PLAN D'ASSURANCE SÉCURITÉ

STATUT : VALIDÉ
VERSION : 2.0

PUBLIQUE	INTERNE	LIMITÉE	CONFIDENTIEL
X			

BUREAU VERITAS

TABLE DES MATIÈRES

GÉNÉRALITÉS

PRÉSENTATION DU PLAN D'ASSURANCE SÉCURITÉ

Le présent Plan d'Assurance Sécurité (PAS) s'appliquera à tout tiers (« Tiers ») qui accède au Système d'information ou aux Données de Bureau Veritas (par exemple, dans le cadre de la fourniture d'un service à Bureau Veritas ou du développement d'un partenariat numérique).

L'objectif est de garantir que les tiers respectent les besoins de Bureau Veritas en matière de sécurité et se conforment aux meilleures pratiques de sécurité lorsqu'ils accèdent au Système d'information ou aux Données de Bureau Veritas.

Ceci permet de garantir que les Données de Bureau Veritas Data sont correctement protégées et que ses systèmes restent efficaces, robustes et résilients.

Le présent PAS dressera la liste des mesures de sécurité et contrôles nécessaires à appliquer et à maintenir dans le cadre du service proposé à Bureau Veritas ou dans le cadre du partenariat développé avec Bureau Veritas.

Il est demandé au Tiers de dûment remplir le présent document et d'apporter les commentaires et informations appropriés afin d'aider Bureau Veritas à évaluer le positionnement du Tiers en matière de sécurité. En cas de non-respect d'une exigence, il est dans l'intérêt du Tiers de définir des mesures alternatives à déployer, le cas échéant, en vue d'atténuer le risque.

Dès réception du document dûment renseigné, Bureau Veritas l'examinera et se réservera le droit de demander d'autres justificatifs relatifs à l'applicabilité / au respect des exigences de sécurité énoncées.

Un PAS rempli avec les éléments saisis par un Tiers de Bureau Veritas devient un **document à diffusion limitée (C3)**. Une fois le document rempli, le niveau de classification figurant dans le pied de page du document sera mis à jour en conséquence.

PORTEE ET DUREE D'APPLICATION

Eu égard au Code de conduite des Partenaires de Bureau Veritas, le PAS fait partie intégrante de la relation contractuelle entre **Bureau Veritas** et :

Nom de la société	
Adresse de la société	
Coordonnées de l'interlocuteur	

Le PAS décrit les mesures de sécurité techniques et organisationnelles mises en œuvre par le Tiers aux fins de se protéger et de protéger les Données de Bureau Veritas contre tout traitement illicite, perte, vol, toute suppression, altération ou destruction accidentelle ou frauduleuse, tout dommage ou toute utilisation ou divulgation non autorisée.

Ces mesures de sécurité s'appliquent au périmètre du service fourni à Bureau Veritas / du partenariat développé avec Bureau Veritas indiqué ci-après :

Elles resteront applicables pendant toute la durée de l'accord sous-jacent conclu avec Bureau Veritas.

Dans le cadre des politiques de Bureau Veritas, Bureau Veritas est en droit de vérifier le respect par les Tiers des dispositions en matière de sécurité qu'ils indiquent dans le PAS.

EXAMEN DU TIERS

Bureau Veritas évalue régulièrement ses Tiers. Par la suite, un examen régulier du PAS sera effectué au plus une fois par an.

Le Tiers sera prié de mettre à jour le présent document, de fournir un document justificatif à jour et d'informer Bureau Veritas de tout changement affectant son positionnement en matière de sécurité ou sa capacité à protéger les Données de Bureau Veritas.

