aruba.it BUSINESS

Sicurezza del Cloud

Allegato A ISO 27001:2017

14.04.2023

Allegato A - ISO 27001 Gli aspetti di Sicurezza del Cloud Aruba			
Area di Controllo		**I nostri controlli**	**Strumenti e funzionalità a disposizione del Cliente**
A.5	**Politiche per la sicurezza delle informazioni**	**Politiche del Sistema di Gestione della Sicurezza delle Informazioni** (SGSI) - Il Gruppo Aruba ha definito l'approccio adottato dall'organizzazione per la gestione dei suoi obiettivi di Sicurezza delle Informazioni all'interno di una specifica Politica aziendale. Tale documento è stato approvato dalla Direzione e pubblicato sulla intranet aziendale. A supporto della suddetta Politica, sono presenti ulteriori politiche e procedure per tematiche specifiche che definiscono il Sistema di Gestione per la Sicurezza delle Informazioni del Gruppo Aruba.	
A.6	**Organizzazione della sicurezza delle informazioni**	**Ruoli e responsabilità** - All'interno dell'ambito di responsabilità del Gruppo Aruba come cloud service provider, così come definito nella pagina dedicata al modello di responsabilità condivisa, il Gruppo Aruba ha definito le figure, i ruoli, le competenze e le responsabilità connesse ai processi, secondo i principi di segregation of duties, least privilege e dual control. **Segregation of Duties (SoD)** - Nell'ambito dei processi operativi dei servizi, una sequenza di procedure viene svolta da diverse persone, mai una sola, a garanzia che il controllo dell'intero processo non sia affidato ad un singolo individuo. **Least privilege** - I permessi di accesso a locali, apparati, dati, funzionalità, ecc. sono concessi, al personale addetto ai servizi, secondo il principio del "least privilege" ossia nella misura necessaria affinché tali risorse possano svolgere i compiti loro assegnati, ma non oltre. **Dual control** - Le procedure più critiche dal punto di vista della sicurezza prevedono il concorso di almeno due persone.	**Ruoli e responsabilità** - La descrizione generale del servizio del Gruppo Aruba è disponibile all'interno della Knowledge Base (KB), alla pagina dedicata alla descrizione generale del sevizio, unitamente alla tabella con i luoghi di erogazione dei servizi e alla tabella del modello di responsabilità condivisa tra il Gruppo Aruba come cloud service provider e i suoi clienti.
A.7	**Sicurezza delle risorse umane**	**Formazione del personale** - Gli addetti al servizio hanno adeguata competenza ed esperienza, e viene loro fornito un addestramento specifico a fronte di ogni importante aggiornamento del sistema. **Consapevolezza (Awareness)** - Periodicamente, il personale viene sensibilizzato sulle tematiche di sicurezza, sul cybercrime in generale e sulle best practice da adottare, mediante specifici corsi di formazione. **Non Disclosure Agreement (NDA)** - Ai nuovi assunti viene richiesto di sottoscrivere un accordo di confidenzialità al fine di tutelare il know-how e le altre informazioni confidenziali dell'azienda.	**Formazione del personale** – il Gruppo Aruba mette a disposizione una Knowledge Base contenente informazioni relative ai servizi del Gruppo Aruba. Al suo interno sono presenti informazioni sui servizi, guide, tutorial, la documentazione sulle Application Programming Interface (API), il glossario e il changelog dei servizi.
A.8	**Gestione degli asset**	**Asset inventory** - È presente un inventario aggiornato degli asset, al cui interno sono censite le macchine virtuali e	**Proprietà degli asset** - All'interno della logica di responsabilità

Aruba Business srl
Via L. Gulinelli 21/A - 44122 Ferrara, Italy, P.IVA 01497070381
PEC: info@pec.arubabusiness.it - Sito Web: www.arubabusiness.it

Allegato A - ISO 27001 Gli aspetti di Sicurezza del Cloud Aruba			
Area di Controllo		**I nostri controlli**	**Strumenti e funzionalità a disposizione del Cliente**
		fisiche che erogano i servizi e la loro collocazione fisica all'interno dell'infrastruttura del Gruppo Aruba. Al termine di ogni attività di installazione di una nuova macchina all'interno dell'infrastruttura viene effettuato l'aggiornamento dell'inventario degli asset. Inoltre, per verificare eventuali scostamenti, con cadenza giornaliera sono effettuate delle scansioni automatiche sulle reti per rilevare eventuali nuovi asset. All'interno dell'inventario è presente una categorizzazione degli asset in cui sono descritte le relative caratteristiche: ad esempio la tipologia di macchina (virtuale o fisica), infrastruttura di appartenenza, ownership interna, ecc. **Handling of assets** - Sono presenti delle procedure interne che definiscono e formalizzano le attività relative alla predisposizione delle nuove macchine e la gestione delle stesse (es. come eseguire un change, come aggiornare i sistemi, ecc.). **Gestione delle configurazioni** - Il regolare censimento dei componenti di sistema consente di poter individuare e gestire in maniera puntuale i singoli componenti, con un dettaglio che arriva al modello di ciascun hardware e alla versione di ogni software. **Manutenzione e assistenza** - I componenti hardware (HW) più importanti ai fini della continuità del servizio sono coperti da contratti di manutenzione che garantiscono la riparazione o sostituzione in tempi sufficientemente rapidi, da parte del fornitore, oppure si conservano a magazzino dei componenti identici che possono essere messi in opera in caso di bisogno. Per quanto riguarda i software (SW) commerciali, sono previsti opportuni contratti di assistenza che garantiscono l'assistenza tecnica del fornitore in caso di malfunzionamenti. **Smaltimento** – Il Gruppo Aruba garantisce l'attuazione di specifiche procedure di smaltimento e distruzione dei componenti hardware dismessi sia per quanto riguarda i data center esteri in colocation che per i data center di proprietà al fine di assicurare che per ogni storage che abbia raggiunto il fine vita e che debba essere sostituito e smaltito, venga effettuata una completa e definitiva rimozione di tutti i dati in esso contenuti.	condivisa, il Gruppo Aruba ha identificato per ciascun servizio le rispettive attribuzioni di proprietà, per quanto riguarda infrastruttura, licenze, indirizzi IP, software forniti dal Gruppo Aruba, software, dati e contenuti immessi dal cliente. Le informazioni relative alla proprietà degli asset dei servizi sono disponibili ai clienti all'interno della KB pubblica nella pagina dedicata. **Cancellazione dei dati** - Attraverso la tecnica del disk wipe in ambiente Cloud, per i servizi VPS (Smart), PRO e Virtual Private Cloud, il cliente ha la possibilità di eliminare definitivamente i dati contenuti nella propria macchina e renderne impossibile il recupero. La pagina dedicata della KB ne riporta gli step operativi. **Labelling** - I servizi del Gruppo Aruba permettono ai clienti di nominare e classificare gli asset sotto il proprio controllo. Le guide pubblicate all'interno della Knowledge Base forniscono le indicazioni puntuali su come eseguire queste operazioni e quali sono i vincoli.
A.9	**Controllo degli accessi**	**Gestione degli accessi logici** - Prima di accedere ai sistemi interni, viene chiesto al personale che ne ha diritto di identificarsi e di autenticarsi (tramite nome utente, password e smartcard). Il personale del Gruppo Aruba può accedere, previa autenticazione, solamente alle risorse (es.	**Gestione degli accessi logici** - Al cliente è garantita in ogni momento la possibilità di registrare, modificare, sospendere, riattivare e cancellare i propri profili utente,

