

PLAN D'ASSURANCE SÉCURITÉ

Marché Propreté

Validation

Nom	Entité	Date

Mise à jour

Version	Date	Auteur	Objet de modification

Table des matières

1 CADRE D'APPLICATION DU PAS.....	4
1.1 Préambule.....	4
1.2 Objet du PAS.....	4
1.3 Domaine d'application du PAS.....	4
1.4 Maîtrise du PAS.....	4
1.4.1 Approbation du PAS.....	4
1.4.2 Modification du PAS.....	5
2 DOCUMENTS APPLICABLES.....	6
3 GOUVERNANCE DE LA CYBERSÉCURITÉ.....	7
3.1 Organisation du TITULAIRE pour la cybersécurité.....	7
3.1.1 Parties prenantes.....	7
3.1.2 Rôles et missions.....	7
3.2 Organisation de la DiRIF pour la cybersécurité.....	7
3.2.1 Parties prenantes.....	7
3.2.2 Rôles et missions.....	7
3.3 Comitologie.....	7
3.4 Transférabilité et réversibilité.....	7
4 PROCESSUS RELATIFS À LA CYBERSÉCURITÉ.....	9
4.1 Processus de gestion des non-conformités.....	9
4.2 Processus de gestion des risques cybersécurité.....	9
4.3 Processus de gestion de crise cybersécurité.....	9
4.4 Formation et sensibilisation à la cybersécurité et à la confidentialité des données.....	9
4.5 Modalité d'échange d'informations.....	10
5 DISPOSITIONS RELATIVES À LA CYBERSÉCURITÉ.....	11
5.1 Gestion des identités et des accès.....	11
5.2 Cybersécurité des réseaux.....	11

5.3 Cybersécurité des systèmes et équipements.....	11
5.4 Maintien en conditions de sécurité.....	12
5.5 Hébergement, sécurité physique et environnementale.....	13
5.6 Journalisation et surveillance.....	13
5.7 Traitement des incidents cybersécurité.....	13
6 DISPOSITIONS RELATIVES AU PILOTAGE ET AUX CONTRÔLES DE LA CYBERSÉCURITÉ.....	14
6.1 Pilotage de la cybersécurité.....	14
6.2 Contrôle cybersécurité.....	16
6.2.1 Contrôles effectués par la DiRIF.....	16
6.2.2 Contrôles effectués par le TITULAIRE.....	16
7 ANNEXE : TERMES ET DÉFINITIONS.....	17

1 CADRE D'APPLICATION DU PAS

1.1 Préambule

Dans la suite du document, les termes de TITULAIRE et de SOUMISSIONNAIRE sont délibérément confondus.

1.2 Objet du PAS

La DiRIF a contracté avec le TITULAIRE dans le cadre du contrat relatif au Marché Propreté, compte tenu du savoir-faire et des compétences reconnues du TITULAIRE dans ce domaine.

Le Plan d'Assurance Sécurité (PAS) constitue une convention qui décrit les engagements de service et les dispositions d'assurance cybersécurité prises par le TITULAIRE pour assurer la prestation décrite dans le contrat. Ce plan est garant de la cybersécurité du service entre le TITULAIRE et la DiRIF.

Il présente l'ensemble des dispositifs que le TITULAIRE s'engage à mettre en œuvre, pour obtenir un service de qualité demandé par la DiRIF. Son but est de présenter les dispositions mises en œuvre par le TITULAIRE en termes d'organisation et de management de la cybersécurité.

L'ensemble des intervenants de la prestation doit prendre connaissance du présent PAS.

1.3 Domaine d'application du PAS

Le PAS couvre l'ensemble des missions opérationnelles réalisées au titre du contrat :

[Ici spécifier les missions ou renvoyer à un PAQ.]

1.4 Maîtrise du PAS

1.4.1 Approbation du PAS

Le PAS est, à l'issue de la phase d'initialisation et durant la vie du contrat :

- Approuvé en interne par le [réfèrent cybersécurité ou autres postes] du TITULAIRE

-
- Validé en comité de pilotage par le chargé de mission de la sécurité de la DiRIF

1.4.2 Modification du PAS

Toute modification du PAS est traitée conjointement entre le TITULAIRE et la DiRIF en comité de pilotage, à l'initiative de l'une des deux parties.

2 DOCUMENTS APPLICABLES

[Ici le TITULAIRE spécifie les documents et références applicables (ex. : Contrats, RGPD, PSSIE, Guides de l'ANSSI, ...).]

3 GOUVERNANCE DE LA CYBERSÉCURITÉ

3.1 Organisation du TITULAIRE pour la cybersécurité

3.1.1 Parties prenantes

Le TITULAIRE, pour la cybersécurité de la mission effectuée pour la DiRIF, est organisé comme suit :

[Ici le TITULAIRE spécifie son organisation pour la cybersécurité de la prestation.]

