Domaine : Systèmes d'Information et télécommunication **Entité émettrice :** DSIT – DESIGN - PRS **Nature du document : Clausier**		**Id. Rte :xxx** **Id. métier** : <Ide
Version 1	**EXIGENCES DE SÉCURITÉ POUR DES SERVICES EXTERNALISÉS : SAAS, IAAS, PAAS**	**Date d'approbation** <Date Approbation>
Statut		**<Caractère prescriptif>** **Date d'applicabilité :** <Date Applicabilité>
Accessibilité <Accessibilité calculée>		**Date de fin de validité :** [Date de fin de validité] **Revue d'exigence :** [simplifiée ou détaillée]
	17 Pages	[00] **Annexes**

***Attention : dans les pages de garde, seules les zones de texte entre les symboles […] sont à saisir à la main, les autres champs sont mis à jour automatiquement.**

Documents annulés :

Documents de référence :

Référence fonctionnelle : […]

Description :

Ce document décrit l'ensemble des clauses « Sécurité SI » applicables aux CCTP dans le cadre de prestations de services externalisés. Celles-ci sont en particulier pour les Logiciels en tant que service.

Il peut également être utilisé dans le cadre d'un contrat en gré à gré comme base de travail pour rédiger des exigences de sécurité

L'objectif de ce clausier est d'indiquer pour chaque consultation la question : Quelles sont les exigences prévues pour le contexte concerné ?

Rte - Réseau de Transport d'Électricité
[00, Nom de la Rue]
[00000 Ville Cedex 00]

Rédacteur(s)		Vérificateur(s)		Approbateur(s)	
Nom(s)	Date(s)	Nom(s)	Dates(s)	Nom	Dates(s)
Nadir AMROUCHE		Cyrille GERARD Benjamin BAA-PUYOULET		Laurent POTIER Jean-Philippe GRAS,	

Lieu de stockage : [Lieu]

Diffusion

Pour action	Pour information
	Nicolas Trinchant, Daphne ZANATTA

Historique

Indice	Date	Projet ou Pour approbation	Rédacteur(s)	Modifications
0.1	28/05/2025	Projet	Nadir AMROUCHE	Création du document
0.2	05/07/2025	Projet	Nadir AMROUCHE	Prise en compte des remarques de C. GERARD, L. POTIER, B. BAA-PUYOULET
1	16/07/2025	Pour approbation	Nadir AMROUCHE	

Sommaire

1 Objet du document

Ce document décrit l'ensemble des clauses de Sécurité SI applicables lors de tout achat de prestations de services externalisés.

Il définit les exigences de sécurité à respecter par le prestataire. Il encadre la protection des données, la confidentialité, l'intégrité et la disponibilité des systèmes. Les clauses imposent souvent des audits, des notifications d'incidents et le respect des normes (ISO 27001, RGPD, etc.). L'objectif est de réduire les risques liés à la sous-traitance et d'assurer la conformité aux politiques internes.

2 Définition d'un service externalisé

Au sens de ce clausier, un service externalisé correspond à un logiciel (SAAS), une infrastructure (IAAS) ou une plateforme (PAAS) opéré(e) par un fournisseur de services depuis un SI externe et dont la mise en œuvre ne nécessite pas de raccordement physique direct au réseau du SI de RTE.
En revanche, l'extension de Data Center (DC) sur Azure pilotée par le CCOE ne relève pas du périmètre des services externalisés tels que définis ci-dessus, car ces infrastructures demeurent soumises aux mêmes exigences de sécurité que les DC On-Premise de RTE

3 Organisation de la sécurité de l'information

3.1 PSSI

Le Titulaire s'engage à disposer d'une Politique de Sécurité des Systèmes d'Information (PSSI) conforme à l'état de l'art, à jour et effectivement appliquée. Cette PSSI devra être révisée et mise à jour au minimum une fois par an. En cas de modifications susceptibles d'avoir un impact sur le périmètre du service fourni, le Titulaire devra en informer préalablement RTE. La PSSI doit être consultable par RTE à tout moment sur demande.
Le Titulaire doit respecter la Politique de Sécurité du SI (PSSI) de RTE
Cette dernière est consultable par les soumissionnaires, sur demande, dans le cadre de l'appel d'offre.