Date de la dernière révision	

EXIGENCES EN MATIÈRE DE SÉCURITÉ

ORGANISATION ET POLITIQUE EN MATIÈRE DE SÉCURITÉ DE L'INFORMATION

ORGANISATION DE LA SÉCURITÉ DE L'INFORMATION	
Le Tiers désignera un employé en charge de la gestion globale de la sécurité de l'information.	☐ Conforme ☐ Partiellement conforme ☐ Non conforme ☐ Non applicable
Commentaires du Tiers :	

POLITIQUE RELATIVE À LA SÉCURITÉ DE L'INFORMATION	
Le Tiers adoptera une politique relative à la sécurité de l'information. La politique portera sur des principes de gouvernance précis et des exigences fondamentales en matière de sécurité à adopter en vue de proposer un service sûr. La politique sera communiquée aux parties concernées et mise à jour régulièrement.	☐ Conforme ☐ Partiellement conforme ☐ Non conforme ☐ Non applicable
Commentaires du Tiers :	

CERTIFICATION DE TIERS	
Le Tiers s'engage à : ▪ informer Bureau Veritas de tout certificat ou toute preuve de conformité relativement à une ou plusieurs normes de sécurité de l'information (par exemple ISO, NIST, etc.) ; ▪ décrire la portée des certificats ; ▪ partager avec Bureau Veritas les certificats ou toute autre preuve de conformité.	☐ Conforme ☐ Partiellement conforme ☐ Non conforme ☐ Non applicable
Commentaires du Tiers :	

SOUS-TRAITANCE	
Le Tiers identifiera et communiquera la liste des sous-traitants qui le soutiennent dans le cadre de la prestation des services à Bureau Veritas. Par le biais d'un processus formel, le Tiers procèdera à une évaluation et veillera à ce que les sous-traitants qui traitent les informations de Bureau Veritas se conforment aux mêmes exigences de sécurité que le Tiers.	☐ Conforme ☐ Partiellement conforme ☐ Non conforme ☐ Non applicable
Commentaires du Tiers :	

DISPOSITIONS SUPPLÉMENTAIRES EN MATIÈRE DE PROTECTION DES DONNÉES PRIVÉES ET DE SÉCURITÉ	
Le Tiers communiquera à Bureau Veritas les documents et preuves nécessaires (p. ex., rapport d'audit de sécurité, analyses de vulnérabilité, etc.) démontrant que les exigences de sécurité et les problèmes sont traités de manière adéquate. Le Tiers fournira à Bureau Veritas les informations nécessaires et l'accès pour effectuer un audit de sécurité si aucun rapport d'audit récent n'est fourni par le Tiers.	☐ Conforme ☐ Partiellement conforme ☐ Non conforme ☐ Non applicable
Commentaires du Tiers :	

RESSOURCES HUMAINES

FORMATION ET SENSIBILISATION À LA SÉCURITÉ	
Le Tiers s'assurera que ses employés amenés à intervenir dans les locaux de Bureau Veritas ou à manipuler les Données de Bureau Veritas sont formés pour se conformer aux exigences de sécurité et aux meilleures pratiques. Le Tiers communiquera les preuves démontrant que sa société mène régulièrement des actions et campagnes de sensibilisation.	☐ Conforme ☐ Partiellement conforme ☐ Non conforme ☐ Non applicable
Commentaires du Tiers :	

RESPECT DES POLITIQUES DE BUREAU VERITAS	
Les employés du Tiers ayant accès aux systèmes et infrastructures de Bureau Veritas reconnaissent et acceptent d'utiliser les ressources de Bureau Veritas en ce qui concerne les politiques et contrôles de Bureau Veritas visés dans le présent document.	☐ Conforme ☐ Partiellement conforme ☐ Non conforme ☐ Non applicable
Commentaires du Tiers :	

ACCÈS LOGIQUE

ACCÈS LOGIQUE AUX RESSOURCES INFORMATIQUES ET AUX DONNÉES	
Le Tiers mettra en place des mesures de sécurité adéquates aux fins de la protection des Données de Bureau Veritas contre l'accès illégal et non autorisé ainsi que des ressources utilisées pour fournir le service ou collaborer avec Bureau Veritas. Ces mesures comprennent (entre autres) : ▪ l'utilisation de comptes nominatifs ; ▪ l'octroi de droits d'accès sur la base du principe du besoin de savoir ; ▪ l'utilisation de méthodes d'authentification individuelle pour valider l'identité des utilisateurs ; ▪ la mise en application d'une politique stricte de protection par mot de passe ; ▪ l'examen régulier des droits d'accès.	☐ Conforme ☐ Partiellement conforme ☐ Non conforme ☐ Non applicable
Commentaires du Tiers :	