Allegato A - ISO 27001 Gli aspetti di Sicurezza del Cloud Aruba			
Area di Controllo		**I nostri controlli**	**Strumenti e funzionalità a disposizione del Cliente**
		sistemi, dati) per cui è stato esplicitamente autorizzato, secondo le effettive necessità del ruolo ricoperto. La gestione degli utenti avviene attraverso domain controller Active Directory (AD). Per garantire il principio di "Segregation of Duty", gli accessi logici all'ambiente di produzione sono gestiti tramite AD su dominio dedicato, al cui interno sono presenti utenti con privilegi e permessi differenti in linea con la job-role del soggetto, nel rispetto del principio di minimo privilegio. Tutte le utenze sono nominali, non ci sono quindi utenze di gruppo e/o condivise e sono periodicamente sottoposte a verifica indipendente da parte del Reparto di Sicurezza. **Password policy** - Coerentemente con le policy di sicurezza di gruppo e nel rispetto della normativa sulla privacy ("misure minime", provvedimenti del Garante), è applicata una politica sicura di gestione delle password. A seguito della creazione di un'utenza è previsto il cambio password obbligatorio al primo log-on e successivamente il cambio password obbligatorio periodico dopo un intervallo di tempo definito.	nonché gestirne gli aspetti commerciali (crediti, soglie, profili associati, ecc.). A livello di permessi ciascun cliente ha la possibilità di gestire dal punto di vista amministrativo i propri asset impostando livelli di sicurezza e gestione dei privilegi di accesso. In particolare, i clienti hanno la possibilità, a seconda del servizio di: • assegnare una o più VM ai propri utenti, appoggiandosi al sistema di accounting all'interno della macchina virtuale; • per i servizi di Cloud Object Storage, Cloud Backup è possibile creare credenziali univoche da assegnare a gruppi di risorse indipendenti; • per il servizio Virtual Private Cloud è possibile creare set di utenti tecnici all'interno del pannello di controllo tecnico con permission differenti; • per i clienti partner è sempre possibile definire i set di operazioni consentite agli utenti mediante opportune regole di profilazione. I permessi sono organizzati in modo gerarchico.
A.10	**Crittografia**	**Canale sicuro TLS** - I flussi di dati da/verso i sistemi , sono protetti da canale sicuro TLS, mediante opportuna configurazione sui server, tale da assicurare: • autenticazione del server; • cifratura della sessione con un algoritmo di cifratura simmetrica considerato sufficientemente sicuro. Questo vale sia per i flussi originati in modo interattivo (web browsing) sia per quelli generati in modo automatico (es. interrogazione di Web Services). Come algoritmo di cifratura simmetrica, ad oggi si utilizza prevalentemente AES.	**Controlli crittografici** - Suggeriamo ai clienti di adottare un approccio basato sul rischio e di implementare controlli crittografici aggiuntivi sulle aree di loro responsabilità (vedi tabella del modello di responsabilità condivisa) nel caso in cui i dati trattati all'interno del servizio del Gruppo Aruba fossero particolarmente sensibili. **Gruppo Aruba Cloud Backup – cifratura** - Il servizio offre la possibilità di cifrare i dati sottoposti a backup, ancor prima del

Aruba Business srl
Via L. Gulinelli 21/A - 44122 Ferrara, Italy, P.IVA 01497070381
PEC: info@pec.arubabusiness.it - Sito Web: www.arubabusiness.it