3.2 Plan d'Assurance Sécurité (PAS)

Le Titulaire s'engage à fournir un Plan d'Assurance Sécurité (PAS) détaillant l'ensemble de ses engagements ainsi que l'organisation mise en place pour répondre aux exigences de RTE.
Ce document devra notamment décrire :

- Les processus opérationnels et de sécurité déployés dans le cadre de la prestation,
- Les rôles et responsabilités des différents acteurs impliqués,
- La nature des documents et données échangés,
- Ainsi que la fréquence de ces échanges.

3.3 Interlocuteur Sécurité SI

Le Titulaire désigne un interlocuteur Sécurité unique, responsable de la sécurité de l'ensemble de la prestation, y compris des éventuels sous-traitants, et ce, pour toutes les phases du contrat.

Le Titulaire garantit que cet interlocuteur — ou son suppléant en cas d'indisponibilité — est joignable par RTE durant les heures ouvrées.

Par ailleurs, le Titulaire s'engage à désigner un contact opérationnel spécifiquement en charge du traitement des incidents de sécurité. Ce contact sera l'interlocuteur de RTE pour tout signalement d'incident et devra être en mesure d'initier les actions correctives nécessaires.
Les coordonnées, modalités de contact et procédures associées devront être précisées dans le Plan d'Assurance Sécurité (PAS).

Le Titulaire informe RTE lorsqu'il désigne un nouvel Interlocuteur Sécurité et met à jour le PAS.

4 Gestion des actifs

4.1 Propriété des données

Par défaut, RTE est seule propriétaire et responsable de traitement de toutes les données au périmètre de la prestation, aussi bien des données confiées au Titulaire par RTE que des données collectées par le Titulaire sur instruction de RTE.

4.2 Classification et protection des informations du patrimoine de RTE

La criticité des informations manipulées par le Titulaire est évaluée à partir des critères DICT (Disponibilité ; Intégrité ; Confidentialité ; Traçabilité) :

	1	2	3	4
Disponibilité	Indisponibilité maximale de 1 mois	Indisponibilité maximale de 5 jours	Indisponibilité maximale de 24h	Indisponibilité maximale de 4h
Intégrité	Pas d'exigence d'intégrité	La conservation de l'intégrité est assurée par un contrôle de base du périmètre d'accès, mais sans surveillance systématique d'une éventuelle modification incontrôlée. La restauration de l'information est possible	Intégrité moyenne. La conservation de l'intégrité est assurée par un contrôle renforcé du périmètre d'accès. La perte d'intégrité est limitée par des moyens d'identification, d'alerte et de restauration	Intégrité forte. La conservation de l'intégrité est garantie. Non-répudiation : la solution apporte la preuve formelle (par exemple par une "signature électronique") que la donnée n'a pas été modifiée volontairement ou non
Confidentialité	Libre - La conservation de la confidentialité n'est pas assurée	La conservation de la confidentialité est assurée par un contrôle de base du périmètre d'accès, mais sans surveillance systématique d'un éventuel contournement	Accès Restreint - La conservation de la confidentialité est assurée par un contrôle renforcé du périmètre d'accès. La perte de confidentialité est limitée par des moyens d'identification et d'alerte	Confidentiel - La conservation de la confidentialité est garantie
Traçabilité	Pas de traçabilité	Vérification a posteriori, uniquement en cas d'incident suspecté par ailleurs, ou par sondage	La journalisation des accès aux ressources et traitements sensibles est contrôlée régulièrement et conservée pendant un délai fixé. Elle garantit l'authentification de ces accès	Traçabilité forte. La journalisation des accès aux ressources et traitements sensibles est contrôlée de manière permanente, conservée pendant un délai fixé, et/ou possède une valeur juridiquement probante

4.3 Type, sécurisation et localisation de l'hébergement des données

Le Titulaire s'engage à cloisonner, physiquement ou logiquement, les ressources (données, paramétrage, traitement, interface…), de RTE (notamment pour répondre à des contraintes réglementaires), et par rapport aux ressources des autres clients. Le Titulaire met en œuvre pour cela des dispositifs de sécurité au niveau réseau ou applicatif, reposant sur du matériel physique ou logiciel.

