Charte de sécurité - Prestataires

Sommaire

1- PREAMBULE

1.1 Objectif et champ dôapplication du document

L'activité de REDAL repose en partie sur les performances, la fiabilité et la sécurité de ses systèmes d'information.

Dans cette optique, un engagement de bonne conduite est demandé à chaque personne morale ou physique, ayant à intervenir sur les systèmes de REDAL ou sur les infrastructures associées, que ce soit en tant que professionnel du domaine technique concerné ou en tant que simple utilisateur.

La présente << charte de sécurité>>, destinée aux prestataires retenus, synthétise ou sein d'un unique document les exigences de sécurité de REDAL à l'égard des systèmes d'information, leurs conséquences sur le déroulement des missions des prestataires et l'engagement de ces derniers à respecter le code déontologique de REDAL en terme de systèmes d'information.

1.2 Structure du document

La charte de sécurité se compose de trois parties :

- La présentation, dans ses grandes lignes, de la politique de sécurité de REDAL, notamment de son organisation et de ses principes de base ;
- La déclinaison de ces principes de sécurité en règles opérationnelles, appliquées au cas de la prestation de service ;
- L'engagement de bonne conduite du prestataire et de son personnel affecté à l'exécution de la mission auprès de REDAL.

1.3 Champ dôapplication

La présente charte de sécurité s'applique aux prestations portant sur :

- Les **infrastructures** (locaux techniques et équipements) nécessaires au fonctionnement des systèmes d'information ;
- Les **matériels** informatiques et de télécommunication ;
- Les **données de configuration de ces matériels** ;
- Les **données de production ou de test** ;
- Les **applications** ;

Que ces prestations aient pour objet :

- La **conception** ;
- La **mise en œuvre** ;
- La **maintenance** ;
- **L'exploitation**.

des éléments constituant les systèmes d'information de REDAL.

La présente charte est systématiquement annexée au CPT ou au cahier des charges pour l'acquisition de Matériels, logiciels, systèmes ou prestation en relation avec le SI.

On en garantit ainsi sa mise en œuvre car elle est signée préalablement à la notification du marché.

1.4 Mise à jour du document

REDAL met en place une procédure de révision périodique de la présente charte.
Cette procédure s'inscrit dans la démarche d'amélioration continue de la SSI.

2- PRESENTATION DE LA POLITIQUE DE SECURITE DES INTERVENANTS EXTERNES

2.1 Objectifs généraux.

Le présent paragraphe reprend les points concernant les intervenants externes à REDAL, qui dans le cadre de contrats de prestation, sont en relation avec les systèmes d'information de REDAL.

2.2 Description de lôorganisation en charge de la sécurité des systèmes dôinformation.

2.2.1 Le responsable de la sécurité des SI

La sécurité des systèmes d'information de REDAL est la préoccupation privilégiée d'une personne détachée à cet effet : le responsable de la sécurité des SI.

Ce dernier à la charge :

- De s'assurer du respect des principes et de l'application des règles de sécurité de REDAL ;
- D'assurer la diffusion et la mise à jour des principes de sécurité de REDAL ;
- De centraliser les éléments opérationnels relevant de la sécurité des systèmes d'information, depuis leur conception jusqu'à leur mise en œuvre et à la gestion des incidents de séurité ;
- D'assurer le relais, en termes de sécurité, à la fois
    - Entre les équipes techniques et les utilisateurs
    - Entre REDAL et les intervenants extérieurs.

A ce titre, le responsable de la sécurité des SI est, in fine, le destinataire de toute remarque relative à la sécurité des systèmes d'information de REDAL.

2.2.2 Les directions métiers

Les différentes directions métiers, au cœur chacune d'une activité clé de REDAL, sont les propriétaires de l'information, des systèmes dédiés à son traitement ou des infrastructures nécessaires à leur fonctionnement.

De ce fait, les directions métiers définissent des exigences spécifiques en termes de sécurité en regard des prestations contractées avec des sociétés externes.