Allegato A - ISO 27001 Gli aspetti di Sicurezza del Cloud Aruba			
Area di Controllo		**I nostri controlli**	**Strumenti e funzionalità a disposizione del Cliente**
		La versione di TLS abilitata è la più alta possibile, tenendo conto delle capacità dei software client. I certificati SSL Server installati sui server esposti su Internet sono emessi da una CA riconosciuta come affidabile dai principali browser e sistemi operativi. Il dettaglio dei certificati in uso sui pannelli cloud e dei protocolli utilizzati su rete pubblica è disponibile nella KB del Gruppo Aruba alla pagina dedicata ai certificati in uso su pannelli cloud. **Cifratura di dati a riposo** - I dati "a riposo" più critici dal punto di vista della sicurezza, quali ad esempio password, seed dei token OTP e altri dati che devono restare confidenziali per assicurare l'affidabilità dei processi, sono conservati mediante cifratura simmetrica, usando un algoritmo considerato sufficientemente sicuro. Per quanto riguarda più specificamente la protezione delle credenziali, le password sono memorizzate all'interno del repository in modalità "hashata" non reversibile (impronta o digest del dato), tramite l'utilizzo dell'algoritmo di hashing SHA-512.	trasferimento, con una password complessa (standard AES-256).
A.11	**Sicurezza fisica e ambientale**	**Data Center** - I sistemi per l'erogazione del servizio Cloud si trovano presso i Data Center di Arezzo IT1 e IT2, siti rispettivamente in Via Gobetti 96 e Via Ramelli 8, e i Data Center IT3 DCA e DCB di Ponte San Pietro (BG) siti in Via San Clemente 53. Oltre ai data center italiani, il Gruppo Aruba si avvale di una rete internazionale di infrastrutture, sia di proprietà che appartenenti a partner qualificati: • data center CZ1, situato a Ktiš in Repubblica Ceca e appartenente alla rete internazionale dei data center di proprietà dell'Organizzazione; • data center FR1, situato a Parigi in Francia e appartenente alla rete dei data center partner; • data center DE1, situato a Frankfurt in Germania e appartenente alla rete dei data center partner; • data center UK1, situato a Londra in Regno Unito e appartenente alla rete dei data center partner; • data center PL1, situato a Varsavia in Polonia e appartenente alla rete dei data center partner. **Edifici a norma antisismica** - I Data Center del Gruppo Aruba rispondono alla normativa antisismica. **Controllo accessi fisici** - L'accesso agli edifici è possibile solo a coloro che ne hanno effettiva necessità, previa	

Allegato A - ISO 27001 Gli aspetti di Sicurezza del Cloud Aruba			
Area di Controllo		**I nostri controlli**	**Strumenti e funzionalità a disposizione del Cliente**
		registrazione alla reception, e l'accesso alle sale tecniche è consentito solo agli addetti autorizzati, previa identificazione mediante badge e relativo PIN. Il sistema di gestione degli accessi prevede la possibilità di abilitare e disabilitare le singole tessere in base alle aree, agli orari e ad altri parametri, in modo da garantire sia la massima sicurezza degli ambienti che la necessaria fluidità degli accessi. **Sistemi antintrusione** - Presso i data center e gli uffici sono disponibili grate, vetrate antiproiettile, porte blindate, cancelli motorizzati (antintrusione passivi) e sono installati sistemi TVCC e/o VMD (antintrusione attivi). Il sistema di allarme antintrusione a zone ha un funzionamento completamente automatico. I data center sono suddivisi al loro interno in più zone, governate da sistemi antintrusione. Inoltre, in tutte le zone sono installati dei sensori di movimento in grado di rilevare la presenza di persone; nelle zone sensibili (sale dati, power center, magazzini) vi sono anche dei sensori che rilevano l'apertura delle porte e il badge viene utilizzato per l'ingresso e l'uscita. **Sistema antincendio** - Realizzato nel rispetto delle norme di legge e degli standard tecnici di riferimento. I sensori per la rilevazione incendio sono presenti in tutti i piani degli edifici. **Sistema antiallagamento** - È realizzato in tutti gli edifici per la rilevazione di liquidi. Gli edifici sono inoltre ubicati in zone pianeggianti e in posizione rilevata rispetto al piano di campagna. **Sistema di alimentazione elettrica** - Tale sistema è presente nei data center, ridondato a tutti i livelli (gruppi di trasformazione, power center, UPS, gruppi elettrogeni, quadri di distribuzione, ecc.) a garanzia della continuità di alimentazione elettrica in ogni prevedibile condizione. Include anche le misure atte a contenere l'effetto di scariche elettriche di origine atmosferica, spike della rete elettrica, ecc. **Sistema di ventilazione e condizionamento (HVAC)** - Garantisce le condizioni ambientali e microclimatiche ottimali per il regolare funzionamento dei server ospitati nei data center. **Connettività internet** - Negli edifici la connettività è ridondata, con capacità almeno doppia rispetto al minimo necessario.	

Aruba Business srl
Via L. Gulinelli 21/A - 44122 Ferrara, Italy, P.IVA 01497070381
PEC: info@pec.arubabusiness.it - Sito Web: www.arubabusiness.it

