Aruba – Solutions Cloud

Annexe A
ISO 27001:2017

14.04.2023

Annexe A - ISO 27001 Les aspects relatifs à la sécurité du Cloud Aruba			
Domaine de contrôle		**Nos contrôles**	**Instruments et fonctionnalités à disposition du Client**
A.5	**Politiques pour la sécurité des informations**	**Politiques du Système de Gestion de la Sécurité des Informations** (SGSI) - Le Groupe Aruba a défini l'approche adoptée par l'organisation pour la gestion de ses objectifs de Sécurité des Informations dans une Politique d'entreprise spécifique. Ce document a été approuvé par la Direction et publié sur l'intranet de l'entreprise. Pour étayer cette dernière, des politiques et des procédures supplémentaires pour les thèmes spécifiques définissant le Système de Gestion pour la Sécurité des Informations du Groupe Aruba ont été adoptées.	
A.6	**Organisation de la sécurité des informations**	**Rôles et Responsabilités** – Dans le cadre de la responsabilité en tant que fournisseur de services Cloud, telle que définie à la page dédiée au modèle de responsabilité partagée, le Groupe Aruba a défini les statuts, les rôles, les compétences et les responsabilités liés aux processus, dans le respect des principes de Segregation of Duties, Least Privilege et Dual Control. **Segregation of Duties (SoD)** – Dans le cadre des processus d'exploitation des Services, des procédures différentes sont exécutées par des personnes différentes, afin que chaque personne n'ait pas le contrôle de tout le processus. **Least Privilege** – Les autorisations d'accès à des locaux, des appareils, des données, des fonctionnalités etc. sont accordées au personnel en charge des services, selon le principe du « least privilege » à savoir dans la mesure du nécessaire afin que ces ressources puissent exécuter les taches qui leur ont été confiées, mais sans en dépasser les limites. **Dual Control** – Les procédures les plus critiques d'un point de vue de la sécurité prévoient la participation d'au moins deux personnes.	**Rôles et Responsabilités** - La description générale du service est disponible dans la Base de connaissance (KB), à la page dédiée à la description générale du service, avec le tableau précisant les lieux de fourniture des services et le tableau du modèle de responsabilité partagée entre le Groupe Aruba en tant que fournisseur de services Cloud et ses clients.
A.7	**Sécurité des ressources humaines**	**Formation du Personnel** – Les employés en charge du service possèdent des compétences ainsi qu'une expérience adéquates, et une formation spécifique leur est dispensée lors des mises à jour importantes du système. **Prise de conscience (Awareness)** – Périodiquement, le personnel est sensibilisé sur les thèmes de sécurité, la cybercriminalité en général et les meilleures pratiques à adopter, par l'intermédiaire de cours de formation spécifiques. **Non Disclosure Agreement (NDA)** – Il est demandé au nouveau personnel employé de signer un accord de confidentialité afin de protéger le savoir-faire ainsi que les autres informations confidentielles de l'entreprise.	**Formation du personnel -** Le Groupe Aruba met à disposition la Base de connaissance reportant les informations relatives aux services Cloud. Celle-ci contient des informations sur les services, des guides, des tutoriels, la documentation concernant l'Application Programming Interface (API), le glossaire et le Changelog des services.

Annexe A - ISO 27001 Les aspects relatifs à la sécurité du Cloud Aruba			
Domaine de contrôle		**Nos contrôles**	**Instruments et fonctionnalités à disposition du Client**
A.8	**Gestion des assets**	**Asset inventory** - Il existe un inventaire mis à jour des assets à l'intérieur duquel sont répertoriées les machines virtuelles et physiques qui fournissent les services et leur environnement physique dans l'infrastructure du Groupe Aruba. À l'issue de chaque activité d'installation d'une nouvelle machine dans l'infrastructure, une mise à jour de l'inventaire des assets est effectuée. De plus, afin de vérifier quotidiennement les éventuels écarts, des analyses automatiques sur les réseaux sont effectuées afin de détecter les éventuels nouveaux assets. Dans l'inventaire se trouve une classification des assets dans laquelle sont décrites les caractéristiques relatives : par exemple, le type de machine (virtuelle ou physique), l'infrastructure d'appartenance, la propriété interne, etc. **Handling of assets** - Il existe des procédures internes qui définissent et formalisent les activités relatives à la préparation des nouvelles machines et la gestion de ces dernières (ex : comment réaliser un changement, comment mettre à jour les systèmes etc.). **Gestion des configurations** - La liste des composantes du Système est définie afin de permettre l'identification de chaque composant hardware et software et, respectivement, de leur modèle et de leur version. **Entretien et assistance** - Les composants hardware (HW) les plus importants pour la continuité du Service font l'objet de contrats d'entretien garantissant la réparation ou le remplacement dans des délais suffisamment brefs par le fournisseur, et des composants identiques pouvant être utilisés en cas de besoin sont conservés en entrepôt. En ce qui concerne les softwares (SW) commerciaux, des contrats d'assistance appropriés garantissant l'assistance technique du fournisseur en cas de dysfonctionnement sont prévus. **Élimination** - Le Groupe Aruba garantit la mise en place de procédures spécifiques d'élimination et de destruction des composants hardware hors service aussi bien en ce qui concerne les data centers étrangers de colocation que les data centers de sa propriété afin de garantir la suppression complète et définitive de toutes les données contenues dans chaque stockage arrivé en fin de vie ou devant être remplacé et éliminé.	**Propriété des assets** - Dans le cadre de la logique de responsabilité partagée, le Groupe Aruba a identifié pour chaque service les attributions de propriété respectives, en ce qui concerne l'infrastructure, les licences, les adresses IP, les logiciels fournis par le Groupe Aruba, les softwares, les données et les contenus fournis par le client. Les informations relatives à la propriété des assets des services sont disponibles pour les clients dans la KB publiée à la page dédiée. **Suppression des données** – Grâce à la technique de disk wipe en environnement Cloud Aruba, pour les services VPS (Smart), PRO et Virtual Private Cloud, le client a la possibilité de supprimer définitivement les données contenues dans sa propre machine et en rendre la récupération impossible. La page dédiée de la KB fournit les étapes opérationnelles. **Labelling** - Les services du Groupe Aruba permettent au client de nommer et de classer les assets sous son propre contrôle. Les guides publiés dans la Base de connaissance fournissent les indications ponctuelles sur la façon d'effectuer ces opérations, et précise quelles sont les contraintes.
A.9	**Contrôle des accès**	**Gestion des Accès Logiques** – Avant d'accéder aux systèmes internes, il est demandé au personnel qui en a le droit de s'identifier et de s'authentifier (grâce à un nom d'utilisateur, un mot de passe et/ou une carte à puce). Le	**Gestion des Accès Logiques** - Le client peut à tout moment enregistrer, modifier, suspendre, réactiver et supprimer ses propres

