POLITIQUE GROUPE DE SECURITE DES SYSTEMES D'INFORMATION

ETAT : VALIDEE

VERSION : 2,2

PUBLIC	INTERNE	RESTREINT	SECRET
X			

BUREAU VERITAS

Shaping a World of Trust

Approbateurs

Nom	Fonction
François VILJOEN	Vice-président directeur, Directeur des systèmes d'information (CIO) Groupe
Julien ANICOTTE	Directeur de la sécurité des systèmes d'information Groupe

Documents de référence

Titre du document	Nom du document

Classification

Niveau	Confidentialité
C1	Public

TABLE DES MATIERES

GLOSSAIRE

B

BCP : Plan de continuité des activités.

BL : Ligne métier.

C

CIO : Directeur des systèmes d'information.

CISO : Directeur de la sécurité des systèmes d'information.

F

Fournisseur : Prestataire sélectionné par Bureau Veritas dans le cadre d'un appel d'offres et fournissant à cette dernière des Services en vertu d'un Contrat.

I

ISMS : Système de gestion de la sécurité de l'information.

O

OG : Groupe opérationnel.

P

Personnel du Fournisseur : collaborateurs du Fournisseur que ce dernier affecte à la fourniture des Services.

Politiques ISS : Politiques de sécurité des systèmes d'information. Comprennent l'ISSP mondiale et les Politiques opérationnelles.

PSSI Groupe : Politique mondiale de sécurité des systèmes d'information. Le présent document.

S

Services : ensemble des services, tous types confondus, fournis par un Fournisseur à Bureau Veritas, y compris notamment l'assistance technique, les services de maintenance, tous services basés sur le cloud comme les SaaS, IaaS, PaaS, etc. ; ils peuvent être fournis sur site ou hors site.

SO : Responsable de la sécurité.

1. INTRODUCTION

La Politique Groupe de sécurité des systèmes d'information définit le cadre de référence de Bureau Veritas en matière de sécurité de l'information, en soulignant les principaux enjeux et objectifs liés à la sécurité. Elle énonce également des principes de gouvernance et des exigences fondamentales de sécurité qui s'appliquent à Bureau Veritas.

La PSSI Groupe vise à garantir la protection des informations à l'aide de quatre critères de classification :

- Disponibilité ;
- Intégrité ;
- Confidentialité et ;
- Traçabilité.

1.1. LA SECURITE DE L'INFORMATION, UN ENJEU CRUCIAL

Les informations sous toutes leurs formes, qu'elles soient écrites, verbales ou électroniques, soumises à un traitement manuel ou automatique, constituent une ressource stratégique dont dépendent la performance de la société, sa durabilité et sa faculté à développer ses activités et à obtenir des résultats.

Pour faire face aux risques d'accidents et d'actes malveillants qui pèsent sur la sécurité de ses systèmes d'information, Bureau Veritas doit protéger avec efficacité son système d'information en mettant en œuvre des mesures de sécurité adéquates, adaptées aux enjeux liés à la sécurité.

Ces mesures de sécurité doivent permettre à Bureau Veritas de respecter ses engagements contractuels, ses obligations légales et réglementaires, et d'assurer la continuité, mais aussi la qualité, des services fournis aux clients. Elles garantiront également la protection et l'amélioration de l'image Bureau Veritas.

1.2. OBJECTIFS COMMUNS POUR UNE PROTECTION EFFICACE

Le cadre applicable à la Sécurité des systèmes d'information de Bureau Veritas est défini par la PSSI Groupe, avec l'appui de Politiques opérationnelles qui détaillent les rôles et les responsabilités en matière de gestion de la sécurité de l'information dans différents domaines.

Les principes de gouvernance et les règles communes énoncés dans les Politiques ISS doivent garantir la protection efficace des informations au sein de Bureau Veritas, de même que la cohérence du système de gestion de la sécurité de l'information. En outre, ils doivent nous permettre de tirer profit des mesures de sécurité et des meilleures pratiques mises en œuvre au sein des diverses entités et filiales de l'organisation.

