LE PREMIER MINISTRE

REPUBLIQUE TOGOLAISE
Travail-Liberté-Patrie

ARRETE N° 2025-009 /PMRT
portant adoption du référentiel d'exigences des prestataires de services d'intégration, d'administration et de maintenance sécurisées

---

LE PREMIER MINISTRE,

Vu la constitution du 06 mai 2024 ;

Vu la loi n° 2018-026 du 07 décembre 2018 sur la cybersécurité et la lutte contre la cybercriminalité modifiée par la loi n° 2022-009 du 24 juin 2022 ;

Vu le décret n° 2019-022/PR du 13 février 2019 portant attributions, organisation et fonctionnement de l'Agence nationale de la cybersécurité ;

Vu l'arrêté n° 2022-040/PMRT du 29 juin 2022 portant adoption des règles de cybersécurité en République togolaise ;

Vu le décret n° 2022-09/PR du 25 août 2022 relatif à la qualification des prestataires de services de confiance de cybersécurité et des produits de sécurité et à l'agrément des centres d'évaluation ;

Vu le décret n° 2024-040/PR du 1er août 2024 portant nomination du Premier ministre ;

Vu le décret n° 2024-041/PR du 20 août 2024 portant composition du gouvernement ;

Vu le procès-verbal de la réunion du Comité stratégique de l'Agence nationale de la cybersécurité (ANCy), en sa séance du 02 décembre 2024 ;

ARRETE :

Article 1er : Objet

Le présent arrêté porte adoption du référentiel d'exigences des prestataires de services d'intégration, d'administration et de maintenance sécurisées en République togolaise.

Article 2 : Application

Les ministres, chacun en ce qui le concerne, veillent à l'application des dispositions du présent arrêté par les administrations et les opérateurs de services essentiels (OSE) relevant de leur ressort.

Article 3 : **Exécution**

Le Directeur général de l'Agence nationale de la cybersécurité (ANCy), est chargé de l'exécution du présent arrêté qui sera publié au Journal officiel de la République togolaise.

Fait à Lomé, le 31 JAN 2025

Le Premier ministre

SIGNE

Victoire S. TOMEGAH-DOGBE

Pour ampliation,
Le Ministre,
Secrétaire général du Gouvernement

Christian Eninam TRIMUA

ANCy
Agence Nationale de la Cybersécurité

RÉPUBLIQUE TOGOLAISE

REFERENTIEL D'EXIGENCES

Prestataires de services d'Intégration, d'Administration et de Maintenance Sécurisées

Version 1.0 du 31 JAN 2025

Premier Ministre	
Comité Stratégique	Agence Nationale de la Cybersécurité (ANCy)

HISTORIQUE DES VERSIONS			
DATE	VERSION	EVOLUTION DU DOCUMENT	REDACTEUR
31/01/2025	1.0	Première version applicable	ANCy

Les commentaires sur le présent document sont à adresser à :

Agence Nationale de la Cybersécurité
63, Boulevard du 13 janvier, Nyékonakpoè
07 BP 7878 Lomé – TOGO
Téléphone : +228 70 60 60 58 / 97 52 58 58
secretariat.ancy@ancy.gouv.tg

Table des matières

FICHE SYNTHETIQUE

1. Qu'est-ce qu'un PIAMS ?

Un **Prestataire de services d'Intégration, d'Administration et de Maintenance Sécurisées (PIAMS)** est une organisation ou une entreprise spécialisée dans la gestion sécurisée des systèmes informatiques d'une autre organisation. Son rôle est de garantir que les infrastructures numériques fonctionnent correctement et restent protégées contre les cyberattaques tout au long de leur cycle de vie.

2. Pourquoi un référentiel d'exigence ?

Le référentiel d'exigence sert à définir des règles claires que les PIAMS doivent respecter pour :

- Offrir des services de qualité ;
- Garantir la sécurité et la confidentialité des données ;
- Répondre aux normes nationales et internationales en cybersécurité.

3. Les principaux objectifs du référentiel

1. Encadrer les activités des PIAMS pour assurer un haut niveau de sécurité ;
2. Protéger les infrastructures critiques et les données sensibles des entreprises et des institutions ;
3. Renforcer la souveraineté numérique du pays.

4. Activités visées

La prestation d'intégration, d'administration et de maintenance regroupe les activités suivantes :

Intégration des solutions de sécurité

C'est l'ensemble des opérations de définition, d'assemblage (de matériels, logiciels, progiciels) et développements permettant, à partir d'un ensemble de produits / solutions, de réaliser un système pour un commanditaire répondant au besoin fonctionnel qu'il a exprimé. Les opérations peuvent inclure :

- La configuration des matériels et logiciels ;
- La réalisation des tests unitaires.

Administration

C'est l'ensemble des opérations telles que l'installation, la suppression, la modification et la consultation d'un système intégré dans le système d'information et qui sont susceptibles de modifier le fonctionnement ou la sécurité du système. Les opérations peuvent inclure :

ANCy Agence Nationale de la Cybersécurité
Tél: 97 52 58 58 / 70 60 60 83 Lomé - TOGO

- L'installation ou la désinstallation de composant ;
- La modification de la configuration ou du paramétrage ;
- La mise à jour des systèmes ou des composants ;
- La gestion de sauvegardes et des restaurations ;
- La gestion des droits d'accès des utilisateurs ;
- L'attribution de ressources informatiques.

Maintenance

C'est l'ensemble des actions entreprises pour assurer la préservation, la correction (maintenance corrective), la prévention (maintenance prédictive) d'un système d'information. Son objectif est de garantir que le système fonctionne de manière à fournir un service conforme aux exigences exprimées par le Client final. La maintenance implique notamment :

- Le maintien en condition opérationnelle (MCO) ;
- Le maintien en condition de sécurité (MCS) ;
- L'évolution du système d'information.

5. Exigences clés pour les PIAMS

a. Organisation et structure

- Le PIAMS doit être une entreprise légalement enregistrée (personne morale) ;
- Il doit disposer d'une équipe compétente en cybersécurité et en administration des systèmes.

b. Protection de l'information

- Mettre en place des mesures strictes pour protéger les données des clients (sauvegarde, chiffrement, accès sécurisé) ;
- Garantir la confidentialité des informations traitées.

c. Compétences et qualifications

- Les PIAMS doivent prouver leur capacité à gérer des infrastructures sécurisées et répondre aux incidents de sécurité ;
- Adopter des pratiques alignées avec les normes internationales comme l'ISO/IEC 27001.

6. Les étapes de qualification d'un PIAMS

a. **Soumission du dossier** : Le PIAMS soumet à l'ANCy un dossier décrivant ses compétences, ses équipements et ses processus ;
b. **Audit de conformité** : L'Agence Nationale de la Cybersécurité (ANCy) vérifie que le PIAMS respecte les exigences ;
c. **Décision :**

- Si le PIAMS est conforme, il obtient un certificat de qualification ;
- En cas de non-conformité, des améliorations sont demandées.