Allegato A - ISO 27001 Gli aspetti di Sicurezza del Cloud Aruba			
Area di Controllo		**I nostri controlli**	**Strumenti e funzionalità a disposizione del Cliente**
		Control Room e Facility Operation Center (FOC) - I data center sono presidiati 24/7 da personale sistemistico qualificato, che assicura il costante monitoraggio dell'infrastruttura e dei servizi e il tempestivo intervento in caso di necessità. **Assicurazione** - L'azienda ha stipulato contratti di assicurazione atti a coprire i rischi non mitigati dalle restanti misure di sicurezza.	
A.12	**Apparecchiature**	**Procedure operative** - Le procedure che prescrivono i comportamenti operativi sono documentate, disponibili e conosciute dal personale interessato. **Hardening dei server** - I server che ospitano componenti critiche per la sicurezza dei servizi sono sottoposti ad interventi sistemistici finalizzati a ridurre la superficie di attacco, quali: rimozione di software non necessario, disabilitazione di servizi/protocolli non necessari, installazione delle patch di sicurezza raccomandate dai vendor, applicazione di policies per la complessità delle password, abilitazione dei log di sicurezza, ecc. **Protezione da Distribuided Denial of Service (DDoS) –** I dati vengono analizzati in ingresso individuando il traffico anomalo e bloccando, quando possibile, i pacchetti potenzialmente dannosi. **Tracciamento** (**logging**) - Vengono raccolti e conservati i log dei server infrastrutturali per gli accessi privilegiati ai sistemi in osservanza ai requisiti di legge. Tali log vengono periodicamente verificati dal Team di Sicurezza attraverso audit interni. Sono messi a disposizione dei clienti i log applicativi delle operazioni effettuate nell'utilizzo dei servizi. Allo stesso modo, l'operato degli amministratori di sistema è oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari del trattamento, in modo da controllarne la rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali, previste dalle norme vigenti. **Monitoraggio e alerting** - I sistemi critici del servizio sono controllati da un sistema di monitoraggio presidiato in modo continuativo. Il sistema ha la capacità di generare degli "alert", sotto forma di messaggi email o SMS, che consentono di informare tempestivamente il personale addetto di un potenziale incidente o disservizio, in modo che le necessarie azioni di rimedio possano essere poste in atto nel più breve tempo possibile.	**Backup** - I servizi Cloud del Gruppo Aruba permettono ai clienti di creare ed impostare i propri backup automatizzati attraverso la soluzione Cloud Backup e Bare Metal Backup, scegliendo le proprie politiche in termini di cifratura, periodicità, tipologia (completi o incrementali) e altre specifiche esigenze. Il servizio opzionale di **Disaster Recovery as a Service (DRaaS)**, inoltre, permette di testare le procedure di failover senza interruzioni di sorta. Tutte le procedure di gestione dei servizi di backup e di restore vengono eseguite in autonomia dagli utenti e sono descritte all'interno della Knowledge Base (KB) del servizio nella pagina dedicata, dove vengono descritti anche i vari metodi che possono essere utilizzati per effettuare backup dei propri dati. Nessun'altra copia di backup dei dati viene effettuata dal Gruppo Aruba oltre a quelle autonomamente definite dagli utenti. **Logging** – Il Gruppo Aruba mette a disposizione dei clienti i log applicativi da loro prodotti nell'utilizzo dei servizi. • Cloud PRO: l'utente può consultare log per operazioni sulle virtual machine quali

Aruba Business srl
Via L. Gulinelli 21/A - 44122 Ferrara, Italy, P.IVA 01497070381
PEC: info@pec.arubabusiness.it - Sito Web: www.arubabusiness.it

Allegato A - ISO 27001 Gli aspetti di Sicurezza del Cloud Aruba			
Area di Controllo		**I nostri controlli**	**Strumenti e funzionalità a disposizione del Cliente**
		Backup (parte di competenza Aruba) - Le componenti funzionali all'erogazione del servizio del Gruppo Aruba, la gestione degli utenti e le altre componenti architetturali del servizio seguono le procedure di backup definite a livello aziendale che vengono periodicamente verificate e testate. **Antivirus** - Tutti gli apparati della rete del Gruppo Aruba sono controllati, monitorati e protetti da sistemi EDR. La tecnologia EDR (Endpoint Detection and Response) è in grado di monitorare in tempo reale ed in modo proattivo le minacce conosciute e sconosciute che riguardano tutti gli endpoint ed i server aziendali. Un gruppo dedicato con copertura 24/7 si occupa di analizzare gli eventi anomali ed intervenire tempestivamente. **Processo di Vulnerability Management** – Il perimetro del Gruppo Aruba viene scansionato regolarmente da strumenti automatici e da professionisti qualificati del settore al fine di identificare ogni possibile vulnerabilità anche solo potenziale. Ogni criticità individuata viene immediatamente segnalata al gruppo competente, dando avvio ad un ciclo di risoluzione della problematica che può concludersi con un nuovo rilascio oppure con una mitigazione (es. virtual patching). Per verificarne l'efficacia, si esegue infine una nuova scansione per avere la certezza del rientro della vulnerabilità. **Capacity Management e Change Management** - Al fine di garantire la corretta consegna/erogazione del servizio, il Gruppo Aruba ritiene fondamentale monitorare le risorse a disposizione, analizzare le capacità e adottare gli opportuni accorgimenti per lo sfruttamento ottimale delle stesse e per assicurare la normale fruizione dei servizi. I livelli di connettività, i livelli di occupazione delle risorse, lo spazio su disco ed il dimensionamento dell'infrastruttura sono monitorati con specifici strumenti dal gruppo di operatori appartenenti alla Control Room, 24/7, il cui compito si estende anche al monitoraggio di qualsiasi evento anomalo. Gli strumenti di monitoraggio permettono l'impostazione di controlli specifici per ciascun servizio, rilevando le anomalie e permettendo di anticipare le necessità di cambiamento. I cambiamenti resi necessari dalle attività di monitoraggio e di gestione delle capacità vengono gestiti in modo controllato per permettere di verificarne i risultati e di mantenere traccia delle attività svolte. **Aggiornamenti e patching** - Sui sistemi viene periodicamente eseguito l'aggiornamento e il patching tramite dei tool e seguendo delle procedure interne che	creazione, cancellazione, archiviazione, restore, accensione, spegnimento, reset, cambio password, cambio caratteristiche, creazione e cancellazione e ripristino snapshot. • Cloud VPS (SMART): l'utente può consultare log per operazioni sulle virtual machine quali creazione, cancellazione, accensione, spegnimento, reset, upgrade. • Virtual switch: l'utente può consultare log per operazioni sui virtual switch come acquisto e rimozione e modifiche caratteristiche. • IP pubblici: l'utente può consultare log per operazioni sugli IP pubblici come acquisto e rimozione di un IP pubblico, gestione e modifiche al reverse DNS. • Bilanciatori: l'utente può consultare log per operazioni sui bilanciatori quali creazione bilanciatore, modifica bilanciatore, cancellazione bilanciatore, attivazione o disattivazione bilanciatore, aggiunta modifica e rimozione di regole. • Unified Storage: l'utente può consultare log per operazioni sui virtual switch come acquisto e rimozione e modifiche caratteristiche. • Servizio FTP: l'utente può consultare log per operazioni sugli account FTP come attivazione e rimozione e modifica spazio. • Virtual Private Cloud: l'utente può consultare log per operazioni sul proprio Virtual Private Cloud quali creazione, cancellazione e modifiche alle risorse.