1.2.1. PERIMETRE ORGANISATIONNEL

La PSSI Groupe doit être appliquée à l'ensemble des entités et filiales du groupe Bureau Veritas dans le monde.

Les Politiques ISS doivent également cadrer les relations avec nos Fournisseurs. Ces politiques doivent énoncer les principes de sécurité fondamentaux qui s'appliquent aux services que Bureau Veritas commande à des Fournisseurs.

Certaines filiales ou entités de Bureau Veritas peuvent être soumises à des politiques de sécurité dédiées et spécifiques adaptées à la nature de leur activité, au pays où elles sont situées (par exemple les obligations légales locales) ou aux exigences contractuelles de leurs Clients ou Fournisseurs.

1.2.2. PERIMETRE FONCTIONNEL

L'ensemble des ressources liées à la gestion des informations du Bureau Veritas sont incluses dans la Système de gestion de la sécurité de l'information, de même que les modes de création, d'acquisition, de traitement, de conservation, de distribution ou de destruction de ces informations qui sont compris dans les éléments suivants, ou les utilisent :

- matériel des utilisateurs (par exemple les ordinateurs de bureau et portables, les smartphones, les tablettes) ;
- ressources opérationnelles (par exemple les serveurs, les imprimantes, les dispositifs de télécommunication) ;
- logiciels (par exemple les systèmes d'exploitation, les bases de données) ;
- supports papier ;
- ressources humaines et organisationnelles.

1.2.3. PERIMETRE TECHNIQUE

Les Politiques ISS doivent être mises en œuvre par le groupe Bureau Veritas et par l'ensemble de ses entités et filiales. Elles visent à garantir l'applicabilité quel que soit le contexte organisationnel, en détaillant non pas les technologies à mettre en œuvre, mais uniquement les exigences fonctionnelles et organisationnelles.

1.2.4. APPROCHE

Au-delà des standards de l'industrie, les politiques ISS doivent prendre en compte les éléments suivants :

- La gestion du risque lié à la sécurité de l'information : les règles établies dans chaque politique doivent être établies afin de pouvoir gérer et réduire les risques qui ont un impact significatif sur les opérations et menacent la confidentialité, l'intégrité, la disponibilité et la traçabilité de l'information.
- Conformité : les règles de sécurité doivent permettre d'assurer la conformité avec les réglementations, contrats et standards de l'industrie, ainsi que mettre en œuvre les mesures adéquates pour s'y conformer.
- Objectifs métiers : les politiques ISS, ainsi que la gouvernance en place, doivent coopérer et coordonner avec les métiers afin d'aligner la stratégie de sécurité avec les objectifs et la stratégie de Bureau Veritas : résilience et protection des données.

2. DOCUMENTS ISS

2.1. STRUCTURE DES DOCUMENTS RELATIFS A LA SECURITE DU SYSTEME D'INFORMATION

Les documents de Bureau Veritas relatifs à sécurité de l'information sont organisés au sein d'un référentiel à trois niveaux :

- **PSSI Groupe** (présent document) : document de référence fixant les enjeux, les principes de gouvernance et les principes fondamentaux de sécurité de l'information pour l'ensemble du groupe Bureau Veritas, conformément à la norme ISO 27001 ;
- **Politiques opérationnelles** : définissent les règles de sécurité de l'information qui s'appliquent à Bureau Veritas, en les classant par thème. Des dérogations temporaires peuvent être accordées aux entités ou aux filiales qui ne sont pas en mesure de garantir la conformité. Elles sont validées par le RSSI du groupe Bureau Veritas ;
- **Guides, normes et procédures** : documents opérationnels, opérations connexes, conformes aux critères définis dans les règles des Politiques opérationnelles. Ces documents peuvent être définis au niveau du groupe ou au niveau local.