GESTION DES COMPTES PRIVILÉGIÉS	
Le Tiers gérera les comptes privilégiés ayant accès aux Données de Bureau Veritas et surveillera étroitement leur activité. La méthode d'authentification adoptée pour les comptes privilégiés sera plus stricte que celle des comptes normaux (p. ex., utilisation de l'authentification multifacteur, politique sur les mots de passe plus stricte, etc.).	☐ Conforme ☐ Partiellement conforme ☐ Non conforme ☐ Non applicable
Commentaires du Tiers :	

SYSTÈME D'AUTHENTIFICATION	
L'accès aux services et aux systèmes du Tiers pour les employés de Bureau Veritas passera par le répertoire de l'entreprise via un système d'authentification unique (SSO) entre Bureau Veritas et le Tiers. En cas d'impossibilité, le Tiers aidera Bureau Veritas à élaborer une procédure de gestion des comptes décrivant (entre autres) : ▪ la création de comptes ; ▪ la politique sur les mots de passe ; ▪ la communication du mot de passe initial ; ▪ la cession / modification / suppression des autorisations.	☐ Conforme ☐ Partiellement conforme ☐ Non conforme ☐ Non applicable
Commentaires du Tiers :	

SÉCURITÉ DES INFRASTRUCTURES, DES RÉSEAUX ET DES SYSTÈMES

MESURES DE PROTECTION	
Le Tiers mettra en œuvre des mesures techniques et organisationnelles suffisantes aux fins de protéger les ressources utilisées pour la prestation du service à Bureau Veritas et les équipements hébergeant / gérant les Données de Bureau Veritas. Les mesures suivantes doivent être prises en compte : ▪ la segmentation adéquate du réseau ; ▪ le déploiement de pare-feu pour protéger les différents réseaux et ressources ; ▪ la mise en œuvre d'un produit de détection et de prévention des intrusions sur les hôtes et la surveillance active des alertes ; ▪ la consolidation des serveurs hébergeant des Données et des applications ; ▪ la protection des serveurs contre les virus par la mise en œuvre de contre-mesures adaptées avec un logiciel antivirus ou un système d'exploitation (« OS ») régulièrement mis à jour ; ▪ le maintien et la mise à jour des systèmes d'exploitation ainsi que des applications qui y sont installées ; ▪ l'analyse régulière du réseau et des hôtes afin de détecter toute configuration non autorisée ou vulnérable (analyse de vulnérabilité) ; ▪ la mise en œuvre et le maintien des technologies de filtrage Web et de protection des courriels.	☐ Conforme ☐ Partiellement conforme ☐ Non conforme ☐ Non applicable
Commentaires du Tiers :	

PROTECTION DES POINTS DE TERMINAISON	
Le Tiers mettra en œuvre des mesures techniques et organisationnelles suffisantes pour sécuriser les postes de travail, ordinateurs portables et autres dispositifs que ses employés utilisent pour remplir leurs missions. Les mesures suivantes doivent être prises en compte : ▪ l'utilisation de systèmes d'exploitation (« OS ») mis à jour et correctement configurés ; ▪ la protection des terminaux à l'aide de produits antivirus et anti-malware et leur mise à jour régulière ; ▪ la mise en place de mesures visant à s'assurer que les solutions antivirus et anti-malware ne sont jamais désactivées sur les terminaux sauf dans la mesure nécessaire ; ▪ la protection de l'accès aux dispositifs (p. ex. par mot de passe individuel) ; ▪ la mise en œuvre et le maintien des technologies de filtrage Web et de protection des courriels.	☐ Conforme ☐ Partiellement conforme ☐ Non conforme ☐ Non applicable
Commentaires du Tiers :	