Aruba Business srl
Via L. Gulinelli 21/A - 44122 Ferrara, Italy, P.IVA 01497070381
PEC: info@pec.arubabusiness.it - Sito Web: www.arubabusiness.it

Allegato A - ISO 27001 Gli aspetti di Sicurezza del Cloud Aruba			
Area di Controllo		**I nostri controlli**	**Strumenti e funzionalità a disposizione del Cliente**
		prevedono il testing prima negli ambienti di sviluppo. Una volta superata questa fase viene eseguita l'applicazione in ambiente di produzione. **Sincronizzazione** - E' utilizzato il sistema NTP per sincronizzare i propri orologi e mantenere coerenza degli eventi. La fonte autoritativa per la sincronizzazione dell'orologio è INRiM (http://www.inrim.it). Il fuso orario su tutti i sistemi utilizzato è CEST, ad eccezione di UK su cui viene utilizzato GMT. Tutte le VM fornite hanno fuso orario basato su CEST e utilizzano come fonte di sincronizzazione clock quella dell'host su cui risiedono. **Multitenancy e cancellazione sicura dei dati** – Il Gruppo Aruba garantisce un sistema multitenancy che permette di separare le istanze dei singoli clienti tra di loro e di separare le istanze dei clienti da quelle del Cloud Service Provider. Il pannello cloud pubblico è stato espressamente sviluppato dal Gruppo Aruba in modalità multitenant secondo le linee guida per la programmazione sicura e permette esclusivamente l'accesso ed il governo della propria infrastruttura cloud. Inoltre, per i servizi PRO, VPS e Virtual Private Cloud, ed ogni qualvolta venga utilizzato un software esterno, la multitenancy è garantita direttamente dai sistemi di virtualizzazione utilizzati. Alla chiusura del servizio, oppure all'esaurimento del credito, secondo quanto definito contrattualmente, il Gruppo Aruba provvede alla cancellazione e rimozione definitiva dei dati dei servizi cloud secondo quanto descritto nella pagina dedicata a cosa avviene all'esaurimento del credito. La cancellazione, a seconda del servizio, può avvenire attraverso API, pannelli tecnici, script o software specifici. Il Gruppo Aruba gestisce con un processo definito la cancellazione periodica dei file temporanei dei propri sistemi cloud.	• Cloud Backup: l'utente può consultare log per operazioni sui propri account backup relativi a creazione, cancellazione e modifiche al piano, cambio o reset password. • Cloud Monitoring: l'utente può consultare log per operazioni sui propri servizi monitoring e relativi controlli quali creazione piano monitoring o aggiunta nuovo controllo, cancellazione piano monitoring o controllo, modifiche al piano monitoring o ad un singolo controllo. • Cloud Object Storage: l'utente può consultare log per operazioni sui propri account Object Storage relativi a creazione, cancellazione e modifiche al piano, cambio o reset password. • Domain Center: l'utente può consultare log per operazioni sui propri domini e DNS relativi a aggiunta nuovo dominio, cancellazione dominio e modifiche a dati relativi al dominio, creazione DNS, cancellazione DNS, modifiche a qualsiasi record DNS. • Jelastic Cloud: l'utente può consultare log per operazioni sui propri account Jelastic Cloud relativi a creazione, cancellazione e modifiche al piano, cambio o reset password. • Database as a Service (DBaaS): l'utente può consultare log per operazioni sui propri account "Database as a Service" relativi a creazione, cancellazione e modifiche al piano, cambio o reset password, backup e restore dei database e restart delle istanze. **Capacity management** - Per quanto riguarda la gestione delle capacità in capo al cliente, il Gruppo Aruba

Aruba Business srl
Via L. Gulinelli 21/A - 44122 Ferrara, Italy, P.IVA 01497070381
PEC: info@pec.arubabusiness.it - Sito Web: www.arubabusiness.it

Allegato A - ISO 27001 Gli aspetti di Sicurezza del Cloud Aruba			
Area di Controllo		**I nostri controlli**	**Strumenti e funzionalità a disposizione del Cliente**
			permette al cliente di tenere sotto controllo costante il consumo delle risorse economiche e tecniche a sua disposizione, permettendogli anche il forecasting. Inoltre, nella fase di acquisto del servizio, vengono descritti i casi in cui sono presenti limiti all'espandibilità delle risorse. **Sincronizzazione** - Quando si ritiene che la sincronizzazione degli orologi possa rappresentare un elemento di difficoltà per il cliente, vengono fornite informazioni di dettaglio in Knowledge Base pubblica (ad esempio nella pagina dedicata alle operazioni schedulate) oppure nei pannelli di gestione. **Multitenancy** Cloud PRO. La multitenancy viene garantita: • Dal pannello cloud pubblico sviluppato espressamente in modalità multitenant dal Gruppo Aruba e dalle API pubbliche autenticate. Tali soluzioni permettono solamente l'accesso e il governo della propria infrastruttura cloud. • Dai sistemi di virtualizzazione Hyper-V, VMware, o Openstack. Il cliente ha accesso solamente alle sue Virtual Machine (VM) che gli hypervisor sottostanti mantengono isolate logicamente dalle altre. Le VM fornite al cliente sono installate con strumenti di controllo accesso le cui credenziali vengono scelte direttamente dal cliente in fase di creazione. Gli strumenti di accesso forniti con le macchine sono SSH per gli ambienti Linux e RDP per gli ambienti Windows. Le reti pubbliche sono condivise tra i clienti ma su tutte le macchine messe a disposizione è

