Exigences de Sécurité complémentaires des Conditions Générales d'Achat Prestations Intellectuelles

*****

Table des matières

Chapitre 1 - Introduction

Le présent document (« Exigences de Sécurité ») complète les Conditions Générales d'Achat de Prestations Intellectuelles datées du 31 juillet 2013 (les « Conditions Générales ») et a pour objet d'énoncer les exigences de sécurité complémentaires que le Prestataire s'engage à respecter, et à faire respecter par son personnel et ses sous-traitants autorisés, dans le cadre d'une Commande régie par ces Conditions Générales afin que soient garantis la disponibilité, le contrôle de l'accès, la confidentialité, l'intégrité des Systèmes d'Information, ainsi que la traçabilité des actions réalisées sur ces Systèmes.

Les Exigences de Sécurité couvertes par les Conditions Générales s'appliquent à tout type de Prestations.
Les exigences de sécurité complémentaires décrites aux chapitres 4, 5 et 6 du présent document sont applicables selon la typologie des Prestations objet de la Commande ou du lot autonome et homogène :
- Le cahier des charges de chaque Commande, ou lot autonome et homogène, précisera les valeurs de caractéristiques des Prestations objet de la Commande ou du lot autonome et homogène selon la typologie définie au chapitre 2 ci-après.
- Les Exigences de Sécurité applicables à la Commande et/ou à chaque lot autonome et homogène seront définies préalablement à tout démarrage des Prestations suivant la matrice d'applicabilité décrite au chapitre 3 ci-après.

Les exigences de sécurité applicables à toute Commande devra faire l'objet d'une validation explicite préalable des Services de Sûreté et de Sécurité Système d'Informations de l'Acheteur. Toute dérogation aux Exigences de Sécurité devra également être soumise à l'accord préalable écrit de ces mêmes services.

En cas d'exigences multiples ayant le même objet, l'(les) exigence la(les) plus contraignante(s) pour le Prestataire s'applique(nt).

Pour assurer le respect des Exigences de Sécurité le Prestataire s'engage :

- à mettre en place un processus de suivi d'application de ces exigences pendant la durée d'exécution des Prestations,
- à accepter la réalisation d'audits dans les conditions décrites au chapitre 7 ci-après.

Les termes des Exigences de Sécurité désignés par une majuscule auront la signification précisée dans les Conditions Générales.

Chapitre 2 - Typologie des Commandes ou lots autonomes et homogènes

Les Exigences de Sécurité que doit respecter, et faire respecter, le Prestataire dépendent des caractéristiques des Prestations objet des Commandes ou lots autonomes et homogènes suivants :

- type de Prestations,
- niveau de responsabilité du Prestataire,
- type de moyens utilisés,
- implantation(s) géographique(s) du Prestataire pour l'exécution des Prestations,
- connexion ou non au réseau informatique de l'Acheteur,
- sensibilité de la Commande ou du lot autonome ou homogène.

2.1. Type de PRESTATIONS

Une Commande peut prévoir l'achat de plusieurs catégories de Prestations.
Ces catégories sont les suivantes :

- intégration de progiciels et logiciels,
- maintenance corrective (logicielle ou progicielle),
- pré-étude et conception de Systèmes d'Information,
- développement de logiciel et maintenance évolutive (sur logiciels ou progiciels),
- déploiement et industrialisation du Système d'Informations (valable pour maintenance corrective, évolutive, et développements logiciels),
- expertise technique.
- exécution de code à distance, télé-intervention
- gestion des sollicitations (centre d'appel)
- gestion de parc
- prise de main à distance postes de travail
- gestion des comptes / accès
- préparation des masters et des lots
- support de proximité(installation /support /maintenance /réforme)
- exploitation et administration de systèmes

2.2. Niveau de responsabilité du Prestataire

La maîtrise d'œuvre des Prestations pourra être de la responsabilité du Prestataire ou de l'Acheteur.

Les principes directeurs de sécurité sont définis par l'Acheteur, et leur déclinaison et leur mise en œuvre lors de l'exécution des Prestations incombent au maître d'œuvre des Prestations. Dans tous les cas, le Prestataire a l'obligation d'appliquer et de faire appliquer les Exigences de Sécurité définies.

2.3. Type de moyens utilisés

Les Exigences de Sécurité seront différentes selon que :

- le matériel et les logiciels utilisés dans le cadre de l'exécution des Prestations sont la propriété de l'Acheteur ou du Prestataire,
- l'installation, l'exploitation et l'administration de ces moyens sont de la responsabilité de l'Acheteur ou du Prestataire.
- le niveau de sensibilité des données traitées et/ou du réseau de l'Acheteur le nécessite.

Il convient de noter que les cas où les matériels et/ou les logiciels sont cédés par le Prestataire à l'Acheteur au titre de la Commande sont assimilés aux cas où ils appartiennent au Prestataire.

Nota : N'est pas couverte par ce paragraphe l'éventuelle liaison informatique au réseau informatique de l'Acheteur. Ce cas est traité à l'article 2.5. ci-après.

2.4. Implantation(s) géographique(s) du PRESTATAIRE

Le(s) lieu(x) d'exécution de la Commande ou du lot autonome et homogène détermine(nt) la prise en compte ou non de certaines Exigences de Sécurité.

Quatre types de lieux sont possibles :

- site de l'Acheteur (y compris établissement d'une entité juridique dont l'Acheteur est directement ou indirectement l'actionnaire majoritaire),
- locaux dédiés au Prestataire sur un site de l'Acheteur,
- site, n'appartenant pas à l'Acheteur, situé sur le territoire national,
- site, n'appartenant pas à l'Acheteur, situé hors du territoire national.

2.5. Connexion au réseau informatique DE L'ACHETEUR

La connexion au réseau informatique de l'Acheteur impliquera pour le Prestataire :

- l'application des Exigences de Sûreté (techniques et organisationnelles) de l'Acheteur dans l'exécution des Prestations,
- le respect des règles de sécurité des systèmes informatisés définies par l'Acheteur, notamment en matière d'architectures informatiques ou d'exploitation de systèmes.

2.6. Sensibilité de la Commande ou du lot autonome et homogène

On distingue quatre niveaux de sensibilité :

- Niveau 0 : domaine public.
- Niveau 1 : soumis aux règles normales de discrétion professionnelle,
- Niveau 2 : à diffusion limitée aux seules personnes ayant le besoin d'en connaître dans le cadre de l'exécution des Prestations et en fonction de leur rôle à ce titre,
- Niveau 3 : confidentiel, c'est-à-dire devant faire l'objet de mesures de protection spécifiques.

Chapitre 3 - Matrice d'applicabilité des Exigences de Sécurité

Les Exigences de Sécurité sont référencées de la façon suivante, yy étant un nombre compris entre 01 et 99 :

« ELE yy »	Exigences de Sécurité spécifiques du lieu d'exécution des prestations
« EPP yy »	Exigence de Protection Physique
« ESI yy »	Exigences de Sécurité des systèmes d'informations

Le premier tableau ci-dessous comporte les numéros des Exigences de Sécurité des systèmes d'Information, de la Sûreté ou du lieu d'exécution applicables pour tout type de Prestations :

Caractéristiques Prestations	Valeur de caractéristique	Lieu d'exécution	Sûreté	Systèmes d'Information
	CLAUSES :	**ELE**	**EPP**	**ESI**
Quelles qu'elles soient	Quelles qu'elles soient	01, 05, 06, 09	01, 02, 03, 04, 05	06, 08, 09, 13, 25, 28, 33 45,46,47,48,49, 50, 51, 53, 55, 56 62, 63, 64, 65, 66, 68, 69, 70, 58

La matrice ci-dessous comporte les Exigences de Sécurité des systèmes d'Information ou du lieu d'exécution applicables aux Prestations fournies par le Prestataire selon les caractéristiques de la Prestation objet de la Commande ou du lot :