3.1.2 Rôles et missions

[Ici le TITULAIRE spécifie ses rôles et missions au titre de la cybersécurité de la prestation.]

3.2 Organisation de la DiRIF pour la cybersécurité

3.2.1 Parties prenantes

La DiRIF, pour le suivi de la cybersécurité de la mission effectuée par le TITULAIRE, est organisé comme suit :

[À remplir par la DiRIF lors de la contractualisation.]

3.2.2 Rôles et missions

[À remplir par la DiRIF lors de la contractualisation.]

3.3 Comitologie

Les exigences en matière de comitologie sont indiquées dans le CCTP.

L'organisation et les attendus seront inscrit au PAQ.

3.4 Transférabilité et réversibilité

[Ici le TITULAIRE spécifie les mesures techniques et organisationnelles mises en place garantissant la cybersécurité des données lors du transfert des prestations couvrant les domaines suivants :

- La gestion des accès et les habilitations,
- Le transfert de responsabilité,

-
- La fourniture d'informations nécessitant des mesures de protection adaptées,
 - La gestion de la continuité de l'activité,
 - Destruction des données.]

4 PROCESSUS RELATIFS À LA CYBERSÉCURITÉ

4.1 Processus de gestion des non-conformités

[Ici le TITULAIRE spécifie son processus pour traiter les écarts constatés avec le niveau d'exigence de cybersécurité requis par la DiRIF.]

Les demandes de dérogation du TITULAIRE seront transmises à la DiRIF qui aura en charge de les étudier et de déterminer si elles sont ou non recevables. Celles-ci feront dans tous les cas l'objet d'un plan d'action permettant de revenir à une situation non dérogatoire.

4.2 Processus de gestion des risques cybersécurité

[Ici le TITULAIRE spécifie son processus de gestion des risques cybersécurité en y incluant :

- Son organisation,
- Les indicateurs du processus,
- Les conditions dans lesquelles les risques sont traités en tenant compte des contraintes techniques et organisationnelles.]

4.3 Processus de gestion de crise cybersécurité

[Ici le TITULAIRE spécifie son processus de gestion de crise en y incluant :

- Son organisation,
- Les indicateurs du processus,
- L'application des mesures techniques,
- Les conditions dans lesquelles les mesures peuvent être appliquées en tenant compte des contraintes techniques et organisationnelles.]

4.4 Formation et sensibilisation à la cybersécurité et à la confidentialité des données

[Ici le TITULAIRE spécifie les dispositions relatives à la formation et à la sensibilisation à la cybersécurité de son personnel mises en place dans le cadre de la prestation.]

4.5 Modalité d'échange d'informations

[Ici le TITULAIRE spécifie les modalités de stockage et d'échanges d'informations qui permettent d'assurer la confidentialité et l'intégrité.]

5 DISPOSITIONS RELATIVES À LA CYBERSÉCURITÉ

5.1 Gestion des identités et des accès

[Ici le TITULAIRE spécifie les dispositions relatives aux thèmes suivants :

- Gestion des comptes d'administrations,
- Gestion des comptes individuels,
- Gestion des comptes de services,
- Recensement des comptes d'accès (autorisés à se connecter sur le SI),
- Application du principe du moindre privilège,
- Protection contre les attaques portant sur les authentifications,
- Modification des comptes par défaut.]

5.2 Cybersécurité des réseaux

[Ici le TITULAIRE spécifie les dispositions de son réseau relatives aux thèmes suivants :

- Cloisonnement,
- Filtrage,
- Durcissement de configuration des équipements réseaux,
- Accès distant,
 - Ségrégation des environnements entre les actifs de la DiRIF et celui des autres activités
 - Interconnexion entre le système du TITULAIRE et le système de la DiRIF.

Le cas échéant celui de la DiRIF si applicable.]

5.3 Cybersécurité des systèmes et équipements

Le TITULAIRE s'engage à ce que les produits du contrat soient, au jour de leur mise en production pour la DiRIF, dépourvus de toute faille, faiblesse ou défaut de conception portant atteinte à la cybersécurité.

[Ici le TITULAIRE spécifie les dispositions relatives aux thèmes suivants :

- Cybersécurité des postes de travail y compris les postes nomades et les postes partagés,
- Cybersécurité des serveurs,
- Cybersécurité des équipements,
- Cybersécurité des supports numériques,
- Contrôle d'innocuité des dispositifs connecté au réseau.]