Allegato A - ISO 27001 Gli aspetti di Sicurezza del Cloud Aruba			
Area di Controllo		**I nostri controlli**	**Strumenti e funzionalità a disposizione del Cliente**
			presente un firewall perimetrale ad uso del cliente. In aggiunta a questo, il cliente ha la possibilità di acquistare il servizio di Virtual Switch che consiste nella fornitura di una VLAN dedicata e non condivisa con altri clienti su cui il cliente può interconnettere le sue macchine per la massima segregazione. Cloud VPS (SMART). La multitenancy viene garantita: • Dal pannello cloud pubblico sviluppato espressamente in modalità multitenant dal Gruppo Aruba e dalle API pubbliche autenticate. Tali soluzioni permettono solamente l'accesso e il governo della propria infrastruttura cloud. • Dai sistemi di virtualizzazione VMware e Opesnstack. Il cliente ha accesso solamente alle sue VM che gli hypervisor sottostanti mantengono isolate logicamente dalle altre. Le VM fornite al cliente sono installate con strumenti di controllo accesso le cui credenziali vengono scelte direttamente dal cliente in fase di creazione. Gli strumenti di accesso forniti con le macchine sono SSH per gli ambienti Linux e RDP per gli ambienti Windows. Le reti pubbliche sono condivise tra i clienti ma su tutte le macchine messe a disposizione è presente un firewall perimetrale ad uso del cliente. Virtual Switch e Hybrid Link: si tratta di risorse dedicate al singolo tenant. La multitenancy è garantita dal pannello cloud pubblico sviluppato espressamente in modalità multitenant dal Gruppo Aruba e dalle API pubbliche autenticate. Tali soluzioni permettono solamente l'accesso e il

Allegato A - ISO 27001 Gli aspetti di Sicurezza del Cloud Aruba			
Area di Controllo		**I nostri controlli**	**Strumenti e funzionalità a disposizione del Cliente**
			governo della propria infrastruttura cloud. Virtual Private Cloud. La multitenancy viene garantita: • Dal pannello vCloud Director, sviluppato espressamente in modalità multitenant da VMware. Tale pannello permette solamente l'accesso e il governo della propria infrastruttura cloud. • Dal sistema di virtualizzazione VMware. Il cliente ha accesso solamente al suo virtual data center VM che gli hypervisor sottostanti mantengono isolato logicamente dagli altri. Le VM fornite al cliente sono installate con strumenti di controllo accesso le cui credenziali vengono scelte direttamente dal cliente in fase di creazione. Gli strumenti di accesso forniti con le macchine sono SSH per gli ambienti Linux e RDP per gli ambienti Windows. Su ciascun virtual data center fornito viene messo a disposizione un firewall software perimetrale (NSX Edge) che permette l'isolamento del proprio virtual data center dagli altri e che permette al cliente di configurare le regole di sicurezza ottimali per il suo scopo. Il cliente ha la possibilità di creare autonomamente reti private dedicate e non condivise da altri clienti per configurare la propria architettura. Anche le reti pubbliche, su richiesta, possono essere fornite dedicate e non condivise con altri clienti. Bare Metal Backup. La multitenancy viene garantita: • Dal pannello cloud pubblico sviluppato espressamente in modalità multitenant dal Gruppo

Allegato A - ISO 27001 Gli aspetti di Sicurezza del Cloud Aruba			
Area di Controllo		**I nostri controlli**	**Strumenti e funzionalità a disposizione del Cliente**
			Aruba e dalle API pubbliche autenticate. Tali soluzioni permettono solamente l'accesso e il governo della propria infrastruttura cloud. • Dal pannello di gestione di Veeam. Il cliente ha accesso solamente al suo set di dati di backup e non ha in alcun modo possibilità di vedere o controllare i sistemi di backup di altri clienti. Disaster Recovery. La multitenancy viene garantita: • Dal pannello cloud pubblico sviluppato espressamente in modalità multitenant dal Gruppo Aruba e dalle API pubbliche autenticate. Tali soluzioni permettono solamente l'accesso e il governo della propria infrastruttura cloud. • Dal pannello di gestione di Zerto , Veeam, VMWare VCAV. Il cliente ha accesso solamente al suo set di dati e non ha in alcun modo possibilità di vedere o controllare i sistemi di Disaster recovery (DR) di altri clienti. Cloud Backup (Evault/Commvault). La multitenancy viene garantita: • Dal pannello cloud pubblico sviluppato espressamente in modalità multitenant dal Gruppo Aruba e dalle API pubbliche autenticate. Tali soluzioni permettono solamente l'accesso e il governo della propria infrastruttura cloud. • Dal sistema di backup Evault o Commvault. Il cliente ha accesso solamente al suo set di dati di backup e non ha in alcun modo possibilità di vedere o controllare i sistemi di backup di altri clienti. Cloud Monitoring: la multitenancy è garantita dal pannello cloud

Aruba Business srl
Via L. Gulinelli 21/A - 44122 Ferrara, Italy, P.IVA 01497070381
PEC: info@pec.arubabusiness.it - Sito Web: www.arubabusiness.it