Annexe A - ISO 27001 Les aspects relatifs à la sécurité du Cloud Aruba			
Domaine de contrôle		**Nos contrôles**	**Instruments et fonctionnalités à disposition du Client**
		personnel du Groupe Aruba peut accéder, en s'identifiant au préalable, seulement aux ressources (ex : systèmes, données) pour lesquelles celui-ci a été expressément autorisé, selon les besoins effectifs liés au poste occupé. La gestion des utilisateurs se fait grâce au domain controller Active Directory (AD). Pour garantir le principe de « Segregation of Duty », les accès logiques à l'environnement de production sont gérés par AD sur un domaine dédié, au sein duquel se trouvent des utilisateurs avec des autorisations et des privilèges différents en accord avec la job-role du sujet, dans le respect du principe de privilège minimum. Toutes les utilisations sont nominatives, il n'y a donc aucune utilisation en groupe et/ou partagée et celles-ci sont périodiquement soumises à une vérification indépendante par le Service de Sécurité. **Password policy** - En accord avec la politique de sécurité du groupe et dans le respect de la réglementation en matière de confidentialité (« mesures minimales », dispositions du Garant), une politique sûre de gestion des mots de passe est appliquée. À la suite de la création d'une utilisation, le changement du mot de passe obligatoire est prévu à la première connexion et, successivement, un changement de mot de passe périodique après un laps de temps prédéfini.	profils utilisateur, et en gérer les aspects commerciaux (crédits, seuils, profils associés, etc.). Au niveau des autorisations, chaque client peut gérer d'un point de vue administratif ses propres assets en définissant les niveaux de sécurité et de gestion des privilèges d'accès. En particulier, les clients peuvent, en fonction du service : • Attribuer une ou plusieurs VM à leurs propres utilisateurs, en s'appuyant sur le système d'accounting dans la machine virtuelle ; • Pour les services de Cloud Object Storage, Cloud Backup, il est possible de créer des identifiants univoques à attribuer à des groupes de ressources indépendants ; • Pour le service Virtual Private Cloud, il est possible de créer des ensembles d'utilisateurs techniques à l'intérieur du panneau de gestion technique avec des permissions différentes ; • Pour les clients partenaires, il est toujours possible de définir les ensembles d'opérations autorisées pour les utilisateurs grâce à des règles de profilage spécifiques. Les autorisations sont organisées de manière hiérarchique.
A.10	**Cryptographie**	**Canal Sécurisé TLS** – Tous les flux de données par/vers les systèmes sont protégés par un canal sécurisé TLS, grâce à une configuration opportune sur les serveurs, afin de garantir : • L'authentification du serveur ; • Le chiffrement de la session par un algorithme de chiffrement symétrique considéré comme suffisamment sécurisé.	**Contrôles cryptographiques** – Nous suggérons aux clients d'adopter une approche basée sur le risque et de mettre en œuvre des contrôles cryptographiques supplémentaires sur leurs domaines de responsabilité (voir le tableau du modèle de responsabilité partagée) si les données traitées dans le cadre du service du Groupe

Annexe A - ISO 27001 Les aspects relatifs à la sécurité du Cloud Aruba			
Domaine de contrôle		**Nos contrôles**	**Instruments et fonctionnalités à disposition du Client**
		Cela vaut aussi bien pour les flux créés de manière interactive (web browsing) que pour ceux générés de manière automatique (ex : interrogation de Services web). À ce jour, AES est principalement utilisé comme algorithme de chiffrement symétrique. La version de TLS habilitée est la plus élevée possible, en tenant compte de la capacité des softwares des clients. Les certificats SSL Server installés sur des serveurs exposés sur Internet sont délivrés par une CA reconnue comme fiable par les principaux navigateurs et systèmes d'exploitation. Le détail des certificats utilisés sur les panneaux Cloud et des protocoles utilisés sur le réseau public est disponible dans la KB à la page dédiée aux certificats utilisés sur les panneaux Cloud. **Chiffrement des Données au Repos** - Les données « au repos » les plus critiques d'un point de vue de la sécurité, comme les mots de passe, les seeds des tokens OTP et les autres données qui doivent rester confidentielles pour garantir la fiabilité des processus, sont conservées par chiffrement symétrique, en utilisant un algorithme considéré comme suffisamment sécurisé. En ce qui concerne plus spécifiquement la protection des identifiants, les mots de passe sont mémorisés dans le repository en mode « hash » non réversible (empreinte ou digest de la donnée), en utilisant l'algorithme de hashing SHA-512.	Aruba sont particulièrement sensibles. **Cloud Backup – Chiffrement** – Le service Cloud Backup offre la possibilité de chiffrer les données soumises à backup avant même le transfert avec un mot de passe complexe (standard AES-256).
A.11	**Sécurité physique et environnementale**	**Data Center** – Les systèmes pour la fourniture du Service Cloud se trouvent dans les data centers d'Arezzo IT1 et IT2, situés respectivement Via Gobetti 96 et Via Ramelli 8, et dans le data center IT3 DCA et DCB de Ponte San Pietro (BG) situé Via San Clemente 53. En plus des data centers italiens, le Groupe Aruba s'appuie sur un réseau international d'infrastructures, qui sont de sa propriété ou qui appartiennent à des partenaires qualifiés : • data center CZ1, situé à Ktiš en République tchèque et qui appartient au réseau international des data centers propriété de l'Organisation ; • data center FR1, situé à Paris en France et qui appartient au réseau des data centers partenaires ; • data center DE1, situé à Francfort en Allemagne et qui appartient au réseau des data centers partenaires ;	