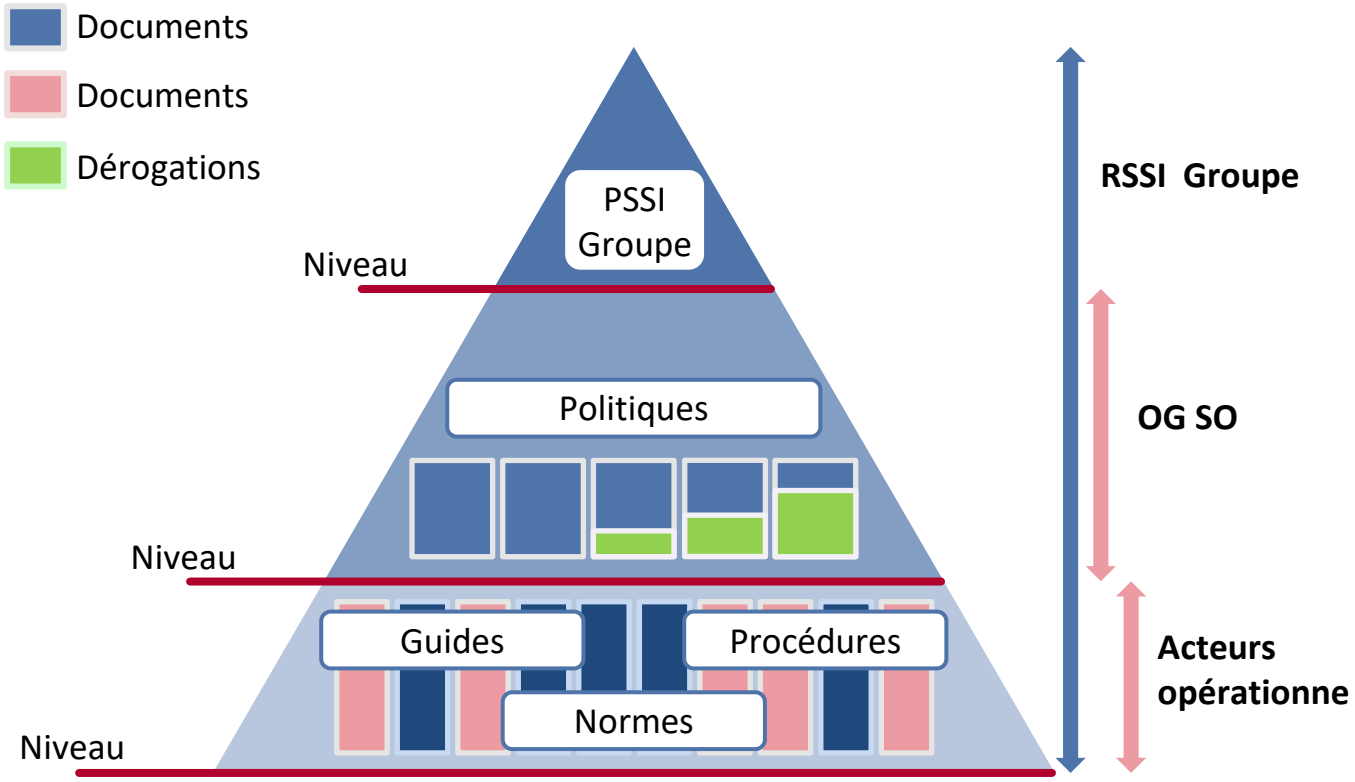

Figure 1 – Référentiel de documents et responsabilités

2.2. MISE EN ŒUVRE DE LA POLITIQUE DE SECURITE

2.2.1. CYCLE DE VIE

Afin de garantir l'efficacité et la durabilité des Politiques ISS au fil du temps et leur adaptation aux exigences de Bureau Veritas sur le plan de la sécurité, les Politiques ISS doivent faire l'objet d'une amélioration continue.