2.3 Les principes fondamentaux de la sécurité des systèmes d'information

Afin de maintenir la fiabilité et les performances des activités de REDAL, toute personne intervenant sur un des éléments des systèmes d'information doit porter une attention particulière :

- A la disponibilité des services ;
- A la confidentialité des informations relatives tant aux systèmes qu'aux métiers de REDAL
- A l'intégrité des informations et des systèmes ;
- A l'auditabilité de ses interventions sur les systèmes.

Les règles de sécurité énoncées par REDAL guident les personnes dans le respect de ces critères de sécurité, mais ne sont en rien exhaustives. Toute action sur les systèmes d'information doit être réalisée dans la mesure où elle ne remet pas en cause sa sécurité, même temporairement. Toute dérogation à ce principe doit être avalisée au préalable par le responsable de la sécurité des SI et les directions métiers concernées par la remise en cause du niveau de sécurité requis.

3- REGLES DE SECURITE APPLICABLES AUX PRESTATAIRES

3.1 Règles générales.

➔ Toute intervention sur un des éléments des systèmes d'information doit faire l'objet d'une autorisation écrite et préalable du responsable de la sécurité des SI, qui valident les conditions de l'intervention et de la réalisation des tâches en collaboration avec le responsable du SI concerné.

➔ Le prestataire se doit d'appliquer un devoir de réserve à l'égard de toute information relative :

- A la nature de son intervention auprès de REDAL ;
- A l'organisation de REDAL et de ses métiers ;
- A l'activité de REDAL ;
- A l'organisation et au fonctionnement de ses systèmes.

➔ L'intervention ne doit, pas porter préjudice :

- Ni l'intégrité des systèmes et des informations ;
- Ni à la continuité des services assurés par ces systèmes ;
- Ni à la confidentialité des données stockées sur ces systèmes.

➔ Dans le cas où le prestataire ne saurait garantir l'une de ces exigences, il doit en aviser REDAL immédiatement et obtenir son accord préalable avant d'intervenir dans tous les cas. Ce dernier est tenu :

- De pouvoir restaurer le système dans son état initial au cas où l'intervention aurait conduit à une modification préjudiciable de l'environnement de REDAL.
- De limiter l'indisponibilité du système à des délais supportables par les directions métiers de REDAL, en accord avec ces dernières.

- ➔ Toute intervention du prestataire doit faire l'objet d'un compte-rendu circonstancié précisant :
  - Le périmètre de l'intervention ;
  - Le mode opératoire suivi ;
  - Les résultats de l'intervention ;
  - Les incidents rencontrés et les anomalies détectées.

- ➔ La détection de toute anomalie ou incident pouvant remettre en cause la sécurité des systèmes d'information doit être rapportée au responsable de la sécurité des SI.

- ➔ Toute dérogation à l'un des principes fondamentaux de sécurité de REDAL ou à l'une des règles décrites dans ce chapitre doit être soumise à l'autorisation préalable du responsable de la sécurité des SI. Cette dérogation ne soustrait en rien le prestataire à son obligation de moyens afin de limiter au maximum les risques potentiels qu'il fait encourir au système d'information dans le champ de son intervention.

Par ailleurs, le prestataire s'engage à respecter dans le cadre de ses interventions les règles détaillées en **Annexe F.**

3.2 Règles spécifiques au domaine de compétence du prestataire

Les règles spécifiques s'appliquant aux prestataires selon le type de prestation réalisée sont données en **Annexe C**.

Outre ces règles associées au domaine d'expertise des prestataires, les personnels de ces derniers sont également soumis aux mêmes règles que le personnel de REDAL concernant l'utilisation des systèmes d'information. A ce titre, REDAL remet au prestataire et à son personnel la « charte informatique».

Les accès distants des prestataires aux plateformes de REDAL sont soumis aux règles de sécurité détaillées en **Annexe D.** Ces règles doivent être implémentées chez le prestataire avant d'établir une connexion distante avec les plateformes de REDAL, il est tenu également de veiller sur la conformité à ces règles durant toute la durée de vie du contrat ou à minima quand un besoin de connexion distante se présente.