Annexe A - ISO 27001 Les aspects relatifs à la sécurité du Cloud Aruba			
Domaine de contrôle		**Nos contrôles**	**Instruments et fonctionnalités à disposition du Client**
		• data center UK1, situé à Londres au Royaume-Uni et qui appartient au réseau des data centers partenaires ; • data center PL1, situé à Varsovie en Pologne et qui appartient au réseau des data centers partenaires. **Bâtiments parasismiques** - Les data centers sont tous conformes à la réglementation parasismique. **Contrôle des accès physiques** - L'accès au bâtiment est uniquement possible pour ceux qui en ont la nécessité effective, après enregistrement à l'accueil, et l'accès aux salles techniques n'est permis que pour les employés autorisés, qui doivent s'identifier avec un badge et le PIN relatif. Le système de gestion des accès prévoit la possibilité d'activer ou de désactiver chaque carte en fonction des zones, des heures et d'autres paramètres, de manière à garantir une sécurité maximale des environnements ainsi que la fluidité nécessaire des accès. **Systèmes anti-intrusion** - Tous les data centers et les bureaux disposent de grilles, de vitres et de portes blindées, de portails motorisés (anti-intrusion passifs) et des systèmes TVCC et VMD (anti-intrusion actifs) sont installés. Le système d'alarme anti-intrusion à zones fonctionne de manière complètement automatique. Les data centers sont partagés à l'intérieur en plusieurs zones possédant des systèmes anti-intrusion. De plus, des détecteurs de mouvement capables de détecter la présence des personnes sont installés ; dans les zones sensibles (Salles des données, Power Centers, entrepôts) se trouvent également des capteurs qui détectent l'ouverture des portes, et un badge doit être utilisé pour entrer et sortir. **Système anti-incendie** – Ce système est réalisé dans le respect des réglementations légales et des normes techniques de référence. Les capteurs pour la détection des incendies sont présents à tous les étages des bâtiments. **Système anti-inondation** – Des systèmes de détection des liquides et des systèmes anti-inondation sont installés. Les bâtiments sont également situés dans des zones de plaine et en position relevée par rapport au plan de campagne. **Système d'Alimentation Électrique** – Ce système est présent dans les data centers, redondant à tous les niveaux (groupes de transformation, power centers, UPS, groupes électrogènes, tableaux de distribution etc.) pour garantir la continuité de l'alimentation électrique dans chaque condition prévoyable. Celui-ci inclut également les mesures destinées à contenir l'effet des décharges électriques d'origine atmosphérique, spike du réseau électrique etc.	

Annexe A - ISO 27001 Les aspects relatifs à la sécurité du Cloud Aruba			
Domaine de contrôle		**Nos contrôles**	**Instruments et fonctionnalités à disposition du Client**
		Système de Ventilation et de Climatisation (HVAC) – Le système est destiné à garantir des conditions climatiques optimales pour le fonctionnement régulier des serveurs hébergés dans les data centers. **Connexion Internet** – Dans les bâtiments se trouve une connexion redondante, avec au moins une capacité double par rapport au minimum nécessaire. **Control Room et Facility Operation Center (FOC)** - Les data centers sont surveillés 24h/24h, 365 jours/an par un personnel systémique qualifié, qui garantit une surveillance constante de l'infrastructure et des services ainsi que l'intervention rapide en cas de nécessité. **Assurance** – L'entreprise a conclu un contrat d'assurance afin de couvrir les risques non atténués par les mesures de sécurité restantes.	

Annexe A - ISO 27001 Les aspects relatifs à la sécurité du Cloud Aruba			
Domaine de contrôle		**Nos contrôles**	**Instruments et fonctionnalités à disposition du Client**
A.12	**Appareils**	**Procédures opérationnelles** – Les procédures qui prescrivent les comportements opérationnels sont documentées, disponibles et connues du personnel concerné. **Hardening des Serveurs** – Les serveurs qui hébergent des composantes critiques pour la sécurité des services sont soumis à des interventions systémiques ayant pour but de réduire la zone d'attaque, comme : retrait de software non nécessaire, désactivation de services/protocoles non nécessaires, installation des patchs de sécurité recommandés par le vendeur, application de politiques pour la complexité des mots de passe, habilitation des logs de sécurité, etc. **Protection contre Distributed Denial of Service (DDoS) –** Un système qui analyse les données en entrée en identifiant le trafic anormal et en bloquant, si possible, les paquets potentiellement malveillants, a été mis en œuvre. **Traçage** (**logging**) - Les logs des serveurs infrastructurels sont collectés et conservés pour les accès privilégiés aux systèmes conformément aux exigences légales. Ces logs sont périodiquement vérifiés par l'Équipe de sécurité qui effectue un audit interne. Les logs d'application des opérations effectuées au cours de l'utilisation des services sont mis à la disposition des clients. De la même manière, les actions des Administrateurs du Système font l'objet, au moins chaque année, d'une activité de vérification de la part des responsables du traitement, afin de contrôler la conformité aux mesures organisationnelles, techniques et de sécurité qui concernent les traitements des données à caractère personnel prévues par les normes en vigueur. **Surveillance et Alerting** – Les systèmes critiques du Service sont contrôlés par un système de surveillance de manière continue. Le système a la capacité de générer des « alertes », sous la forme de courriels ou de SMS, qui permettent d'informer rapidement le personnel en charge d'un potentiel incident ou dysfonctionnement, afin que les actions correctives nécessaires puissent être mises en œuvre le plus rapidement possible. **Backup (partie de la compétence du Groupe Aruba)** – Les composants fonctionnels à la fourniture du service, à la gestion des utilisateurs et aux autres composants architecturaux du service suivent les procédures de backup définies au niveau de l'entreprise et qui sont périodiquement vérifiées et testées.	**Backup** - Les services Cloud offerts par le Groupe Aruba permettent aux clients de créer et de définir leurs propres backups automatisés grâce à la solution de Cloud Backup et Bare Metal Backup, en choisissant leurs propres politiques en termes de chiffrement, de périodicité, de type (complets ou incrémentiels) et d'autres exigences spécifiques. Le service optionnel de **Disaster Recovery as a Service (DRaaS)**, permet également de tester les procédures de failover sans aucune interruption. Toutes les procédures de gestion des services de backup et de restauration sont réalisées par les utilisateurs de manière autonome et sont décrites dans la Base de connaissance (KB) du service à la page dédiée, où sont décrites également les différentes méthodes qui peuvent être utilisées pour effectuer le backup de ses propres données. Aucune autre copie de backup des données n'est effectuée par le Groupe Aruba en plus de celles définies de manière autonome par les utilisateurs. **Logging** – Le Groupe Aruba met à la disposition des clients les logs d'application qu'ils produisent au cours de l'utilisation des services. • Cloud PRO : l'utilisateur peut consulter le log pour les opérations sur les machines virtuelles comme la création, la suppression, l'archivage, la restauration, l'allumage, l'arrêt, la réinitialisation, le changement de mot de passe, le changement des caractéristiques, la création

