

PSSI Niv 3 DIRECTIVE Exigences marché

DIFFUSION RESTREINTE@DGAC

Tout ou partie de ce document à diffusion restreinte ne doit être communiqué qu'aux personnes ayant à en connaître le contenu pour les besoins de leurs fonctions.

Sa rediffusion est de la responsabilité des agents à qui il a été diffusé.

Approbation du document

	TITRE	NOM	DATE
REDACTION	DSNA/DTI/D/SMI	Gaëtan POLLET	12/09/2019 
VERIFICATION	MSQS/RSSI NA	Loïc ROBIN	12.09.2019 
APPROBATION	DGAC/RSSI DGAC	Jean CARLIOZ	16.09.2019 

Diffusion

MODE DE DIFFUSION / FORMAT	DESTINATAIRES
Diffusion simple / Document papier	
Diffusion simple / Document électronique (GEODE)	

Responsable document

DSNA/DTI/SMI

Date d'applicabilité du document

A la date de signature

Plan de classement

Emplacement sous GEODE : PSSI DGAC - /Documents/PSSI DGAC/Guides et Directives/



Relevé des modifications

ÉDITION	DATE	MOTIF DES CHANGEMENTS	REDACTEUR
V3R0	25/02/2019	Version DTI mise à jour suite PSSI	Vivien MALERBA
V3R1	05/06/2019	Renvoi au CCAP pour les exigences concernant la confidentialité des données	Vivien MALERBA

Table des matières

1	INTRODUCTION ET CONTEXTE	5
2	PILOTAGE & GESTION DES INTERVENANTS.....	6
2.1	Pilotage	6
2.2	intervenants du titulaire	7
3	PROTECTION DES DONNEES	9
4	INTERVENTIONS SUR SITE DSNA	10
5	INFRASTRUCTURE TECHNIQUE	11
5.1	Poste de travail des intervenants	11
5.2	VPN	12

1 INTRODUCTION ET CONTEXTE

Ce document recense les exigences globales exprimées par la DGAC en matière de Sécurité des Systèmes d'Information (SSI); Ce document définit les exigences SSI par défaut à prendre en compte par le titulaire du marché et ce quel que soit l'objet du marché. Ce document peut donc être intégré à l'ensemble des CCTP produits pour les marchés DGAC.

Ces exigences sont réparties selon plusieurs axes :

1. **Pilotage** : Mise à disposition de la PSSI du titulaire sur les activités concernées par l'objet du marché, Désignation d'un correspondant dédié sur les aspects SSI, rédaction d'un plan d'assurance sûreté sur les activités objet du marché,
2. **Intervenants du titulaire** : Décrit les exigences à prendre en compte par le titulaire vis-à-vis de ces personnels en termes de sensibilisation et de maîtrise de la confidentialité,
3. **Protection des données** : Décrit l'ensemble des exigences relatives à la confidentialité des informations transmises, traitées, stockées ou hébergées par le titulaire,
4. **Intervention sur sites DSNA** : décrit les exigences en lien avec la conformité des règles DSNA en la matière (habilitation, accès aux sites, etc.)
5. **Infrastructures techniques** : décrit l'ensemble des exigences en lien avec les outils et infrastructures mis en œuvre par le titulaire sur le SI GP de la DSNA pour réaliser les activités objet du marché (poste de travaux, mise en œuvre du VPN)

Dans le cas d'un marché ayant pour l'objet **l'acquisition ou le développement d'un système ou constituant du SI NA ou du SI GP**, ce référentiel d'exigences est complété par le document « PSSI DGAC – Guide - Acquisition de systèmes du SI NA ou SI GP » qui définit l'ensemble des exigences SSI en terme organisationnel et techniques spécifiques à cette activité.

En outre, d'autres exigences (exprimées dans le reste de la consultation, type CCTP) peuvent compléter cette liste pour répondre à des besoins spécifiques en matière de SSI, notamment lorsque l'objet de la prestation est la production et/ou l'exploitation de logiciels.

Dans ce document, le terme « exigences SSI » fait référence à toutes les exigences SSI (celles exprimées dans ce document et celles éventuelles exprimées dans le reste du dossier de consultation).

L'ensemble des exigences SSI est à prendre en compte par l'industriel qui doit afficher sa conformité ou son niveau de conformité en réponse à ce référentiel d'exigences.

En cas de difficulté (d'ordre technique par exemple), ou dans un contexte ou pour un besoin spécifique, le titulaire peut adresser à la DTI une demande de dérogation, argumentée, à une ou plusieurs exigences. La DTI se réserve le droit de refuser ou d'accepter chaque demande (éventuellement en fixant une période de validité à la dérogation accordée).

2 PILOTAGE & GESTION DES INTERVENANTS

2.1 PILOTAGE

Exi_01. Le titulaire **DOIT** définir, appliquer et mettre à disposition de la DGAC une Politique de Sécurité des Systèmes d'Information et l'organisation associée lui permettant de mettre en œuvre et de s'assurer de la prise en compte des exigences SSI dans le cadre des activités qui lui sont confiées.