Caractéristiques Prestations	Valeur de caractéristique	Lieu d'exécution	Sûreté	Systèmes d'Information
		ELE	**EPP**	**ESI**
Type de Prestations	Intégration de Progiciels et logiciels			01, 02, 04, 10, 11, 12, 37
	Maintenance corrective (logicielle et progicielle)			02, 03, 04, 05, 11, 30, 31, 34, 37
	Pré-étude et conception de systèmes d'Information			01, 04, 10, 11, 12, 37
	Développement de logiciels et maintenance évolutive (sur logiciels et progiciels)			01, 02, 04, 11, 12, 31, 34, 37
	Déploiement et industrialisation du système d'informations			02, 03, 05, 10, 11, 12, 31, 34, 37 59, 60
	Expertise technique			01, 02, 03, 04, 05, 10, 11, 12, 30, 31, 34, 35, 37 54, 59, 60, 61, 67
	Exécution de code à distance, télé-intervention			01, 02, 03, 05, 10, 11, 12, 34, 35, 36, 37 60, 67, 69
	Gestion des sollicitations (centre d'appel)			01, 02, 04, 05, 37
	Gestion de parc			01, 03, 10, 11, 12, 37

Caractéristiques Prestations	Valeur de caractéristique	Lieu d'exécution	Sûreté	Systèmes d'Information
		ELE	EPP	ESI
Types de prestations (suite)	Prise de main à distance postes de travail			01, 02, 10, 11, 12, 35, 37 60, 61 67, 69
	Gestion des comptes / accès			01, 10, 11, 12, 34, 35, 36, 37 52
	Préparation des masters et des lots			01, 02, 05, 10, 11, 12, 31, 34, 36, 37 54
	Support de proximité(installation /support /maintenance /réforme)			01, 02, 03, 05, 10, 11, 12, 30, 35, 37 54, 59, 60, 61 67
	Exploitation et administration de systèmes			01, 02, 03, 05, 10, 11, 12, 16, 17, 19, 24, 26, 27, 28, 30, 35, 37 52, 54, 59, 60, 61 67, 68, 69, 70
Niveau de responsabilité du Prestataire	Maîtrise d'œuvre assurée par le Prestataire			38, 39
	Maîtrise d'œuvre assurée par l'Acheteur			Sans objet
Type de moyens utilisés	Administré par l'Acheteur pendant la durée d'exécution des Prestations			10, 20
	Administré par le Prestataire, pendant la durée d'exécution des Prestations, et de propriété de l'Acheteur ou transféré à l'Acheteur en fin de Prestations			17, 20, 40, 44 52, 54, 59, 60, 61
	Administré par le Prestataire et sans transfert à L'Acheteur en fin de Prestations			23, 24, 36, 41, 52, 54,59, 60, 61
Implantation géographique du Prestataire pour l'exécution des Prestations	Site de l'Acheteur	08		26
	Locaux dédiés au Prestataire sur un site de l'Acheteur	03, 08		25, 26, 27
	Site, n'appartenant pas à l'Acheteur, situé sur le territoire national	02, 07		06, 22, 25, 26, 27, 28
	Site, n'appartenant pas à l'Acheteur, situé hors du territoire national	02, 07		06, 22, 25, 26, 27, 28

Caractéristiques Prestations	Valeur de caractéristique	Lieu d'exécution	Sûreté	Systèmes d'Information
		ELE	EPP	ESI
Connexion au réseau informatique de l'Acheteur	Non connecté			
	Connexion distante au réseau de l'Acheteur	04, 07		43
	Connexion sur réseau local site de l'Acheteur	04, 07		17, 43,
Sensibilité des Prestations	Niveau 0			Sans objet
	Niveau 1			16
	Niveau 2			16, 19, 24, 29, 32, 35, 36, 41
	Niveau 3			07, 16, 19, 24, 29, 32, 35, 36, 41

Chapitre 4 - Exigences liées au lieu d'exécution des Prestations

ELE 01 :
Dans tous les cas, le lieu d'exécution des Prestations de même que toutes modifications de celui-ci sont soumis à l'accord préalable écrit du Service de Sûreté de l'Acheteur.

ELE 02 :
Dans l'hypothèse où les Prestations sont réalisées dans les établissements du Prestataire et/ou de ses sous-traitants autorisés en vertu de l'article 21.2 des Conditions Générales, le local utilisé doit comporter un système de contrôle d'accès avec traçabilité des accès, être protégé contre les intrusions et surveillé ou télé-surveillé pendant et en dehors des heures de travail.

A ce titre, le Prestataire doit, dans un délai de 1 mois avant l'exécution des Prestations, mettre à disposition du Service de Sûreté de l'Acheteur pour validation, une description détaillée des dispositifs de sûreté du ou des sites, dont notamment :

- Un descriptif du lieu d'exécution des Prestations précisant les dispositifs de protection, de contrôle et de traçabilité d'accès mis en œuvre y compris les moyens de gardiennage et de télésurveillance.
- Un descriptif des infrastructures informatiques et dispositifs de sécurité associés.

Toute modification des dispositifs de sûreté mis en œuvre par le Prestataire pouvant impacter le Système d'Information ou les données de l'Acheteur devra faire l'objet d'un accord préalable écrit du Service de Sûreté de l'Acheteur avant sa mise en œuvre.

Si le Prestataire est amené à échanger des données concernant les Prestations entre ses différents sites ou lieux de travail, ces échanges devront être cryptés et le processus mis en place devra être soumis au préalable au Service de Sûreté de l'Acheteur pour accord.

En outre, les locaux de l'entrepreneur et de ses connexions aux systèmes informatiques seront soumis à une inspection préliminaire de la conformité par le Département de la sécurité de l'acheteur.

ELE 03 :
Dans l'hypothèse où l'Acheteur met à la disposition du Prestataire pour l'exécution des Prestations un local dédié sur l'un de ses sites, le Prestataire s'engage à fournir, dans un délai de 1 mois avant l'exécution des Prestations pour validation par le Service de Sûreté de l'Acheteur, un descriptif des dispositifs de sûreté (procédures, accès, authentification, etc.…) applicables sur le lieu d'exécution des Prestations et la liste des moyens et procédures de contrôle de ces dispositifs.
Ce local dédié et ses connexions informatiques feront l'objet d'une visite de conformité initiale par le Service de Sûreté de l'Acheteur.

ELE 04 :
Dans l'hypothèse où l'exécution des Prestations nécessite la mise en place d'une liaison informatique reliant le lieu d'exécution des Prestations au réseau de l'Acheteur, cette liaison ne pourra être installée qu'après validation formelle par le Service de Sûreté de l'Acheteur :
- Des caractéristiques de la liaison, notamment techniques, et de l'identification de la chaîne des opérateurs assurant la liaison,
- De l'architecture d'interconnexion proposée.
Dans le cas où le Prestataire aurait des équipes réparties sur plusieurs sites ou dans des locaux différents sur un même site, il ne pourra disposer que d'une seule liaison informatique vers le réseau de l'Acheteur.

ELE 05 :
En cas de détection d'une défaillance de sécurité dans l'infrastructure ou l'architecture informatique du site de réalisation des Prestations, l'Acheteur se réserve le droit de suspendre l'exécution des Prestations immédiatement aux torts du Prestataire et d'exiger que le Prestataire remette en conformité dans les meilleurs délais l'infrastructure ou l'architecture informatique concernée.

ELE 06 :
La participation de toute personne (y compris les experts visés à l'article ELE 09 ci-après) susceptible d'accéder aux Informations, résultats et leurs supports, sous quelque forme que ce soit, ainsi qu'au système informatique utilisé pour les besoins de l'exécution des Prestations est soumise en cas d'exécution sur le site de l'Acheteur à déclaration écrite préalable du Prestataire auprès du Service de Sûreté de l'Acheteur 15 jours ouvrés minimum avant l'exécution des Prestations.
Cette déclaration est accompagnée de la photocopie de la pièce d'identité de la personne, et doit comporter les coordonnées de l'entreprise auprès de laquelle la personne est salariée, ainsi que le type de contrat qui la lie à cette entreprise.
Pour les sites acheteur soumis à la réglementation, la législation actuelle s'applique (voir EPP 02 pour les sites français: ERR, PS1, PS2, PS3, ESDA)
Quel que soit le site d'exécution, le Prestataire fait signer aux membres de son personnel ainsi qu'à toute autre personne intervenant dans le cadre de l'exécution des Prestations (i) la Charte d'usage et de sécurité des systèmes d'information de l'Acheteur ainsi que (ii) un engagement de non-divulgation, et fait parvenir une copie des documents signés au Service de Sûreté de l'Acheteur. Ces trois documents sont référencés dans l'annexe 1 « documents applicables ».
La procédure décrite dans l'exigence ELE 06 s'applique également aux personnes que le Prestataire aurait désignées pour remplacer une personne participant à l'exécution des Prestations.