Le Titulaire s'engage à cloisonner, physiquement ou logiquement l'environnement de production de la prestation, des autres environnements (développement, recette, etc.) Les modalités de cloisonnement seront décrites dans le PAS.

Le Titulaire décrit de manière exhaustive ces mécanismes de protection dans le PAS et transmet à RTE un schéma d'architecture technique.

Le Titulaire héberge l'ensemble des données de RTE pour tous les environnements (développement, recette, préproduction, production) en Union Européenne y compris pour les données hébergées chez ses sous-traitants. La description détaillée de la localisation des données de RTE devra être précisé dans le PAS.

Le Titulaire précisera également la localisation des différents composants de son infrastructure.
RTE se laisse la possibilité de réaliser (à ses frais) des audits de vérification.

RTE dispose d'une classification des données, le Titulaire s'engage à la prendre en compte et la respecter dans le cadre de la prestation.

5 Politique de contrôle d'accès

5.1 Gestion des habilitations des ressources internes du Titulaire

Le Titulaire s'engage à mettre en place un processus de gestion des habilitations pour l'ensemble des accès aux environnements liés à la prestation, qu'ils soient réalisés par ses propres utilisateurs ou par ceux de ses sous-traitants. Ce processus, formalisé dans le Plan d'Assurance Sécurité (PAS), devra être soumis à validation de RTE.

Le processus devra couvrir l'ensemble du cycle de vie des accès, incluant les demandes de création, de modification et de suppression.

Par ailleurs, le Titulaire s'engage à transmettre à RTE, au minimum une fois par an, un compte rendu détaillé de la revue des habilitations réalisée.

5.2 Fédération d'identités

Le Titulaire s'engage à permettre aux utilisateurs internes de RTE de s'authentifier pour accéder aux services et fonctions décrits dans le CCTP, y compris pour les besoins d'administration.

Quel que soit le type d'application fourni (web ou mobile), le service d'accès devra assurer une continuité de l'authentification de manière transparente pour les utilisateurs de RTE, en déléguant cette authentification au gestionnaire d'identités de RTE (G@IA).

Le service d'accès doit être compatible avec les standards OpenID Connect et OAuth (version 2.0 minimum) ou, à défaut, avec le protocole SAML 2.0. Dans ce dernier cas, le Titulaire s'engage à faire évoluer son système vers OpenID Connect sur simple demande de RTE.

Par ailleurs, tout autre protocole d'authentification en vigueur ou imposé par des exigences réglementaires ou de sécurité pourra être exigé par RTE.

Les habilitations des utilisateurs de RTE seront gérées via un mécanisme de rôles ou profils. Le Titulaire reste responsable du contrôle des habilitations lors de la connexion, sur la base des informations transmises par le service WebSSO de RTE. En cas d'évolution des rôles pendant la durée de la prestation, le Titulaire s'engage à adapter son système en conséquence.

Le PAS reprendra et détaillera les engagements du Titulaire en matière de contrôle d'accès des utilisateurs internes de RTE.

5.3 Inscription et enregistrement des utilisateurs sur le service d'accès

Quelle que soit la méthode utilisée, le Titulaire s'engage à sécuriser l'enregistrement ou l'inscription des utilisateurs internes et/ou externes de RTE au service d'accès.

Le Titulaire devra décrire dans le Plan d'Assurance Sécurité (PAS) les processus mis en œuvre pour l'enregistrement et l'inscription des utilisateurs, ainsi que les mesures de sécurisation associées.

6 Sécurité physique et environnementale

6.1 Sécurité physique des installations et sites du Titulaire

Lorsque des prestations sont réalisées sur un ou plusieurs sites du Titulaire, ce dernier s'engage à mettre en œuvre des mesures de protection physique adaptées au périmètre de la prestation, conformément à la politique de contrôle d'accès applicable (celle du Titulaire ou celle de RTE, selon la nature de la prestation).

