

**EXIGENCES DE SECURITE SIMPLIFIEES**

**DE L’ECONOMAT DES ARMEES**

Table des matières

[1. Documents de référence 3](#_Toc202956904)

[2. Référentiels de sécurité 3](#_Toc202956905)

[3. Introduction 3](#_Toc202956906)

[4. Parties prenantes 3](#_Toc202956907)

[5. Objet du document 3](#_Toc202956908)

[6. Description du système externalisé 3](#_Toc202956909)

[7. Organisation 5](#_Toc202956910)

[8. Responsabilités liées au PAS 7](#_Toc202956911)

[9. Procédure d’évolution du PAS 7](#_Toc202956912)

[10. Exigences et mesures de sécurité 7](#_Toc202956913)

[a. Mise en place : 7](#_Toc202956914)

[b. Transférabilité/Réversibilité : 8](#_Toc202956915)

# Documents de référence

|  |  |  |
| --- | --- | --- |
| Document de référence | Version | Publié(e) |
| Cahier des Clauses Techniques Particulières 2025-0375 | V |  |
| Cahier des Clauses Administratives Particulières 2025-0375 | V |  |
| Politique de la Sécurité des Systèmes d’Information de l’EdA (PSSI) | V 1.0 | 22/06/2020 |
| Politique de sécurité des données personnelles | V |  |

# Référentiels de sécurité

* Guide d’hygiène de l’ANSSI v2
* Règlement Général sur la Protection des Données référencée 2016/679 du 27 avril 2016

# Introduction

L’Economat des armées (EdA) fait le choix de confier à un tiers, tout ou partie d’une activité qui pourrait être réalisée en interne. Dans le domaine des systèmes d'information (SI), cette externalisation est appelée infogérance.

Ces prestations d’infogérance peuvent induire, en fonction du contexte dans lequel elles sont réalisées, des risques pour le système d'information (SI) comme pour les données (intégrité, disponibilité, confidentialité). On identifie trois grands domaines de risques pour l’EdA :

* La perte de maîtrise de son SI ;
* Les interventions à distance sur son SI ;
* L'hébergement mutualisé de son SI.

Il est donc indispensable que l’EdA s’adresse à des titulaires qui s'engagent en matière de sécurité.

# Parties prenantes

|  |  |
| --- | --- |
| Statut | Identification |
| Pouvoir adjudicateur | Economat des armées |
| Titulaire |  |
| Sous-traitants/co-traitants  *(Sociétés identifiées comme agissant pour le compte du candidat dans le cadre du présent marché ou accord cadre)* |  |
|  |
|  |
|  |
|  |

# Objet du document

Le présent document présente l'ensemble des exigences de sécurité et CyberSécurité imposées que le titulaire doit suivre afin de garantir un niveau de sécurité suffisant sur toutes les parties dont il a la responsabilité (Virtualisation, réseau, flux, matériels, …)..

# Description du système externalisé

Le présent marché est établi afin d’externaliser les activités suivantes :

*Le candidat décrit ici l’objet du marché*

Le projet de mise en place se décrit de la manière suivante :

*Le candidat décrit ici succinctement le projet qu’il envisage de réaliser pour la mise en place*

L’infogérance recouvre un large spectre de prestations dont le type de service dans le présent marché est :

*Le candidat sélectionne ici le ou les choix correspondant au type de prestations identifiée dans le contrat*