Exi_02. Le titulaire **DOIT** identifier un responsable sûreté, responsable de l'application des exigences SSI et correspondant privilégié de la DGAC sur ce sujet. Tout changement de responsable doit être signalé à la DGAC.

Exi_03. Le titulaire **DOIT** notifier à l'ASSI de l'entité tout incident SSI sur son système d'information pouvant impacter les activités réalisées pour le compte de la DGAC, ou le système d'information de la DGAC, dans un délai maximal de 48h ouvré.

Exi_04. Le titulaire **DOIT** notifier à l'ASSI de l'entité tout incident SSI sur son système d'information pouvant impacter les activités réalisées pour le compte de la DGAC, ou le système d'information de la DGAC, dans un délai maximal de 48h ouvré.

Exi_05. Le titulaire **DOIT** se soumettre à tout audit de la DGAC ou mandaté par la DGAC portant sur le respect et la mise en œuvre des exigences SSI sur les activités et prestations, objet du marché.

Exi_06. Le titulaire **DOIT** réaliser, maintenir et livrer un Plan de Gestion Sûreté de l'information (ISMP – Information Security Management Plan) listant et décrivant toutes les mesures mises en œuvre pour respecter les exigences SSI.

Exi_07. Le titulaire **DOIT** Identifier un correspondant à la Protection des Données pour le périmètre de la prestation. Tout changement doit être signalé à la DGAC.

2.2 INTERVENANTS DU TITULAIRE

Exi_08. Les exigences, procédures et contraintes de sureté exprimées dans l'ICMP **DOIVENT** s'appliquer au Fournisseur ainsi qu'à l'ensemble des parties impliquées dans l'exécution du contrat : sous-traitants, cotraitants, prestataires du Fournisseur, etc.

Exi_09. Le titulaire **DOIT** établir et maintenir à jour une liste nominative des intervenants sur les activités et prestations, qui accèdent au système d'informations de la DGAC (sur site DGAC ou via des services offerts à distance par la DGAC) précisant leur rôle sur la prestation; cette liste doit être communiquée à la DGAC à chaque arrivée et/ou départ d'un intervenant.

Exi_10. Le titulaire **DOIT** assurer la sensibilisation de ses personnels en matière de SSI :
- en déclinant dans sa charte informatique interne (ou autre document interne jouant ce rôle) l'ensemble des exigences SSI énoncées dans ce document et les mesures de sûreté associées,
- en s'assurant que chaque personnel intervenant sur l'activité objet du marché, ait pris connaissance et approuvé la dite charte informatique applicable.

Exi_11. Chaque intervenant du titulaire qui accède au système d'information de la DGAC **DOIT** suivre une session de sensibilisation à la sécurité des systèmes d'information organisée par la DGAC.

NOTA :

La DGAC se réserve le droit de refuser l'intervention d'une personne (personnel du titulaire ou d'un sous-traitant) si elle juge que celle-ci représente potentiellement une menace (la DGAC n'étant pas dans l'obligation de produire une justification auprès du titulaire).

Exi_12. Le titulaire **DOIT** s'assurer que ses intervenants et personnels respectent les exigences ci-dessous :

- ne pas fournir sur Internet (réseaux sociaux, forums, ...) des informations relatives à son activité professionnelle pour le compte de la DGAC (ce qui ne l'empêche pas par exemple de faire état de ses compétences et expériences ou de mentionner le fait de travailler ou avoir travaillé pour la DGAC) ;
- respecter les critères de gestion des mots de passe (robustesse, renouvellement) imposés par la DGAC, et ne jamais utiliser de mot de passe similaire à ceux qu'il utilise dans la sphère privée ; ;
- ne jamais divulguer son (ou ses) mot(s) de passe ou code PIN à qui que ce soit, ni utiliser un système d'information au nom d'une autre personne (pas d'usurpation d'identité);

- *changer son mot de passe ou code PIN dès qu'il a connaissance d'un risque d'utilisation frauduleuse (par ex. suite à intrusion sur PC, compromission d'un mot de passe, etc.) ;*
- *ne jamais stocker de mot de passe « en clair » où que ce soit (post-it, fichier texte, etc.) ;*

3 PROTECTION DES DONNEES

En référence aux exigences de confidentialité des données mentionnées dans le CCAP, le titulaire explicitera, dans l'ISMP, les processus et mesures techniques mis en œuvre afin de garantir le respect de ces exigences, ainsi que les moyens de vérification de leur bonne application.

4 INTERVENTIONS SUR SITE DSNA

Exi_13. Lors d'intervention sur un site DGAC (donc y compris la DTI), le titulaire DOIT prendre connaissance et respecter le règlement intérieur du site DGAC concerné, ainsi que les consignes spécifiques en matière de contrôle d'accès, de sûreté physique, de SSI.

Exi_14. Si requis par les règles en vigueur sur site, les intervenants DOIVENT disposer de titre de circulation et/ou d'habilitation pour pouvoir accéder physiquement au site.

La DSNA sensibilise ici le titulaire que le délai de prise en compte demandes d'accès de circulation ou d'habilitation sont variables d'un site un autre et sont de l'ordre de 2 mois.