Ce processus d'amélioration continue doit être cyclique et basé sur la Roue de Deming (méthode PDCA, Plan-Do-Check-Act) :

- **Définition et planification (« Plan »)** : le RSSI Groupe (CISO) élabore un plan d'action comprenant les Politiques ISS à mettre à jour, les améliorations nécessaires et la phase de communication ;
- **Mise en œuvre (« Do »)** : le plan d'action défini au cours la phase précédente est mis en œuvre. Les améliorations sont appliquées aux Politiques ISS correspondantes ; les politiques mises jour sont communiquées aux personnes adéquates pour revue et validation.
- **Contrôle et surveillance (« Check »)** : cette phase permet d'identifier les impacts sur les activités opérationnelles. L'application des politiques est ainsi contrôlée.
- **Entretien et amélioration (« Act »)** : les officiers de sécurité et autres partenaires identifient les écarts et informent le RSSI (CISO). Les retours sont analysés pour identifier des améliorations et nourrir la prochaine phase « Plan ».

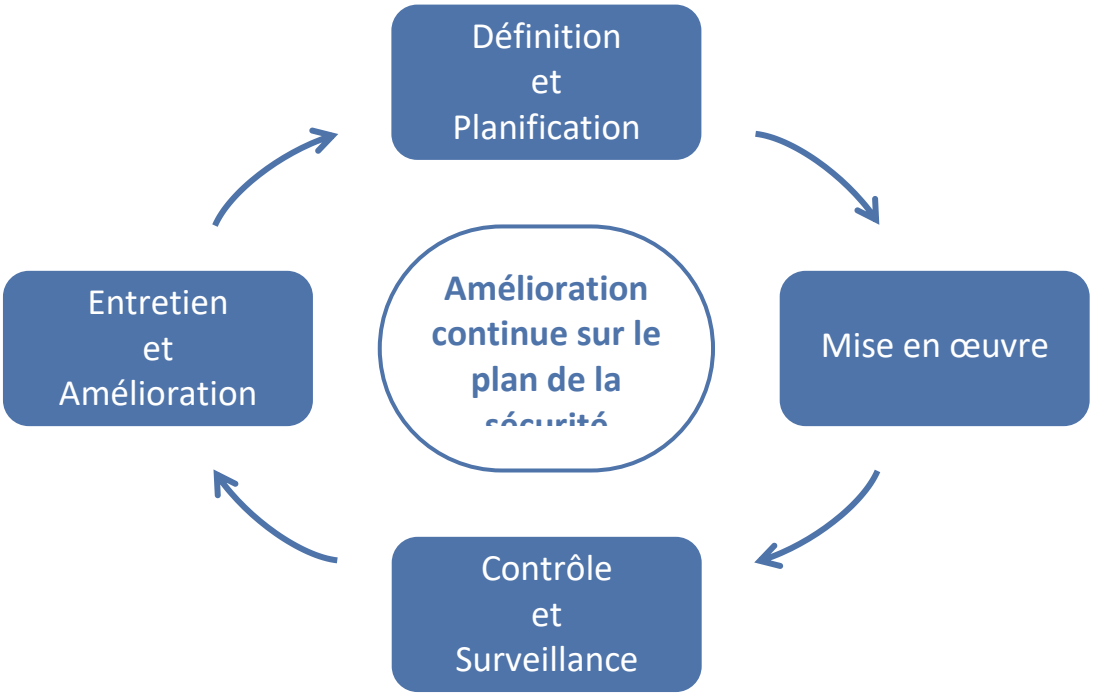

Figure 2 - Cycle de vie de l'amélioration continue

La PSSI Groupe et les Politiques opérationnelles doivent être révisées au moins une fois par an. Les demandes de mise à jour motivées par des besoins internes ou des facteurs externes sont centralisées et validées par le RSSI Groupe. Les Politiques ISS mises à jour sont soumises à la validation de la Direction exécutive de Bureau Veritas.