5.4 Maintien en conditions de sécurité

[Ici le TITULAIRE spécifie les dispositions relatives aux thèmes suivants :

- Cartographie réseaux,
- Cartographie systèmes,
- Documentations relatives aux procédures et modes opératoires de la sécurité,
 - Gestion des mots de passe,
 - Gestion de la sauvegarde et du stockage des données et des codes sources,
- Protection et documentation des codes sources,
 - Disponibilité des données et des systèmes d'informations,
 - Mise en place d'une veille cybersécurité,
 - Gestion des mises à jour des logiciels et mise à jour des logiciels,
 - Gestion des systèmes obsolètes,
- Gestion des licences,
 - Règles de cybersécurité et exploitation, [L'installation, l'exploitation et l'administration des moyens mis en œuvre dans le cadre des prestations sont conformes aux bonnes pratiques et aux règles de cybersécurité et d'exploitation établies par la PSSIE. Toute exception fera l'objet d'un accord préalable écrit des équipes de l'acheteur]

5.5 Hébergement, sécurité physique et environnementale

[Ici le TITULAIRE spécifie les dispositions relatives aux thèmes suivants :

- Hébergement informatique,
- Localisation des données,
- Sécurité physique et environnementale.]

5.6 Journalisation et surveillance

[Ici le TITULAIRE spécifie les dispositions relatives aux thèmes suivants :

- Journalisation,
- Corrélation des journaux,
- Traçabilité des actions de développement,

Ces procédures devront notamment porter sur la journalisation des authentifications des utilisateurs à la gestion des comptes, à la gestion des droits d'accès et l'accès aux ressources du SI.]

5.7 Traitement des incidents cybersécurité

[Ici le TITULAIRE spécifie les dispositions relatives aux thèmes suivants :

- Remontée d'alerte,
- Enregistrement, traçabilité et gestion des incidents,
- Traitement des incidents cybersécurité,
- Base de connaissance.]

6 DISPOSITIONS RELATIVES AU PILOTAGE ET AUX CONTRÔLES DE LA CYBERSÉCURITÉ

6.1 Pilotage de la cybersécurité

[Ici le TITULAIRE spécifie les indicateurs de cybersécurité propres à la prestation, ainsi que les seuils qui doivent déclencher un plan d'actions correctifs en cas de non-respect. Les indicateurs suivants sont donnés à titre d'exemple ; à la cible, ils doivent être cohérents avec les dispositions de cybersécurité spécifiées dans le présent document.]

Indicateurs	Formule	Seuil	Fréquence
AUD-01 Audit et contrôle Application du plan de contrôle		90 %	Mensuelle
MCS-01 Patch Nombre de serveurs dont la version OS est à jour		100 %	Mensuelle
MCS-02 Disponibilité et continuité Application du plan de sauvegarde		100 %	Mensuelle
PRO-01 Gestion des dérogations [Ici spécifier un indicateur ad hoc]			
PRO-02 Gestion des risques [Ici spécifier un indicateur ad hoc]			

Indicateurs	Formule	Seuil	Fréquence
PRO-03 Gestion de crises [Ici spécifier un indicateur ad hoc]			
[À compléter]			

6.2 Contrôle cybersécurité

6.2.1 Contrôles effectués par la DiRIF

Le TITULAIRE garantit à la DiRIF qu'il est conforme à l'état de l'art de la cybersécurité pour les services fournis dans le cadre des prestations. À première demande, le TITULAIRE fournit la preuve de cette conformité sous quinze jours ouvrés.

La DiRIF se réserve le droit d'auditer ou de faire auditer par un tiers indépendant la cybersécurité des prestations du marché. À l'issue de l'audit, le rapport d'audit est soumis au TITULAIRE, incluant les mesures correctives à mettre en œuvre afin d'assurer la cybersécurité du marché.

Le TITULAIRE met en œuvre les mesures de cybersécurité correctives décidées d'un commun accord dans le délai précisé dans le plan d'actions défini en commun. Le suivi des actions de cybersécurité est régulièrement soumis à la DiRIF.

Si le rapport d'audit ne recommande pas explicitement les mesures à mettre en œuvre, ou si celles-ci ne peuvent raisonnablement être mises en œuvre dans de bonnes conditions, la DiRIF proposera les actions correctives nécessaires avec l'accord du TITULAIRE.

6.2.2 Contrôles effectués par le TITULAIRE

[Ici le TITULAIRE décrit les dispositions relatives aux contrôles cybersécurité, en phase nominale et en phase projet.]

7 ANNEXE : TERMES ET DÉFINITIONS

Termes	Définition
MIISST	Marché d'Infogérance de l'informatique support et de sécurité des tunnels d'Île-de-France
Système à jour	[Ici le TITULAIRE spécifie ce qui est considéré à jour en fonction du score CVSS de la vulnérabilité concernée]
[À compléter]	