SURVEILLANCE ET CONNEXION

SURVEILLANCE ET ENREGISTREMENT CONTINUS	
Le Tiers mettra en place des mesures permettant de surveiller et enregistrer en permanence tout événement de sécurité (p.ex. tentatives d'accès non autorisées) affectant les Données de Bureau Veritas ainsi que les infrastructures et systèmes utilisés dans le cadre du contrat. Le niveau des journaux enregistrés permet de rendre compte des actions réalisées et de l'accès aux données de Bureau Veritas. Bureau Veritas sera autorisé à demander des journaux concernant l'accès à ses Données. Ces journaux doivent être utilisés à des fins d'enquête. Le Tiers communiquera les modalités selon lesquelles Bureau Veritas peut demander des journaux.	☐ Conforme ☐ Partiellement conforme ☐ Non conforme ☐ Non applicable
Commentaires du Tiers :	

SURVEILLANCE ET ENREGISTREMENT CONTINUS	
Le Tiers devra continuellement mettre en corrélation et analyser les journaux afin de détecter les incidents de sécurité, les fuites de données ou tous événements susceptibles de compromettre la sécurité des Données et des services.	☐ Conforme ☐ Partiellement conforme ☐ Non conforme ☐ Non applicable
Commentaires du Tiers :	

DÉVELOPPEMENT ET MAINTENANCE SÉCURISÉS

DÉVELOPPEMENT SÉCURISÉ	
Le Tiers respectera des pratiques de développement sécurisé lors du développement d'applications pour le compte de Bureau Veritas. Ces pratiques de développement sécurisé doivent prendre en compte les recommandations de références reconnues (p. ex. OWASP).	☐ Conforme ☐ Partiellement conforme ☐ Non conforme ☐ Non applicable
Commentaires du Tiers :	

DOCUMENTATION OPÉRATIONNELLE	
Le Tiers devra tenir et mettre à jour régulièrement la documentation adéquate et suffisante sur l'application et les services. Les éléments de la documentation sont convenus avec Bureau Veritas. Les éléments suivants seront pris en considération : ▪ le schéma d'architecture ; ▪ les flux de réseau ; ▪ la liste des environnements de production et de préproduction, leur finalité et les mesures de sécurité mises en place pour les protéger ; ▪ les cycles de correction fonctionnelle et technique ; ▪ la documentation opérationnelle pour la gestion de l'application. Bureau Veritas demandera régulièrement des copies de la documentation.	☐ Conforme ☐ Partiellement conforme ☐ Non conforme ☐ Non applicable
Commentaires du Tiers :	

SÉCURITÉ PHYSIQUE ET ENVIRONNEMENTALE

CONTRÔLES DE SÉCURITÉ PHYSIQUE ET ENVIRONNEMENTALE	
Le Tiers mettra en œuvre des mesures et des contrôles suffisants pour protéger la sécurité physique des installations hébergeant les Données de Bureau Veritas. Ces mesures et contrôles protégeront les locaux du Tiers contre l'accès non autorisé ainsi que les menaces externes et environnementales. Les mesures suivantes seront prises en compte : ▪ l'accès donné depuis les portails à des espaces privés et des espaces hébergeant des Données verrouillées ; ▪ la limitation de l'accès aux employés autorisés uniquement ; ▪ la protection contre les intrusions (alarmes et vidéo-surveillance, système de détection des intrusions, dispositifs de protection) ; ▪ l'application de mesures visant à contrôler l'accès aux salles du serveur (contrôles d'accès individuel) ; ▪ l'identification des visiteurs et l'accompagnement des visiteurs lors de leurs visites ; ▪ la mise en place de procédures visant à s'assurer que les problèmes environnementaux (inondations, incendies, tremblements de terre, etc.) ne causent pas de perturbation du service ou de perte des Données.	☐ Conforme ☐ Partiellement conforme ☐ Non conforme ☐ Non applicable
Commentaires du Tiers :	