Exi_15. En cas d'intervention sur un site DGAC, le titulaire ne DOIT connecter aucun équipement ou matériel non DSNA – incluant des matériels sous responsabilité du titulaire, PCs, smartphones, tablettes, équipements réseau, ou périphériques externes - au système d'information de la DGAC, et ce quel que soit le mode de connexion du dit équipement à l'exception des réseaux réservés à cet usage tels que des réseaux invités ou des réseaux Wifi dédiés ;

Exi_16. Dans le cas de l'utilisation d'un PC libre-service mis à disposition par la DGAC, le titulaire DOIT supprimer du PC les fichiers temporaires et les fichiers de travail qui auront été créés.

5 INFRASTRUCTURE TECHNIQUE

5.1 POSTE DE TRAVAIL DES INTERVENANTS

Ce chapitre identifie les exigences à respecter par le titulaire dans le cas où ce dernier met à disposition de ses intervenants, des postes de travail pouvant contenir des données DGAC.

Exi_17. Les postes du travail mis à disposition par le titulaire DOIVENT être équipés d'un système d'exploitation supporté par l'éditeur du logiciel qui fournit les correctifs de sécurité.

Exi_18. Les postes du travail mis à disposition par le titulaire DOIVENT être configurés pour fonctionner selon le principe du moindre privilège. En particulier les utilisateurs ne doivent pas travailler avec des privilèges d'administration (i.e. pas de session graphique interactive avec un compte privilégié). Pour les postes Windows, si besoin justifié (par ex. pour installer des logiciels, ou des imprimantes), il est recommandé de créer un second compte local disposant de privilèges d'administration et de n'utiliser ce compte que pour des besoins spécifiques (ne pas avoir recours à la technologie UAC).

Exi_19. les correctifs de sécurité DOIVENT être appliqués systématiquement dès leur publication par les éditeurs concernés, pour le système d'exploitation et les logiciels installés dans un délai de 5 jours ouvrés maximum (par exemple le cas échéant : navigateurs Web et leurs extensions, logiciel de messagerie, lecteurs PDF, lecteurs vidéo, outils métier, etc.) En cas d'alerte du CERT-FR, lorsqu'aucun correctif n'est disponible, les recommandations de l'éditeur ou de l'ANSSI doivent être mises en œuvre (suivant l'exposition au risque).

Exi_20. Le titulaire DOIT :

- chiffrer intégral du ou des disques internes (les logiciels Cryhcod de Prim'X pour Windows, Filevault pour MacOSX et LUKS pour Linux sont recommandés);
- activer un firewall pour filtrer toute connexion non souhaitée (notamment toutes les connexions entrantes).

Exi_21. Le titulaire DOIT équiper les postes de travail sous OS WINDOWS d'un antivirus actif et à jour vis-à-vis des bases de signatures.

Le titulaire détaillera dans sa réponse technique la manière dont il s'assure du bon fonctionnement de ce composant et comment il gère les alertes ainsi remontées ;

NOTA :

Il est recommandé de désactiver, dans les navigateurs Web utilisés, les modules complémentaires et greffons non strictement nécessaire aux missions des intervenants. Il est aussi recommandé d'activer l'option « Click to Play » qui requiert une intervention de l'utilisateur avant d'exécuter les greffons.

Le titulaire détaillera dans l'ISMP les processus et mesures techniques mis en œuvre afin de garantir le respect de ces exigences, ainsi que les moyens de vérification de leur bonne application.

5.2 VPN

Exi_22. En cas de mise en place d'un VPN entre la DGAC et le site du titulaire, celui-ci doit nommer un correspondant technique responsable de la mise en œuvre technique du VPN (configuration du VPN, configuration réseau, configuration des PC des intervenants utilisant le VPN, conservation des clés de chiffrement fournies par la DGAC, etc.). Ce correspondant technique est le contact en cas de dysfonctionnement (détecté par la DGAC ou par le titulaire).

Exi_23. Le titulaire DOIT informer la DGAC de tout changement du correspondant technique dans un délai de 5 jours ouvrés maximum.

Exi_24. Le titulaire DOIT informer la DGAC lorsque le VPN n'est plus utilisé afin qu'il puisse être désactivé, et ce dans un délai de 5 jours ouvrés maximum.

Exi_25. Le titulaire DOIT protéger les éléments de configuration du VPN (limitation d'accès aux équipements réseau qui implémentent le VPN et stockage sécurisé de la clé de chiffrement).

Le titulaire détaillera dans sa réponse technique les moyens mis en œuvre pour cette protection.

Exi_26. le titulaire doit identifier les types de systèmes ayant la capacité réseau à se connecter, via le VPN avec la DGAC, aux services offerts par la DGAC via celui-ci, que ce soit directement ou par routage interne par l'infrastructure du titulaire (postes de travail des intervenants sur le SI de la DGAC, postes de travail d'autres personnels, serveurs, réseaux externes à l'entreprise).

Le titulaire détaillera, dans l'ISMP, les éléments techniques en réponse à ces exigences.