Ces mesures doivent permettre de prévenir les dommages liés :

- aux intrusions,
- aux incendies,
- aux fuites d'eau,
- aux risques environnementaux,
- ainsi qu'aux actes physiques, accidentels ou malveillants.

Le Titulaire s'engage à effectuer des contrôles physiques et environnementaux afin de sécuriser le périmètre de la prestation, de manière proportionnée au niveau de risque identifié. Il devra informer RTE des résultats de ces contrôles, lesquels seront réalisés selon une fréquence pertinente (par exemple, au minimum une fois par an).

En cas de recours à un sous-traitant, le Titulaire s'assurera que ce dernier a mis en place des mesures équivalentes de protection physique sur ses propres installations.

7 Sécurité liée à l'exploitation

7.1 Correctifs de sécurité et gestion des vulnérabilités

Le Titulaire met en place les protections nécessaires pour sécuriser son SI et l'ensemble des ressources couvertes par la prestation contre les menaces, incluant les vulnérabilités, les logiciels malveillants et les attaques externes. Une veille technologique permanente est assurée sur l'ensemble des produits et solutions utilisés dans le cadre de la prestation.

En cas de détection d'une vulnérabilité, le Titulaire s'engage à mettre en œuvre, sans délai, un plan de correction complet et informer le Cert RTE. Les mesures correctives sont appliquées dans des délais contrôlés, sans générer de surcoûts pour RTE.

Le Titulaire s'engage à réaliser ou faire réaliser des contrôles réguliers de sécurité, et des revues de code permettant de quantifier ou qualifier la bonne application des engagements de sécurité du Titulaire.

Le Titulaire fournit à RTE, sur simple demande, l'ensemble des justificatifs attestant de la réalisation effective de ces contrôles de sécurité et des corrections apportées.

7.2 Chiffrement des données de RTE

Le Titulaire s'engage à assurer le chiffrement des informations « interne » (équivalent C=2), sensibles classées « Restreint » (équivalent C=3) et « Confidentiel » (équivalent C=4) de RTE, à la fois au repos (données stockées) et en transit (données transférées). Cette exigence est obligatoire sur l'ensemble du périmètre de la prestation.

Toute opération de chiffrement, qu'elle concerne les données au repos ou en transit, devra être réalisée à l'aide d'algorithmes de chiffrement conformes à l'état de l'art, et en accord avec les exigences de l'ANSSI.

La création, la distribution, ainsi que la gestion des clés cryptographiques devront impérativement respecter les règles et recommandations de l'ANSSI.

7.3 Chiffrement des communications

Toute opération de chiffrement des données (au « repos » ou en « transit ») sur le périmètre de la prestation, doit s'effectuer via des algorithmes de chiffrement à l'état de l'art conformément au Référentiel Général de Sécurité de l'ANSSI.

7.4 Journalisation des accès et traitements

Le Titulaire doit tracer l'activité (accès, écriture, mise à jour, suppression,) des accès et traitements des données de RTE.

Le Titulaire met également en œuvre une journalisation des activités système (dont sauvegardes) dans le périmètre de la prestation.

7.5 Supervision des traces

Le Titulaire s'engage à superviser les traces du périmètre de la prestation et des composants logiciels et matériels utilisés, par exemple via un SIEM, notamment pour prévenir et détecter des tentatives d'attaques et des incidents de sécurité.

Le Titulaire s'engage à donner accès aux traces du périmètre de la prestation, ou à envoyer ces traces, aux entités de RTE qui le demandent.

Les modalités d'accès aux traces seront définies avec le Titulaire et décrites dans le PAS.

7.6 Sauvegardes

Le Titulaire s'engage à disposer de sauvegardes régulières lui permettant de satisfaire le besoin de disponibilité et les SLA annoncés. Il s'engage également à sécuriser ces sauvegardes selon le niveau de confidentialité demandé.

Le Titulaire procède à la vérification régulière des sauvegardes via des tests de restauration, a minima à la mise en place de la prestation et une fois par an.