MCO (maintien en condition opérationnelle),

TMA (tierce maintenance applicative),

ASP (Application Service Provider),

SAAS (Software as a service),

MSSP (Managed Security Service Provider),

Autre : *(à expliciter)*

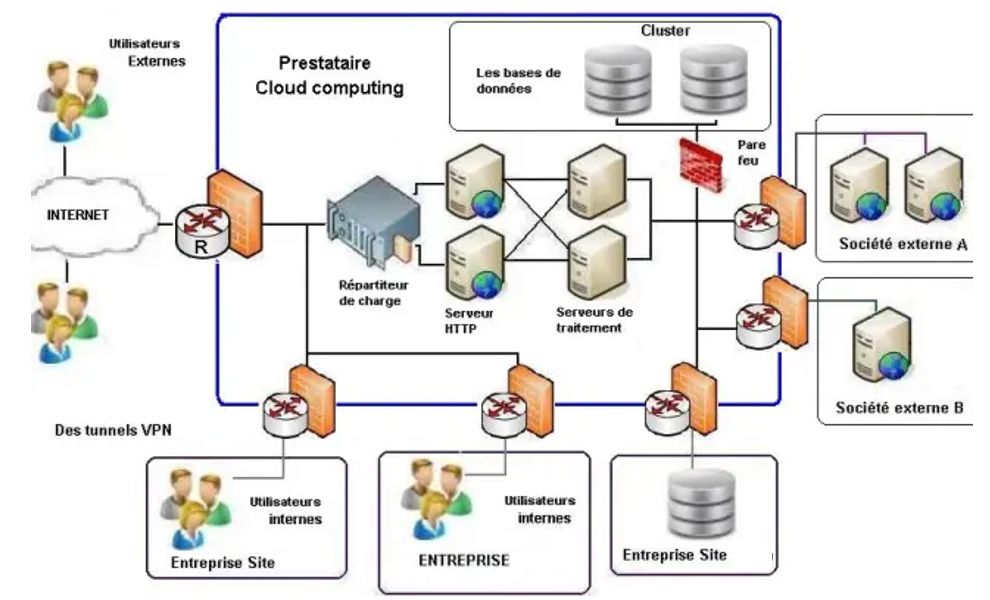
Le système faisant l’objet de l’opération d’externalisation se présente de la manière suivante :

*Le candidat présente succinctement le système faisant l’objet de l’opération d’externalisation.*

*L’accent sera mis sur les points qui justifient la mise en œuvre de mesures de sécurité.*

*Il n’est pas attendu ici une description détaillée de l’offre.*

*Exemple non exhaustif :*



# Organisation

*Le candidat indique l’organisation qu'il propose pour gérer la sécurité durant le présent marché ou accord cadre*

*On y trouve au minimum :*

*Le pouvoir adjudicateur agissant en tant que maitre d’ouvrage et le candidat en qualité de maitre d’œuvre.*

*Si des co-traitants, sous-traitants ou fournisseurs sont amenés à intervenir, il indique leur rôle et précise éventuellement les modalités de leur participation à la gestion de la sécurité du projet.*

*Le candidat décrit l’organisation mise en place pour assurer les relations avec le pouvoir adjudicateur concernant les aspects sécurité en renseignant les éléments suivants :*

**Comité de suivi de la sécurité** :

Fréquence :

Participants :

Modalités :

Périmètre du suivi :

**Organisation du candidat :**

Responsable sécurité,

Rôle et moyens ;

Responsables techniques et domaines associés

Identification des co-traitants et sous-traitants éventuels (compléter autant que nécessaire) ;

Société 1 :

Nationalité :

Rôle

Périmètre d’intervention :

**Diffusion du Plan d’assurance sécurité et des documents de suivi** *;*

**Audits, contrôles réalisés par la maîtrise d’ouvrage ou à la demande de celle-ci** *:*

Modalités :

Périmètre :

Exploitation des résultats :

**Procédure d’alerte en cas de dysfonctionnement :**

Contact :

Moyens de contact :

Délai d’information :

Communication du plan de traitement :

Communication de résolution :

# Responsabilités liées au PAS

Le titulaire, au travers de son responsable de la sécurité désigné, est responsable de la rédaction, de l’évolution et de l’application du Plan d’Assurance Sécurité pendant toute la durée du marché ou accord cadre concerné.

Le PAS doit être approuvé par le pouvoir adjudicateur ; sa bonne exécution est de la responsabilité du titulaire en tant que maître d’œuvre.

La cohérence de l’ensemble des mesures est analysée et réévaluée lors des réunions d’avancement (ou revues de pilotage).

# Procédure d’évolution du PAS

Le titulaire est responsable de la rédaction du PAS initial et de ses évolutions pour répondre aux exigences de sécurité du pouvoir adjudicateur, en qualité de donner d’ordre, pendant toute la durée du contrat.

Voici une liste (non exhaustive) des situations susceptibles d’entraîner une modification du PAS :

* Evolution du système d’information (configuration logicielle ou matérielle) ;
* Evolution de l’environnement du système d’information (locaux, personnels, procédures, etc.) ;
* Evolution de la sous-traitance ou de son périmètre ;
* Evolution du périmètre de l’opération ;
* Evolution de normes et législations ;
* Evolution du périmètre du marché/Accord cadre.

En cas d’évolution du système, de son environnement, ou du périmètre de l’opération d’externalisation, le titulaire vérifie si le PAS doit être modifié.