7. Suivi et renouvellement

- Les PIAMS doivent régulièrement démontrer qu'ils maintiennent leurs pratiques de sécurité ;
- Un audit périodique permet de renouveler la qualification et de vérifier la conformité continue.

8. Pourquoi est-ce important ?

Les PIAMS sont essentiels pour :

- Assurer la continuité des activités numériques en cas de problème ;
- Renforcer la résilience des infrastructures face aux cybermenaces ;
- Protéger les données sensibles et stratégiques des entreprises et des institutions.

9. Conclusion

Le référentiel d'exigence pour les PIAMS établit un cadre rigoureux afin de garantir la sécurité, la fiabilité et la souveraineté des systèmes numériques au Togo. Il aide à protéger les organisations contre les cyberattaques tout en maintenant un niveau élevé de performance opérationnelle.

1. PRESENTATION GENERALE

1.1. AVANT-PROPOS

La prestation d'intégration sécurisée est particulièrement importante dans un contexte où la cybermenace est constamment présente. Cette prestation vise à garantir la résilience des systèmes informatiques face aux attaques potentielles. Elle se réfère à la fourniture de services visant à intégrer divers composants, systèmes ou solutions au sein d'un ensemble fonctionnel et cohérent. Cela peut concerner divers domaines tels que l'informatique, les télécommunications, les réseaux, la sécurité, etc. L'objectif principal de la prestation d'intégration est de garantir que les différents éléments fonctionnent de manière harmonieuse et efficace pour répondre aux besoins spécifiques d'une organisation.

Le service d'administration et de maintenance sécurisées s'adresse à des organisations qui désirent maintenir un environnement informatique sécurisé, à minimiser les risques de cyberattaques et à garantir la disponibilité, la confidentialité et l'intégrité des données de leurs systèmes d'information.

Les missions de ce service concernent la gestion continue et la protection des systèmes informatiques, des réseaux et des données d'un système d'information.

1.2. OBJECTIF DU REFERENTIEL ET DOMAINE D'APPLICATION

Ce document constitue le référentiel d'exigences applicable à un Prestataire d'intégration, administration et maintenance sécurisées.

Il vise à établir un cadre permettant la qualification de Prestataire de service d'intégration, d'administration et de maintenance sécurisées. Il permet d'accompagner d'une part le Prestataire dans la fourniture des services d'administration et de maintenance sécurisées et de permettre d'autre part au Client final de la prestation de disposer de garanties sur les compétences du Prestataire et de son personnel, sur la qualité des prestations d'intégration, d'administration et de maintenance et sur la confiance que le Client final peut accorder au Prestataire en particulier en ce qui concerne la confidentialité.

Il a vocation à permettre la qualification de cette famille de Prestataires conformément à la règlementation en vigueur selon les modalités décrites dans le Modèle de qualification des Prestataires de service de confiance en cybersécurité.

1.3. DOCUMENTS DE REFERENCE

Le présent Référentiel s'inscrit dans un cadre légal et règlementaire plus global en vigueur au Togo, et est applicable aux Prestataires de services de confiance en cybersécurité.

L'ensemble des textes découlant de ce cadre légal et règlementaire et susceptibles de s'appliquer aux Prestataires d'intégration, d'administration et maintenance sécurisées ainsi qu'à leurs prestations sont listés ci-dessous de manière non-exhaustive. Ils sont identifiés dans le Référentiel en tant que « Documents de référence ».

Le présent Référentiel s'applique en complément des Documents de référence dont il n'exclut pas l'application. Il n'exclut pas non plus l'application des règles générales imposées aux Prestataires en leur qualité de professionnels, et notamment leur devoir de conseil vis-à-vis des Clients finaux.

Le référentiel peut être utilisé à titre de bonnes pratiques en dehors de tout contexte règlementaire.

1.3.1. Normes internationales

- La norme ISO 27001 : 2022, Sécurité de l'information, cybersécurité et protection de la vie privée ;
- La norme ISO 27002 : 2022, Sécurité de l'information, cybersécurité et protection de la vie privée- Mesures de sécurité de l'information ;
- La norme ISO 27005 : 2022, Sécurité de l'information, cybersécurité et protection de la vie privée- Préconisations pour la gestion des risques liés à la sécurité de l'information ;
- La norme ISO 27035, Gestion des incidents de sécurité de l'information ;
- La norme ISO 20000, Norme internationale sur la gestion de services ;
- La norme NIST SP 800-53 : Cadre de contrôles de sécurité et de confidentialité des systèmes d'information ;
- Le référentiel ITIL, Bibliothèque pour l'infrastructure des technologies de l'information.

1.3.2. Textes législatifs et règlementaires

- La loi n° 2017-007 du 22 juin 2017 relative aux transactions électroniques en République togolaise ;
- La loi n° 2018-026 du 07 décembre 2018 sur la cybersécurité et la lutte contre la cybercriminalité, modifiée par la loi n° 2022-009 du 24 juin 2022 ;

- Le décret n°2018-062/PR du 21 mars 2018 portant réglementation des transactions et services électroniques au Togo ;
- L'arrêté n°016/MPEN/CAB du 17 décembre 2018 fixant les conditions de reconnaissance au Togo des certificats et signatures électroniques délivrés par des prestataires de services de confiance établis hors du territoire national ;
- La loi n°2019-014 du 29 octobre 2019 relative à la protection des données à caractère personnel ;
- La loi n°2020-009 du 10 septembre 2020 relative à l'identification biométrique des personnes physiques au Togo ;
- Le décret n° 2019-022/PR du 13 février 2019 portant attributions, organisation et fonctionnement de l'ANCY ;
- Le décret n° 2019-095/PR du 08 juillet 2019 relatif aux opérateurs de services essentiels, aux infrastructures essentielles et aux obligations y afférentes ;
- Le décret n°2019-098/PR du 11 juillet 2019 portant création, attributions et organisation de la société CYBER DEFENSE AFRICA (CDA) ;
- Le décret n° 2022-09/PR du 25 août 2022 relatif à la qualification des prestataires de services de confiance de cybersécurité et des produits de sécurité et à l'agrément des centres d'évaluation ;
- L'arrêté n° 2022-040/PRMT du 29 juin 2022 portant adoption des règles de cybersécurité en République togolaise.

Ces documents sont disponibles auprès de l'ANCy.

1.3.3. Documents de l'ANCy

- Décision ANCy portant liste des pays tiers de confiance ;
- Modèle de qualification des Prestataires de services de confiance en cybersécurité ;
- Déclaration de la politique de qualification.

1.4. IDENTIFICATION DU DOCUMENT ET DATE D'APPLICATION

Le présent document est dénommé « Référentiel d'exigences des Prestataires d'intégration, d'administration et de maintenance sécurisées ». Il peut être identifié par son nom, sa référence, son numéro de version et sa date de mise à jour.

Ce document est applicable à compter de sa publication.