PROTECTION DES DONNÉES DE BUREAU VERITAS

LOCALISATION ET ACCÈS DES DONNÉES	
Le Tiers définira la localisation géographique de ses centres de données ou de son cloud Tiers (à savoir AWS) où les Données de Bureau Veritas Data seraient stockées. Le Tiers sera en mesure d'identifier individuellement les employés et machines ayant accès aux Données de Bureau Veritas.	☐ Conforme ☐ Partiellement conforme ☐ Non conforme ☐ Non applicable
Commentaires du Tiers :	

SAUVEGARDES DE DONNÉES	
Le Tiers adoptera une procédure de sauvegarde et la testera régulièrement. Les Données de Bureau Veritas seront sauvegardées. Les règles de conservation et de sauvegarde seront définies avec le représentant de Bureau Veritas si nécessaire, afin de répondre aux besoins opérationnels. Les sauvegardes doivent être répliquées sur un site secondaire. Toutes les Données seront stockées, sauvegardées et supprimées conformément aux lois et réglementations applicables en matière de protection des données et aux obligations contractuelles.	☐ Conforme ☐ Partiellement conforme ☐ Non conforme ☐ Non applicable
Commentaires du Tiers :	

CHIFFREMENT DES DONNÉES	
Le Tiers s'assurera que les Données de Bureau Veritas sont protégées contre tout accès non autorisé. Le chiffrement des données est effectué sur demande de Bureau Veritas. Le Tiers s'engage à chiffrer les Données de Bureau Veritas en transit sur des réseaux publics extérieurs, y compris l'Internet. Les Données seront échangées via des protocoles correctement configurés et sécurisés (SFTP, TLS). En outre, le chiffrement sera déployé sur les ordinateurs et les terminaux contenant des Données sensibles de Bureau Veritas.	☐ Conforme ☐ Partiellement conforme ☐ Non conforme ☐ Non applicable
Commentaires du Tiers :	

DESTRUCTION DES DONNÉES	
Le Tiers adoptera une procédure de destruction des Données pour la destruction définitive des Données à l'expiration ou à la résiliation du contrat et sur consentement de Bureau Veritas. Grâce à la procédure de destruction, les Données de Bureau Veritas ne pourront être récupérées par aucun Tiers après la suppression définitive.	☐ Conforme ☐ Partiellement conforme ☐ Non conforme ☐ Non applicable
Commentaires du Tiers :	

GESTION DES INCIDENTS DE SÉCURITÉ

PROCESSUS DE GESTION DES INCIDENTS	
Le Tiers mettra en œuvre un processus d'intervention en cas d'incident de sécurité ainsi que des mécanismes de partage des informations pendant et après un incident. Le Tiers décrira : ▪ la portée de l'incident de sécurité de l'information qu'il signalera à Bureau Veritas ; ▪ le niveau d'information divulgué à Bureau Veritas ; ▪ le délai pour signaler les incidents de sécurité ; ▪ la procédure de notification ; ▪ les coordonnées spécifiques ; ▪ les solutions existantes qui pourront s'appliquer dans certains cas d'incidents de sécurité. Le processus de gestion des incidents respectera les lois et réglementations applicables (p. ex., délai de notification aux autorités locales).	☐ Conforme ☐ Partiellement conforme ☐ Non conforme ☐ Non applicable
Commentaires du Tiers :	

SIGNALEMENT D'INCIDENTS	
Le Tiers et Bureau Veritas conviendront des mécanismes et des canaux de communication permettant : ▪ à Bureau Veritas de signaler au Tiers les événements de sécurité de l'information qu'il a détectés ; ▪ au Tiers de signaler à Bureau Veritas les événements de sécurité de l'information qu'il a détectés ; ▪ à Bureau Veritas de suivre l'état d'un événement de sécurité de l'information signalé.	☐ Conforme ☐ Partiellement conforme ☐ Non conforme ☐ Non applicable
Commentaires du Tiers :	