4- ENGAGEMENT DU PRESTATAIRE

4.1 Engagement du prestataire.

Le prestataire, en tant que personne morale, s'engage à respecter les principes et règles exposés dans la présente charte en signant et retournant une copie de la page présentée en annexe A.

Le prestataire devra respecter toutes les exigences de sécurité en matière de protection du système d'information notamment les aspects de :

1- Classification de l'information,
2- Accès physiques aux bâtiments et aux locaux,
3- Accès logiques aux systèmes informatiques,

4- Echanges sous toutes ses formes (électroniques, papier, …) ,
5- Gestion d'incidents,
6- Gestion de changement,
7- Respect des lois nationales en vigueur (propriété intellectuelle, protection de la vie privée et des données personnelles, cryptographie,…).

4.2 Engagement du personnel du prestataire

Le personnel affecté par le prestataire à la réalisation de la mission auprès de REDAL signe et retourne une copie de l'engagement individuel fourni en **annexe B**.

Toute intervention ne pourra être réalisée sans la signature préalable des engagements du prestataire et de son personnel.

5- PLAN D'ASSURANCE SECURITE (PAS)

Le fournisseur devra établir un PAS qui décrit les dispositions de sécurité qu'il met en œuvre pour sa prestation. Ce PAS peut être un sous-ensemble du plan d'assurance qualité (PAQ).

À la signature du contrat, le responsable de la sécurité des SI doit pouvoir indiquer s'il accepte le PAS du fournisseur ou non.

Selon le type de projet / prestation, le PAS doit traiter au minimum les thèmes suivants:

- Critères de sécurité utilisés dans la désignation des personnes chargées de l'intervention, engagement de sécurité, information de ces personnes sur la sécurité de la prestation et sensibilisation ;
- Règles de protection des informations relatives au SI ou à l'intervention et détenues par le prestataire (copie, diffusion, conservation, destruction, transmission) ;
- Désignation des sites d'exécution de la prestation, protection et accès physiques des locaux utilisés, séparation vis-à-vis d'autres prestations ;
- Architecture générale de la plateforme utilisée pour l'intervention à distance, cloisonnement technique vis-à-vis d'autres prestations, fonctions de sécurité activées dans la plateforme ;
- Accès logique des intervenants à la plateforme, identification et authentification, mise en veille et déconnexions automatiques, séparation des tâches, gestion des droits, traçabilité des actions ;
- Dispositions prises pour continuer à assurer les activités de la prestation à la suite d'un sinistre majeur ;
- Assurance et contrôle de la sécurité des services d'intervention fournis.

Si l'objet de la prestation porte sur la fourniture ou le développement d'une nouvelle solution informatique ou tout autre projet ayant trait au système d'information, le prestataire doit préciser dans le PAS fourni les règles de sécurité qu'il compte mettre en place pour répondre aux exigences de la DGSSI et se conformer aux bonnes pratiques de manière générale, notamment:

- Les exigences DNSSI (Directive nationale de la sécurité des SI)

- OWASP (Top 10) pour les applications Web
- OWASP (MASVS) pour les applications mobiles (L2 Minimum)

NB : Le PAS fourni sera soumis à l'appréciation du RSSI pour évaluer la pertinence des mesures de sécurité prises par le soumissionnaire.

6- RECETTE SECURITE

La recette sécurité des projets d'acquisition ou de développement de nouvelles solutions consistera en un audit de code et/ou à des tests de pénétration. L'audit sera effectué par des cabinets externes spécialisés dans le domaine, l'objectif étant de s'assurer que ces nouvelles solutions sont conformes aux bonnes pratiques de sécurité et qu'elles ne comportent pas des vulnérabilités pourront mettre à mal la sécurité des SI existant. Toute vulnérabilité et/ou manquement dans la prise en charge des bonnes pratiques de sécurité devront être corrigés obligatoirement par le titulaire de cet appel d'offres avant la mise en production de sa solution et sans avoir à demander des frais supplémentaires à ce titre.