Annexe A - ISO 27001 Les aspects relatifs à la sécurité du Cloud Aruba			
Domaine de contrôle		**Nos contrôles**	**Instruments et fonctionnalités à disposition du Client**
		Antivirus – Tous les appareils du réseau du Groupe Aruba sont contrôlés, surveillés et protégés par des systèmes EDR. La technologie EDR (Endpoint Detection and Response) est capable de surveiller en temps réel et de manière proactive les menaces connues et inconnues qui concernent tous les endpoints et les serveurs de l'entreprise. Un groupe dédié avec une couverture 24h/24h s'occupe d'analyser les évènements anormaux et d'intervenir rapidement. **Processus de Vulnerability Management** – Tout le périmètre du Groupe Aruba est régulièrement analysé par des instruments automatiques et par des professionnels qualifiés du secteur afin d'identifier chaque vulnérabilité possible, même seulement potentielle. Chaque problème identifié est immédiatement signalé au groupe compétent, en lançant un cycle de résolution du problème qui peut se conclure par une nouvelle délivrance ou une migration (ex : virtual patching). Pour en vérifier l'efficacité, une nouvelle analyse est effectuée pour avoir la certitude du retrait de la vulnérabilité. **Capacity Management et Change Management** – Afin de garantir la bonne livraison/fourniture du service, le Groupe Aruba considère qu'il est fondamental de surveiller les ressources à disposition, d'analyser les capacités et d'adopter les mesures appropriées pour utiliser de manière optimale ces dernières et pour garantir une utilisation normale des services. Les niveaux de connexion, les niveaux d'occupation des ressources, l'espace sur disque et le dimensionnement de l'infrastructure sont surveillés à l'aide d'instruments spécifiques par le groupe d'opérateurs appartenant à la Control Room, 24 heures sur 24, 365 jours par an, dont la tâche s'étend également à la surveillance de tout évènement anormal. Les instruments de surveillance permettent de définir les contrôles spécifiques pour chaque service, en relevant les anomalies et en permettant d'anticiper les besoins de changement. Les changements que les activités de surveillance et de gestion des capacités rendent nécessaires sont gérés de manière contrôlée pour permettre d'en vérifier les résultats et de conserver une trace des activités réalisées. **Mises à jour et Patching** – Sur tous les systèmes, une mise à jour et patching sont périodiquement effectués grâce à des instruments centralisés en suivant des procédures internes qui prévoient le testing préalable dans les environnements de développement. Une fois cette phase	et la suppression ainsi que la récupération snapshot. • Cloud VPS (SMART) : l'utilisateur peut consulter le log pour les opérations sur les machines virtuelles comme la création, la suppression, l'allumage, l'arrêt, la réinitialisation, l'upgrade. • Virtual switch : l'utilisateur peut consulter le log pour les opérations sur les Virtual Switchs comme l'achat, la suppression et les modifications des caractéristiques. • IP Publiques : l'utilisateur peut consulter le log pour les opérations sur les IP Publiques comme l'achat et la suppression d'une IP publique, la gestion et les modifications au reverse DNS. • Équilibreurs : l'utilisateur peut consulter le log pour les opérations sur les équilibreurs comme la création de l'équilibreur, la modification de l'équilibreur, la suppression de l'équilibreur, l'activation ou la désactivation de l'équilibreur, l'ajout et la suppression de règles. • Unified Storage : l'utilisateur peut consulter le log pour les opérations sur les Virtual Switchs comme l'achat, la suppression et les modifications des caractéristiques. • Service FTP : l'utilisateur peut consulter le log pour les opérations sur les comptes FTP comme l'activation, la suppression et la modification de l'espace.