NIVEAU DE SERVICE ET CONTINUITÉ

PLAN DE CONTINUITÉ DES ACTIVITÉS	
Le Tiers adoptera un plan de continuité des activités afin d'assurer la continuité des services fournis à Bureau Veritas dans une situation défavorable, conformément au niveau de service défini dans le contrat (SLA).	☐ Conforme ☐ Partiellement conforme ☐ Non conforme ☐ Non applicable
Commentaires du Tiers :	

CONFORMITÉ

CONFORMITÉ AU RGPD	
Le Tiers respectera les lois et réglementations applicables en matière de protection des données à caractère personnel, y compris le RGPD. En particulier, le Tiers mettra en œuvre des mesures techniques et organisationnelles appropriées pour protéger les Données de Bureau Veritas, y compris les données à caractère personnel.	☐ Conforme ☐ Partiellement conforme ☐ Non conforme ☐ Non applicable
Commentaires du Tiers :	

GLOSSAIRE

RSSI désigne le responsable de la sécurité des systèmes d'information.

Données (ou Données de Bureau Veritas) désigne les données, fichiers et contenus appartenant à Bureau Veritas, y compris les Données à caractère personnel.

RGPD désigne le Règlement général de l'UE n° 2016/679 du 27 avril 2016 relatif à la protection des données. Le règlement vise à assurer la protection des personnes physiques eu égard au traitement des données à caractère personnel et à la libre circulation de ces données.

Système d'information désigne un ensemble intégré de composants (y compris des équipements informatiques) pour la collecte, le stockage et le traitement des données et la remise d'informations.

SSI désigne la sécurité des systèmes d'information.

Politiques de SSI désigne les politiques de sécurité des systèmes d'information, parmi lesquelles figurent la politique mondiale de sécurité des systèmes d'information et les politiques opérationnelles. Il s'agit d'un ensemble de documents qui définit le cadre de la sécurité des systèmes d'information (SSI) au moyen de principes de gouvernance et de règles pragmatiques à mettre en œuvre au sein de l'ensemble du groupe Bureau Veritas.

LDAP désigne le protocole de gestion d'annuaires *Lightweight Directory Access Protocol*.

Logiciel malveillant (ou *malware*) désigne tout logiciel utilisé en vue de perturber des opérations informatiques ou mobiles, de collecter des informations critiques, d'accéder à un système d'information privé ou d'afficher du contenu publicitaire indésirable. Ce terme renvoie à une diversité de formes de logiciels hostiles ou intrusifs, y compris les virus informatiques, les vers, les chevaux de Troie, les logiciels d'extorsion (*ransomware*), les logiciels espions (*spyware*), les logiciels publicitaires (*adware*), les logiciels destinés à effrayer les utilisateurs (*scareware*) et d'autres programmes malveillants.

AND désigne un accord de non-divulgation.

Données à caractère personnel désigne toute information relative à une personne physique identifiée ou identifiable (« Personne concernée ») ; une personne physique identifiable est une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant tel qu'un nom, un numéro d'identification, des Données de localisation, un identifiant en ligne ou un ou plusieurs facteurs spécifiques propres à son identité physique, physiologique, génétique, mentale, économique, culturelle ou sociale.

SFTP désigne le protocole de transfert sécurisé de fichiers *Secure File Transfer Protocol*.

PAS désigne le présent plan d'assurance Sécurité.

TLS désigne le protocole de sécurisation des échanges sur Internet *Transport Layer Security*. Il s'agit d'un protocole de chiffrement qui permet de sécuriser de bout en bout les communications sur les réseaux.

« Tiers » désigne toute partie qui n'appartient pas au groupe Bureau Veritas, y compris notamment les prestataires de services, partenaires, sous-traitants ou clients.

Approbateurs

Nom	Fonction	Date
Julien ANICOTTE	RSSI du Groupe	13/10/2020
Sonia DELPY	DPD du Groupe	13/10/2020

Versions

Version	Auteur	Nature des modifications	Date
1.0	Meryem OUKEMENI	Validation et diffusion	27/07/2018
2.0	Youness TASTIFT	Révision du PAS	09/10/2020