7- ANNEXES :

7.1 Annexe A : Engagement de bonne conduite du prestataire

7.2 Annexe B : Engagement de bonne conduite du personnel du prestataire

7.3 Annexe C : Règles de sécurité spécifiques à chaque type de prestation.

7.4 Annexe D : Règles de sécurité applicables aux accès distants des prestataires

7.5 Annexe E : Règles de sécurité applicables à la DSI REDAL

7.6 Annexe F : Règles régissant les interventions

7.1 Annexe A : Engagement de bonne conduite du prestataire

Engagement de bonne conduite de la société ….

- Attendu que REDAL a demandé à la société_____,

  Société anonyme au capital de _____Dhs,

  Ayant son siège social_____,

  Immatriculée au Registre du Commerce de _____,

  Sous le numéro _____,

  Représentée par M/Mme/Mlle _____, dûment habilité (e) aux fins des présentes,

  Une prestation de

  _____

  Pour l'exécution de laquelle ladite société est amenée à avoir accès à des systèmes ou à des informations ou se voir remettre des informations verbales ou sous toute autre forme qui appartiennent à REDAL.

- Attendu que la divulgation ou l'atteinte à l'intégrité ou à la disponibilité physique ou logique de ces systèmes ou informations est susceptible de nuire aux intérêts de REDAL,
- Et après avoir pris connaissance, au travers du document intitulé << charte de sécurité prestataire>>, des exigences de REDAL en termes de sécurité de ses systèmes d'information ;

La société _____

Reconnait accepter expressément les termes et conditions explicitées dans la << charte de sécurité prestataire>>, et avoir envers REDAL un devoir de réserve et une obligation de satisfaire aux exigences de cette dernière.

Le prestataire s'engage également à communiquer la << charte de sécurité prestataire>> à son personnel qui sera amené, dans le cadre de la prestation, à avoir accès aux informations et systèmes d'information de REDAL, et à faire signer le personnel concerné l'engagement individuel joint ci-après. Le prestataire se porte garant de la bonne exécution par son personnel des obligations susnommées.

Fait à_____, le _____

Pour le prestataire,

Nom : _____

Prénom : _____

Fonction : _____

Signature

7.2 Annexe B : Engagement de bonne conduite du personnel du prestataire

Engagement individuel de bonne conduite du personnel du prestataire

La société _____ a souscrit vis-à-vis de REDAL un engagement de bonne conduite relatif à la sécurité des systèmes et informations de REDAL selon les termes et conditions exposés dans le document libellé << charte de sécurité prestataire>> et dont le présent formulaire constitue une annexe.

Conformément à l'engagement ci-dessus mentionné, le prestataire doit s'assurer que ses collaborateurs engagés dans la réalisation de prestation auprès de REDAL signent un formulaire confirmant qu'ils ont été informés et souscrivent aux obligations contenues dans ladite << charte de sécurité prestataire>>.

Je confirme être employé de la société **présentatrice**, et avoir lu, compris et accepté les termes de la « charte de sécurité prestataire ».

Fait à_____, le _____

Nom : _____

Prénom : _____

Fonction : _____

Signature

7.3 Annexe C : Règles de sécurité spécifiques à chaque type de prestation

Règles de sécurité spécifiques aux prestations de maintenance matérielle

Champ d'application :

Les présentes règles s'appliquent dans le cadre de prestations de maintenance des matériels informatiques (serveurs, postes de travail, imprimantes …).

Enoncé des règles

- **Confidentialité des informations**

Dans la mesure du possible, tout support contenant des informations relatives à l'activité de REDAL doit être maintenu dans les locaux de REDAL.

Si cette disposition ne peut être respectée, l'aval de la direction métier concernée doit être obtenu et le prestataire engage sa responsabilité quant au maintien de la confidentialité desdites informations.

- **Intégrité des informations**

Le prestataire s'assure que ses interventions ne portent aucun préjudice à l'état des informations hébergées par le système, tant pour les données de production que pour les données de configuration du matériel et des logiciels.