8 Acquisition, Développement, Maintenance des Systèmes d'Information

8.1 Sécurité des développements

Le Titulaire garantit la sécurisation des développements (portails, scripts d'administration, etc.) conformément aux bonnes pratiques en vigueur pour chaque technologie utilisée.

Le Titulaire peut recourir à ses propres outils ou à ceux de RTE pour assurer cette sécurisation.

Le Titulaire s'engage à effectuer – ou à faire effectuer – des audits de sécurité et des revues de code régulières afin d'évaluer le respect de ses obligations en matière de sécurité et d'en présenter le résultat et les plans d'actions associées à RTE.

Toute vulnérabilité identifiée lors des revues de code sera corrigée par le Titulaire à ses frais. Il devra établir un plan de correction, et remédier aux anomalies dans des délais raisonnables, sans coût supplémentaire pour RTE.

Le Titulaire devra préciser dans le PAS (Plan d'Assurance Sécurité) la méthodologie de développement adoptée et les procédures de revue de code appliquées.

RTE se réserve la possibilité de réaliser ses propres revues de code à tout moment.

8.2 Sécurité des accès administrateurs

Le Titulaire garantit la sécurisation de toutes les voies d'administration des composants applicatifs et techniques inclus dans le périmètre de la prestation, notamment par les mesures suivantes (liste non exhaustive) :

- Implémentation d'une politique stricte de filtrage des adresses IP autorisées pour l'administration

- Établissement de connexions VPN sécurisées pour tous les accès techniques aux composants (serveurs, etc.)
- Mise en œuvre de mécanismes d'authentification forte pour les administrateurs (MFA, certificats numériques, etc.)
- Application rigoureuse du principe de moindres privilèges
- Maintien d'un registre exhaustif et actualisé des administrateurs
- Surveillance accrue des comptes à privilèges élevés (applicatifs, réseau et systèmes)

Les opérations d'administration sur les livrables du Titulaire doivent être protégées en confidentialité et intégrité par des protocoles de chiffrement à l'état de l'art. Les protocoles d'administration non retenus par RTE doivent pouvoir être désactivés.

8.3 Exigences relatives aux URL

Le Titulaire doit fournir à RTE la liste des URL d'accès Web au service :

- URL du site Web principal ;
- URL vers lesquelles tout ou partie du site est redirigé ;
- URL des éléments utilisés par ce site depuis des sites tiers,

en précisant :

- le nom de domaine complètement qualifié (FQDN DNS) ;
- le protocole de communication (https, sftp uniquement) ;
- le n° de port de communication ;

Le Titulaire doit utiliser uniquement des URL avec nom de domaine et doit proscrire tout accès par adresse IP.

8.4 Exigences relatives aux certificats

Pour les noms de domaines appartenant à RTE, le Titulaire s'engage à utiliser des certificats fournis par RTE après la fourniture d'un CSR par le Titulaire.

Dans les autres cas, le Titulaire s'engage à utiliser des certificats conformes aux bonnes pratiques :

- Des certificats du marché fournis par un tiers de confiance au Titulaire et reconnu par RTE ;
- Une durée de vie au plus de 13 mois pour les certificats utilisés pour les échanges
- Une taille des clés d'au moins 4096 bits pour l'AC et au minimum 2048 pour le certificat serveur
- Les certificats fournis doivent être basés à minima sur du SHA256
- L'existence d'une CRL consultable par les destinataires finaux
  L'utilisation de certificats dits "wildcard" est interdite
- Le PAS reprendra et détaillera les engagements du Titulaire en matière d'usage de certificats

8.5 Exigences relatives aux noms de domaines

Le Titulaire doit être en mesure de gérer des noms de domaine appartenant à RTE, ou à ses filiales, et qui lui sont délégués à des fins techniques dans le cadre de la prestation.

À ce titre, le Titulaire s'engage à fournir à RTE l'ensemble des informations techniques nécessaires à la mise en place des délégations DNS, conformément aux procédures de RTE.