Annexe A - ISO 27001 Les aspects relatifs à la sécurité du Cloud Aruba			
Domaine de contrôle		**Nos contrôles**	**Instruments et fonctionnalités à disposition du Client**
		réalisée, il convient d'effectuer l'application dans l'environnement de production. **Synchronisation** - Le système NTP est utilisé pour synchroniser les propres horloges et maintenir la cohérence des évènements. L'autorité pour la synchronisation de l'horloge est INRiM (http://www.inrim.it). Le fuseau horaire utilisé sur tous les systèmes est CEST à l'exception de UK qui utilise le GMT. Toutes les VM fournies possèdent un fuseau horaire CEST et utilisent comme source de synchronisation clock celle de l'host sur lequel elles résident. **Multitenancy et Suppression sécurisée des données** – Le Groupe Aruba garantit un système multitenancy qui permet de séparer les demandes de chaque client entre elles et de séparer les demandes des clients de celles du fournisseur de services Cloud. Le panneau Cloud public a été expressément développé par le Groupe Aruba en mode multitenant selon les lignes directrices pour la programmation sécurisée et permet exclusivement d'accéder et de gouverner sa propre infrastructure Cloud. De plus, pour les services PRO, VPS et Virtual Private Cloud, à chaque fois qu'un software externe est utilisé, la multitenancy est garantie directement par les systèmes de virtualisation utilisés. À la fin du service, ou si le crédit est épuisé, selon ce qui a été contractuellement défini, le Groupe Aruba se charge de l'élimination et de la suppression définitive des données des services Cloud conformément à ce qui est décrit à la page dédiée sur ce qui se passe lorsque le crédit est épuisé. La suppression, selon le service, peut se faire par API, panneaux techniques, scripts ou softwares spécifiques. Le Groupe Aruba gère, grâce à un processus défini, la suppression périodique des fichiers temporaires de ses propres systèmes Cloud.	• Virtual Private Cloud : l'utilisateur peut consulter le log pour les opérations sur son propre Virtual Private Cloud comme la création, la suppression et les modifications aux ressources. • Cloud Backup : l'utilisateur peut consulter le log pour les opérations sur ses propres comptes backup relatifs à la création, à la suppression et aux modifications du plan, au changement ou à la réinitialisation du mot de passe. • Cloud monitoring : l'utilisateur peut consulter le log pour les opérations sur ses propres services monitoring et les contrôles relatifs comme la création du plan monitoring ou l'ajout de nouveau contrôle, la suppression du monitoring ou le contrôle, les modifications du plan monitoring ou d'un seul contrôle. • Cloud Object Storage : l'utilisateur peut consulter le log pour les opérations sur ses propres comptes Object Storage relatifs à la création, à la suppression et aux modifications du plan, au changement ou à la réinitialisation du mot de passe. • Domain Center : l'utilisateur peut consulter le log pour les opérations sur ses propres domaines et DNS relatifs à un ajout de nouveau domaine, à la suppression d'un domaine et aux modifications des données relatives au domaine, à la création DNS, à

Annexe A - ISO 27001 Les aspects relatifs à la sécurité du Cloud Aruba			
Domaine de contrôle		**Nos contrôles**	**Instruments et fonctionnalités à disposition du Client**
			la suppression DNS, aux modifications de tout record DNS. • Jelastic Cloud : l'utilisateur peut consulter le log pour les opérations sur ses propres comptes Jelastic Cloud relatifs à la création, à la suppression et aux modifications du plan, au changement ou à la réinitialisation du mot de passe. • Database as a Service (DBaaS) : l'utilisateur peut consulter le log pour les opérations sur ses propres comptes « Database as a Service » relatifs à la création, à la suppression et aux modifications du plan, au changement ou à la réinitialisation, backup et restauration de la base de données et restart des demandes. **Capacity Management** – En ce qui concerne la gestion des capacités appartenant au client, le Groupe Aruba permet au client de tenir constamment sous contrôle la consommation des ressources économiques et techniques à sa disposition, en lui permettant également le forecasting. De plus, lors de la phase d'achat du service, les cas où il existe des limites à l'extensibilité des ressources sont décrits. **Synchronisation** – Quand la synchronisation des horloges peut représenter un problème pour le client, des informations détaillées dans la Base de connaissance publique (par exemple à la page dédiée aux tâches planifiées) ou

Annexe A - ISO 27001 Les aspects relatifs à la sécurité du Cloud Aruba			
Domaine de contrôle		**Nos contrôles**	**Instruments et fonctionnalités à disposition du Client**
			dans les panneaux de gestion sont fournies. **Multitenancy** Cloud PRO. La multitenancy est garantie : • Par le panneau Cloud public développé expressément en mode multitenant par le Groupe Aruba et par les API publiques authentifiées. Ces solutions permettent seulement d'accéder et de gouverner sa propre infrastructure Cloud. • Par le système de virtualisation Hyper-V, VMware ou Openstack. Le client a accès seulement à ses Virtual Machines (VM) que les hyperviseurs sous-jacents maintiennent isolées logiquement des autres. Les VM fournies au client sont installées avec des instruments de contrôle d'accès dont les identifiants sont choisis directement par le client au moment de la création. Les instruments d'accès fournis avec les machines sont SSH pour les environnements Linux et RDP pour les environnements Windows. Les réseaux publics sont partagés entre les clients mais sur toutes les machines mises à disposition se trouve un firewall périmétrique à l'usage du client. En plus de cela, le client a la possibilité d'acheter le service de Virtual Switch

Annexe A - ISO 27001 Les aspects relatifs à la sécurité du Cloud Aruba			
Domaine de contrôle		**Nos contrôles**	**Instruments et fonctionnalités à disposition du Client**
			qui consiste à fournir une VLAN dédiée et non partagée avec d'autres clients sur laquelle celui-ci peut interconnecter ses machines pour une ségrégation maximale. Cloud VPS (SMART). La multitenancy est garantie : • Par le panneau Cloud public développé expressément en mode multitenant par le Groupe Aruba et par les API publiques authentifiées. Ces solutions permettent seulement d'accéder et de gouverner sa propre infrastructure Cloud. • Par les systèmes de virtualisation VMware et Openstack. Le client a accès seulement à ses VM que les hyperviseurs sous-jacents maintiennent isolées logiquement des autres. Les VM fournies au client sont installées avec des instruments de contrôle d'accès dont les identifiants sont choisis directement par le client au moment de la création. Les instruments d'accès fournis avec les machines sont SSH pour les environnements Linux et RDP pour les environnements Windows. Les réseaux publics sont partagés entre les clients mais sur toutes les machines mises à disposition se trouve un firewall périmétrique à l'usage du client.