ELE 07 :
La liste des personnes participant à l'exécution des Prestations sur un site du Prestataire et/ou de ses sous-traitants autorisés en vertu de l'article 21.2. des Conditions Générales, par lieu d'exécution, est tenue à jour par le Prestataire et mise à la disposition du Service de Sûreté de l'Acheteur sur simple demande de sa part.

ELE 08 :
Pour les Prestations effectuées dans les locaux de l'Acheteur, la liste des personnes opérant sur les systèmes informatiques de l'Acheteur est tenue à jour par le Service de Sûreté de l'Acheteur. Le Prestataire s'engage à signaler au Service de Sûreté de l'Acheteur, dans un délai de 2 jours ouvrés, toute cessation de participation d'une personne à l'exécution des Prestations.
En ce qui concerne les personnes participant à l'exécution des Prestations sur un site de l'Acheteur, le Prestataire doit exiger qu'elles n'accèdent à aucune installation du site de l'Acheteur autre que celles concernées par l'exécution de la Prestation

ELE 09 :
Si le Prestataire fait appel pour l'exécution de la Prestation à des experts susceptibles d'intervenir ponctuellement, la liste de ces experts devra être validée par le Service de Sûreté de l'Acheteur.

Chapitre 5 - Exigences de Sûreté

5.1. CONFIDENTIALITE

EPP 01 :
En application de l'article 18.11. des Conditions Générales, le Prestataire s'engage à assurer la sécurité des Informations et des Résultats et de leurs supports, sous quelque forme que ce soit, en appliquant les règles de Sûreté de l'Acheteur, en particulier en prenant toutes les mesures utiles et nécessaires telles que :
· L'apposition d'une mention de confidentialité, au minimum « Réservé (nom de la société de l'Acheteur) », sur tous les documents ou supports confidentiels remis par l'Acheteur qui ne porteront pas déjà une telle mention ;
· La détention dans un espace sécurisé des documents ou supports confidentiels ne devant être accessibles qu'aux personnes agréées par l'Acheteur,
· Des processus de gestion des documents et de leurs supports, de leur réception à leur destruction ou restitution, conformément à la réglementation applicable et aux exigences de sécurité de l'Acheteur.

EPP 02 :
Le Prestataire doit se conformer à la réglementation locale où le site est implanté.

5.2. Sous-traitance

EPP 03 :
Dans le cadre de la procédure d'autorisation des sous-traitants prévue à l'article 21.2. des Conditions Générales et pour des raisons de sûreté, le Prestataire devra préalablement informer l'Acheteur par écrit des raisons du recours à un sous-traitant.
L'Acheteur se réserve le droit de refuser le sous-traitant sans avoir à se justifier d'une quelconque manière ou de l'autoriser, le cas échéant sous réserve que le sous-traitant s'engage à respecter des clauses de sûreté supplémentaires à celles imposées au Prestataire

5.3. Non sollicitation de personnel

EPP 04 :
Le Prestataire s'interdit, sauf accord préalable écrit de l'Acheteur, de faire, directement ou indirectement, des offres d'engagement à un collaborateur de l'Acheteur ou de le prendre à son service, sous quelque statut que ce soit.
Cet engagement est valable pendant la durée des Prestations augmentée d'une période de 12 mois.
Dans le cas où le Prestataire ne respecterait pas cet engagement, il devra dédommager l'Acheteur en lui versant une indemnité égale à la rémunération brute totale versée à ce collaborateur au cours des 6 mois précédant son départ.

EPP 05 :
Le Prestataire s'engage à respecter la réglementation applicable aux traitements des données à caractère personnel et à fournir à l'Acheteur toutes les informations nécessaires aux déclarations légales.
Il s'y engage également pour ses propres collaborateurs et sous-traitants et en fournira les preuves sur simple demande de l'Acheteur.

Chapitre 6 - Exigences de Sécurité Système d'Informations

6.1. Authentification – Gestion des droits d'accès

ESI 01 :
Le système doit permettre de déléguer l'authentification des utilisateurs à un annuaire tiers ou de permettre la mise en place d'une propagation automatique de mots de passe depuis cet annuaire.
Il doit, en outre, permettre de déléguer la gestion des droits d'accès des utilisateurs à cet annuaire tiers ainsi que d'automatiser les interfaces de mises à jour entre le système et l'annuaire.

6.2. Gestion de configuration

ESI 02 :
Les évolutions logicielles doivent être gérées en configuration. Il doit être possible de revenir à la version antérieure à la modification

ESI 03 :
Le Prestataire garantit à l'Acheteur la capacité à remettre les produits (matériels, logiciels,…) sur lesquels il intervient à l'état précédant le démarrage de son intervention (retour arrière)
Toute exception devra être soumise à l'accord préalable explicite du Service de Sécurité Système d'Information de l'Acheteur.

6.3. Environnement matériel et logiciel

DROITS D'ACCES DU PRESTATAIRE

ESI 04 :
Sauf contrainte déterminante expressément approuvée par l'Acheteur, les Prestations seront effectuées sur un environnement dédié, sans accès permanent à la plate-forme de production.
Si besoin, selon les contraintes opérationnelles, un accès pourra être donné temporairement en consultation sur la plate-forme de production, uniquement par l'Acheteur ou toute personne mandatée par lui, et suivant les conditions validées par le Service de Sécurité des Systèmes d'Information de l'Acheteur.

ESI 05 :
Le Prestataire n'a pas d'accès en mise à jour aux données de production.
En fonctionnement opérationnel, les rattrapages de données sont faits par le personnel de l'Acheteur.

ESI 06 :
Dans le cas d'implantation sur le site du Prestataire de ressources informatiques nécessaires à l'exécution de la Prestation, le Prestataire s'engage à mettre en œuvre les moyens et les procédures permettant de contrôler efficacement les accès à ces ressources.
Ces moyens et procédures doivent permettre d'assurer une traçabilité individuelle effective et non ambiguë des personnes physiques ayant accédé à ces ressources.

ESI 07 :
Dans le cas de Prestations de sensibilité de niveau 3, le Prestataire s'engage à mettre en œuvre des moyens d'authentification forte.
Les composants de ces moyens d'authentification forte doivent être conformes à l'état de l'art au moment du déroulement des Prestations et aux standards techniques du Groupe Safran (cf. annexe 1).

ESI 08 :
Les accès aux ressources informatiques utilisées dans le cadre de l'exécution des Prestations sont affectés nominativement à chaque personne physique concernée.
Si le Prestataire fait appel, pour l'exécution de la Prestation, à des experts susceptibles d'intervenir en urgence, ceux-ci utiliseront, le cas échéant, des comptes d'urgence conformément à la « Procédure de gestion des comptes d'urgences » référencée en annexe 1.

ESI 09 :
Les moyens et procédures d'autorisation d'accès et d'authentification des personnels devant accéder aux ressources informatiques utilisées dans le cadre de l'exécution des Prestations devront permettre de limiter les rôles et privilèges des personnels au strict nécessaire à la réalisation de leur mission.

ARCHITECTURE

ESI 10 :
Le Prestataire respecte les standards et technologies en vigueur selon les bonnes pratiques en matière d'architectures et développements de systèmes informatiques sécurisés.

ESI 11 :
Le Prestataire respecte les choix d'architecture et de technologies de l'Acheteur ainsi que les standards techniques en vigueur dans le Groupe Safran (Cf. Annexe 1).

ESI 12 :
En application de l'article 3.3. des Conditions Générales, le Prestataire doit être force de proposition pour faire évoluer les architectures existantes, en vue de maintenir, voire d'améliorer le niveau de sécurité de ces architectures.
L'évolution de ces architectures est en tout état de cause soumise à l'accord écrit de l'Acheteur.

ESI 13 :
Le Prestataire doit respecter les principes et règles de sécurité de l'Acheteur, tels que décrits dans les documents traitant de ce domaine (Cf. Annexe 1).

ESI 14 :
Sans objet.

ESI 15 :
Sans objet.

ESI 16 :
Le Résultat fourni par le Prestataire dans le cadre de sa Prestation doit comporter un système de trace adapté au niveau de sensibilité des Prestations. En préalable à la fourniture du système complet, le Prestataire fournit au Service de Sécurité de l'Acheteur pour validation un descriptif détaillé du système de trace et de son fonctionnement.
En cas de refus par l'Acheteur, le Prestataire proposera une nouvelle solution pour validation écrite de l'Acheteur.