À l'issue du contrat de service, le Titulaire s'engage à assurer la réversibilité complète des noms de domaine délégués, afin de garantir la restitution sans rupture de service ni perte de données, dans des conditions définies conjointement avec RTE.

8.6 Exigences relatives à l'envoi des mails

Le Titulaire s'engage à mettre en œuvre les standards dans la règle de l'art pour la protection des mails contre le spam et le phishing.

8.7 Sécurité des API

Le Titulaire s'engage à mettre en œuvre le niveau de sécurité requis pour sécuriser l'ensemble des APIs mises à disposition de RTE.

Le service d'accès doit authentifier les applications interfacées via API, soit via un certificat serveur, soit via une solution IAM supportant des normes de type OAuth ou OpenID Connect.

Les accès via API au service d'accès et les échecs d'authentification doivent être journalisés.

Dans le cas de l'utilisation d'un certificat serveur, celui-ci peut être délivré soit par le Titulaire soit par RTE. L'autorité qui délivre le certificat doit gérer la suspension et la révocation des certificats d'authentification des applications.

Le Titulaire doit maintenir à jour ce niveau de sécurité.

Pour ce faire, le Titulaire s'engage à (non exhaustif) :

- Dresser un inventaire précis de l'ensemble des API utilisés dans le cadre du service délivré
- Surveiller de manière permanente le comportement des API : identifier les divers consommateurs et analyser les utilisations qui en sont faites (nombre de sollicitations…)
- Assurer la gestion des droits d'accès aux API
- Sécuriser les échanges en mettant en œuvre des protocoles sécurisés.
- Le Titulaire décrit de manière exhaustive dans le PAS les dispositions qu'il prend dans le cadre de la sécurisation de ses APIs..

8.8 Protocoles standards réseaux

Le Titulaire doit utiliser uniquement les ports standards des protocoles réseau, sans encapsulation de protocoles tiers dans un tunnel TLS, en websocket, etc.

Pour les accès bureautiques, le Titulaire doit limiter la liste de ces protocoles à https.

8.9 Exigences relatives aux navigateurs

Le Titulaire doit garantir le fonctionnement de son service d'accès pour les accès bureautiques, mobiles et d'administration, avec un navigateur standard à jour, sans aucun greffon, extension ou client lourd.

Le -ou les- navigateurs de référence et leurs systèmes d'exploitation seront définis entre RTE et le Titulaire.

Sur les postes de travail de RTE, le SERVICE doit fonctionner sur ces navigateurs tels que définis précédemment, dans la version courante ainsi qu'a minima dans une version majeure antérieure.

Sur les postes de travail n'appartenant pas à RTE, le SERVICE doit fonctionner sur les principaux navigateurs Web du marché (Chrome, Firefox, IE, Edge et Safari) dans leur version courante ainsi qu'a minima dans une version majeure antérieure.

8.10 Règles de mise en cache

Le Titulaire doit déployer des règles de mise en cache, permettant la mise à jour du SERVICE sans intervention sur les serveurs mandataires (proxy) et navigateurs de RTE.

8.11 Gestion de la continuité d'activité

Le Titulaire garantit le maintien du service en toutes circonstances, y compris lors d'incidents majeurs ou de crises exceptionnelles voire de pandémies

Un Plan de Continuité d'Activité (PCA) est mis en place et testé régulièrement, avec la participation de RTE. Ce plan prévoit :

- Les mesures permanentes de préparation à la reprise d'activité
- L'organisation pour basculer sur une plateforme de secours sous un délai conforme aux engagements.
- Les modalités de test et de retour à la normale

RTE peut demander à tout moment les résultats des tests du PCA dans le cadre du suivi de la prestation.

9 Gestion des incidents liés à la sécurité de l'information

9.1 Remontée des événements et des failles liés à la sécurité de l'information

Le Titulaire définit conjointement avec RTE une classification (en fonction de leur typologie, de leur volumétrie et/ou de leur impact) des évènements et incidents de Sécurité SI sur le périmètre de la prestation.

Ce travail est réalisé avec le responsable désigné au sein de RTE dans le cadre de la prestation (à défaut le pilote opérationnel de la prestation ou son manager).