Annexe A - ISO 27001 Les aspects relatifs à la sécurité du Cloud Aruba			
Domaine de contrôle		**Nos contrôles**	**Instruments et fonctionnalités à disposition du Client**
			Virtual Switch et Hybrid Link : il s'agit de ressources dédiées à chaque tenant. La multitenancy est garantie par le Cloud public développé expressément en mode multitenant par le Groupe Aruba et par les API publiques authentifiées. Ces solutions permettent seulement d'accéder et de gouverner sa propre infrastructure Cloud. Virtual Private Cloud. La multitenancy est garantie : • Par le panneau vCloud Director, développé expressément en mode multitenant par VMware. Ce panneau permet seulement d'accéder et de gouverner sa propre infrastructure Cloud. • Par le système de virtualisation VMware. Le client a accès seulement à son Virtual Datacenter VM que les hyperviseurs sous-jacents maintiennent isolé logiquement des autres. Les VM fournies au client sont installées avec des instruments de contrôle d'accès dont les identifiants sont choisis directement par le client au moment de la création. Les instruments d'accès fournis avec les machines sont SSH pour les environnements Linux et RDP pour les environnements Windows. Sur chaque Virtual Datacenter fourni se trouve un firewall software périmétrique (NSX Edge) qui permet d'isoler son propre Virtual

Annexe A - ISO 27001 Les aspects relatifs à la sécurité du Cloud Aruba			
Domaine de contrôle		**Nos contrôles**	**Instruments et fonctionnalités à disposition du Client**
			data center des autres et qui permet au client de configurer les règles de sécurité optimales pour son utilisation. Le client a la possibilité de créer de manière autonome des réseaux privés dédiés et non partagés avec les autres clients pour configurer sa propre architecture. Même les réseaux publics, sur demande, peuvent être fournis dédiés et non partagés avec d'autres clients. Bare Metal Backup. La multitenancy est garantie : • Par le panneau Cloud public développé expressément en mode multitenant par le Groupe Aruba et par les API publiques authentifiées. Ces solutions permettent seulement d'accéder et de gouverner sa propre infrastructure Cloud. • Par le panneau de gestion de Veeam. Le client a accès seulement à son set de données de backup et il n'a aucun moyen de voir ou de contrôler les systèmes de backup des autres clients. Disaster Recovery. La multitenancy est garantie : • Par le panneau Cloud public développé expressément en mode multitenant par le Groupe Aruba et par les API publiques authentifiées. Ces

Annexe A - ISO 27001 Les aspects relatifs à la sécurité du Cloud Aruba			
Domaine de contrôle		**Nos contrôles**	**Instruments et fonctionnalités à disposition du Client**
			solutions permettent seulement d'accéder et de gouverner sa propre infrastructure Cloud. • Par le panneau de gestion de Zerto, Veeam, VMWare VCAV. Le client a accès seulement à son set de données de backup et il n'a aucun moyen de voir ou de contrôler les systèmes de Disaster recovery (DR) des autres clients. Cloud Backup (Evault/Commvault). La multitenancy est garantie : • Par le panneau Cloud public développé expressément en mode multitenant par le Groupe Aruba et par les API publiques authentifiées. Ces solutions permettent seulement d'accéder et de gouverner sa propre infrastructure Cloud. • Par le système de backup Evault ou Commvault. Le client a accès seulement à son set de données de backup et il n'a aucun moyen de voir ou de contrôler les systèmes de backup des autres clients. Cloud Monitoring : la multitenancy est garantie par le panneau Cloud public développé expressément en mode multitenant par le Groupe Aruba et par les API publiques authentifiées. Ces solutions permettent seulement d'accéder et de gouverner sa propre infrastructure Cloud. Cloud Object Storage. La multitenancy est garantie :

Annexe A - ISO 27001 Les aspects relatifs à la sécurité du Cloud Aruba			
Domaine de contrôle		**Nos contrôles**	**Instruments et fonctionnalités à disposition du Client**
			• Par le panneau Cloud public développé expressément en mode multitenant par le Groupe Aruba et par les API publiques authentifiées. Ces solutions permettent seulement d'accéder et de gouverner sa propre infrastructure Cloud. • Par le système d'Identity and Access Management, Scality et CEPH. Le client a accès seulement à son compte de stockage et il n'a aucun moyen de voir ou de contrôler les comptes des autres clients. IaaS pour SAP HANA. La multitenancy et la ségrégation sont garanties grâce à différents dispositifs : • Une VPN SSL dédiée qui permet aux clients d'accéder au système de gestion de la plateforme. • Un compte univoque présent sur le système de virtualisation VMware qui permet d'accéder seulement aux VM du client. • La ségrégation offerte par le réseau dédié mis à la disposition du client et non partagé avec les autres clients. • Les instruments internes fournis avec la VM qui permettent la création de multiples profils utilisateurs et administratifs.

Annexe A - ISO 27001 Les aspects relatifs à la sécurité du Cloud Aruba			
Domaine de contrôle		**Nos contrôles**	**Instruments et fonctionnalités à disposition du Client**
			Domain Center. La multitenancy est garantie par le panneau Cloud public développé expressément en mode multitenant par le Groupe Aruba et par les API publiques authentifiées. Ces solutions permettent seulement d'accéder et de gouverner sa propre infrastructure Cloud. Jelastic Cloud. La multitenancy est garantie par deux modalités : • Par le panneau Cloud public développé expressément en mode multitenant par le Groupe Aruba et par les API publiques authentifiées. Ces solutions permettent seulement d'accéder et de gouverner sa propre infrastructure Cloud. • Par le système de Jelastic. Le client a accès seulement à son compte jelastic et il n'a aucun moyen de voir ou de contrôler les comptes des autres clients. Database as a service (DBaaS) : la multitenancy est garantie par le panneau Cloud public développé expressément en mode multitenant par le Groupe Aruba et par les API publiques authentifiées. Ces solutions permettent seulement d'accéder et de gouverner sa propre infrastructure Cloud.
A.13	**Sécurité des communications**	**Firewall et IPS** – Les portails web exposés pour les services sont protégés par le firewall du data center du service Cloud et protégés par IPS. En ce qui concerne les services computing, toutes les machines virtuelles fournies par le Groupe Aruba sont façonnées et rendues disponibles sous la forme d'images. Ces images sont produites et testées par les techniciens du Groupe Aruba et en particulier, après avoir installé le Système d'Exploitation et effectué la première configuration, le système de firewall est activé en accordant	**Firewall** – Le client est l'administrateur de son propre serveur et il a donc la possibilité de modifier les réglages de firewalling. Les guides et les tutoriels présents dans la KB fournissent certaines informations sur la ségrégation et la protection de la sécurité du réseau, ainsi que sur la prédisposition d'un firewall sur son propre Aruba Cloud.