- **Intégrité des ressources**

Le prestataire s'assure qu'un retour arrière est possible, dans les délais raisonnables, éventuellement fixés en fonction des attentes de la direction fonctionnelle concernée.

- **Continuité de service**

Le prestataire s'engage à ne pas altérer la continuité de service du système ou à limiter toute éventuelle interruption à la durée la plus réduite possible, sur la période la moins pénalisante pour les entités métiers.

- **Accès physiques**

L'accès aux locaux techniques doit se faire selon les modalités en vigueur à REDAL.

Il peut notamment être exigé que le personnel du prestataire soit accompagné par un collaborateur de REDAL pendant son intervention.

- **Accès logiques**

Dans le cas où un accès au système est indispensable, le prestataire se voit remettre un accès restreint et temporaire qu'il devra utiliser dans le seul cadre de la prestation en cours.

- **Auditabilité**

Les interventions du prestataire sont consignées par écrit et remises à la direction fonctionnelle à la fin de la prestation.

Règles de sécurité spécifiques aux prestations de maintenance des infrastructures

Champ d'application

Les présentes règles s'appliquent dans le cadre de prestations de maintenance des infrastructures indispensables au bon fonctionnement des systèmes d'information.

Il s'agit notamment des locaux techniques, de la climatisation, de l'alimentation électrique des câblages et gaines techniques…

Enoncé des règles

- **Intégrité des informations**

Le prestataire veillera à ce que les paramétrages des équipements dans le périmètre de sa prestation ne soient pas modifiés sans l'accord de la direction opérationnelle (DSI) de REDAL.

- **Intégrité des ressources**

L'intervention du prestataire ne doit en aucun cas altérer l'état ni le fonctionnement des ressources de REDAL, que ces dernières soient ou non dans le périmètre de sa prestation.

- **Continuité de service**

Le prestataire s'engage à ne pas porter atteinte à la continuité de service du système ou à limiter toute éventuelle interruption à la durée la plus réduite possible, sur la période la moins pénalisante pour les entités métiers.

- **Accès physiques**

L'accès aux locaux techniques doit se faire selon les modalités en vigueur à REDAL.

Il peut notamment être exigé que le personnel du prestataire soit accompagné par un collaborateur de REDAL pendant son intervention.

- **Accès logiques**

Dans le cas où un accès au système est indispensable, le prestataire se voit remettre un accès restreint et temporaire qu'il devra utiliser dans le seul cadre de la prestation en cours.

- **Auditabilité**

Les intervention du prestataire sont consignées par écrit et remises à la direction fonctionnelle à la fin de la prestation.

Règles de sécurité spécifiques aux prestations de maintenance des moyens de télécommunication

Champ d'application

Les présentes règles s'appliquent dans le cadre de prestations de maintenance des équipements de communication, voix et données (autocommutateurs, brassage…)

Enoncé des règles

- ### Confidentialité des informations

Le prestataire s'engage à ne pas divulguer d'informations relatives à l'architecture ou aux paramétrages des moyens de télécommunication de REDAL.

- ### Intégrité des informations

Le prestataire s'assure que ses interventions ne portent aucun préjudice à l'état des informations hébergées par le système, tant pour les données de production que pour les données de configuration du matériel et des logiciels.
Notamment, le personnel du prestataire veillera à ne pas altérer ou empêcher la journalisation des actions réalisées sur les équipements dans le périmètre de la prestation.

- ### Intégrité des ressources

Le prestataire s'assure qu'un retour arrière est possible, dans des délais raisonnables, éventuellement fixés en fonction des attentes de la direction métier concernée.

- ### Continuité de service

Le prestataire s'engage à ne pas altérer la continuité de service du système ou à limiter toute éventuelle interruption à la durée la plus réduite possible, sur la période la moins pénalisante pour les entités métiers.

- ### Accès physiques

L'accès aux locaux techniques doit se faire selon les modalités en vigueur à **REDAL**.

Il peut notamment être exigé que le personnel du prestataire soit accompagné par un collaborateur de **REDAL** pendant son intervention.