Le Titulaire indique, dans sa procédure de gestion des incidents liés à la sécurité du SI, les différentes classes d'évènements et d'incidents identifiées.

9.2 Mise sous contrôle

Le Titulaire s'engage à prendre toutes les mesures nécessaires pour confiner les conséquences d'un incident de sécurité SI (au sens ITIL du terme) et mettre en œuvre les moyens nécessaires afin de recueillir les traces liées à cet incident, afin de pouvoir faire une analyse approfondie des causes et effets, pour :

- Déterminer les mesures correctives et permettre un retour à un fonctionnement nominal ;
- Définir les mesures préventives pour éviter une reproduction de l'incident ;
- Permettre à RTE d'engager les mesures nécessaires.

Le Titulaire s'engage à ce que les traces recueillies puissent servir de preuve en cas de recours légal.

Le Titulaire s'engage à mettre à disposition de RTE les fichiers journaux permettant au système de supervision de RTE de détecter automatiquement des alertes.

9.3 Communication

Le Titulaire s'engage à prendre les dispositions pour limiter le nombre et les impacts des incidents de sécurité SI. Le Titulaire s'engage à mettre en place un circuit d'alerte, de traitement et de reporting associé.

Ces dispositions sont formalisées dans le PAS.

9.4 Gestion de crises

Une situation de crise peut être déclenchée par le Titulaire ou par RTE.

Le Titulaire doit prendre en compte les exigences de RTE dans son processus de gestion de crises.

Le Titulaire doit s'impliquer dans le suivi des crises même si leur origine n'est pas de sa responsabilité et agir en coordination avec l'ensemble des acteurs concernés de RTE pour sortir au plus vite des crises.

Dès le démarrage d'une crise, RTE et le Titulaire organisent une réunion pour établir un diagnostic de la situation, évaluer les risques et mettre en place des moyens et une organisation permettant de gérer la crise.

RTE et le Titulaire conviennent d'un plan d'actions pour résoudre les problèmes et revenir au plus vite vers une situation normale.

Le Titulaire doit indiquer ses solutions pour travailler en mode dégradé en cas de crise durable.

Une fois la crise terminée, RTE et le Titulaire font un retour d'expérience.

10 Conformité

10.1 Règlementations particulières, normes et conformité technique

Le Titulaire s'engage à être en tous points conformes aux lois et règlementations en vigueur, notamment RIA[1]. Cette conformité doit être assurée pour toute la durée de la prestation et prendre en compte les éventuelles évolutions de la réglementation Française et Européenne.

10.2 Respect des principes RGPD

Le Titulaire s'engage à respecter l'intégralité des principes du Règlement Général sur la Protection des données conformément aux éléments transmis avec le CCTP, notamment avec les mises en œuvre de recommandations d'un AIPD en ce qui concerne les données à caractère hautement personnel.

10.3 Auditabilité

RTE se réserve le droit de procéder à des audits de sécurité — portant sur les services, les processus associés, l'infrastructure et la sécurité des flux — afin de vérifier, ou faire vérifier, la conformité du Titulaire à l'organisation décrite dans le PAS, ainsi que le respect des procédures et normes mentionnées dans ce document.

Le périmètre concerné couvre les services fournis, y compris l'IHM, les infrastructures, la sécurité de flux et les processus associés.

Afin de permettre la réalisation des audits de sécurité, RTE transmettra préalablement au Titulaire un protocole précisant les modalités de déroulement ainsi que le périmètre de l'audit.

RTE se réserve également la possibilité d'utiliser des outils de vérification de la conformité aux règles de sécurité (tels que des scanners web). Ces outils ou scripts pourront être fournis au Titulaire.

Le Titulaire s'engage à mettre en œuvre toutes les dispositions nécessaires pour permettre le bon déroulement des audits. À ce titre, il devra faciliter le travail des auditeurs, notamment en répondant à leurs questions, en fournissant la documentation requise, et, si nécessaire, en donnant accès à une plateforme de test représentative de l'environnement de production.