Annexe A - ISO 27001 Les aspects relatifs à la sécurité du Cloud Aruba			
Domaine de contrôle		**Nos contrôles**	**Instruments et fonctionnalités à disposition du Client**
		les privilèges minimum possibles et en ouvrant seulement les ports nécessaires. **Virtual Private Network (VPN)** – L'accès à distance au réseau (LAN) de l'entreprise est permis seulement pour le personnel autorisé qui en a la nécessité ; l'accès à distance est possible exclusivement grâce à une VPN qui garantit la confidentialité de la communication, l'authentification forte du serveur et l'authentification forte (à deux facteurs) de l'utilisateur.	**Virtual Switch** – Le client a la possibilité d'acheter le service de Virtual Switch qui consiste à fournir une VLAN dédiée et non partagée avec d'autres clients sur laquelle celui-ci peut interconnecter ses machines pour une ségrégation maximale et créer de manière autonome des réseaux privés dédiés et non partagés par d'autres clients pour configurer sa propre architecture (Virtual Private Cloud). Les réseaux publics, sur demande, peuvent également être fournis dédiés et non partagés avec d'autres clients. **Position géographique des données en garantie de la Sécurité et de la Conformité** – En alternative, les services fournis par le Groupe Aruba peuvent être des service activables sur une base data center ou sur une base régionale (qui coïncide avec un pays). Le client a la possibilité d'indiquer le data center ou les data centers à l'intérieur desquels ses propres services seront activés et ses propres données transférées ; pour les services sur une base régionale, les clients ont la possibilité de sélectionner le Pays à l'intérieur duquel le service doit être activé. En aucun cas le Groupe Aruba ne déplacera les systèmes ou les contenus en dehors des zones géographiques (DC ou régions) configurées par ses propres clients.
A.14	**Achat, développement et manutention des systèmes**	**Gestion des Modifications** – Les modifications au software d'application sont soumises à une évaluation et à l'approbation avant d'être réalisées ; elles sont par la suite soumises à un test avant d'être produites, afin de vérifier la bonne mise en œuvre des nouvelles fonctionnalités et l'absence de régressions. De plus, tout le software développé est géré par un système de versioning.	**Gestion des Modifications** – Le Groupe Aruba met à disposition des clients un changelog (comme détaillé à la page dédiée relative à la KB) pour communiquer les délivrances, les fixs, les corrections et les mises à jour des services offerts.

Annexe A - ISO 27001 Les aspects relatifs à la sécurité du Cloud Aruba			
Domaine de contrôle		**Nos contrôles**	**Instruments et fonctionnalités à disposition du Client**
A.15	**Relations avec les fournisseurs**	**Gestion des fournisseurs** - La politique de l'entreprise qui régit les relations avec les fournisseurs stipule que, pour une définition et une gestion correctes d'une nouvelle relation avec un fournisseur, les aspects suivants doivent toujours être pris en considération, avec une attention particulière à la sécurité de l'information : • Analyse du risque et enquêtes préliminaires à effectuer pour l'évaluation complète d'un nouveau fournisseur ; • Choix des clauses des contrats, afin d'évaluer si les contrats standards couvrent les risques identifiés ou s'il est nécessaire d'ajouter/de modifier des clauses spécifiques ; • Contrôle des accès aux informations, pour fournir l'accès au fournisseur selon la logique « Need-to-know » et donc seulement aux données et aux informations qui sont effectivement exigées et nécessaires pour la réalisation de son activité ; • Contrôle des accès aux systèmes du Groupe Aruba, si la fourniture prévoit que le fournisseur accède aux systèmes, par l'intermédiaire d'utilisations spécifiques, en utilisant un Réseau Privé (VPN) et un système spécifique de Detection Response et Virtual Desktop Infrastructure (VDI) fournis par le Groupe Aruba ; • Surveillance des non-conformités pour la réalisation régulière des contrôles afin de pouvoir certifier la conformité du fournisseur aux exigences contractuelles convenues et à la sécurité des informations. De plus, les fournitures externes nécessaires pour le développement, la maintenance et la fourniture du Service sont soumises à des vérifications destinées à diminuer le risque d'incidents de sécurité causés par un matériel non conforme ou par des actions inappropriées du fournisseur. Tous les fournisseurs de prestation professionnels sont tenus de signer un accord de confidentialité (NDA). Les modèles contractuels utilisés par le Groupe Aruba pour la fourniture du service prévoient la possibilité que le Groupe Aruba puisse recourir à des tiers pour la réalisation de ses propres activités. Cette collaboration se base sur l'engagement, contractuellement prévu avec des éventuels sous-fournisseurs par le Groupe Aruba, de vérifier que ces derniers, en fonction du type de service fourni, possèdent la capacité de respecter les mêmes exigences et niveaux de sécurité auxquels le Groupe Aruba s'engage. Le Groupe Aruba conserve une liste des sous-fournisseurs des services	