Si tel est le cas, il propose une modification au pouvoir adjudicateur.

Si cette modification est acceptée, le PAS est révisé et soumis au pouvoir adjudicateur pour validation formelle.

Sinon, le titulaire justifie la raison de ne pas apporter de modification et valide ce fait avec le pouvoir adjudicateur.

# Exigences et mesures de sécurité

Dans ce chapitre, le candidat décrit les mesures destinées à assurer la sécurité du système cible de l’opération d’externalisation pendant les différentes phases contractuelles : phase de mise en place, phase d’exploitation, phase de réversibilité ou fin de contrat.

## Mise en place

*Le candidat présente les mesures proposées pour sécuriser la phase de mise en place du système (matériels ou logiciels dans un projet d’externalisation)*

*Il décrit les procédures de contrôle de la sécurité mises en œuvre et identifie ses obligations de reporting au comité de suivi sécurité*

*Les exigences de sécurité formulées par le pouvoir adjudicateur indiquent le niveau de confidentialité maximum des informations manipulées.*

*Une liste de personnes susceptibles de participer à la mise en place pourra être rédigée et communiquée au pouvoir adjudicateur sur sa demande ainsi le pouvoir adjudicateur indiquera s’il juge nécessaire que le personnel soit soumis à une clause de confidentialité ou procéder à une habilitation*

## Transférabilité/Réversibilité

*Le candidat décrit ici comment il s’engage à apporter l’assistance nécessaire durant la période de migration pour faciliter le transfert des moyens de sécurité matériels et logiciels, et la reprise de leur exploitation par l’EdA, ou par un autre titulaire de service*

## Exploitation

Le candidat présente les mesures mises en place pour assurer la protection du système externalisé en réponse aux exigences identifiées par l’EdA.

|  |  |
| --- | --- |
| 1. Exigences relatives à la protection contre les logiciels malveillants | |
| 1.a | Une politique antivirale stricte est mise en place au niveau des serveurs dont le titulaire a la charge. |
| *Réponse du candidat :* | |
| 1.b | La mise à jour des signatures doit être automatique et d'une fréquence élevée (30 minutes). |
| *Réponse du candidat :* | |
| 1.c | La politique antivirale appliquée sur le système d’information du titulaire doit être précisée (y compris les postes de travail des exploitants). |
| *Réponse du candidat :* | |
| 1.d | Un contrôle de non contamination des serveurs doit être effectué périodiquement. Le candidat précise les modalités de mise en œuvre de ce contrôle. |
| *Réponse du candidat :* | |
| *Le candidat peut ajouter d’éventuels compléments :* | |

|  |  |
| --- | --- |
| 1. Exigences relatives aux mises à jour, correctifs de sécurité | |
| 2.a | Le titulaire applique les correctifs recommandés par les fournisseurs de solutions matérielles ou logicielles (logiciels système ou applicatifs, logiciels embarqués) sur tous les matériels dont il a la charge. |
| *Réponse du candidat :* | |
| 2.b | **En cas d’alerte grave** (attaque virale, faille critique) annoncée par le CERTA\* le correctif doit être appliqué dans un **délai de 24 heures** sur les infrastructures hébergeant le système de l’EdA (serveurs, pare-feu, routeurs ouverts vers l’extérieur). |
| *Réponse du candidat :* | |
| 2.c | Lorsqu’aucun correctif n’est disponible, le titulaire doit suivre les recommandations de l’éditeur ou du CERTA dans le cadre d’un contournement provisoire.  Si le contournement nécessite la désactivation d’une fonctionnalité indispensable au système, le titulaire s’engage à proposer des mesures permettant d’éviter l’exploitation de la vulnérabilité. |
| *Réponse du candidat :* | |
| 2.d | Le traitement des alertes mineures peut intervenir durant les périodes de maintenance hebdomadaires ou mensuelles. |
| *Réponse du candidat :* | |
| 2.e | Les passages de correctifs doivent être précédés d’une sauvegarde spécifique du système et des données qu’il contient, ainsi que de tests sur un environnement de pré production. |
| *Réponse du candidat :* | |
| 2.f | Le titulaire doit mettre à jour le dossier de définition avec la liste des correctifs de sécurité appliqués sur les serveurs et communiquer au donneur d’ordres la version actualisée du document. |
| *Réponse du candidat :* | |
| 2.g | La validation du bon fonctionnement du système se fait conjointement avec les équipes techniques du titulaire et le chef de projet du pouvoir adjudicateur responsable de l’application hébergée. |
| *Réponse du candidat :* | |
| 2.i | Le titulaire s’engage à fournir une adresse mail, un numéro de téléphone et les périodes correspondantes d’opération (H24, heures ouvrables, …) permettant au maître d’ouvrage de suivre le traitement d’une alerte |
| *Réponse du candidat :* | |
| *Le candidat peut ajouter d’éventuels compléments :* | |