En particulier, le Titulaire s'engage à transmettre à RTE toute information permettant de démontrer le respect de ses obligations en matière de traitement des données à caractère personnel, dans le cadre des audits ou inspections réalisés par RTE.

RTE se réserve la possibilité de mandater un auditeur tiers pour la conduite de ces audits.

Le Titulaire devra fournir aux auditeurs les documents demandés en langue française et désigner, le cas échéant, un interlocuteur technique francophone.

Sur demande de RTE, le Titulaire s'engage à fournir des rapports d'audits récents, réalisés à son initiative ou à celle d'un tiers, hors audits commandités par RTE.

[1] RIA (AI Act) : Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle (Règlement - UE - 2024/1689 - EN - EUR-Lex)

Dans le cas où le Titulaire ne souhaiterait pas que RTE procède directement à des audits ou contrôles, il devra lui transmettre les rapports issus des audits équivalents déjà réalisés.

10.4 Audits internes

Le Titulaire met en œuvre des contrôles et des audits internes sur le périmètre de la prestation afin de s'assurer du respect des :

- Règles et procédures de Sécurité SI de RTE
- Engagements contractualisés

Le Titulaire fournit à RTE un planning prévisionnel à jour des audits et contrôles, ainsi que les résultats obtenus.

10.5 Corrections à la suite des audits

RTE sélectionne les non-conformités et/ou vulnérabilités à corriger parmi celles détectées lors des audits, des contrôles et des revues de vulnérabilités réalisés par RTE et/ou le Titulaire en interne.

Le Titulaire doit proposer un plan de résorption de ces non-conformités et/ou vulnérabilités (intégrant un planning) et s'engager à le respecter.

RTE pourra procéder à un contrôle pour s'assurer de la mise en œuvre du plan d'actions.

Les flux entre le SI de RTE et le ou les sites du Titulaire doivent pouvoir être audités

Les flux entrants et sortants des services doivent pouvoir être audités.

Si des prestations sont réalisées sur un ou des sites du Titulaire, ce dernier doit fournir le nécessaire pour permettre à RTE de déchiffrer le flux et auditer les informations qui transitent dans les canaux de communications entre le Titulaire et RTE.

11 Réversibilité

11.1 Réversibilité de la prestation

En cas cessation total ou partiel du service, le Titulaire doit :

- Transférer toutes les compétences nécessaires
- Fournir l'ensemble de la documentation technique
- Remettre les livrables dans leur dernière version
- Transmettre les données générées dans un format standard sécurisé
- Maintenir jusqu'à la fin effective une qualité de service et un niveau de sécurité inchangés
- Désactiver immédiatement tous les accès et autorisations de son personnel
- Soumettre un plan de réversibilité détaillé dans les 3 mois suivant le début du contrat en s'appuyant sur le modèle fourni dans l'offre technique initiale
- Prévoir une assistance technique à RTE ou au tiers désigné

La phase de réversibilité sera exécutée pendant la période de 3 mois précédant la date effective de cessation de la prestation ou si cette date n'est pas connue, pendant 3 mois suivant la date de réception de la notification de la résiliation du contrat.

11.2 Restitution et/ou destruction des données

Le Titulaire s'engage à restituer de manière sécurisée toutes les données déchiffrées de RTE sur un support et format exploitable convenu entre les deux parties.

Le Titulaire s'engage sur toute la durée du contrat, à avoir la capacité de purger à la demande de RTE, toutes ou partie des données liées à la prestation (destruction sécurisée). Dans des conditions qui assurent l'effacement définitif et irréversible de l'ensemble des données et sauvegardes relatives à la ressource. Le Titulaire s'engage à fournir un rapport mentionnant le succès ou l'échec de l'opération et la méthode utilisée pour réaliser la purge.

Le Titulaire s'engage à détruire toutes les copies existantes des données dans ses systèmes d'information avant le terme du marché, et à le justifier par écrit en fournissant un PV de destruction (effacement sécurisé) à RTE. Le Titulaire s'engage à obtenir l'accord de RTE avant d'effectuer cette destruction.