CHOIX DES MATERIELS ET LOGICIELS

ESI 17 :
Les matériels et logiciels utilisés ou fournis par le Prestataire dans le cadre de l'exécution des Prestations devront être conformes aux standards de matériels et logiciels de l'Acheteur en vigueur (Cf. Annexe 1).

ESI 18 :
Sans objet.

ESI 19 :
Les matériels et logiciels utilisés dans le cadre des Prestations et installés dans les locaux du Prestataire seront isolés du réseau propre au Prestataire, sans aucune autre connexion avec l'extérieur que celles explicitement approuvées par le Service de Sécurité de l'Acheteur.

INSTALLATION, ADMINISTRATION, EXPLOITATION

ESI 20 :
L'installation, l'exploitation et l'administration des moyens mis en œuvre dans le cadre des Prestations devront être conformes aux bonnes pratiques et aux règles de sécurité et d'exploitation établies par l'Acheteur (Cf. Annexe 1).
Toute exception fera l'objet d'un accord préalable écrit du Service de Sécurité de l'Acheteur.

ESI 21 :
Sans objet.

ESI 22 :
Le Prestataire s'engage à conserver les traces des accès issues du dispositif de contrôle d'accès aux locaux pendant une durée de trois (3) mois.
L'Acheteur pourra y accéder sans délai sur simple demande.

ESI 23 :
Pendant la durée des Prestations, les serveurs et les postes de travail devront être installés et administrés selon les bonnes pratiques en matière de protection des données et de système anti-intrusion et être conformes aux standards de sécurité du Groupe Safran (Cf. annexe 1)

ESI 24 :
Pour des Prestations de sensibilité de niveau 2 et de niveau 3, les dispositifs de sûreté associés aux moyens d'exploitation et d'administration seront soumis préalablement au démarrage des Prestations à l'approbation explicite du Service de Sûreté de l'Acheteur

ESI 25 :
Le Prestataire s'engage à conserver les traces des accès aux ressources informatiques, y compris aux applicatifs pendant une durée de six (6) mois.
L'Acheteur pourra y accéder sans délai sur simple demande.

ESI 26 :
Le Prestataire devra fournir au Service de Sécurité de l'Acheteur sur simple demande par écrit (mail, courrier, fax) l'intégralité des traces (éléments de service et actes des administrateurs) afférentes aux Prestations sur les différents systèmes informatiques utilisés.

ESI 27 :
Le Prestataire devra définir un système permettant une traçabilité des Systèmes d'Information préalablement au déroulement des Prestations et devra le soumettre pour validation au Service de Sécurité de l'Acheteur.
Il en assurera la mise en œuvre.
La traçabilité des systèmes informatiques ne devra comporter aucune lacune, sauf accord formel préalable du Service de Sécurité de l'Acheteur

ESI 28 :
L'ensemble des opérations de transferts de mémoire, de disques durs, de supports d'archives ou de sauvegarde est inscrit dans un registre des opérations indiquant pour :
- Tous les niveaux de sensibilité des Prestations : qui (émetteur et destinataire), quoi (détaillé), le nombre, la date,
- Niveau 2 et 3 de sensibilité des Prestations : l'heure, le lieu d'enlèvement, et le lieu de dépôt, l'identité du transitaire,
- Niveau 3 de sensibilité des Prestations : l'itinéraire effectué de manière détaillée, l'identité des personnels du transitaire en charge du transfert.

Sur simple demande, ce registre sera mis à la disposition de l'Acheteur par le Prestataire.

Le Prestataire devra respecter en sus de cette exigence, l'ensemble des règles de sécurité en vigueur chez l'Acheteur

EXECUTION DE PRESTATION SUR UN SITE DE L'ACHETEUR

ESI 29 :
Les moyens de communication utilisés doivent permettre de garantir la confidentialité des informations échangées.
Sauf décision contraire écrite du Service de Sécurité de l'Acheteur, la liaison entre le Prestataire et l'Acheteur et/ou les échanges d'informations sensibles au titre des Prestations via des liaisons propres au Prestataire entre ses lieux d'exécution, devront être chiffrés.
Le moyen de chiffrement devra être soumis par le Prestataire au Service de Sécurité de l'Acheteur pour approbation ou refus. La fourniture des moyens nécessaires, les frais de mise en place et liés à l'utilisation de ces moyens de chiffrement seront à la charge du Prestataire.

5.4. Politique de Tests

ESI 30 :
Le Prestataire effectue systématiquement des tests de non-régression élémentaires.

ESI 31 :
Le Prestataire effectue systématiquement des tests de non-régression fonctionnels avant mise en production.

ESI 32 :
Les jeux de données fournis au Prestataire comportent des données blanchies.
Le Prestataire reconnaît en avoir été averti et prendre à sa charge les risques associés.

5.5. Livrables

ESI 33 :
Le Prestataire s'engage à fournir, en préalable au démarrage de la Prestation, une proposition de Plan d'Assurance Sécurité couvrant :
- d'une part les mesures existantes et/ou proposées garantissant la conformité des Prestations aux exigences de sécurité telles que définies dans le présent document et son annexe 1,
- d'autre part le plan de mise en œuvre et de suivi de ces mesures ainsi que les jalons de sécurité correspondants.

Ce dossier fera l'objet d'une validation préalable au démarrage des Prestations par le Service de Sécurité de l'Acheteur.

ESI 34 :
Le Prestataire a l'obligation de fournir un Livrable correspondant à la check-list « SSI » (Sécurité des Systèmes d'Information) d'installation et d'exploitation opérationnelle, à savoir la liste des consignes sécurité à suivre pendant l'installation et/ou l'exploitation du produit.
Ce Livrable comprendra également la liste des comptes de servitude utilisés par le Prestataire ou générés par lui.

ESI 35 :
Le Prestataire a l'obligation de fournir
Pour les Prestations de Sensibilité 3, un Livrable décrivant l'intégralité des actions qu'il a effectuées pendant l'exécution des Prestations (y compris la liste des données ou ensemble de données de l'Acheteur auxquelles il a eu accès),
Pour les Prestations de sensibilité 1 ou 2, a minima un rapport d'intervention dont le niveau de précision est à définir par l'Acheteur en début de Prestation.

ESI 36 :
Pour des Prestations de Sensibilité de niveau 2 ou 3, le Prestataire devra fournir à l'Acheteur en préalable à la mise en place de la plate-forme et/ou au démarrage des Prestations un Livrable décrivant les modalités d'installation, d'administration et d'exploitation des produits.
Ce Livrable sera soumis à l'accord formel du Service de Sécurité de l'Acheteur.

6.6. Méthodologie / Pratiques

ESI 37 :
Le Prestataire devra respecter les recommandations émises dans le document « Standards techniques Groupe» (cf. annexe 1). Le Prestataire a une obligation de conseil et une mission de proposition dans ce domaine en application de l'article 3.3. des Conditions Générales.

ESI 38 :
Le Prestataire doit intégrer des jalons de sécurité pendant la durée d'exécution des Prestations. A chacun de ces jalons, le Prestataire doit démontrer qu'il suit les Exigences de Sécurité de l'Acheteur issues de la Commande, des Conditions Générales, des termes du présent document, et ce en fonction des caractéristiques des Prestations.

ESI 39 :
Toute modification susceptible d'impacter la sécurité du Livrable, du Système d'Information ou des données de l'Acheteur sera soumise par le Prestataire à validation formelle du Service de Sécurité de l'Acheteur au préalable à sa prise en compte en application de l'article 7.1. ci-après.

ESI 40 :
Au préalable à tout transfert de matériel ou de logiciel du Prestataire vers l'Acheteur, un audit sécurité sera effectué sur les matériels et logiciels pour vérifier leur conformité par rapport aux règles de sécurité de l'Acheteur applicables dans le cadre des Prestations..