- ### Accès logiques

Dans le cas où un accès au système est indispensable, le prestataire se voit remettre un accès restreint et temporaire qu'il devra utiliser dans le seul cadre de la prestation en cours.

Les codes d'accès seront confiés aux personnels du prestataire à titre individuel et feront l'objet d'une journalisation.

- **Auditabilité**

Les intervention du prestataire sont consignées par écrit et remises à la direction métier à la fin de la prestation.

Règles de sécurité spécifiques aux prestations de Télémaintenance

Champ d'application

Les présentes règles s'appliquent dans le cadre de prestations de télémaintenance.

Enoncé des règles

- **Confidentialité des informations**

Dans le cas où les environnements de REDAL ne permettraient pas de masquer les informations de production au personnel maintenant, le prestataire s'engage à ne pas accéder à ces informations, ou à ne pas les divulguer et à ne pas les télécharger si un accès à ces dernières doit être envisagé.

- **Intégrité des informations**

Le prestataire s'engage à ne pas modifier les données ni les paramétrages des équipements et logiciel en dehors du périmètre de sa prestation.

Intégrité des ressources

Le prestataire s'assure qu'un retour arrière est possible, dans des délais raisonnables, éventuellement fixés en fonction des attentes de la direction métier concernée.

- **Continuité de service**

Le prestataire s'engage à ne pas altérer la continuité de service du système ou à limiter toute éventuelle interruption à la durée la plus réduite possible, sur la période la moins pénalisante pour les entités fonctionnelles.

- **Accès logiques**

Les accès aux systèmes de REDAL doivent se faire par des liaisons temporaires (commutées), avec une procédure de rappel par REDAL.

Les droits octroyés sur le système de REDAL sont restreints et attachés à des identifiants nominatifs.

Enfin, le personnel du prestataire peut éventuellement se voir remettre des outils d'authentification renforcée.

- **Auditabilité**

Les interventions réalisées sous les noms des identifiants attribués aux personnels du prestataire font l'objet d'une journalisation systématique de la part de REDAL, qui se réserve le droit d'effectuer les contrôles nécessaires.

REDAL se réserve également le droit d'auditer les installations du prestataire afin de vérifier que les opérations de télémaintenance sont réalisées dans un environnement correspondant aux normes de sécurité de REDAL.

Règles de sécurité spécifiques aux prestations de développement et de maintenance applicative

Champ d'application

Les présentes règles s'appliquent dans le cadre de prestations portant sur le développement de nouvelles applications ou sur la maintenance d'applications existantes.

Enoncé des règles

- **Confidentialité des informations**

Toute information sur le projet en cours, sur les métiers de REDAL ou sur leur organisation, ainsi que les données de production auquel le prestataire peut avoir accès doivent rester confidentielles.

- **Continuité de service**

Toute application doit faire l'objet des tests documentés avant sa mise en production, autorisée par la direction métier concernée.

- **Accès logiques**

Les accès au système d'information doivent se limiter au seul environnement de développement.

- **Auditabilité**

Toute application doit faire l'objet de documentations à l'attention des utilisateurs et des administrateurs.

- **Conformité**

Toute prestation relative à la conception d'une nouvelle application ou à l'intégration d'une nouvelle fonctionnalité applicative doit se faire conformément aux exigences de sécurité de la DNSSI et aux bonnes pratiques en la matière.

Règles de sécurité spécifiques aux prestations d'administration et d'exploitation

Champ d'application

Les présentes règles s'appliquent dans le cadre de prestations d'administration ou d'exploitation des systèmes d'information de REDAL.

Enoncé des règles

- ### Confidentialité des informations

Toute information sur l'architecture, la configuration et le type des systèmes d'information de REDAL, ainsi que les données de production auquel le prestataire peut avoir accès doivent rester confidentielles.

- ### Intégrité des informations

Le prestataire s'assure que ses interventions ne portent aucun préjudice à l'état des informations hébergées par le système, tout pour les données de production que pour les données de configuration du matériel et des logiciels.