Il est élaboré, mis à jour et publié par l'ANCy, qui précisera les modalités de transition et la date d'effet pour chaque mise à jour.

1.5. ACTIVITES D'INTEGRATION, D'ADMINISTRATION ET DE MAINTENANCE VISEES PAR LE REFERENTIEL

La prestation d'intégration, d'administration et de maintenance regroupe les activités suivantes :

- ***Intégration des solutions de sécurité***

C'est l'ensemble des opérations de définition, d'assemblage (de matériels, logiciels, progiciels) et développements permettant, à partir d'un ensemble de produits / solutions, de réaliser un système pour un commanditaire répondant au besoin fonctionnel qu'il a exprimé. Les opérations peuvent inclure :

- La configuration des matériels et logiciels ;
- La réalisation des tests unitaires.

- ***Administration***

C'est l'ensemble des opérations telles que l'installation, la suppression, la modification et la consultation d'un système intégré dans le système d'information et qui sont susceptibles de modifier le fonctionnement ou la sécurité du système. Les opérations peuvent inclure :

- L'installation ou la désinstallation de composant ;
- La modification de la configuration ou du paramétrage ;
- La mise à jour des systèmes ou des composants ;
- La gestion de sauvegardes et des restaurations ;
- La gestion des droits d'accès des utilisateurs ;
- L'attribution de ressources informatiques.

- ***Maintenance***

C'est l'ensemble des actions entreprises pour assurer la préservation, la correction (maintenance corrective), la prévention (maintenance prédictive) d'un système d'information. Son objectif est de garantir que le système fonctionne de manière à fournir un service conforme aux exigences exprimées par le Client final. La maintenance implique notamment :

- Le maintien en condition opérationnelle (MCO) ;
- Le maintien en condition de sécurité (MCS) ;
- L'évolution du système d'information.

1.6. ARCHITECTURE DU SYSTEME D'INFORMATION

1.6.1. LE SYSTEME D'INFORMATION DU SERVICE

Le système est composé des ressources nécessaires à l'administration du système d'information administré :

- Les administrateurs du système d'information du service ;
- Les administrateurs du service ;
- Les postes d'administration ou de maintenance ;
- Les consoles de programmation ;
- Les serveurs d'administration ;
- Les infrastructures d'administration ;
- Le réseau d'administration.

1.6.2. LES RESSOURCES ADMINISTREES

Les ressources comprennent tous les dispositifs virtuels ou physiques (postes de travail, serveurs de production, composants réseaux, automates, applications, etc.) du système d'information administré nécessitant des actions d'administration, indépendamment de leur localisation.

1.6.3. ACTIONS D'ADMINISTRATION

Les actions d'administration peuvent être menées par :

▪ le Prestataire ;

▪ le Client final ;

Le système d'information administré peut être :

▪ hébergé par le Client final ou un hébergeur tiers ;

▪ administrable à distance ou non administrable à distance, nécessitant des interventions sur site.

Les différentes combinaisons de gestion des ressources peuvent être regroupées comme suit :

- ***Service d'administration interne***
  - Le client réalise les actions d'administration sur ses propres ressources dans des conditions conformes au présent référentiel ;
  - Il peut être amené à intervenir sur des ressources également administrées par un administrateur tiers et peut par ailleurs confier une partie des actions d'administration

à un Prestataire opérant via une prestation de mise à disposition de personnels dans le cadre du service interne ;

- Les ressources administrées peuvent se situer dans les locaux du Client final, dans les locaux du Prestataire ou dans les locaux d'un hébergeur tiers (y compris des services cloud).

➢ ***Service d'administration externalisé***

- Le Prestataire réalise les actions d'administration sur les ressources du client final conformément au présent référentiel ;
- Il peut être amené à intervenir sur des ressources également administrées par un administrateur tiers et peut par ailleurs confier une partie des actions d'administration à un Prestataire opérant via une prestation de mise à disposition de personnels dans le cadre du service interne ;
- Les ressources administrées peuvent se situer dans les locaux du Client final ou dans les locaux d'un hébergeur tiers (y compris les services de cloud).

1.7. DEFINITIONS ET ACRONYMES

1.7.1. Client final

C'est la partie qui sollicite ou commande la réalisation de la prestation d'administration et de maintenance sécurisées.

1.7.2. Prestataire de service d'intégration, d'administration et de maintenance sécurisées qualifié

Un Prestataire de service d'intégration, d'administration et de maintenance sécurisées qualifié est un Prestataire qui dispose d'une qualification pour la réalisation des prestations d'intégration, d'administration et de maintenance sécurisées.

1.7.3. Intégration

C'est l'acte de déploiement et de configuration de dispositifs ou systèmes de sécurité (composants matériels/logiciels) au sein d'un environnement informatique ou d'un réseau.

1.7.4. Prestation d'intégration

La prestation d'intégration se réfère à la fourniture de services visant à intégrer divers composants, systèmes ou solutions de sécurité au sein d'un système d'information. Cette prestation englobe

l'installation physique des équipements, la configuration appropriée des paramètres de sécurité, et l'interconnexion avec le reste des composants du système d'information.

1.7.5. Administration

C'est l'acte d'installation, suppression, modification ou consultation d'une configuration d'un composant du système d'information.

1.7.6. Maintenance

C'est l'acte de réglage, vérification ou réparation des composants matériels ou logiciels du système d'information.

1.7.7. Service d'administration et de maintenance sécurisé

Le service d'administration et de maintenance sécurisé se réfère à la fourniture d'une offre qui englobe la gestion quotidienne, la surveillance, la mise à jour et la maintenance des systèmes informatiques, tout en mettant l'accent sur la sécurité. Ce type de service vise à assurer le bon fonctionnement des infrastructures informatiques tout en minimisant les risques liés à la sécurité informatique.

1.7.8. Intégrateur

La personne qui participe à la conception et à l'intégration de la solution de sécurité avec les différents composants du système d'information. Il peut gérer également l'administration et la maintenance au quotidien.

1.7.9. Administrateur du service

La personne disposant de droits privilégiés sur un système d'information, chargée des actions d'administration ou de maintenance. Il peut être un employé du Prestataire affecté chez le Client final via une prestation de mise à disposition de personnels.

1.7.10. Administrateur du système d'information du service

Tout administrateur employé du Prestataire qui permet d'assurer l'administration du système d'information permettant d'assurer le service pour le compte des Clients finaux.

1.7.11. Système d'information administré

Le système d'information incluant les ressources administrées.

1.7.12. Système d'information d'administration

Système d'information utilisé pour administrer des ressources qui sont présentes dans le système d'information administré.

1.7.13. Système d'information du service

Système d'information permettant la délivrance du service et incluant son propre système d'information d'administration accessible uniquement par les administrateurs du système d'information du service.

1.7.14. Ressources administrées

L'ensemble des dispositifs physiques ou virtuels du système d'information administré qui nécessitent des actions d'administration.