L'ensemble du cycle de vie des Politiques ISS doit être inclus dans le Système de gestion de la sécurité de l'information (ISMS) afin de garantir la mise en œuvre de celles-ci. Les différents éléments de l'ISMS doivent être formalisés et documentés afin de garantir la traçabilité de ses opérations.

2.2.2. APPLICABILITE

Les Politiques ISS doivent être appliquées et pouvoir faire l'objet d'une exécution forcée.

Tout manquement commis au regard des Politiques ISS doit être soumis à un plan d'action correctif formel doté d'un calendrier de réalisation ou de dérogations spécifique(s).

2.2.3. PUBLICATION

La PSSI Groupe doit être publiée publiquement sur le site du Groupe afin de montrer clairement l'engagement de Bureau Veritas à protéger son système d'information.

Les politiques Opérationnelles sont publiées en interne et doivent être accessible à tous les collaborateurs de Bureau Veritas.

Chaque actualisation des politiques doit être suivie par une communication aux parties prenantes pour les informer des changements.

3. GOUVERNANCE DE LA SECURITE DES SYSTEMES D'INFORMATION

3.1. PRESENTATION DE LA GOUVERNANCE

La gouvernance de la sécurité des systèmes d'information vise à définir la structure de la fonction de Bureau Veritas dédiée à la sécurité de l'information ainsi que les rôles et responsabilités assignés à l'ensemble des personnes concernées qui composent cette structure (RSSI Groupe, OG SO, Service de sécurité de l'information, etc.).

Cette gouvernance doit nous permettre d'encadrer l'activité de la fonction de Bureau Veritas dédiée à la sécurité des systèmes d'information en définissant les processus utiles, en articulant cette fonction et en fournissant les éléments nécessaires (Politiques ISS, supports de formation et de sensibilisation, guides).

La gouvernance inclut également tout rôle nécessaire à l'articulation de la sécurité des systèmes d'information dans le cadre des opérations d'entreprise, des fonctions de contrôle et de la gestion de projet.