Notamment, le personnel du prestataire veillera à ne pas altérer ou empêcher la journalisation des actions réalisées sur les équipements dans le périmètre de la prestation.

- ### Continuité de service

Des sauvegardes de recours doivent être régulièrement réalisées et les dispositifs de cours doivent faire l'objet de tests fréquents afin d'en vérifier le caractère opérationnel.

- ### Accès logiques

La gestion des mots de passe doit faire l'objet d'une attention plus rigoureuse que pour un simple utilisateur.

L'attribution de droit d'accès à une ressource doit se faire uniquement avec l'accord de la direction fonctionnelle propriétaire du système ou des informations qu'il héberge.

- ### Auditabilité

Les interventions du prestataire doivent être journalisées, les journaux étant diffusés au responsable de la sécurité des SI à des fins de contrôle.

Les incidents rencontrées lors des interventions et ayant trait à la sécurité du système d'information font l'objet de fiches de relevé et d'analyse communiquées au responsable de la sécurité des SI.

7.4 Annexe D : Règles de sécurité relatives aux accès distants des prestataires

- Le prestataire doit assurer la sécurité de sa plateforme d'intervention à distance, des points de vue accessibilité, protection des données et des logiciels.
- Le prestataire doit restreindre les accès logiques des postes d'intervention aux seules personnes autorisées.
- Le prestataire doit restreindre autant qu'il est possible de faire les accès physiques des postes d'intervention aux seules personnes autorisées.
- S'il le désire, le responsable de la sécurité des SI a la possibilité de faire réaliser des contrôles des dispositions de sécurité prises par le prestataire pour la réalisation de sa prestation.
- Le prestataire doit être en mesure de déterminer en toute circonstance l'identité de toute personne qui se connecte ou s'est connectée sur sa plateforme et en assurer la traçabilité.
- Le prestataire doit mettre en œuvre des moyens et des procédures conformes aux règles de l'art, pour lutter contre les incidents pouvant affecter la sécurité des SI de REDAL ou ses informations ou la sécurité de l'intervention elle-même. Cette exigence concerne :

    - la lutte contre les incidents de sécurité dans l'environnement humain, organisationnel, technique ou physique du prestataire et pouvant affecter la sécurité de la prestation fournie;

    - la lutte contre les codes malveillants et contre l'exploitation de vulnérabilités connues, dans les moyens informatiques ou de télécommunication mis en place pour la prestation, sous la responsabilité du prestataire. Par exemple : signaler les vulnérabilités en vue d'une prise de décision commune à leur égard ;

    - la lutte contre la propagation de codes malveillants ou d'incidents de sécurité à partir de la plateforme du prestataire, au travers des échanges électroniques effectués au titre de la prestation ;

    - la lutte contre les codes malveillants dans les logiciels transmis au titre de la prestation ou dans leur mise à jour, et contre l'exploitation de vulnérabilités connues dans ces éléments.

- Le prestataire doit mettre en œuvre un dispositif de gestion de configuration permettant de contrôler les accès aux composants produits ou fournis au titre de la télémaintenance des logiciels (code source, code exécutable, documentation, données de tests etc…). Il s'agit bien de tracer sur la plateforme du prestataire les interventions sur les composants de télémaintenance, afin d'éviter la mise en place d'accès mal maitrisés.
- Le prestataire doit veiller à ce qu'à l'issue de chaque intervention à distance, les données résiduelles (fichiers temporaires ou zones de mémoire vive) en provenance du SI soient effacées de la plateforme.

- Il est à noter que certaines interventions nécessitent plusieurs sessions de connexion sur le SI (pour des raisons d'investigation par exemple). Une intervention n'est considérée comme terminée que lorsque l'objectif de l'intervention est atteint (résolution d'un incident, mise à jour d'un composant...) ou que le responsable de la sécurité des SI et le prestataire déclarent d'un commun accord que l'objectif n'est pas atteignable.

