuelle |
|   | est activé et protège les machines de façon proactive |
|   | est installé sur tous les téléphones mobiles connectés au réseau |
|   | est utilisé de temps à autre pour analyser la bonne santé d'une machine, même sans événements externes |
| **X** | **est utilisé pour analyser le réseau en cas de suspicion d'infection** |

|  |  |
| --- | --- |
| **11** | **Les postes utilisateurs sont** |
|   | laissés sans consignes à discrétion des utilisateurs ; |
|   | mis à jour de façon automatique ou manuelle (logiciels comme système d'exploitation) ; |
|   | soumis aux droits d'administration afin de limiter l’installation de logiciels ; |
| **X** | **soumis à des règles strictes concernant les téléchargement et les installation de programmes ;** |
| **X** | **verrouillés en cas d’absence de l’utilisateur, même pour une durée très courte** |

|  |  |
| --- | --- |
| **12** | **Les sauvegardes** |
|   | Sont inexistantes ou ne fonctionnent pas |
| **X** | **Sont réalisées par le(s) prestataire(s) informatiques** |
|   | concernent toutes les données de l’entreprises et sont réalisées de manière exhaustives. |
| **X** | **sont programmées de manière quotidienne** |
| **X** | **permettent de remonter plusieurs semaines en arrière**  |
| **X** | **sont localisées à l’extérieur de l’entreprise** |
| **X** | **sont déconnectées après chaque transfert de données** |
| **X** | **font l’objet de tests périodiques** |
| **X** | **Sont chiffrées, pour éviter tout accès non autorisé aux données** |

|  |  |
| --- | --- |
| **13** | **La pratique du BYOD (Bring your own device) dans l'environnement professionnel (réseau connecté au serveur)** |
|   | est interdite ou impossible dans l'organisme |
| **X** | **est soumise à des règles précises, particulièrement en cas d'insertion sur le réseau interne de l'organisme** |
|   | est soumise à un contrôle strict |
| **X** | **a été expliquée aux employés à travers des formations ou des explications** |

Page web résultats :

## Résumé:

Voici la liste des recommandations qui vous permettront d’améliorer le niveau sécurité de l'information dans votre entreprise, à condition que vos réponses reflètent correctement les pratiques internes de votre entreprise. Tenez également compte du fait qu’il s’agit d’une évaluation partielle de la sécurité de l’information et qu’elle ne constitue donc pas une analyse des risques complète.

#### Règles/Chartes

1. L'entreprise doit définir des règles pour éviter toutes incompréhensions.
2. Les règles (qu'elles soient organisationnelles, métier, ou à l'usage de l'informatique) doivent être connues et expliquées à tous.
3. Si une transmission orale suffit dans un cadre "familial", les règles devraient être mises dans une charte ou un règlement, écrites et signées par tous, particulièrement en cas de croissance.
4. Les règles écrites et signées ont l'avantage : - d'éviter les oublis. - d'avoir une preuve juridique que les règles sont connues.
5. Dans la mesure du possible, ses dernières doivent être simples et courtes surtout pour être attractive et lisible.
6. Les règles peuvent être accompagnées d’astuces, de tutoriaux ou d’outils permettant de les appliquer facilement. Il faut penser à l’ergonomie de la cybersécurité…
7. Parfois, des petites adaptations doivent être prévue selon le poste ou le rôle de l’employé, ou bien si le contrat est temporaire, par exemple.

#### GDPR

1. Le cycle de vie des données personnelles doit être accessible pour n'importe qui (registre de traitement) ; - Comment sont-elles obtenues ? - Comment sont-elles traitées ? - Comment sont-elles accessibles et par qui, sous quelles clauses ? - Comment sont-elles modifiables ? - Combien de temps sont-elles conservées ? - Comment sont-elles détruites ? Ce cycle devrait être décrit quelque part et accessible à tous (contrat de vente, site web, fichier présentable en cas d'interrogation ...).
2. Une autorisation doit être demandée pour le droit à l'image (droit de prendre le cliché comme sa diffusion), et les personnes doivent être informées de l’existence d'une vidéosurveillance.