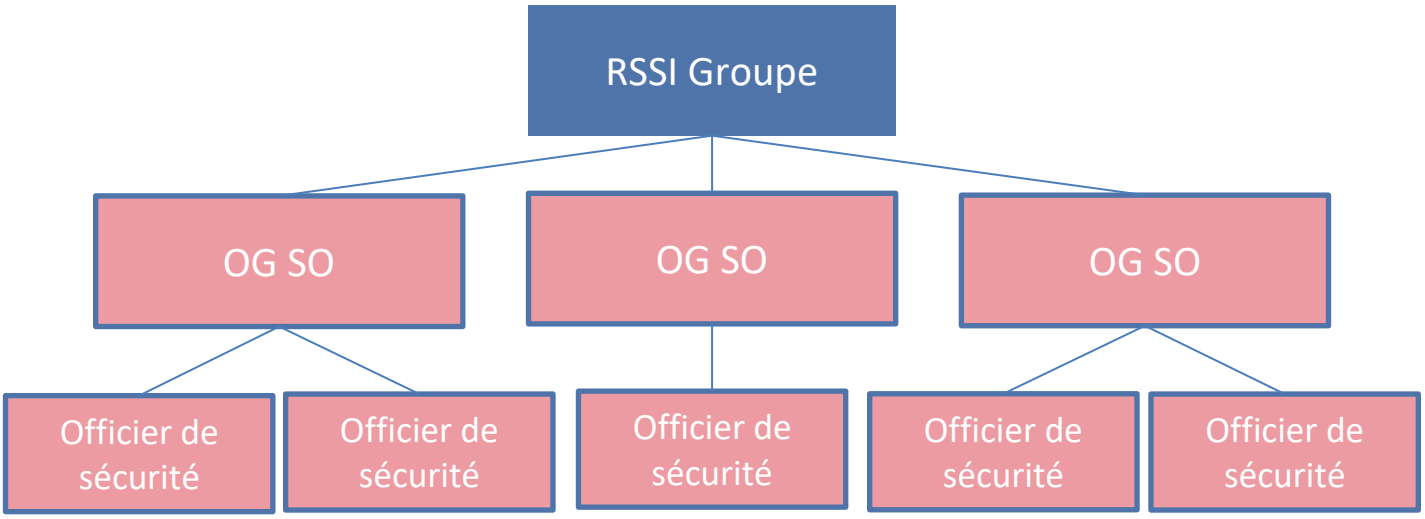

Figure 3 - Organisation de la gouvernance ISS de Bureau Veritas

3.2. LE DIRECTEUR MONDIAL DE LA SECURITE DE L'INFORMATION (RSSI GROUPE) DE BUREAU VERITAS

3.2.1. PRESENTATION DU RSSI GROUPE

Le RSSI Groupe de Bureau Veritas est le garant de la sécurité et de la continuité des systèmes d'information du groupe Bureau Veritas, de ses entités et de ses filiales. À ce titre, il est responsable du Système de gestion de la sécurité de l'information de Bureau Veritas.

Le RSSI Groupe exerce ses fonctions au sein de Bureau Veritas et aux côtés des Fournisseurs, des Clients et des tiers externes (par exemple des entités publiques, des organismes de certification).

3.2.2. MISSIONS DU RSSI GROUPE

Le RSSI Groupe de Bureau Veritas est responsable du Système de gestion de la sécurité de l'information de l'organisation et de son maintien en bon état. Dans le cadre de cette fonction, ses missions sont les suivantes :

- Formaliser, coordonner et maintenir en bon état la fonction de Bureau Veritas dédiée à la sécurité des systèmes d'information ;
- Définir des campagnes de formation et de sensibilisation ;
- Valider la désignation des OG SO ;
- Produire des tableaux de bord mondiaux relatifs à la sécurité, centraliser les indicateurs obtenus auprès des OG SO et réaliser des analyses de performance mondiales sur la sécurité des systèmes d'information ;
- Développer et mettre à jour les ISS ;
- Faire valider les Politiques ISS par la Direction exécutive ;
- Imposer et accompagner l'application des Politiques ISS au sein du groupe Bureau Veritas, de ses entités et de ses filiales ;
- Surveiller le respect des Politiques ISS au sein du groupe Bureau Veritas ;
- Traiter les demandes de dérogation aux Politiques ISS ayant une portée mondiale ou un impact important ;
- Planifier et superviser des audits sur les systèmes d'information axés sur la sécurité et appliquer le plan d'action correctif élaboré à partir des recommandations formulées à l'issue des audits ;
- Approuver les audits locaux sur la sécurité de l'information, y contribuer et les surveiller, en collaboration avec les OG SO ;
- Participer aux Comités d'approbation des changements (CAB), en particulier concernant les changements ayant un impact critique ou étendu sur les systèmes d'information de Bureau Veritas ;

- Surveiller la mise en œuvre et le maintien en bon état du processus de gestion des incidents de sécurité de Bureau Veritas, ainsi que son test régulier, en particulier afin de garantir l'efficacité du plan de gestion de crise et de l'unité de crise ;
- Surveiller la mise en œuvre et le maintien en bon état du Plan de continuité des activités de Bureau Veritas et son test régulier.

3.3. RESPONSABLES DE LA SECURITE DU GROUPE OPERATIONNEL (OG SO) DE BUREAU VERITAS

3.3.1. PRESENTATION DES OG SO

Les Responsables de la sécurité d'OG sont les garants de la sécurité et de la continuité des systèmes d'information de Bureau Veritas au niveau des OG. Désignés au niveau de chaque OG, ils seront les partenaires fiables de l'équipe centrale.