Allegato A - ISO 27001 Gli aspetti di Sicurezza del Cloud Aruba			
Area di Controllo		**I nostri controlli**	**Strumenti e funzionalità a disposizione del Cliente**
			pubblico sviluppato espressamente in modalità multitenant dal Gruppo Aruba e dalle API pubbliche autenticate. Tali soluzioni permettono solamente l'accesso e il governo della propria infrastruttura cloud. Cloud Object Storage. La multitenancy viene garantita: • Dal pannello cloud pubblico sviluppato espressamente in modalità multitenant dal Gruppo Aruba e dalle API pubbliche autenticate. Tali soluzioni permettono solamente l'accesso e il governo della propria infrastruttura cloud. • Dai sistemi di Identity and Access Management, Scality e CEPH. Il cliente ha accesso solamente al suo account storage e non ha in alcun modo possibilità di vedere o controllare account di altri clienti. IaaS per SAP HANA. La multitenancy e la segregazione sono garantite grazie a vari accorgimenti: • una VPN SSL dedicata che permette al cliente di accedere al sistema di gestione della piattaforma; • un account univoco presente sul sistema di virtualizzazione VMware che permette di accedere alle sole VM del cliente; • la segregazione offerta dalla rete dedicata messa a disposizione del cliente e non condivisa con altri clienti; • gli strumenti interni forniti con la VM che permettono la creazione di molteplici profili utenti ed amministrativi. Domain Center. La multitenancy è garantita dal pannello cloud pubblico sviluppato espressamente in modalità multitenant dal Gruppo

Allegato A - ISO 27001 Gli aspetti di Sicurezza del Cloud Aruba			
Area di Controllo		**I nostri controlli**	**Strumenti e funzionalità a disposizione del Cliente**
			Aruba e dalle API pubbliche autenticate. Tali soluzioni permettono solamente l'accesso e il governo della propria infrastruttura cloud. Jelastic Cloud. La multitenancy viene garantita attraverso due modalità: • Dal pannello cloud pubblico sviluppato espressamente in modalità multitenant dal Gruppo Aruba e dalle API pubbliche autenticate. Tali soluzioni permettono solamente l'accesso e il governo della propria infrastruttura cloud. • Dal sistema di Jelastic il cliente ha accesso solamente al suo account jelastic e non ha in alcun modo possibilità di vedere o controllare account di altri clienti. Database as a Service (DBaaS): la multitenancy è garantita dal pannello cloud pubblico sviluppato espressamente in modalità multitenant dal Gruppo Aruba e dalle API pubbliche autenticate. Tali soluzioni permettono solamente l'accesso e il governo della propria infrastruttura cloud.
A.13	**Sicurezza delle comunicazioni**	**Firewall e IPS** - I portali web esposti per i servizi sono protetti dal firewall di data center del servizio cloud e da IPS. Per quanto riguarda i servizi computing, tutte le virtual machine fornite dal Gruppo Aruba sono modellate e rese disponibili sotto forma di immagini. Tali immagini vengono prodotte e testate dai tecnici del Gruppo Aruba ed in particolare, dopo aver installato il sistema operativo ed effettuato la prima configurazione, viene abilitato il sistema	**Firewall** - Il cliente è amministratore del proprio server e quindi ha la possibilità di modificare le impostazioni di firewalling. Le guide ed i tutorial presenti in KB forniscono alcune informazioni su come segregare e proteggere la sicurezza di rete e predisporre un firewall sul Cloud del Gruppo Aruba.

Allegato A - ISO 27001 Gli aspetti di Sicurezza del Cloud Aruba			
Area di Controllo		**I nostri controlli**	**Strumenti e funzionalità a disposizione del Cliente**
		di firewall concedendo i privilegi minimi possibili ed aprendo solo le porte necessarie. **Virtual Private Network (VPN)** - L'accesso remoto alla rete (LAN) aziendale è consentito solo al personale autorizzato che ne ha necessità; l'accesso remoto è possibile esclusivamente attraverso una VPN che assicura confidenzialità della comunicazione, autenticazione forte del server e autenticazione forte (a due fattori) dell'utente.	**Virtual Switch** - Il cliente ha la possibilità di acquistare il servizio di Virtual Switch che consiste nella fornitura di una VLAN dedicata e non condivisa con altri clienti su cui il cliente può interconnettere le sue macchine per la massima segregazione e la possibilità di creare autonomamente reti private dedicate e non condivise da altri clienti per configurare la propria architettura (Virtual Private Cloud). Anche le reti pubbliche, su richiesta, possono essere fornite dedicate e non condivise con altri clienti. **Posizione geografica dei dati a garanzia della sicurezza e della conformità** - I servizi del Gruppo Aruba possono essere in alternativa attivabili su base data center o su base regionale (che coincide con una nazione). Il cliente ha la possibilità di indicare il data center o i data center all'interno dei quali verranno attivati i propri servizi e trasferiti i propri dati; per i servizi su base regionale, i clienti hanno la possibilità di selezionare il Paese all'interno del quale attivare il servizio. In nessun caso il Gruppo Aruba sposta sistemi o contenuti al di fuori delle località geografiche (DC o regioni) configurate dai propri clienti.
A.14	**Acquisizione, sviluppo e manutenzione dei sistemi**	**Gestione delle modifiche** - Le modifiche al software applicativo sono sottoposte a valutazione e approvazione prima di essere realizzate; sono poi sottoposte a test prima di essere promosse in produzione, al fine di verificare la corretta implementazione delle nuove funzionalità e l'assenza di regressioni. Inoltre, tutto il software sviluppato è gestito da un sistema di versioning.	**Gestione delle modifiche** – Il Gruppo Aruba mette a disposizione dei clienti un changelog (come dettagliato nella pagina dedicata sulla KB) per comunicare i rilasci, le fix, le correzioni e gli aggiornamenti dei servizi offerti.