1.7.15. Segmentation du système

La séparation ou l'isolation des différentes composantes, unités ou fonctions au sein d'une organisation du service d'administration et de maintenance sécurisée ou du système du Client final. Cette segmentation assure notamment le stockage sécurisé de l'historique des actions déployées.

1.7.16. Zone de confiance

L'ensemble des ressources informatiques regroupées en fonction de l'homogénéité de facteurs divers, liés ou non à la sécurité (ex : exposition aux menaces, vulnérabilités résiduelles technologiques intrinsèques, localisation géographique, etc.).

1.7.17. Plan de réversibilité

C'est le plan qui permet d'assurer le retour à un système antérieur après une mise à niveau ou un changement, de manière efficace et sans perte de données ou de fonctionnalités.

2. EXIGENCES RELATIVES AU PRESTATAIRE DE SERVICE D'ADMINISTRATION ET DE MAINTENANCE SECURISEES

2.1. EXIGENCES GENERALES

a. Le Prestataire d'intégration, d'administration et de maintenance sécurisées doit être une entité ou une partie d'une entité, dotée de la personnalité morale, dûment enregistrée au RCCM (Registre

du Commerce et du Crédit Mobilier) pour les besoins de l'activité d'intégration, d'administration et de maintenance sécurisées, de façon à pouvoir en être tenu juridiquement responsable ;

b. Le Prestataire doit mettre en œuvre, pour son propre compte, un service de support interne, portant sur le système d'information du service d'administration et de maintenance sécurisées.
c. Le Prestataire d'intégration, d'administration et de maintenance sécurisées doit décrire l'organisation de son activité au bénéfice de chaque Client final et garantir que les informations qu'il fournit sont exactes ;
d. Le Prestataire d'intégration, d'administration et de maintenance sécurisées réalise ses prestations dans le cadre d'un contrat de prestation avec le Client final. Ce contrat doit être en accord avec les lois en vigueur au Togo et approuvé formellement, par écrit, par les deux parties ;
e. Le Prestataire d'intégration, d'administration et de maintenance sécurisées doit solliciter le Client final afin d'obtenir toute information relative aux exigences légales et réglementaires qui lui sont applicables, en mettant particulièrement l'accent sur celles associées à son domaine d'activité spécifique ;
f. Le prestataire d'intégration, d'administration et de maintenance sécurisées doit réaliser la prestation de manière loyale et faire preuve de respect personnel et professionnel à l'égard du Client final, de son personnel et de ses infrastructures et veiller à ce que les activités qu'il effectue soient réalisées en toute impartialité ;
g. Le Prestataire d'intégration, d'administration et de maintenance sécurisées doit informer le Client final en cas de détection d'incident fonctionnel ou de sécurité ;
h. Le Prestataire d'intégration, d'administration et de maintenance sécurisées doit fournir au Client final un service de support à distance. Ce service devrait faciliter au Prestataire la résolution des problèmes de production liés aux dispositifs qu'il gère et lui permettre d'assister et conseiller le Client final. Ce service doit être accessible via un numéro téléphonique ou une adresse e-mail ;
i. Le Prestataire doit garantir la confidentialité, l'intégrité et la non-répudiation de toutes les informations échangées entre le système d'information du service d'intégration, d'administration et de maintenance sécurisées et le système d'information du Client final dans le cadre de la prestation, à l'aide de solutions qualifiées par l'ANCy ;
j. Le prestataire doit mettre en place une chaîne de responsabilité de la cybersécurité pour les besoins de ses prestations. En particulier, il doit définir un point de contact pour la cybersécurité lors de la prestation, qui sera en charge : de la liaison avec la chaîne de responsabilité du client final, de la garantie du respect de la politique de cybersécurité, de la communication sur les divergences par rapport aux exigences et des éventuelles non-conformités ;

k. Le prestataire doit déployer un processus de veille sur les menaces et vulnérabilités sur les produits et technologies mises en œuvre sur les systèmes qu'il a déployés. Il pourra s'appuyer sur les informations publiées par les CERTs ainsi que les sites web des équipementiers ;

l. Le prestataire doit mettre en œuvre un processus de veille sur l'évolution des moyens techniques pour renforcer le niveau de cybersécurité des systèmes industriels.

2.2. ORGANISATION DU PRESTATAIRE ET GOUVERNANCE

2.2.1. Gestion des ressources et des compétences

a. Le Prestataire doit en permanence, disposer d'une équipe d'un minimum de trois (03) intervenants. Le non-respect de cette condition sur une période au moins égale à six (06) mois constitue pour l'ANCy un motif de suspension de la qualification du prestataire d'intégration, d'administration et de maintenance sécurisées ;

b. Le Prestaire doit disposer d'un nombre suffisant d'administrateurs / intégrateurs, et être en mesure d'assurer totalement et dans tous ses aspects, la prestation qualifiée notamment la maitrise des technologies spécifiques déployées par le Client final ;

c. Le Prestataire doit désigner un responsable administrateur opérationnel pour le Client final, qui est l'interlocuteur privilégié concernant le fonctionnement opérationnel du service. Le Prestataire doit informer le Client final de tout changement de l'interlocuteur opérationnel pour le service d'administration et de maintenance sécurisé ;

d. Le Prestataire doit s'assurer de créer et de fournir la liste complète des guides d'administration des dispositifs du service, des guides d'exploitation des zones du système d'information du service, et des guides d'administration des dispositifs des systèmes d'information administrés dans le cadre de la délivrance du service d'information ;

e. Le Prestataire doit instaurer un système d'astreinte assurant la disponibilité des administrateurs du système d'information du service en dehors des heures normales de travail.

f. Le Prestataire doit s'assurer de la compétence de ses ressources et du maintien de cette compétence, à travers un processus de formation continue et une veille technologique devant inclure une partie sur la cybersécurité des systèmes industriels ;

g. La formation continue du Prestataire et de son personnel peut prendre plusieurs formes notamment des modules d'auto-formation, des séminaires internes, ou des séminaires

assurés par le CERT.tg ou par l'ANCy. Le Prestataire doit à tout moment, être en mesure de documenter son plan de formation continue à l'ANCy sur simple demande de celle-ci ;

h. Le Prestataire justifie, au travers de ses ressources (dont l'évaluation a été faite au moment de la qualification en tant que Prestataire d'intégration, d'administration et de maintenance sécurisée) qu'il dispose des compétences techniques, théoriques et pratiques nécessaires pour mener des activités de détection des incidents de sécurité couvertes par la portée de la qualification obtenue ;

i. Le Prestataire doit définir et formaliser la liste exhaustive des différents rôles d'administrateur de service et des différents rôles d'administrateurs du système d'information du service ainsi que leurs missions associées. Les rôles définis doivent respecter les principes du moindre privilège ;

j. Le Prestataire doit justifier, au travers de ses ressources proposées au titre de la qualification du Prestataire d'intégration, d'administration et de maintenance sécurisées, qu'il dispose des compétences techniques, théoriques et pratiques nécessaires pour mener des activités d'administration et de maintenance sécurisées. Plus spécifiquement, le prestataire nécessite les compétences suivantes :