7.5 Annexe E : Règles de sécurité applicables à la DSI REDAL

Cette annexe liste un ensemble de dispositions qui doivent être mise en œuvre par la DSI :

- La connexion directe du télé-mainteneur sur des équipements contenant des applications ou des informations à caractère personnel doit être évitée.
- Dans la mesure du possible, un point (ou passerelle) d'accès distant est mis en place pour accéder aux équipements objets de l'intervention à distance. Dans ce cas :
    - Les équipements sont reliés à ce point d'accès par un réseau d'administration mis en œuvre soit via un réseau dédié physiquement distinct du reste des SI , soit via une DMZ ou tout autre mécanisme permettant une isolation logique entre les flux d'administration et le reste des SI. Cette isolation logique se fera de préférence au moyen d'un VPN.

    - Le point d'accès distant doit être protégé contre les attaques logiques en provenance des réseaux et son contournement en vue d'accéder au réseau des SI ne doit pas être possible dans la pratique.

    - Le point d'accès doit faire l'objet d'audits de sécurité renouvelés destinés à vérifier sa mise en œuvre et sa résistance aux tentatives d'intrusion.

    - Les échanges entre la plateforme d'intervention et le point d'accès distant aux SI doivent être protégés par des fonctions de chiffrement et d'authentification mutuelle.

Si le point d'accès distant n'est pas la solution adoptée, il appartient au responsable de la sécurité des SI de décider sur recommandation du fournisseur de la solution et du protocole utilisés pour l'échange entre les équipements objets de l'intervention et la plateforme. Dans ce cas :

- les échanges doivent être protégés de bout en bout par des fonctions de chiffrement et d'authentification mutuelle ;
- un dispositif de filtrage doit autoriser uniquement les flux nécessaires à l'intervention à distance. Ce dispositif peut être à base de filtrage d'adresse IP ou de liste blanche de certificat par exemple.

Chaque équipement objet d'une télésurveillance ou d'une télémaintenance doit disposer d'un compte réservé à cette fin et dont les paramètres d'identification et d'authentification sont différents de ceux de tout autre équipement. Tous les comptes existant par défaut doivent être supprimés ou désactivés, ou leurs paramètres d'identification et d'authentification modifiés.

En cas d'absence prolongée de trafic dans une session, des mécanismes de surveillance doivent clore automatiquement toute session d'échange établie (en direct ou de part et d'autre du point d'accès) entre la plateforme et un équipement objet de l'intervention. Le délai de déconnexion automatique, à convenir en fonction des caractéristiques de l'intervention à distance, doit être aussi court que possible. Ces mécanismes sont à mettre en œuvre au niveau des SI. Dans le cas contraire, leur mise en œuvre peut être déléguée par contrat au fournisseur qui les met en œuvre à partir de ses équipements utilisé pour les interventions à distance.

La DSI doit disposer d'un espace de stockage dans lequel les traces des accès et des opérations effectuées à distance sont centralisées et conservées sous son contrôle, en vue d'être exploitées en cas de litige ou d'incident.

Dans le cas où une centralisation des traces n'est pas possible, le stockage des traces peut s'effectuer sur l'équipement objet de l'intervention.

7.6 Annexe F : Règles régissant les interventions

Le prestataire s'engage formellement à :

- Ne prendre aucune copie des documents et supports d'informations qui lui sont confiés, à l'exception de celles nécessaires à l'exécution de la prestation prévue au présent contrat, l'accord préalable du maître du fichier est nécessaire ;
- Ne pas utiliser les documents et informations traités à des fins autres que celles spécifiées au présent contrat ;
- Ne pas divulguer ces documents ou informations à d'autres personnes, qu'il s'agisse de personnes privées ou publiques, physiques ou morales ;

- Prendre toutes mesures permettant d'éviter toute utilisation détournée ou frauduleuse des fichiers informatiques en cours d'exécution du contrat ;
- Prendre toutes mesures de sécurité, notamment matérielle, pour assurer la conservation et l'intégrité des documents et informations traités pendant la durée du présent contrat ;
- Et en fin de contrat procéder à la destruction de tous fichiers manuels ou informatisés stockant les informations saisies.