Leurs principales fonctions sont l'exécution et la supervision des opérations liées à la sécurité de l'information qui relèvent de leur périmètre au sein des équipes commerciales et techniques, mais aussi de garantir la bonne mise en œuvre des initiatives du groupe au sein de leur périmètre, notamment l'application des politiques et des cadres liés à la conformité.

3.3.2. MISSIONS DES OG SO

Les Responsables de la sécurité d'OG de Bureau Veritas sont responsables de la mise en œuvre du Système de gestion de la sécurité de l'information et de son maintien en bon état au sein de leur périmètre. Dans le cadre de cette fonction, leurs missions sont les suivantes :

- Signaler des informations importantes au RSSI Groupe ;
- Imposer l'application des Politiques ISS ;
- Traiter les demandes de dérogations au respect des Politiques ISS au sein de leur périmètre ;
- S'assurer que les bonnes pratiques de sécurité sont respectées ;
- Définir des campagnes de formation et de sensibilisation dédiées ;
- Produire des tableaux de bord locaux relatifs à la sécurité, analyser les indicateurs de sécurité et les transmettre au RSSI Groupe;
- Coordonner les mesures de sécurité locales ;
- Contribuer, en collaboration avec les unités opérationnelles et les départements informatiques, à la conversion des Politiques opérationnelles en procédures techniques (portant par exemple sur l'installation, l'exploitation et le traitement des incidents), en guides et en normes ;

- Approuver les audits locaux sur la sécurité de l'information, y contribuer et les surveiller, en collaboration avec le RSSI Groupe ;
- Participer aux Comités d'approbation des changements (CAB) portant sur les changements des systèmes d'information qui ont des répercussions à leur niveau ;
- Garantir le maintien en bon état du processus de gestion des incidents de sécurité au sein de leur périmètre ;
- Garantir le maintien en bon état du Plan de continuité des activités au sein de leur périmètre.

3.4. PREPOSES A LA SECURITE LOCAUX

Outre le RSSI Groupe et les OG SO décrits ci-dessus, l'organisation dédiée à la sécurité de l'information comprend des préposés à la sécurité locaux.

Les Responsables de la sécurité d'OG identifient et supervisent des préposés à la sécurité locaux au sein des entités, des filiales, des départements et des unités opérationnelles, dans la mesure du nécessaire. Les préposés à la sécurité locaux prêtent assistance aux OG SO dans le cadre de leurs missions, mettent en œuvre la sécurité de l'information au sein de leur périmètre de responsabilité ou élaborent des projets visant à répondre à des besoins spécifiques liés à la sécurité.

4. ANNEXES

4.1. ANNEXE 1 : HISTORIQUE DES REVISIONS

Version :	Auteur	Description	Date
1,5	Conformité SSI	Désignation du RSSI Groupe	12/01/2017
2.0	Conformité SSI	Mise à jour du contenu en vue d'un alignement sur la stratégie du groupe	27/03/2017
2.1	Conformité SSI	Mise à jour rôles liés à la sécurité Mise à jour de la fréquence de révision de la politique Ajout d'une nouvelle politique opérationnelle à l'annexe	19/12/2019
2.2	Conformité SSI	Ajout approche de création des politiques Ajout des prérequis de publication	19/03/2021

4.2. ANNEXE 2 : POLITIQUES OPERATIONNELLES

Les Politiques opérationnelles qui complètent la PSSI Groupe sur des thèmes propres à Bureau Veritas sont les suivantes :

- Sécurité des ressources humaines
- Classification de l'information
- Contrôle des accès logiques
- Sécurité physique
- Sécurité des opérations
- Gestion des traces informatiques
- Traitement des supports
- Matériel des utilisateurs
- Sécurité du réseau
- Sécurité du cloud
- Développement et maintenance des applications
- Relations avec les Fournisseurs
- Gestion des incidents de sécurité
- Continuité des activités