

Depuis 1971 |

Centre d'études et de recherches sur les qualifications
Site École centrale méditerranée - Plot 3

38 rue Frédéric Joliot Curie, CS 80377

13455 Marseille Cedex 13

www.cereq.fr

Marché à procédure adaptée n°2025-02-SUN1

EXTERNALISATION DES SAUVEGARDES

PLAN D'ASSURANCE SÉCURITÉ

Annexe au CADRE DE MEMOIRE TECHNIQUE

En tant qu'établissement public, producteur de données, le Céreq est fortement concerné par la sécurisation de système d'information. C'est dans ce cadre qu'il fait le choix d'externaliser ses sauvegardes auprès d'un prestataire spécialisé.

Le présent **Plan d'Assurance Sécurité (PAS)** a pour objectif de formaliser les exigences, les mesures et les engagements de sécurité relatifs à la prestation d'externalisation des sauvegardes informatiques.

Il pose un cadre de référence partagé entre le Céreq et le titulaire, décrivant les attentes du Céreq en termes de :

- méthodes et procédures de sécurité informatique mises en place ;
- garanties techniques et organisationnelles assurant la confidentialité, l'intégrité et la disponibilité des informations ;
- modalités de gestion des risques, notamment en cas d'incident ou d'attaque.

Les engagements du Céreq vis-à-vis du prestataire sont écrits en fin de document.

Préambule

Ce Plan d'Assurance Sécurité (PAS) est établi spécifiquement pour la prestation d'externalisation des sauvegardes du Céreq et des sauvegardes immuables d'une sélection de serveurs jugés critiques.

Dans le cadre de cette prestation, le prestataire s'engage à ce que l'ensemble des sauvegardes du Céreq soit hébergé en France.

Le PAS pourra être revu autant que de besoin pour s'adapter aux évolutions réglementaires et / ou des risques cyber qui pourraient survenir pendant la durée du marché.

Sommaire

Préambule	1
Méthodes et procédures de sécurité informatique mises en place	3
Sécurité des données	3
Contrôle d'accès	3
Sécurisation des infrastructures.....	3
Garanties techniques et organisationnelles assurant la confidentialité, l'intégrité et la disponibilité des informations.....	3
Respect des réglementations	3
Confidentialité	3
Organisation et procédures.....	3
Réversibilité et restitution des données en fin de marché	4
Modalités de prévention et gestion des risques, notamment en cas d'incident ou d'attaque	4
Politique de sauvegarde	4
Tests de restauration.....	4
Plan de reprise d'activité (PRA)	4
Détection et surveillance.....	4
Notification et communication	4
Engagements de reprise.....	4
Les engagements du Céreq vis-à-vis du prestataire.....	5

Méthodes et procédures de sécurité informatique mises en place

Le prestataire s'engage à disposer ou mettre en œuvre un ensemble de mesures de sécurité conformes aux bonnes pratiques du secteur et aux exigences réglementaires.

Sécurité des données

- Chiffrement des données : toutes les données sont chiffrées à l'aide d'algorithmes robustes lors de leur transfert et de leur stockage (voir les recommandations de l'ANSSI).
- Séparation des environnements : les données du Céreq sont isolées des autres clients via des mécanismes de cloisonnement logique ou physique.
- Protection contre la perte et la corruption : des mécanismes de vérification d'intégrité sont utilisés pour garantir la fiabilité des sauvegardes.

Contrôle d'accès

- Gestion des droits : les accès sont accordés selon le principe du moindre privilège et régulièrement révisés.
- Traçabilité des accès : toutes les connexions et actions sont journalisées et conservées selon les durées légales.

Sécurisation des infrastructures

- Protection réseau : pare-feu, systèmes de détection/prévention d'intrusion (IDS/IPS), segmentation réseau.
- Surveillance continue : supervision des systèmes 24/7 avec alertes en cas d'anomalie ou de tentative d'intrusion.
- Mise à jour et patch management : les systèmes sont régulièrement mis à jour pour corriger les vulnérabilités connues.

Garanties techniques et organisationnelles assurant la confidentialité, l'intégrité et la disponibilité des informations

Le prestataire est responsable de la sécurité des données confiées par le Céreq dans le cadre de la prestation. Concernant la confidentialité, l'intégrité et la disponibilité des informations, le prestataire s'engage à respecter les réglementations et éléments listés ci-après.

