**Demande de dispense à l’application de certaines exigences des règlements Partie-IS conformément à l’IS.I/D.OR-200 (e)**

*Sur la base de l’analyse de risques menée par l’organisme, le risque vis-*à*-vis de la* sécurité *aérienne,* généré *par l’activité réalisée au titre de l’agrément XXX est limité* *au regard de l’exposition globale de l’organisme dans son activité quotidienne.*

*En cons*é*quence et* conformément à *l’IS.I/D.OR-200 (e) je soussigné, XX, Cadre/Dirigeant responsable de [Nom de l’organisme], organisme ATO/FSTD/CAT/SPO/NCC/CAMO/145/21G[[1]](#footnote-1) demande que l’exploitant soit dispensé de mettre en œuvre un Système de Management de la Sécurité de l’Information (SMSI) au titre de la Partie-IS.*

*Vous trouverez en pièce justificative l’analyse de risque, effectuée* *dans le cadre du Système de Gestion de la sécurité (SGS) qui a amené à conclure que le risque « sécurité de l’information » impactant les missions de* sécurité *aérienne de l’organisme est limité* *au regard de l’exposition globale de l’organisme dans son activité quotidienne.*

*Ainsi, je m’engage à :*

* *Gérer le risque « sécurité de l’information » comme un risque à part entière dans le cadre du SGS relatif à ces activités et donc à intégrer la gestion de la cybersécurité dans la politique SGS et dans le manuel et les procédures SGS appropriées,*
* *Me conformer aux exigences en matière de comptes rendus d’incidents énoncées dans le règlement (UE) No 376/2014,*
* *Considérer les bonnes pratiques extraites du Guide d’hygiène informatique de l’ANSSI – Niveau Standard (Voir Annexe II)* pour l’élaboration du plan d’actions ou du plan de traitement des risques *résultant des analyses de risques « sécurité de l’information » impactant la sécurité aérienne,*
* *Appliquer les dispositions de l’IS.I/D.200 (a)(13) de la Partie-IS,*
* *Réévaluer périodiquement (*à *l’issue du cycle d’audit de surveillance ou à une fréquence au moins égale à la durée du cycle de surveillance interne) ou* à *la suite d’un changement de contexte majeur, l’analyse de risque pour vérifier* *que les conditions d’obtention de la dispense sont toujours vérifiées,*
* *Garder* à *disposition de l’Autorité les éléments de preuve qui ont amené* à *conclure que le risque impactant les missions de* sécurité *aérienne est limité* *au regard de l’exposition globale de l’organisme dans son activité quotidienne.*

*A [lieu], le [date]*

*Signature du Dirigeant Responsable*

**Annexe I - Extrait des règlements Partie-IS, relatif à la dispense**

**Dispositions Partie-IS relative à la dispense d’application de certaines exigences de la Partie-IS**

**IS.I.OR.200 Système de gestion de la sécurité de l’information (SGSI)**

…//…

1. Sans préjudice de l’obligation de se conformer aux exigences en matière de comptes rendus énoncées dans le règlement (UE) n o 376/2014 et aux exigences du point IS.I.OR.200 a), point 13), l’organisme peut recevoir l’autorisation de l’autorité compétente de ne pas mettre en œuvre les exigences visées aux points a) à d), ni les exigences connexes figurant aux points IS.I.OR.205 à IS.I.OR.260, s’il démontre à la satisfaction de cette autorité que ses activités, ses installations et ses ressources, ainsi que les services qu’il exploite, fournit, reçoit et gère ne présentent aucun risque en matière de sécurité de l’information susceptible d’avoir une incidence sur la sécurité aérienne, ni pour lui-même ni pour d’autres organismes.

L’autorisation doit reposer sur une évaluation documentée des risques liés à la sécurité de l’information effectuée par l’organisme ou un tiers conformément au point IS.I.OR.205 et examinée et approuvée par son autorité compétente.

L’autorité compétente examinera le maintien de la validité de cette autorisation à l’issue du cycle d’audit de supervision applicable et chaque fois que des modifications sont mises en œuvre dans le cadre des travaux de l’organisme.

**Dispositions Partie-IS qu’un organisme dispensé doit malgré tout appliquer**

**IS.I.OR.200 Système de gestion de la sécurité de l’information (SGSI)**

1. Afin d’atteindre les objectifs énoncés à l’article 1 er , l’organisme doit établir, mettre en œuvre et entretenir un système de gestion de la sécurité de l’information (SGSI) qui garantit que l’organisme:

…//…

13) protège, sans préjudice des exigences applicables en matière de comptes rendus des incidents, la confidentialité de toute information que l’organisme aurait reçue d’autres organismes, en fonction de son niveau de sensibilité.