|  |  |  |
| --- | --- | --- |
| 1. Exigences relatives aux sauvegardes et restaurations | | |
| 3.a | Une politique de sauvegarde doit être appliquée pour les données confiées au titulaire ainsi que les informations essentielles au bon fonctionnement du SI dont il a la responsabilité (configuration des équipements, VM…) |
| *Réponse du candidat :* | |
| 3.b | Le titulaire doit prendre toutes les mesures qui s’imposent en termes de sauvegarde et de restauration pour se conformer au niveau de service exigé. |
| *Réponse du candidat :* | |
| 3.c | Les opérations de sauvegardes donnent lieu à un compte-rendu quotidien par messagerie avec indicateur de réussite ou d’échec. |
| *Réponse du candidat :* | |
| 3.d | La fiabilité des sauvegardes est mise à l’épreuve par des tests de restauration mensuels, dont les rapports sont communiqués dans les 15 jours suivant les tests. |
| *Réponse du candidat :* | |
| 3.e | Le titulaire doit prendre des mesures permettant de garantir la confidentialité des données relatives aux sauvegardes :   * confidentialité des flux lors des opérations de sauvegardes ; * stockage sécurisé des sauvegardes. |
| *Réponse du candidat :* | |

|  |  |  |
| --- | --- | --- |
| 1. Exigences relatives à la continuité d’activité | | |
| 4.a | Le titulaire doit prendre toutes les mesures nécessaires pour assurer la disponibilité du système d’information, conformément aux exigences définies dans la clause relative au niveau de service explicité dans le CCTP. |
| *Réponse du candidat :* | |

|  |  |  |
| --- | --- | --- |
| 1. Exigences relatives à l’authentification | | |
| 5.a | Pour chaque interface d’accès au système, (Interface Homme-Machine, interface entre applications) le titulaire doit fournir une documentation précisant :   * les mécanismes d’authentification mis en œuvre (protocoles, algorithmes de hachage et de chiffrement utilisés) ; * la liste exhaustive des comptes d’accès existants ainsi que des rôles et privilèges qui y sont associés. |
| *Réponse du candidat :* | |
| 5.b | Les interfaces d’accès aux fonctionnalités bas niveau (exemple : configuration du BIOS) doivent impérativement authentifier un utilisateur (mise en place d’un mot de passe pour l’utilitaire de configuration du BIOS). |
| *Réponse du candidat :* | |
| 5.c | Les identifiants des comptes d’accès sont nominatifs.  L’utilisation d’un même compte par plusieurs personnes n’est pas autorisée.  Si une contrainte justifie l’obligation d’utiliser un compte par plusieurs personnes, ceci doit être accepté par le pouvoir adjudicateur, et doit faire l’objet d’un suivi sous forme de dérogation de sécurité par le titulaire et de sa révision lors des instances de sécurité.  Dans ce cas, le candidat présente les mesures techniques et/ou organisationnelles pour garantir l’imputabilité. |
| *Réponse du candidat :* | |
| 5.d | L’utilisation de mots de passe constructeur ou par défaut est interdite. |
| *Réponse du candidat :* | |
| 5.e | L’utilisation de protocoles dont l’authentification est en clair est interdite |
| *Réponse du candidat :* | |
| 5.f | Les mots de passe doivent satisfaire aux contraintes de complexité suivantes :   * Avoir une longueur minimale de 10 caractères (sauf limitation technique) ; * Comporter au minimum une majuscule, un chiffre et un caractère spécial ; * Ne pas être vulnérables aux attaques par dictionnaire. |
| *Réponse du candidat :* | |
| 5.g | Le stockage des mots de passe doit être sécurisé en termes d’intégrité et de confidentialité et de façon dématérialisée, dans un gestionnaire de mot de passe disposant d’un visa de sécurité ANSSI |
| *Réponse du candidat :* | |
| *Le candidat peut ajouter d’éventuels compléments :* | |