#### Formations

1. Les formations métier sont importantes et doivent être mises régulièrement à jour pour s'assurer d'avoir les dernières pratiques et éviter les pertes de temps inutiles.
2. Des formations sur les logiciels utilisés de façon quotidienne évitent principalement les mauvaises gestions et les erreurs de manipulations.
3. Des formations faites en interne n'ont parfois pas le même impact que celles faites en externe, mais sont tout aussi valables, et parfois même plus appropriées pour la maîtrise du sujet et de la bonne orientation du discours.
4. Sensibiliser les utilisateurs à la sensibilité des informations manipulés pour attirer leur attention sur les protections à mettre en œuvre.

#### Télétravail/Mobilité

1. Une attention particulière doit être apportée à l'environnement visuel pour éviter les regards indiscrets ou de l'éventuel espionnage.
2. Le matériel doit être chiffré s'il contient des données confidentielles pour éviter toute perte de confidentialité.

#### Contrats (SLA/NDA)

1. Si les moyens et le contexte le permettent et le nécessitent, un contrat est nécessaire pour assurer la disponibilité, tant les informations nécessaires, que le matériel pour les manipuler.
2. Il faut régulièrement revoir les contrats assurant une certaine disponibilité pour s'assurer: - de ne pas se retrouver sans intervention dans un délai où cette dernière serait indispensable; - de ne pas surpayer un prestataire pour un temps d'intervention trop élevé; - que les services rendus sont d'un niveau de qualité suffisant à ce qui est nécessaire.

#### Nettoyage des Locaux

1. Des règles doivent être données pour principalement spécifier ce qu'il faut faire où éviter de toucher.
2. Il faut également un contrat de confidentialité, car il est souvent possible d'entendre ou de remarquer des données confidentielles, même si l'accès n'est pas spécifiquement officiel.
3. Pour éviter les problèmes de curiosité humaine, les documents confidentiels doivent être inaccessibles, surtout à première vue.
4. Le personnel d'entretien ne doit pas intervenir dans un local à accès restreint, comme une salle d'archive ou une salle serveur.

#### Mots de passe

1. Les mots de passe ne doivent pas former des mots ou des dates cohérentes pour qu'ils ne soient pas facilement devinables.
2. Des phrases complètes peuvent être utilisées comme mot de passe, même s'ils forment des mots complets.
3. Les mots de passe doivent être changés de temps à autre pour prévenir une possible fuite de ses dernières.
4. Les mots de passe réutilisés dans d'autres sites offrent plus de chance de divulgation. De plus, une seule perte de mot de passe suffit à compromettre la totalité des accès.

#### Antivirus

1. Ce dernier doit être mis à jour, au moins de façon automatique pour couvrir le plus de menaces possible.
2. Il doit être également activé en permanence pour protéger en continu la machine.
3. Tout appareil, y compris des appareils plus nomades comme les ordinateurs portables, les téléphones et les tablettes doivent avoir un antivirus, même ceux proposés par défaut dans les systèmes d'exploitation.
4. Dans l'idéal, il ne faut pas hésiter à faire des tests de temps à autre.

#### Postes Utilisateurs/Mises à jour

1. Une machine doit être le plus à jour possible pour éviter le plus de failles, et ainsi éviter au possible les attaques par intrusion dans le réseau. Si beaucoup de systèmes d'exploitation se mettent à jour sans aide particulière, les logiciels doivent recevoir une attention particulière.
2. Les droits d'administration peuvent être laissés à des utilisateurs avertis et informés des consignes pour utiliser leur machine, mais nécessitent des règles précises.

#### Sauvegardes

1. Les sauvegardes doivent concerner toutes les données de l'entreprise, et il est important d'en faire le rappel aux utilisateurs pour qu'ils puissent entreposer leurs données dans un endroit qui aura une telle copie.

#### BYOD

1. Il doit être sous un contrôle antiviral pour s'assurer d'éviter un maximum d'infection sur le réseau.