**Les exigences en matière de comptes rendus d’incidents énoncées dans le règlement (UE) N° 376/2014**

**Annexe II - Mesures de sécurité des systèmes d’information**

Le tableau ci-dessous résume les mesures de sécurité des systèmes d’information – **Niveau STANDARD** - à considérer pour l’élaboration du plan d’actions ou du plan de traitement des risques. Elles sont extraites du **Guide d’hygiène informatique[[2]](#footnote-2)** publié par l’ANSSI et constituent le socle minimal de sécurité des systèmes d’information.

|  | **Mesures de sécurité des systèmes d’information** | **Standard** |
| --- | --- | --- |
| **1** | Former les équipes opérationnelles à la sécurité des systèmes d’information | X |
| **2** | Sensibiliser les utilisateurs aux bonnes pratiques élémentaires de sécurité informatique | X |
| **3** | Maîtriser les risques de l’infogérance (sous-traitance des tâches informatiques) | X |
| **4** | Identifier les informations et serveurs les plus sensibles et maintenir un schéma du réseau | X |
| **5** | Disposer d’un inventaire exhaustif des comptes privilégiés et le maintenir à jour | X |
| **6** | Organiser les procédures d’arrivée, de départ et de changement de fonction des utilisateurs | X |
| **7** | Autoriser la connexion au réseau de l’entité aux seuls équipements maîtrisés | X |
| **8** | Identifier nommément chaque personne accédant au système et distinguer les rôles utilisateurs/administrateurs | X |
| **9** | Attribuer les bons droits sur les ressources sensibles du système d’information | X |
| **10** | Définir et vérifier des règles de choix et de dimensionnement des mots de passe | X |
| **11** | Protéger les mots de passe stockés sur les systèmes | X |
| **12** | Changer les éléments d’authentification par défaut sur les équipements et services | X |
| **13** | Privilégier lorsque c’est possible une authentification forte | X |
| **14** | Mettre en place un niveau de sécurité minimal sur l’ensemble du parc informatique | X |
| **15** | Se protéger des menaces relatives à l’utilisation de supports amovibles | X |
| **16** | Utiliser un outil de gestion centralisée afin d’homogénéiser les politiques de sécurité | X |
| **17** | Activer et configurer le pare-feu local des postes de travail | X |
| **18** | Chiffrer les données sensibles transmises par voie Internet | X |
| **19** | Segmenter le réseau et mettre en place un cloisonnement entre ces zones | X |
| **20** | S’assurer de la sécurité des réseaux d’accès Wi-Fi et de la séparation des usages | X |
| **21** | Utiliser des protocoles sécurisés dès qu’ils existent | X |
| **22** | Mettre en place une passerelle d’accès sécurisé à Internet | X |
| **23** | Cloisonner les services visibles depuis Internet du reste du système d’information | X |
| **25** | Sécuriser les interconnexions réseau dédiées avec les partenaires | X |
| **26** | Contrôler et protéger l’accès aux salles serveurs et aux locaux techniques | X |
| **27** | Interdire l’accès à Internet depuis les postes ou serveurs utilisés pour l’administration du système | X |
| **28** | Utiliser un réseau dédié et cloisonné pour l’administration du système d’information | X |
| **29** | Limiter au strict besoin opérationnel les droits d’administration sur les postes de travail | X |
| **30** | Prendre des mesures de sécurisation physique des terminaux nomades | X |
| **31** | Chiffrer les données sensibles, en particulier sur le matériel potentiellement perdable | X |
| **32** | Sécuriser la connexion réseau des postes utilisés en situation de nomadisme | X |
| **33** | Adopter des politiques de sécurité dédiées aux terminaux mobiles | X |
| **34** | Définir une politique de mise à jour des composants du système d’information | X |
| **35** | Anticiper la fin de la maintenance des logiciels et systèmes et limiter les adhérences logicielles | X |
| **36** | Activer et configurer les journaux des composants les plus importants | X |
| **37** | Définir et appliquer une politique de sauvegarde des composants critiques | X |
| **~~38~~** | ~~Procéder à des contrôles et audits de sécurité réguliers puis appliquer les actions correctives~~  | **~~Sans objet~~** |
| **39** | Désigner un référent en sécurité des systèmes d’information et le faire connaître auprès du personnel | X |
| **40** | Définir une procédure de gestion des incidents de sécurité | X |

1. *Sélectionner les mentions applicables* [↑](#footnote-ref-1)
2. *https://cyber.gouv.fr/publications/guide-dhygiene-informatique* [↑](#footnote-ref-2)