2.2.2. Intégrateur

La mission principale d'un intégrateur est de déployer et configurer les dispositifs ou systèmes de sécurité dans le système d'information

Expériences et formation
Minimum Niveau Bac +5 /ingénieur en technologie des systèmes d'information et de communication
Formation et expérience
↓ Formation en opérations de cybersécurité dans un domaine connexe (p. ex. opérations de sécurité, sécurité des réseaux, durcissement des réseaux,) ↓ Formation spécifique à un produit ou solution ↓ Avoir une expérience minimale de (02) ans

Principales missions
↓ Assemblage et intégration des dispositifs de sécurité avec les différents composants du SI, ↓ Gestion des Systèmes en assurant la disponibilité, la fiabilité et la performance des systèmes informatiques, ↓ Définir les interfaces et les composantes à faire évoluer pour permettre leur intégration, ↓ Documenter les solutions de sécurité, ↓ Maintenance préventive par la mise en en œuvre des stratégies de maintenance préventive et la documentation des procédures, ↓ Maintenance en condition de sécurité du système par le dépoilement des mesures de sécurité robustes et la surveillance des performances des systèmes et détecter les anomalies, ↓ Mise en place des procédures de mise en œuvre, de mise à jour et d'exploitation des composants de sécurité ↓ Support technique pour les utilisateurs finaux (Prestataire ou Client final) et résolution des anomalies liés aux systèmes. ↓ Collaboration avec les équipes de développement et les équipes de sécurité, pour assurer une intégration harmonieuse des systèmes.
Compétences techniques
↓ Maîtrise parfaite des systèmes Windows, Linux, Unix ↓ Maitrise de la sécurité des systèmes d'information (SIEM, Firewall, VPN, antivirus, proxy) ↓ Maitrise des techniques d'interconnections des réseaux et de leur administration ↓ Maitrise des protocoles et architectures réseau et maitrise des techniques de corruption et d'intrusion ↓ Maitrise des environnements techniques de détection et réponse ↓ Maitrise des environnements cloud ↓ Connaissance en gestion des incidents ↓ Connaissances en outils d'automatisation ↓ Connaissances des systèmes SCADA ↓ Compétence en administration des systèmes ↓ Compétence en durcissement des systèmes et déploiement des mesures de sécurité

2.2.3. Administrateur

La mission principale d'un administrateur est d'administrer le système d'information et de maintenir les conditions opérationnelles des dispositifs de l'infrastructure du système d'information et leur niveau de sécurité

Expériences et formation
Minimum Niveau Bac +5 /ingénieur en technologie des systèmes d'information et de communication
Formation et expérience
↓ Formation en opérations de cybersécurité dans un domaine connexe (p. ex. opérations de sécurité, sécurité des réseaux, durcissement des réseaux,) ↓ Formation spécifique à un produit ou solution ↓ Avoir une expérience minimale de (02) ans
Principales missions
↓ Gestion des Systèmes en assurant la disponibilité, la fiabilité et la performance des systèmes informatiques, ↓ Maintenance préventive par la mise en en œuvre des stratégies de maintenance préventive et la documentation des procédures, ↓ Maintenance en condition de sécurité du système par le déploiement des mesures de sécurité robustes et la surveillance des performances des systèmes et détecter les anomalies, ↓ Support technique pour les utilisateurs finaux (Prestataire ou Client final) et résolution des anomalies liés aux systèmes. ↓ Collaboration avec les équipes de développement et les équipes de sécurité, pour assurer une intégration harmonieuse des systèmes.
Compétences techniques
↓ Maîtrise parfaite des systèmes Windows, Linux, Unix ↓ Maitrise de la sécurité des systèmes d'information (SIEM, Firewall, VPN, antivirus, proxy ↓ Maitrise des techniques d'interconnections des réseaux et de leur administration

- Maitrise des protocoles et architectures réseau et maitrise des techniques de corruption et d'intrusion
- Maitrise des environnements techniques de détection et réponse
- Maitrise des environnements cloud
- Connaissance en gestion des incidents
- Connaissances en outils d'automatisation
- Connaissances des systèmes SCADA
- Compétence en administration des systèmes
- Compétence en durcissement des systèmes et déploiement des mesures de sécurité

2.2.4. Organes de pilotage

La gouvernance du service d'administration et de maintenance sécurisées doit s'appuyer des instances de suivi et de pilotage. L'objectif de ces comités est de coordonner l'ensemble des parties impliquées dans la prestation.

a. Comité de pilotage :

Le Prestataire établit en collaboration avec le Client final, des réunions de pilotage planifiées de manière mensuelle dont le but est d'assurer le bon pilotage du service. Elle est animée par le responsable opérationnel du service qui doit traiter, à minima, les points suivants :

- Le périmètre du service (contexte, changements déployés au niveau du système d'information cible),
- Suivi des engagements de sécurité pris dans le cadre de la prestation (indicateurs, incidents détectés).

b. Comité stratégique :

Le Prestataire établit un comité stratégique, en présence des représentants de la direction du Client final, des réunions planifiées de manière annuelle ou semestrielle, clôturées par un procès-verbal.

Le comité stratégique doit traiter, à minima, les thèmes suivants :

- Revue de la convention des services ;
- Revue du plan de réversibilité,
- Revue du plan du périmètre de la prestation.

2.2.5. Recrutement et Code d'éthique

Le Prestataire doit procéder à une vérification des formations, qualifications, références professionnelles des candidats, et de la véracité de leur curriculum vitae préalablement à leur embauche.

Le Prestataire doit demander aux candidats de lui fournir une preuve qu'ils ne font pas l'objet d'une inscription au bulletin n° 3 du casier judiciaire.

Les opérateurs, les administrateurs et les experts du service d'administration et de maintenance sécurisés doivent être liés contractuellement avec le Prestataire.

Le Prestataire doit disposer d'un code d'éthique intégré au règlement intérieur, signé et/ou ratifié par chaque membre du personnel, et dont une copie doit être adressée à l'ANCy.

Le Code d'éthique inclut au minimum les exigences ci-après :

- Les prestations sont réalisées avec loyauté, discrétion et impartialité ;
- Les membres du personnel ne recourent qu'aux méthodes, outils et techniques validés par le Prestataire ;
- Les membres du personnel s'engagent à ne pas divulguer d'informations à un tiers, même anonymisées et décontextualisées, obtenues ou générées dans le cadre de la prestation, sauf autorisation formelle écrite et préalable du Client final ;
- Les membres du personnel s'engagent à signaler au Prestataire tout contenu manifestement illicite découvert pendant la prestation ;
- Les membres du personnel s'engagent à respecter la législation et la réglementation nationale en vigueur et les bonnes pratiques liées à leurs activités.

Le Prestataire est dans l'obligation de faire signer et/ou ratifier à l'ensemble de son personnel le Code d'éthique préalablement à la réalisation de la prestation.