ESI 41 :
Sans préjudice des dispositions de l'article 18.6. des Conditions Générales, à l'arrêt de Prestations :
De niveau de sensibilité 3 , les disques durs utilisés par le Prestataire dans le cadre de l'exécution des Prestations seront détruits physiquement ou remis à l'Acheteur, sur simple demande de sa part et dans les conditions fixées par lui. La réaffectation de matériels n'est pas autorisée.
De niveau de sensibilité 2, le Prestataire s'engage à pratiquer a minima un effacement fort des disques durs utilisés en respectant une méthode validée par le Service de Sécurité de l'Acheteur préalablement au début des Prestations. Le Prestataire enverra ensuite à l'Acheteur une attestation d'effacement de données datée et signée par lui.
De niveau de sensibilité 1, le Prestataire s'engage à pratiquer a minima un effacement simple (par exemple 7 passes) des disques durs utilisés en respectant une méthode validée par le Service de Sécurité de l'Acheteur préalablement au début des Prestations. Le Prestataire enverra ensuite à l'Acheteur une attestation d'effacement de données datée et signée par lui

Dans tous les cas, les médias utilisés par le Prestataire dans le cadre de l'exécution des Prestations pour le stockage, les transferts et les sauvegardes d'informations seront détruits physiquement ou remis à l'Acheteur, sur simple demande de sa part et dans les conditions fixés par lui.
En cas de destruction, le Prestataire s'engage à adresser à l'Acheteur une attestation de destruction des médias datée et signée par lui avec l'identification des dits médias.

ESI 42 :
Sans objet

ESI 43 :
Le Prestataire s'engage à respecter les stratégies de sécurité implémentées sur les postes utilisés ou fournis au titre de Prestations (timeout, anti-virus, pas de double connexion…) ainsi que les règles de Sécurité des Systèmes d'Information (mots de passe, …).
Les règles de Sécurité des Systèmes d'Information (SSI) sont les règles Groupe Safran complétées, le cas échéant, des règles propres à l'Acheteur (Cf. annexe 1) Ces règles SSI sont communiquées au Prestataire dans le cadre de la consultation.

6.7. Transfert de compétences

ESI 44 :
Tout transfert de matériel ou de logiciels du Prestataire vers l'Acheteur sera accompagné d'un transfert formalisé de compétences vers les équipes de l'Acheteur ou mandatées par l'Acheteur pour reprendre l'administration et l'exploitation de ces matériels.
ESI 45 :
Outre les dispositions générales de la Charte d'Usage et de Sécurité des Systèmes d'Information Groupe Safran (Cf. ELE 06), le Prestataire s'engage à appliquer les directives du Groupe Safran en matière d'administration de systèmes et notamment à mettre en application les Règles de déontologie et de sécurité des Administrateurs de Systèmes d'Information Groupe Safran, et à faire signer par ses personnels intervenant dans le cadre de la Prestation le formulaire d'adhésion individuel intitulé « Engagement de respecter les règles de déontologie et de sécurité des Administrateurs des Systèmes d'Information du Groupe SAFRAN »

ESI 46 :
La gestion des comptes Administrateurs doit être effectuée conformément à la directive de sécurité Groupe Safran relative à l'administration des SI (Cf. Annexe 1).
En particulier, les mots de passe des comptes "Administrateurs" des systèmes doivent respecter les règles de gestion des mots de passe Administrateurs Safran.
Ces dispositions sont applicables à tout compte d'accès individuel ou non disposant de privilèges techniques sur tout ou partie des équipements et systèmes de l'Acheteur et que le Prestataire pourrait être amené à utiliser ou gérer dans le cadre de la Prestation.

ESI 47 :
Le Prestataire s'engage à désactiver ou faire désactiver immédiatement tout compte d'accès utilisé par ses intervenants dans les cas suivants : fin de mission d'un intervenant du Prestataire pour quelque raison que ce soit, compromission (ou suspicion de compromission) du compte d'accès.

ESI 48 :
Sauf disposition particulière explicitement prévue entre le Prestataire et l'Acheteur, le Prestataire s'engage à ne pas attribuer de privilèges d'administration sur les Systèmes de l'Acheteur sans une validation préalable formelle du Service de Sécurité de l'Acheteur.

ESI 49 :
Le Prestataire s'engage à mettre en place et tenir à jour un séquestre de l'ensemble des comptes « Administrateurs » dont il assure la gestion auprès du Service de Sécurité de l'Acheteur

ESI 50 :
La plate-forme d'administration des systèmes de l'Acheteur devra être sur un réseau isolé, être protégée par un pare-feu contre les intrusions externes et ne comporter aucune liaison vers des réseaux tiers et/ou le réseau de l'Internet, sans accord préalable explicite du service de Sécurité de l'Acheteur.

ESI 51 :
Les moyens techniques (outils et procédures) utilisés dans le cadre de l'exploitation et administration des équipements doivent respecter les principes de sécurité Groupe Safran en la matière. C'est le cas notamment pour les interventions en local ou à distance et l'exécution de code sur des systèmes et équipements de l'Acheteur (cf. gestes techniques en annexe 1).
En l'absence de standard de sécurité du Groupe Safran en la matière, les moyens techniques proposés par le Prestataire devront faire l'objet d'une validation préalable explicite par le Service de Sécurité de l'Acheteur.

ESI 52 :
Les moyens techniques et procédures de gestion des mots de passe doivent respecter les principes de sécurité Groupe Safran en la matière, dont notamment ceux relatifs :
- aux stratégies de mots de passe Utilisateurs et Administrateurs
- aux dispositifs de dépannage ou d'auto-dépannage
(Cf. annexe 1)

ESI 53 :
Toutes les informations appartenant à l'Acheteur stockées sur des supports mobiles utilisés par le Prestataire dans le cadre des Prestations devront être chiffrées par un moyen validé par l'Acheteur et ce, dès lors que ces informations ne relèvent pas du domaine public (niveau 0).

ESI 54 :
Les opérations de maintenance et de transfert des matériels sont soumises aux règles de sécurité Groupe Safran et procédures de sécurité de l'Acheteur. Il en est ainsi des sorties de matériels des sites de l'Acheteur, de la réutilisation et du remplacement des matériels, de la réforme ou destruction des équipements.

ESI 55 :
Le Prestataire s'engage à mettre en œuvre les dispositifs de protection antivirale sur les équipements dont il assure l'administration conformément à la politique antivirale Groupe (Cf. Annexe 1) et aux directives fournies par l'Acheteur au démarrage des Prestations.
Il s'engage en outre à alerter le Service de Sécurité de l'Acheteur en cas d'attaque virale et à contribuer à la gestion de crise virale Groupe Safran.

ESI 56 :
Le Prestataire s'engage à n'utiliser dans le cadre des Prestations que des logiciels ayant fait l'objet d'un agrément préalable par le Service de Sécurité de l'Acheteur.

ESI 57 :
Sans objet

ESI 58 :
Le Prestataire mettra en œuvre les moyens techniques de supervision et surveillance des systèmes, de gestion des espaces disques et de planification des traitements afin d'assurer le bon fonctionnement et la sécurité des systèmes, dans la limite des Prestations qui lui sont confiées.
Le Prestataire s'engage dans les meilleurs délais :
- À alerter le Service de Sécurité de l'Acheteur de tout incident pouvant impacter la Sécurité des Systèmes d'Information de l'Acheteur.
- À réaliser ou à contribuer à toutes actions susceptibles de palier à l'incident ou a minima d'en réduire les effets et conséquences.

ESI 59 :
Le Prestataire mettra en œuvre les moyens nécessaires pour garantir la continuité du service et la disponibilité des données conformément aux attendus de services de l'Acheteur d'une part et aux

standards de sécurité Groupe Safran en la matière d'autre part (Cf. Annexe 1).

Il s'engage a minima :
- A mettre en œuvre une stratégie de sauvegarde/restauration incluant le lancement, la surveillance d'exécution et les tests de restauration,
- A prévoir une architecture avec un niveau de redondance suffisant.
- A tenir à disposition les comptes rendus d'exécution de sauvegardes et de tests de reprise ainsi que ses procédures et tableaux de bord.
- A stocker les médias de sauvegardes dans un lieu sécurisé, à la fréquence convenue avec l'Acheteur, hors salle serveurs et de préférence hors du site d'hébergement des systèmes.