Annexe A - ISO 27001 Les aspects relatifs à la sécurité du Cloud Aruba			
Domaine de contrôle		**Nos contrôles**	**Instruments et fonctionnalités à disposition du Client**
		qui est disponible, à la demande des clients. De plus, en cas de changement de sous-fournisseurs ou de sous-fournisseurs supplémentaires, le Groupe Aruba s'engage à le communiquer à ses clients en temps voulu afin de permettre l'opposition ou la résiliation des clients.	
A.16	**Gestion des incidents relatifs à la sécurité des informations**	**Processus de Gestion des Incidents de Sécurité des Informations** - Le Groupe Aruba a identifié et documenté dans une politique spécifique son approche structurée et programmatique pour la gestion des évènements et/ou des incidents de sécurité des informations qui surviendraient dans le cadre du fonctionnement de la société du Groupe Aruba, en appliquant les lignes directrices ISO 27035 dans son propre flux de gestion des incidents de sécurité des informations. Ce processus est mis en œuvre grâce à un plan spécifique, en réglementant les mesures opérationnelles qui doivent être mises en œuvre en cas d'incidents de sécurité des informations. Un flux de gestion des incidents a été défini et les responsabilités liées à son application ont été identifiées, aussi bien en termes de gestion et de résolution des incidents que d'assistance stratégique pour l'adoption rapide des décisions nécessaires pour faire face aux Incidents de Sécurité les plus importants (par exemple Major Incident, Incidents non connus, Data Breach). De plus, les délais et les modalités ont été définis pour la prédisposition et l'envoi des communications relatives aux incidents de sécurité des informations à des autorités, des clients et des tiers.	
A.17	**Aspects relatifs à la sécurité des informations dans la gestion de la continuité opérationnelle**	**Procédure de Gestion des Sinistres** – Le Groupe Aruba a formalisé un plan de continuité des activités, une politique et des plans BC spécifiques pour les data centers relatifs aux services essentiels à leur fonctionnement, tels que l'électricité, la climatisation et la connectivité. Les data centers sont certifiés ISO 27001 et les principales mesures visant à garantir la sécurité physique et la continuité opérationnelle des structures y sont mises en œuvre. En particulier, les data centers IT1, IT3 DCA et DCB du Groupe Aruba sont conformes au niveau le plus élevé (Rating 4) parmi ceux requis par la norme ANSI TIA 942-B-2017. Ce résultat, qui indique la capacité d'éviter les interruptions de service même en présence de pannes graves (fault-tolerance), a été obtenu grâce à une série de mesures de conception et de construction qui ont impliqué	**Disaster Recovery as a Service (DRaaS)** – Le Groupe Aruba met à disposition le service Disaster Recovery as a Service conçu pour garantir la continuité de service des entreprises, qui permet de répliquer et de restaurer rapidement l'accès et les fonctionnalités de l'infrastructure IT à la suite d'une interruption due à une attaque informatique, une panne ou un sinistre. Grâce à un Panneau Web self-service, sur une connexion sécurisée, le client peut en toute autonomie créer des directives et

Annexe A - ISO 27001 Les aspects relatifs à la sécurité du Cloud Aruba			
Domaine de contrôle		**Nos contrôles**	**Instruments et fonctionnalités à disposition du Client**
		tous les aspects du data center : sélection du site, aspects architecturaux, sécurité physique, systèmes d'incendie, système électrique, système mécanique et réseau de données. Un data center de Rating 4 (ancien Tier 4) comporte des composants redondants permanents, ainsi que plusieurs chemins pour l'alimentation et le refroidissement du hardware. Enfin, les data centers sont structurés pour résister à une panne en tout point du système sans provoquer de temps d'arrêt et sont protégés contre les événements physiques, notamment les catastrophes naturelles (par exemple, incendie, inondation, tremblement de terre, etc.). Les data centers IT3 DCA et DCB du Groupe Aruba sont certifiés ISO/IEC 22237, norme internationale de référence pour l'ensemble du cycle de vie du data center, de la conception stratégique à la construction et la mise en service, conformément à ANSI/TIA 942 (norme américaine) et EN 50600 (norme européenne). L'environnement Cloud est composé d'une infrastructure multi-data center, dont les services sont interconnectés par un réseau IPSEC haut débit et sécurisé. Étant une structure conçue pour être multi-data center, elle est nativement préparée pour la reprise après sinistre car tous les data centers sont logiquement indépendants les uns des autres. Les machines client virtualisées ne sont pas soumises à une reprise après sinistre géographique, car les clients eux-mêmes disposent de tous les outils nécessaires pour créer des systèmes et des procédures de reprise après sinistre personnalisés.	des politiques de Reprise après sinistre, en sélectionnant la source (Site primaire) et la destination (Site secondaire) aux choix entre ses propres infrastructures virtuelles VMware on-premise et/ou data centers du Groupe Aruba habilités au service Virtual Private Cloud.
A.18	**Conformité**	**Protection des Données à caractère Personnel** – Tous les services fournis sont gérés dans le respect de la réglementation en vigueur en matière de protection des données à caractère personnel conformément au Règlement UE 2016/679 (« RGPD »), au Décret législatif 196/2003, modifié par le Décret législatif 101/2018, et aux mesures de l'Autorité Garante pour la protection des données à caractère personnel. **Révision** (**auditing**) – Les évènements enregistrés grâce au traçage, et en particulier ceux qui pourraient indiquer une menace pour la sécurité, sont analysés périodiquement. **Inspections internes** – Le Responsable des contrôles et des inspections (auditing) garantit la réalisation des contrôles de conformité du service Cloud aux dispositions prévues	

Annexe A - ISO 27001 Les aspects relatifs à la sécurité du Cloud Aruba			
Domaine de contrôle		**Nos contrôles**	**Instruments et fonctionnalités à disposition du Client**
		dans le présent document et aux normes en vigueur au moins une fois par an.	

HISTORIQUE DES VERSIONS

VERSION 1.1 DU 14/04/2023	***NATURE DES CHANGEMENTS : Mise à jour des contrôles A.12, A.13, A.17***

VERSION 1.0 DU 01/01/2022	***NATURE DES CHANGEMENTS : Première édition***