Le Prestataire doit veiller au respect du Code d'éthique par son personnel et prévoir des sanctions disciplinaires en visant a minima les opérateurs, les administrateurs et les experts du service d'administration et de maintenance sécurisées ayant enfreint les règles de sécurité ou le Code d'éthique.

A cet égard, le Prestataire doit élaborer et mettre en œuvre un plan de sensibilisation de son personnel à la sécurité des systèmes d'information et des mesures de sécurité associées ainsi qu'à la législation et la réglementation nationale en vigueur en rapport avec le service d'administration et de maintenance sécurisées.

2.2.6. Politique de sécurité

- Le Prestataire doit établir une appréciation des risques et un plan de traitement des risques associé, sur tout le périmètre du service d'administration et de maintenance sécurisées. L'appréciation des risques et le plan de traitement doivent être formellement validés et consignés auprès de la direction générale du Prestataire. Cette appréciation du risque doit faire objet d'une revue au moins une (01) fois par an ;
- L'appréciation des risques doit prévoir une liste d'incidents appréhendés qui pourraient affecter le système d'information du service d'administration et de maintenance sécurisées, à savoir :
    - Les tentatives d'intrusion sur le système d'information du service d'administration et de maintenance sécurisées depuis une de ses interconnexions ;
    - Les tentatives de rebond entre les systèmes d'information des Clients finaux à travers le système d'information du service d'administration et de maintenance sécurisées ;
    - Les tentatives d'élévation de privilèges par les utilisateurs ou les administrateurs du service d'administration et de maintenance sécurisées ;
    - La perte de communication avec un ou plusieurs équipements du service d'administration et de maintenance sécurisées ;
    - Les infections virales originaires de codes malveillants rencontrés dans le cadre de la prestation.
- En cas de modifications significatives du service d'administration, notamment celles liées à son hébergement, son infrastructure ou son architecture, le Prestataire doit procéder à une révision de l'appréciation des risques ainsi que le plan de traitement des risques associé.
- Le Prestataire doit disposer d'une politique de sécurité des systèmes d'information basée sur l'appréciation des risques ;
- Le Prestataire doit réaliser un audit et faire appel à un Prestataire de service d'audit qualifié et disposer d'un programme d'audit sur trois (03) ans couvrant toutes les activités d'intégration, d'administration et de maintenance sécurisées ;
- Le programme de l'audit doit couvrir un audit de la configuration des serveurs et équipements réseau et un audit de code source si le service bénéficie d'outils développés en interne

- Le Prestataire doit respecter l'ensemble des mesures et préconisations relatives à la sécurisation des sauvegardes telles que définies dans la norme ISO 27002.
- Le Prestataire doit se conformer à la norme ISO27001.
- Il est fortement recommandé que le service du Prestataire soit certifié ISO27001.

3. EXIGENCES RELATIVES AU SERVICE D'ADMINISTRATION ET DE MAINTENANCE SECURISEES

3.1. EXIGENCES GENERALES DU SERVICE D'ADMINISTRATION ET DE MAINTENANCE SECURISEES

- Le Prestataire doit disposer d'une localisation physique des équipes et de son propre système d'information, d'un accès de secours et d'un ensemble de matériels dédiés au service d'administration et de maintenance. Le local doit être protégé par un système de contrôle d'accès physique, un système de vidéosurveillance et d'un système anti-incendie ;
- Le Prestataire doit tenir à jour l'inventaire de l'ensemble des équipements mettant en œuvre le service ;
- Le Prestataire doit disposer de l'ensemble des procédures de sécurité préconisées dans la norme ISO27001 (restitution des postes d'administration, de mise au rebus des actifs du système d'information, de sauvegarde, de protection du matériel, etc.) ;
- Le Prestataire doit déployer des équipements qualifiés par l'ANCy dans son service. La salle abritant ces systèmes doit disposer d'une bonne protection physique et environnementale.
- Le Prestataire doit mettre en œuvre des moyens de détection des incidents pour le système d'information du service ;
- Le Prestataire doit s'assurer de la protection de l'information du service.

3.2. EXIGENCES MINIMALES DU SERVICE D'ADMINISTRATION ET DE MAINTENANCE SECURISEES

3.2.1. Maintien en condition de sécurité

- Le Prestataire doit s'assurer du maintien en condition de sécurité de toutes les ressources du service ;
- Le Prestataire doit élaborer, tenir à jour et mettre en œuvre une procédure de maintien en condition de sécurité de toutes les ressources du service ;

- Le Prestataire doit élaborer et maintenir à jour un inventaire exhaustif de tous les logiciels qui sont utilisés pour mettre en œuvre le service. Cet inventaire doit spécifier, pour chaque logiciel, sa version ainsi que les équipements sur lesquels le logiciel est installé ;
- Le Prestataire doit installer et maintenir les dispositifs du service, en veillant à ce qu'ils fonctionnent sur des versions stables bénéficiant des correctifs de sécurité les plus récents.
- Le Prestataire doit vérifier l'impact de l'installation des mises à jour sur le système d'information du service dans le cas où l'impact est significatif, le Prestataire doit définir et mettre en œuvre des mesures de réduction des risques ;
- Le Prestataire doit s'assurer de l'authenticité et l'intégrité des mises à jour téléchargées à partir de sources de mise à jour reconnues pour garantir leur fiabilité ;
- Le Prestataire doit effectuer une veille sur les vulnérabilités, les mises à jour de sécurité et les mesures de réduction des risques concernant les ressources du système d'information du service ;
- Le Prestataire doit pouvoir générer un ensemble d'indicateurs relatifs aux mises à jour des postes d'administration, pour le domaine du service et être en mesure de les présenter au Client final ;

3.2.2. Étendue géographique du service

- Le Prestataire doit héberger, traiter, exploiter et administrer les données relatives au service d'administration et de maintenance sécurisées exclusivement au sein du territoire togolais.
- Le Prestataire doit documenter et communiquer, à la demande du Client final, la localisation du stockage et du traitement des données à sa disposition (documents d'architecture, éléments de configuration, informations d'authentification, etc.) ;
- Cependant, l'Agence Nationale de la Cybersécurité (ANCy) peut accorder une dérogation à cette obligation d'hébergement, sous réserve que le prestataire concerné fournisse une justification crédible et documentée de son incapacité à satisfaire cette exigence. La demande de dérogation sera soumise à une évaluation rigoureuse avant approbation.