ESI 60 :
L'administration et l'exploitation des systèmes et équipements font l'objet de procédures techniques correspondant aux besoins de l'Acheteur et conformes aux bonnes pratiques et aux règles de sécurité Groupe Safran (Cf. Annexe 1)
C'est le cas notamment pour les activités de supervision de fonctionnement des services, arrêt et démarrage, gestion des correctifs de sécurité, déploiements de systèmes et gestion de changements, surveillance des capacités et performances, etc.)
ESI 61 :
Outre les dispositions prévues au titre de l'ECI34, le Prestataire mettra en œuvre les dispositifs (outils et procédures) nécessaires pour garantir l'application périodique et homogène des correctifs de sécurité sur les systèmes et équipements dont il assure l'exploitation et/ou l'administration.
Les attendus et modalités de mise en œuvre de ces dispositifs seront définis au démarrage des Prestations et soumis à validation du Service de Sécurité de l'Acheteur.

ESI 62 :
Dans le cadre des contrôles réalisés par le service de Contrôle Interne de l'Acheteur, le Prestataire sera tenu de fournir les justificatifs requis sous contrôle du Service de Sécurité de l'Acheteur.
L'objet de ces contrôles et leurs modalités de réalisation sont définies au démarrage de la Prestation.

ESI 63 :
Les mesures de protection physique et environnementale des systèmes et équipements doivent être conformes aux bonnes pratiques en la matière et aux standards de sécurité Groupe Safran.

ESI 64 :
Le Prestataire mettra en place un suivi de l'activité sécurité et une revue régulière des journaux d'événements conformément aux directives de l'Acheteur.

ESI 65 :
Les procédures de gestion des comptes et des droits d'accès aux équipements et systèmes sont formalisées.
Elles incluent une revue mensuelle devant porter a minima sur :
- Les comptes disposant de privilèges d'administration sur les SI,
- Les comptes obsolètes, conformément aux définitions et règles de sécurité standard du Groupe Safran (Cf. Annexe 1).
Les procédures et rapports de revue devront être remis au Service de Sécurité de l'Acheteur sur simple demande de sa part par écrit (mail, courrier, fax).

ESI 66 :
Le Prestataire s'engage à mettre en place une organisation respectant le principe de séparation des privilèges conformément aux directives de sécurité Groupe Safran (Cf. Annexe 1)

ESI 67 :
Les équipements informatiques et composants d'infrastructure (serveurs, postes de travail, imprimantes, routeurs, switches, etc.) sont installés et configurés par le Prestataire conformément aux bonnes pratiques en la matière et aux directives et recommandations de sécurité Groupe Safran (Cf. Annexe 1).

ESI 68 :
Le Prestataire s'engage à pratiquer périodiquement des audits d'intrusion sur l'ensemble des systèmes dont il assure l'exploitation et l'administration.
Il s'engage en outre à communiquer à l'Acheteur les rapports d'audit,
à proposer les plans d'actions correctrices et de progrès pour validation par le Service de Sécurité de l'Acheteur, ainsi qu'à réaliser ces plans d'actions et de progrès une fois validés.
La fréquence et le périmètre de ces audits seront convenus avec l'Acheteur en début de Prestation, et seront réalisés a minima tous les 3 ans dans le cadre des campagnes générales d'audit de sécurité des SI Groupe Safran.

ESI 69 :
Toute évolution des systèmes et a minima des composants d'infrastructure impactant la sécurité des SI et/ou leur disponibilité doit être validée formellement par le Service de Sécurité de l'Acheteur. Les modalités de gestion de changement de ces composants seront définies au démarrage de la Prestation avec le Service de Sécurité de l'Acheteur.

ESI 70 :
Le Prestataire s'engage à mettre en place un plan de secours informatique (PSI) pour les systèmes qu'il exploite et administre, conformément aux exigences de services et de continuité d'activité définies par l'Acheteur d'une part et aux règles standard de sécurité Groupe Safran d'autre part (Cf. Annexe 1).
Il s'engage notamment :

- A tester et actualiser ce PSI a minima annuellement,
- A communiquer à l'Acheteur les comptes rendus d'exécution des tests et plans de progrès associés,
- A mettre en œuvre les plans de progrès nécessaires.

Chapitre 7 - Audits de sûreté - Sanctions

7.1. AUDIT SECURITE

7.1.1.
En application de l'article 3.8. des Conditions Générales, l'Acheteur pourra réaliser ou faire réaliser des audits de sûreté par tout intervenant de son choix soumis à des engagements de confidentialité, à tout moment, avant et pendant l'exécution de la Commande, sans qu'il soit nécessaire d'en justifier les raisons. L'intervenant désigné ne saurait, sauf dans des cas exceptionnels notamment de marchés très concentrés, être une société directement concurrente du Prestataire dans son domaine de compétence. L'Acheteur s'engage par ailleurs à faire signer à chaque expert chargé d'une mission d'audit, un engagement personnel de confidentialité.

Des audits pourront également être effectués :

- par les autorités de tutelle de l'Acheteur dans le cadre de leur mission de contrôle de l'Acheteur.
- dans le cadre des processus de Contrôle Interne de l'Acheteur

Le Prestataire s'engage à collaborer de bonne foi et sans réserve avec tout auditeur désigné. Ainsi, il répondra à toutes questions et facilitera l'accès des auditeurs à tout document ou information ou autre élément utile au bon déroulement de la mission d'audit.

Par ailleurs, le Prestataire s'engage, dans le cas où il sous-traite une part des travaux, qui lui ont été confiés par l'Acheteur, à effectuer à ses frais, a minima une fois par an, un audit de sûreté de ses sous-traitants. Cet audit aura pour but de vérifier la conformité des opérations du(des) sous-traitant(s) aux Exigences de Sécurité explicitées dans les Conditions Générales et dans le présent document. A l'issue de l'audit, le Prestataire fera parvenir le compte rendu d'audit au Service de Sûreté de l'Acheteur.
En cas de sous-traitance à n niveaux, le Prestataire s'engage à obtenir que chaque sous-traitant, à quelque niveau que ce soit, puisse être soumis à ce type d'audit.
L'audit fera l'objet d'un compte-rendu qui conservera un caractère de confidentialité entre l'Acheteur et le Prestataire.

Ces audits ne dispenseront en aucun cas le Prestataire du respect de l'ensemble de ses obligations contractuelles ni n'emporteront de la part de l'Acheteur accord ou ratification des éventuelles non-conformités du Prestataire aux Exigences de Sécurité.

7.1.2.
Ces audits portent sur le respect des exigences de sécurité applicables aux Prestations, dont notamment :

- La sûreté des locaux et des personnels ;
- Les outils, moyens et procédures mis en œuvre par le Prestataire pour l'exécution des Prestations, y compris moyens de sécurité relatifs à l'exploitation et l'administration des systèmes le cas échéant ;
- Les choix techniques et de sécurité, ainsi que la validation des ressources utilisées dans le cadre des Prestations ;
- Le contrôle des traces physiques et informatiques relatives à l'exécution des Prestations ;
- L'exactitude des éléments de reporting, notamment concernant les volumes d'activités et les niveaux de service produits ;
- le respect des règles prévues de maintien des conditions de réversibilité ;

- Les règles de sécurité mises en œuvre ;
- La vulnérabilité des systèmes du Prestataire ou mis en place par le Prestataire.

Il est convenu, à cet égard, qu'aucun supplément de prix ne sera facturé par le Prestataire du fait du supplément de travail occasionné par les audits sécurité, dans la limite d'une franchise de 30 Jours-Homme par an et par Acheteur. Au-delà de ce crédit, le Prestataire facture les temps passés par ses personnels sur justificatifs et selon les tarifs convenus préalablement avec l'Acheteur.

Si un rapport d'audit quelconque, diligenté par l'Acheteur ou non, fait apparaître un manquement relatif aux obligations du Prestataire, celui-ci doit mettre en œuvre, et/ou faire mettre en œuvre par ses sous-traitants autorisés, les mesures correctives selon le délai exigé par l'Acheteur en fonction de la criticité du manquement (cf. tableau ci-dessous au §7.3), à compter de la notification de l'Acheteur et aux frais exclusifs du Prestataire, sans préjudice des sanctions prévues à l'article 7.2. ci-dessous.

7.2. Sanctions

Tout manquement aux Exigences de Sécurité constaté par l'Acheteur pourra le conduire à refuser l'accès des personnes non autorisées à ses sites ou à ses systèmes d'informations sans que le Prestataire puisse se prévaloir de ce refus d'accès pour se soustraire à l'exécution de l'ensemble de ses obligations au titre de la Commande et exposera, le cas échéant, le Prestataire à des poursuites judiciaires notamment en application de la réglementation applicable sur la divulgation d'informations couvertes par le secret de Défense.