Respect des réglementations

- Le Règlement Général sur la Protection des Données (RGPD) pour les données personnelles.
- Les normes de sécurité reconnues (ex. : ISO/IEC 27001, ISO/IEC 22301).

Confidentialité

- Non-divulgence des informations traitées ou stockées.
- Interdiction d'usage des données à des fins personnelles ou non autorisées.
- Engagements de confidentialité individuels du personnel.

Organisation et procédures

- Politique de sécurité : le prestataire dispose d'une politique de sécurité formalisée et communiquée à ses équipes.
- Formation du personnel : les collaborateurs sont formés aux bonnes pratiques de sécurité et à la protection des données.
- Gestion des incidents : un processus structuré de gestion des incidents est en place, incluant la notification au Céreq en cas de violation de données.

Réversibilité et restitution des données en fin de marché

- Restitution de données sauvegardées dans un format exploitable conformément aux besoins définis dans le CCATP (page 9).
- Suppression toutes les copies résiduelles dans ses systèmes à l'issue d'un délai de 1 mois après la fin du marché.

Modalités de prévention et gestion des risques, notamment en cas d'incident ou d'attaque

Le prestataire s'engage à disposer de procédures visant à détecter, traiter et résoudre rapidement tout événement susceptible d'affecter la sécurité, l'intégrité ou la disponibilité des données sauvegardées.

Politique de sauvegarde

- Fréquence des sauvegardes : les données sont sauvegardées selon une politique définie en fonction de leur criticité.
- Durée de rétention : les sauvegardes sont conservées pendant une période conforme aux exigences réglementaires et aux besoins opérationnels du Céreq.
- Multiplication des copies : les sauvegardes sont répliquées sur plusieurs sites géographiques pour limiter les risques liés à une perte physique.

Tests de restauration

- Tests réguliers : des tests de restauration sont effectués à intervalles définis pour vérifier l'intégrité des sauvegardes et la capacité à restaurer les données dans les délais requis.
- Documentation des procédures : les procédures de restauration sont formalisées, documentées et accessibles aux équipes concernées.

Plan de reprise d'activité (PRA)

- Scénarios couverts : le PRA inclut les scénarios de défaillance technique, cyberattaque, sinistre physique ou erreur humaine.
- Ressources mobilisables : le prestataire garantit la disponibilité des ressources humaines et techniques nécessaires à la reprise.

Détection et surveillance

- Mise en œuvre de systèmes de monitoring en temps réel pour détecter les anomalies et comportements suspects.
- Utilisation de journaux d'événements et de systèmes de corrélation pour identifier les incidents de sécurité.
- Définition de seuils d'alerte et de déclenchement automatique des procédures de réponse.

Notification et communication

- Engagement du prestataire à notifier le Céreq dans les 24 heures en cas d'incident affectant les sauvegardes ou les données.
- Mise en place d'un point de contact dédié pour la gestion des incidents.
- Transmission d'un rapport d'incident détaillé incluant la nature de l'incident, les impacts, les mesures prises et les actions correctives.

Engagements de reprise

- RTO (Recovery Time Objective) : 48 à 72 heures pour restaurer les systèmes et reprendre l'activité après un incident.
- RPO (Recovery Point Objective) : 24 heures maximum pour les jours ouvrés (à l'exception du dimanche) de perte de données admissible entre deux sauvegardes.

Les engagements du Céreq vis-à-vis du prestataire

Dans le cadre de la prestation d'externalisation de ses sauvegardes, le Céreq s'engage à fournir ou informer le prestataire dans les cas listés ci-après.

- Fournir une description précise des données à sauvegarder (type, sensibilité, volumétrie)
- Fournir les accès techniques nécessaires dans un cadre sécurisé.
- Mettre à disposition les documents utiles (schémas d'architecture, procédures, etc.)
- Informer le prestataire de tout changement pouvant impacter la prestation (ex : migration, modification des systèmes, changement de politique de sécurité).
- Participer à la gestion des incidents de sécurité en lien avec les sauvegardes.
- Collaborer à la notification des violations de données si nécessaire.

Le Céreq s'engage à informer le prestataire dans les plus brefs délais de tout incident de sécurité sur ses infrastructures susceptibles d'avoir un impact sur la qualité, la fiabilité ou l'intégrité des sauvegardes confiées.

Signature du candidat :

Nom, prénom et qualité du signataire (*)	Lieu et date de signature	Signature

(*) Le signataire doit avoir le pouvoir d'engager la personne qu'il représente.