3.2.3. Sécurité physique

- Le Prestataire doit documenter et mettre en œuvre des périmètres de sécurité, incluant le marquage des zones physiques et les différents moyens de limitation et de contrôle des accès.
- Le Prestataire doit adopter un marquage du périmètre permettant d'avoir :
    - Des zones publiques accessibles par tous ;
    - Des zones privées hébergeant les postes d'administration ou de maintenance et le local à partir duquel le Prestataire opère ;

- Des zones sensibles hébergeant le système d'information du service hors postes d'administration ou de maintenance ;

- Le Prestataire doit déployer des points d'accès au niveau de ces zones ;
- Le Prestataire doit élaborer et tenir à jour la liste des personnes autorisées à accéder aux zones privées et sensibles ;
- Le Prestataire doit mettre en œuvre les mécanismes permettant de journaliser les accès aux zones privées et sensibles ;
- Le Prestataire doit définir et mettre en œuvre les mesures permettant d'assurer la confidentialité et l'intégrité des journaux d'accès aux zones privées et sensibles à l'aide de solutions respectant les mécanismes d'authentification ;
- Le Prestataire doit documenter et mettre en œuvre des mécanismes de surveillance et de détection des accès non autorisés aux zones privées et sensibles ;
- Le Prestataire doit journaliser l'ensemble des accès aux dispositifs du service ainsi que les actions réalisées sur le dispositif ou via les mécanismes du service ;
- Le Prestataire doit documenter et mettre en œuvre les moyens permettant de minimiser les risques inhérents aux sinistres physiques (incendie, dégât des eaux, etc.) et naturels (risques climatiques, inondations, séismes, etc.) ;
- Le Prestataire doit procéder à des tests réguliers des équipements de détection et de protection physique ;
- Le Prestataire doit documenter et mettre en œuvre des procédures relatives au travail en zones privées et sensibles ;
- Le Prestataire doit documenter et mettre en œuvre des mesures permettant de protéger le câblage électrique et de télécommunication des dommages physiques et des possibilités d'interception ;
- Le Prestataire doit documenter et mettre en place un plan de contrôle définissant le champ d'application et la fréquence des vérifications en conformité avec la gestion du changement, les politiques, et les résultats de l'évaluation des risques. Ce plan vise à assurer la mise en œuvre adéquate des mécanismes de sécurité et de protection de l'information, dont le Prestataire est responsable, incluant les accès logiques et physiques aux dispositifs du service d'administration et de maintenance sécurisées, ainsi que la revue des privilèges et des droits d'accès aux dispositifs ;
- Ce plan doit être révisé en cas de modification ou au minimum annuellement ;
- Les conclusions des contrôles doivent être officiellement confirmées et consignées par écrit auprès de la direction.

3.2.4. Sauvegardes

- Le Prestataire doit documenter et mettre en place un plan de sauvegarde et de restauration des dispositifs du service (sauvegardes des systèmes, des configurations et des données) ;
- Ce plan doit être testé au minimum annuellement ;
- Le dispositif de sauvegarde doit être hébergé dans un segment du système du service (segment d'administration) en accord avec le plan de sauvegarde préétabli.

3.2.5. Réseau d'administration, segmentation et cloisonnement du système d'information du service

- Le Prestataire doit segmenter le système d'information du service en plusieurs zones de confiance dans lesquelles sont répartis tous les dispositifs impliqués dans le service. La segmentation minimale comporte les zones de confiance suivantes :
  - zone(s) d'exploitation, regroupant les postes d'administration ou de maintenance utilisés par les administrateurs du service ;
  - zone(s) de serveurs, regroupant l'ensemble des serveurs hébergeant des outils d'administration pour les ressources administrées ;
  - zone(s) d'administration du système d'information du service, regroupant l'ensemble des outils d'administration du système d'information du service et les postes d'administration des administrateurs du système d'information du service ;
  - zone(s) de mise à jour, regroupant l'ensemble des dispositifs impliqués dans le processus de récupération et de mise à disposition des mises à jour des dispositifs du service ;
  - zone(s) d'infrastructures du système d'information du service, regroupant l'ensemble des serveurs d'infrastructure suivants : référentiel(s) d'identité, serveur(s) de temps, serveur(s) DHCP, serveur(s) DNS et infrastructure(s) de gestion de clés ;
  - zone(s) de service interne du système d'information du service, regroupant l'ensemble des services qui ne sont pas dans la ou le(s) zone(s) d'administration du système d'information du service et zone(s) d'infrastructure.

Ainsi que les zones de confiance d'interconnexion suivantes :

- zone d'échange Prestataire, regroupant les dispositifs permettant l'échange de fichiers avec des systèmes d'information du Prestataire extérieurs au système d'information du service ;
- zone d'accès à Internet, regroupant l'ensemble des composants permettant un accès sécurisé à Internet, par exemple pour l'administration de systèmes dont les outils

d'administration ne sont accessibles que par Internet (cloud, téléchargement de mises à jour, etc.) ;

- zone d'accès aux ressources administrées, regroupant l'ensemble des dispositifs permettant un accès sécurisé aux interfaces d'administration des ressources du Client final (hors exposition sur Internet) administrées dans le cadre de la prestation ;
- zone d'échange Client final, regroupant les ressources permettant à un Client final et au Prestataire d'échanger de manière sécurisée les informations nécessaires à la réalisation de la prestation ;
- zone des compartiments d'administration tierce, regroupant l'ensemble des dispositifs mis à disposition des administrateurs tiers à la prestation qualifiée en vue d'encadrer la sécurité de leurs interventions ;
- zone d'échange tiers, regroupant les dispositifs permettant l'échange d'informations de façon sécurisée avec des tiers ;
- zone d'accès distants, permettant aux administrateurs du service et aux administrateurs du système d'information du service en situation de nomadisme d'accéder au système d'information du service de manière sécurisée en vue de réaliser leurs actions.

- Le Prestataire doit mettre en œuvre des mesures garantissant le cloisonnement entre les différentes zones de confiance ;
- Le Prestataire doit mettre en œuvre une mesure de cloisonnement réseau pour que les postes d'administration ou de maintenance ne soient pas en mesure de communiquer directement entre eux ;
- Le Prestataire doit durcir les configurations des équipements réseau et de sécurité mis en œuvre pour le système d'information du service ;
- Le Prestataire doit établir et tenir à jour une cartographie du système d'information du service, en lien avec l'inventaire des actifs, (la liste des ressources matérielles ou virtualisées, les noms et fonctions des applications supportant le service, le schéma d'architecture réseau, la matrice des flux réseau autorisés, etc.).

3.2.6. Administration du système d'information du service

- Le Prestataire doit mettre à disposition des administrateurs du système d'information du service des postes d'administration sous sa maîtrise et dédiés exclusivement aux actions d'administration et de maintenance du système d'information du service ;
- Le Prestataire doit héberger les serveurs de la zone d'administration du système d'information du service sur un ou plusieurs dispositifs physiques dédiés ;

- Le Prestataire doit mettre en œuvre des serveurs d'administration dédiés à l'administration du système d'information du service ;
- Le Prestataire doit accéder aux ressources du système d'information du service en utilisant des protocoles permettant l'authentification et le chiffrement au niveau applicatif ou, à défaut, au niveau IP ;
- Le Prestataire doit activer et configurer un dispositif de filtrage réseau local sur les serveurs d'administration pour n'autoriser que les connexions répondant aux besoins des actions d'administration ou de maintenance du système d'information du service ;
- Le Prestataire doit durcir les configurations système des serveurs d'administration du système d'information du service.