En cas de non-respect par le Prestataire, son personnel ou ses sous-traitants, des dispositions énoncées dans les Exigences de Sécurité, l'Acheteur se réserve par ailleurs la possibilité de :

- refuser pour raison de sécurité de réceptionner des Livrables au titre de la Commande.
- appliquer des pénalités au Prestataire ,
- mettre fin à la Commande de plein droit sans préavis par simple notification adressée au Prestataire, sans dommages et intérêts au profit du Prestataire de fait de cette résiliation en application des Conditions Générales,
- le cas échéant, engager une action judiciaire. L'Acheteur se réserve notamment le droit d'engager une action devant une juridiction pénale à l'encontre des personnels du Prestataire et sous-traitants qui ont utilisé ou tenté d'utiliser l'accès au réseau de l'Acheteur dans l'intention de copier frauduleusement, de modifier ou de détruire sans autorisation ou d'utiliser aux fins de nuire des données, logiciels ou parties de logiciels appartenant à l'Acheteur.

A chaque Exigence de Sécurité est associé un (ou des risques), qui est(sont) qualifié(s) par un niveau de criticité et une (des) directive(s) de résolution de(s) ce(s) risque(s).

Le niveau de criticité est défini par une valeur entre 1 et 5 . La valeur 5 correspond à une criticité maximum. La valeur 1 correspond à la criticité minimum.

Les risques sont de deux types :
- risque impactant le niveau de sécurité de l'Acheteur (données utilisées, règles de sécurité),
- risque impactant le niveau de sécurité du produit réalisé par le Prestataire.

Risque impactant le niveau de sécurité de l'Acheteur :
A chaque risque impactant le niveau de sécurité de l'Acheteur sera associé un des trois délais possibles de remise en conformité :
- remise en conformité immédiate (0 jour)
- remise en conformité sous 5 jours
- remise en conformité sous 10 jours

Risque impactant le niveau de sécurité des Résultats réalisés par le Prestataire :
A chaque risque impactant le niveau de sécurité sera associé un délai de remise en conformité.
Ce délai de remise en conformité sera proposé par le Prestataire et soumis à la validation du Service de Sûreté de l'Acheteur.

Principes de calcul des pénalités :

Des pénalités sont applicables en cas d'anomalie pouvant impacter la sécurité de l'Acheteur ainsi qu'en cas de dépassement des délais de remise en conformité tels que définis dans le présent chapitre et/ou au démarrage des Prestations..

Le montant et le mode de calcul des pénalités seront définis préalablement au démarrage des Prestations et devront respecter les principes suivants :

- Graduation de la pénalité en fonction de la criticité de l'impact de l'anomalie
- Augmentation exponentielle et non linéaire de la pénalité en fonction du nombre de jours de retard pour la remise en conformité
- Augmentation exponentielle et non linéaire de la pénalité en cas de répétition de l'anomalie.

Un état des anomalies sécurité recensées lors de l'exécution des Prestations, comportant pour chaque anomalie l'état de remise en conformité et le délai de remise en conformité, est constitué périodiquement.
Cet état sert à calculer les pénalités associées.

Le paiement des pénalités par le Prestataire ne le libère pas de son obligation de respecter les Exigences de Sécurité, et est sans préjudice des droits de l'Acheteur de demander réparation des dommages qu'il aurait subis du fait du manquement du Prestataire.

Le tableau ci-dessous présente la classification servant de base à l'élaboration des pénalités financières évoquées ci-dessus. Classification des risques associés aux exigences :

Référence de l'exigence	Libellé du risque (si plusieurs risques associés à la même exigence)	Niveau de criticité	Remise en conformité sous délai
ELE 01	Site non déclaré au préalable	5	0 jour
ELE 02	Modification de site effectuée sans accord préalable Acheteur	5	0 jour
ELE 02	Dossier non fourni par le Prestataire	4	0 jour
ELE 02	Dossier fourni par le Prestataire s'avère incomplet ou moyens proposés refusés par l'Acheteur	2	5 jours
ELE 02	Locaux non conformes	5	0 jour
ELE 02	Connexions non conformes	5	0 jour
ELE 03	Dossier non fourni par le Prestataire	4	0 jour
ELE 03	Dossier fourni par le Prestataire s'avère incomplet ou moyens proposés refusés par l'Acheteur	2	5 jours
ELE 03	Connexions non conformes	5	0 jour
ELE 04	Liaisons non validées ou refusées par l'Acheteur et utilisées par le Prestataire	5	0 jour
ELE 05	Lacunes avérées, sans accord préalable de l'Acheteur	5	0 jour
ELE 06	Non signature des documents par l'intervenant	1	0 jour
ELE 06	Non déclaration intervenant avant la prise de fonction	4	0 jour
ELE 06	Non-respect de la charte informatique	4	Sans objet
ELE 06	Non prise en compte, ostensible et répétée des Exigences de Sécurité par le Prestataire ou la personne intervenant en son nom	5	0 jour
ELE 06	Non-respect de la procédure de signature	2	Sans objet
ELE 07	Pas de déclaration de fin de fonction	4	0 jour
ELE 07	Pas de liste ou liste incomplète	3	2 jours
ELE 08	Pas de déclaration de fin de fonction	4	0 jour
ELE 08	Non port du badge	2	0 jour
ELE 08	Pas de liste ou liste incomplète	3	2 jours
ELE 09	Non-respect procédure intervention urgence	3	0 jour
EPP 01	Transmission à une personne non autorisée	5	0 jour
EPP 01	Non application mesures protection données	5	10 jours
EPP 02	Non-respect des obligations légales	4	0 jour
EPP 03	Sous traitance non autorisée	4	0 jour
EPP 03	Non-respect des règles de sécurité par le sous-traitant	5	10 jours
EPP 04	Sans objet	Sans objet	Sans objet
EPP 05	Sans objet	Sans objet	Sans objet
ESI 01	Pas de gestion droits d'accès à l'extérieur du progiciel ou propagation authentification non automatique	2	Fonction Prestations
ESI 02	Pas de gestion de configuration	3	Fonction Prestations

Référence de l'exigence	Libellé du risque (si plusieurs risques associés à la même exigence)	Niveau de criticité	Remise en conformité sous délai
ESI 02	Impossibilité de revenir à la version antérieure	4	Fonction Prestations
ESI 03	Impossible de revenir à la version antérieure	4	Fonction Prestations
ESI 04	Prestations effectuées sur un environnement non dédié	4	0 jour
ESI 04	Accès à la plate-forme de production : non-respect des règles – modification / consultation en accès permanent, respects règles RSSI local	5	0 jour
ESI 05	Accès aux données de production par le Prestataire	5	0 jour
ESI 05	Rattrapage de données par du personnel externe	5	0 jour
ESI 06	Accès à des données par une personne dont on ne sait pas retrouver l'identité	2	Sans objet
ESI 06	Pas de système de traçabilité ou système de traçabilité amenant des équivoques	3	5 jours
ESI 06	Contrôle d'accès aux ressources inexistant ou inefficace	4	5 jours
ESI 06	Un identifiant correspond à plusieurs individus	4	0 jour
ESI 07	Moyen d'authentification mis en place par le Prestataire pas au niveau requis	5	0 jour
ESI 08	Non-respect de la procédure de compte d'urgences	1	0 jour
ESI 09	Privilèges d'accès trop étendus par rapport au besoin	3	0 jour
ESI 10	Non-respect des standards et technologies sécurisées	5	Fonction Prestations
ESI 11	Non-respect des choix d'architecture et des technologies Acheteur	3	Fonction Prestations
ESI 12	Le Prestataire n'est pas force de proposition	2	Fonction Prestations
ESI 13	Non-respect du référentiel sécurité	3	Fonction Prestations
ESI 14	Sans objet	Sans objet	Sans objet
ESI 15	Sans objet	Sans objet	Sans objet
ESI 16	Produit non conforme en terme de traçabilité	3	Fonction Prestations
ESI 17	Matériels et/ou logiciels non standards connectés au réseau local de l'Acheteur ou administrés par l'Acheteur	4	0 jour
ESI 17	Matériels et/ou logiciels non standards NON connectés au réseau local de l'Acheteur et NON administrés par l'Acheteur	2	5 jours
ESI 18	Sans objet	Sans objet	Sans objet
ESI 19	Moyens du Prestataire non isolé	5	0 jour
ESI 19	Détection de connexion extérieure non agréée	5	0 jour
ESI 20	Installation, procédures non conformes à l'état de l'art	3	5 jours
ESI 20	Installation, procédures non conformes aux règles	5	0 jour