3.2.7. Postes d'administration ou de maintenance

- Le Prestataire doit mettre à disposition des administrateurs de service des postes dédiés exclusivement au service ;
- Le Prestataire doit appliquer des mesures de durcissement des configurations système des postes d'administration ou de maintenance ;
- Le Prestataire doit mettre en œuvre des mécanismes de chiffrement pour le contenu des postes d'administration ou de maintenance ;
- Le Prestataire doit s'assurer que les postes d'administration ou de maintenance disposent d'un dispositif de filtrage réseau local activé et configuré pour n'autoriser que les connexions répondant strictement au besoin opérationnel du service ;
- Le Prestataire doit fournir un équipement, physiquement distinct, déployé en dehors du système d'information du service pour permettre l'accès à Internet.

3.2.8. Outils d'administration

- Le Prestataire doit s'assurer que les outils de gestion des configurations, qu'il met en œuvre, garantissent la confidentialité, l'intégrité et la traçabilité des éléments qu'ils contiennent et suivant les besoins ;
- Le Prestataire doit déployer des serveurs d'administration en cas de besoins,
- Le Prestataire doit cloisonner les serveurs d'administration en dédiant des systèmes d'exploitation ou des dispositifs physiques ;
- Le Prestataire doit accéder aux outils d'administration en utilisant des protocoles permettant l'authentification et le chiffrement au niveau applicatif ou, à défaut, au niveau IP ;
- Le Prestataire doit accéder aux ressources administrées en utilisant des protocoles permettant l'authentification et le chiffrement au niveau applicatif ou, à défaut, au niveau IP ;

- Le Prestataire doit activer et configurer un dispositif de filtrage réseau local sur les serveurs d'administration pour n'autoriser que les connexions répondant strictement au besoin opérationnel du service. Le Prestataire doit durcir les configurations système des serveurs d'administration.

3.2.9. Droits d'administration

- Le Prestataire doit mettre en place un annuaire des droits d'administration des administrateurs de l'infrastructure technologique et des administrateurs du service. Cet annuaire doit faciliter l'authentification sur toutes les ressources du système d'information du service, y compris les postes d'administration et de maintenance ;
- Le Prestataire doit mettre en œuvre une séparation logique entre les groupes d'administrateurs de services et les administrateurs du système d'information au sein de l'annuaire centralisé. Cette séparation concerne l'authentification ainsi que la gestion des autorisations ;
- Le Prestataire doit mettre en place des mécanismes d'authentification pour les administrateurs de services sur les outils d'administration (une authentification double facteur) ;
- Le Prestataire doit déployer un outil de gestion sécurisée des mots de passe sur les postes d'administration ou de maintenance, et doit s'assurer que les mots de passe sont stockés au sein de cet outil ;
- Le Prestataire doit modifier les mots de passe par défaut des équipements ou services utilisés au sein du système d'information du service au moment de l'installation.

3.2.10. Accès aux ressources administrées

a. Si les outils d'administration du système d'information sont exposés sur Internet :
   - Le Prestataire doit mettre en œuvre une infrastructure de postes de rebond (Jump Server) dédiés à l'accès aux ressources administrées. Cette infrastructure est hébergée dans une zone de serveurs dédiée ;
   - Le Prestataire doit s'assurer que toutes les actions d'administration, à destination des outils d'administration exposés sur Internet, sont effectuées via la zone d'accès à Internet, depuis les postes de rebond ;
   - Le Prestataire doit s'assurer, au minimum de façon quotidienne, de la réinitialisation de la configuration initiale des postes de rebond utilisés pour l'administration (dont les outils d'administration sont exposés sur Internet) ;
   - Le Prestataire doit assurer une traçabilité nominative des accès aux ressources administrées et des actions d'administration réalisées au travers de la zone d'accès à Internet.

b. Le système d'information du Client final non administrable à distance, pour des raisons réglementaires, de criticité ou de nécessité technique (comme dans le cas des systèmes d'information de type industriel) :
   - Le Prestataire doit tracer formellement l'ensemble des actions d'administration ou de maintenance réalisées ;
   - Si le Prestataire utilise un ou plusieurs systèmes de stockage amovibles pour ses actions d'administration ou de maintenance, il doit les dédier physiquement ;
   - Le Prestataire doit procéder à une analyse régulière du système de stockage.

c. Le système d'information du Client final est administrable à distance :
   - Le Prestataire doit s'assurer que toute action d'administration d'un système d'information du Client final (administrable à distance) est effectuée via la zone d'accès aux ressources administrées.
   - Le Prestataire doit assurer une traçabilité nominative des accès aux ressources administrées et des actions d'administration réalisées au travers de la zone d'accès aux ressources administrées.

4. EXIGENCES RELATIVES À UNE PRESTATION D'INTEGRATION

4.1. ÉTENDUE GEOGRAPHIQUE DU SERVICE

- Le Prestataire doit héberger, traiter, exploiter et administrer les données relatives au service d'intégration exclusivement au sein du territoire togolais.
- Le Prestataire doit documenter et communiquer, à la demande du Client final, la localisation du stockage et du traitement des données à sa disposition (documents d'architecture, éléments de configuration, informations d'authentification, etc.).
- Cependant, l'Agence Nationale de la Cybersécurité (ANCy) peut accorder une dérogation à cette obligation d'hébergement, sous réserve que le prestataire concerné fournisse une justification crédible et documentée de son incapacité à satisfaire cette exigence. La demande de dérogation sera soumise à une évaluation rigoureuse avant approbation.

4.2. EXIGENCES MINIMALES DU SERVICE D'INTEGRATION

a. Le prestataire doit prendre en considération les caractéristiques de cybersécurité des équipements et s'assurer de leur qualification par l'ANCy, en tant que critères essentiels lors du processus d'achat ;

b. Le prestataire doit soumettre à validation par le Client final la liste et les caractéristiques de l'ensemble des équipements qui seront intégrés chez le Client final ;

c. Dans le cas où les équipements sont imposés par le client final, le prestataire doit être en mesure de lui apporter un conseil pour lui signaler que le niveau de cybersécurité des équipements n'est pas en adéquation avec le niveau de cybersécurité visé pour le système final ;

d. Le prestataire doit vérifier la mise en œuvre des règles de bonnes pratiques lors de la configuration des équipements de sécurité ;

e. Le prestataire doit être en mesure d'accepter, sur demande explicite du commanditaire, un audit d'architecture et de configuration ou toute autre vérification nécessaire ;

f. Le prestataire doit être en mesure de réaliser des tests unitaires et d'ensemble pour vérifier que les exigences de cybersécurité sont bien implémentées ;

g. Le prestataire doit être en mesure de tracer les mises à jour et modifications qu'il a apportées aux systèmes déployés et de fournir ces traces au client final ;

h. Le prestataire doit garantir, dans son processus de livraison, l'intégrité et l'authenticité de l'ensemble des logiciels, programmes, éléments de configuration et documentation.