Référence de l'exigence	Libellé du risque (si plusieurs risques associés à la même exigence)	Niveau de criticité	Remise en conformité sous délai
	établies par l'Acheteur et ESI 24 non applicable		
ESI 21	Sans objet	Sans objet	Sans objet
ESI 22	Pas de conservation des traces d'accès sur 3 mois ou pas de réponse aux demandes de l'Acheteur	4	5 jours
ESI 23	Non-respect de l'état de l'art	3	5 jours
ESI 24	Non-conformité par rapport aux exigences Acheteur	5	Fonction Prestations
ESI 24	Pas de validation préalable par l'Acheteur	3	Fonction Prestations
ESI 25	Pas de conservation des traces d'accès sur 6 mois ou pas de réponse aux demandes de l'Acheteur	4	5 jours
ESI 26	Pas de réponse aux demandes de l'Acheteur	4	0 jour
ESI 27	Pas de validation formelle préalable de l'Acheteur	5	Fonction Prestations
ESI 27	Lacunes avérées, sans accord préalable de l'Acheteur	4	5 jours
ESI 28	Pas de registre ou registre incomplet	5	0 jour
ESI 28	Non-respect des règles Acheteur	5	0 jour
ESI 29	Liaisons non chiffrées	5	0 jour
ESI 29	Mise en place d'un système de chiffrage refusé ou non validé par l'Acheteur	4	0 jour
ESI 30	Pas de test élémentaire de non régression	4	Fonction Prestations
ESI 30	Tests de non régression élémentaires incomplets	3	Fonction Prestations
ESI 31	Pas de test fonctionnel de non régression	4	Fonction Prestations
ESI 31	Tests de non régression fonctionnels incomplets	3	Fonction Prestations
ESI 32	Sans objet	Sans objet	Sans objet
ESI 33	Pas d'étude de compatibilité fournie par le Prestataire	4	Fonction Prestations
ESI 33	Démarrage sans validation Acheteur	5	Fonction Prestations
ESI 34	Pas de livrable fourni par le Prestataire ou livrable comportant des lacunes majeures	5	Fonction Prestations
ESI 34	Fourniture incomplète comportant des lacunes mineures	3	Fonction Prestations
ESI 35	Pas de livrable fourni par le Prestataire	5	Fonction Prestations
ESI 35	Livrable comportant des lacunes majeures	5	Fonction Prestations
ESI 35	Fourniture incomplète comportant des lacunes mineures	3	Fonction Prestations
ESI 36	Pas de livrable fourni par le Prestataire	4	Fonction Prestations
ESI 36	Démarrage sans validation Acheteur	5	Fonction

Référence de l'exigence	Libellé du risque (si plusieurs risques associés à la même exigence)	Niveau de criticité	Remise en conformité sous délai
			Prestations
ESI 37	Non-respect des standards Acheteur sans autorisation préalable	5	Fonction Prestations
ESI 37	Prestataire n'est pas force de proposition	3	Fonction Prestations
ESI 38	Pas de jalons de sécurité dans le déroulement des Prestations	5	Fonction Prestations
ESI 38	Pas de corrélation avec les exigences lors d'un jalon	4	Fonction Prestations
ESI 38	Non-respect des Exigences de Sécurité	5	Fonction Prestations
ESI 39	Pas de demande effectuée par le Prestataire	5	Fonction Prestations
ESI 39	Démarrage sans validation préalable Acheteur	5	Fonction Prestations
ESI 40	Pas d'audit sécurité effectué	4	Fonction Prestations
ESI 40	Matériels et logiciels non conformes	2	Fonction Prestations
ESI 41	Pas d'envoi d'attestation, mais effacement effectué	1	5 jours
ESI 41	Effacement non effectué	5	0 jour
ESI 42	Sans objet	Sans objet	Sans objet
ESI 42	Effacement non effectué	4	0 jour
ESI 43	Non-respect des règles et stratégies sécurité de l'Acheteur	5	0 jour
ESI 44	Pas de transfert de compétences	3	5 jours
ESI 44	Transfert incomplet de compétences	1	10 jours
ESI 45	Engagement de respecter les Règles de déontologie des Administrateurs	5	Fonction prestations
ESI 46	Gestion des comptes Administrateurs non conforme à la directive de sécurité Groupe Safran relative à l'administration des SI	5	Fonction prestations
ESI 47	Non désactivation de compte compromis ou de compte Prestataire en fin de mission	5	0 jours
ESI 48	Privilèges d'administration sur les SI de l'Acheteur sans une validation préalable formelle du Service de Sécurité de l'Acheteur.	5	Fonction prestations
ESI 49	Absence de séquestre des comptes « Administrateurs » du Prestataire	4	0 jours
ESI 50	Plate-forme d'administration des systèmes de l'Acheteur non-conforme aux recommandations	3	Fonction prestations
ESI 51	Moyens techniques utilisés dans le cadre de l'exploitation et administration des équipements non-conformes	3	Fonction prestations
ESI 52	Moyens techniques et procédures de gestion des mots de passe non-conformes aux principes de sécurité Groupe Safran	5	2 jours
ESI 53	Absence de chiffrement des informations	2	5 jours

Référence de l'exigence	Libellé du risque (si plusieurs risques associés à la même exigence)	Niveau de criticité	Remise en conformité sous délai
	appartenant à l'Acheteur stockées sur des supports mobiles utilisés par le Prestataire		
ESI 54	Opérations de maintenance et de transfert des matériels non-conformes aux règles de sécurité Groupe Safran et procédures de sécurité de l'Acheteur	2	5 jours
ESI 55	Absence de dispositifs de protection antivirale sur les équipements administrés par le Prestataire	5	0 jours
ESI 56	Utilisation de logiciels n'ayant pas fait l'objet d'un agrément préalable par le Service de Sécurité de l'Acheteur.	2	Fonction prestations
ESI 57	Sans objet	Sans objet	Sans objet
ESI 58	Absence de mise en œuvre de moyens techniques de supervision et surveillance des systèmes, de gestion des espaces disques et de planification des traitements	3	Fonction prestations
ESI 59	Absence de mise en œuvre des moyens garantissant la continuité de service	3	Fonction prestations
ESI 60	Procédures techniques d'administration et d'exploitation des systèmes et équipements ne correspondant pas aux besoins de l'Acheteur ou non conformes aux bonnes pratiques et aux règles de sécurité	2	Fonction prestations
ESI 61	Correctifs de sécurité non appliqués sur les systèmes et équipements dont il assure l'exploitation et/ou l'administration	5	2 jours
ESI 62	Absence ou refus de fourniture des justificatifs requis par le service de Contrôle Interne de l'Acheteur	4	5 jours
ESI 63	Protection physique et environnementale des systèmes et équipements non conformes	4	10 jours
ESI 64	Absence de suivi de l'activité sécurité et de revue régulière des journaux d'événements	4	Fonction prestations
ESI 65	Procédures de gestion des comptes et des droits d'accès aux équipements et systèmes non conformes	5	0 jours
ESI 66	Organisation ne respectant pas le principe de séparation des privilèges	4	5 jours
ESI 67	Installation et configuration des équipements informatiques et composants d'infrastructure conformes aux recommandations	3	10 jours
ESI 68	Absence de réalisation des audits d'intrusion périodiques	4	Fonction prestations
ESI 69	Evolution des systèmes et des composants d'infrastructure impactant la sécurité sans validation formelle du Service de Sécurité de l'Acheteur	5	Fonction prestations
ESI 70	Absence de mise en place de Plan de secours (PSI) pour les systèmes exploités et administrés par le Prestataire	4	10 jours

Annexe 1 : liste des documents applicables

Les Exigences de Sécurité sont susceptibles d'être modifiées régulièrement (évolutions des documents ci-dessous, ajout de nouveaux documents…). A chaque modification, la nouvelle version des Exigences de Sécurité sera fournie au Prestataire qui s'engage à la respecter dans sa nouvelle version en vigueur.

Les documents applicables à la prestation seront transmis et étudiés lors de la phase de contractualisation.