Aruba Business srl
Via L. Gulinelli 21/A - 44122 Ferrara, Italy, P.IVA 01497070381
PEC: info@pec.arubabusiness.it - Sito Web: www.arubabusiness.it

Allegato A - ISO 27001 Gli aspetti di Sicurezza del Cloud Aruba			
Area di Controllo		**I nostri controlli**	**Strumenti e funzionalità a disposizione del Cliente**
A.15	**Relazioni con i fornitori**	**Gestione dei fornitori** - La politica aziendale che regola i rapporti con i fornitori prevede che, per una corretta definizione e gestione di un nuovo rapporto di fornitura, si debbano sempre tenere in considerazione i seguenti aspetti, con particolare attenzione alla sicurezza delle informazioni: • valutazione del rischio ed indagini preliminari da effettuare per la completa valutazione di un nuovo fornitore; • selezione delle clausole dei contratti, al fine di valutare se i contratti standard coprono i rischi individuati o se sia necessario aggiungere/modificare delle clausole specifiche; • controllo degli accessi alle informazioni, per fornire l'accesso al fornitore secondo la logica del "need-to-know" e pertanto soltanto ai dati e alle informazioni che sono effettivamente richieste e necessarie per lo svolgimento della propria attività; • controllo degli accessi ai sistemi del Gruppo Aruba, in caso la fornitura preveda che il fornitore acceda ai sistemi, tramite utenze specifiche, utilizzando una Private Network (VPN) ed un sistema specifico di detection response e virtual desktop infrastructure (VDI) forniti dal Gruppo Aruba stessa; • monitoraggio delle non conformità, per il regolare svolgimento dei controlli al fine di poter accertare la conformità del fornitore rispetto ai requisiti contrattuali concordati ed alla sicurezza delle informazioni. Inoltre, le forniture esterne necessarie per lo sviluppo, la manutenzione e l'erogazione del servizio sono soggette a verifiche volte a mitigare il rischio di incidenti di sicurezza causati da materiale non conforme oppure da azioni improprie da parte dei fornitori. Tutti i fornitori di prestazioni professionali sono tenuti alla sottoscrizione di un accordo di riservatezza (NDA). I modelli contrattuali utilizzati dal Gruppo Aruba per la fornitura del servizio prevedono la possibilità che il Gruppo Aruba si avvalga di terzi per lo svolgimento delle proprie attività. Tale collaborazione si basa sull'impegno, contrattualmente previsto con eventuali subfornitori, da parte del Gruppo Aruba, a verificare che essi, in base alla tipologia di servizio erogato, abbiano le capacità di rispettare i medesimi requisiti e livelli di sicurezza a cui si impegna il Gruppo Aruba. Il Gruppo Aruba mantiene un elenco dei subfornitori dei servizi che è	

Aruba Business srl
Via L. Gulinelli 21/A - 44122 Ferrara, Italy, P.IVA 01497070381
PEC: info@pec.arubabusiness.it - Sito Web: www.arubabusiness.it

Allegato A - ISO 27001 Gli aspetti di Sicurezza del Cloud Aruba			
Area di Controllo		**I nostri controlli**	**Strumenti e funzionalità a disposizione del Cliente**
		disponibile, su richiesta dei clienti. Altresì, nel caso di subentro di nuovi/ulteriori subfornitori, il Gruppo Aruba si impegna a comunicarlo ai propri clienti con congruo anticipo tale da permettere l'opposizione o il recesso da parte dei clienti stessi.	
A.16	**Gestione degli incidenti relativi alla sicurezza delle informazioni**	**Processo di gestione degli incidenti di sicurezza delle informazioni** - Il sistema di gestione per la sicurezza delle informazioni del Gruppo Aruba si contraddistingue per l' approccio strutturato e programmatico nella gestione degli eventi e/o incidenti di sicurezza delle informazioni che dovessero verificarsi nell'ambito delle operazioni delle società del Gruppo, e fa capo alle linee guida ISO 27035 del flusso di gestione degli incidenti di sicurezza delle informazioni. Tale processo è attuato mediante apposito piano, disciplinando le misure operative che devono essere implementate nel caso in cui siano riscontrati incidenti di sicurezza delle informazioni. È stato definito un flusso di gestione degli incidenti e sono state identificate le responsabilità connesse alla sua applicazione, sia in termini di gestione e risoluzione degli Incidenti che di supporto strategico per la tempestiva adozione delle decisioni necessarie a fronteggiare gli incidenti di sicurezza più rilevanti (ad esempio major incident, incidenti non noti, data breach). Sono stati altresì definiti tempi e modalità per la predisposizione e l'invio delle comunicazioni relative agli incidenti di sicurezza delle informazioni verso autorità, clienti e terze parti.	
A.17	**Aspetti relativi alla sicurezza delle informazioni nella gestione della continuità operativa**	**Procedura di gestione dei disastri** – Il Gruppo Aruba ha formalizzato un Piano di Business Continuity, una Policy e piani specifici di BC per data centerrelativi ai servizi essenziali per il funzionamento degli stessi, quali ad esempioenergia elettrica, condizionamento e connettività I data center sono certificati ISO 27001 ed in essi sono attuate le principali misure volte a garantire la sicurezza fisica e la cointinuità operativa delle strutture. In particolare, i Data Center IT1, IT3 DCA e DCB del Gruppo Aruba sono conformi al massimo livello (Rating 4) tra quelli previsti dalla normativa ANSI TIA 942-B-2017. Tale risultato, che indica la capacità di evitare interruzioni dei servizi anche in presenza di guasti gravi (fault-tolerance), è stato ottenuto grazie ad una serie di accorgimenti progettuali e realizzativi che hanno interessato tutti gli aspetti del data	**Disaster Recovery as a Service (DRaaS)** – Il Gruppo Aruba mette a disposizione il servizio Disaster Recovery as a Service progettato per garantire la business continuity delle aziende, consente di replicare e ripristinare rapidamente l'accesso e le funzionalità dell'infrastruttura IT in seguito ad una interruzione dovuta a un attacco informatico, un guasto o un evento disastroso. Attraverso un pannello web self-service, su connessione sicura, il cliente può autonomamente creare direttive e politiche di Disaster Recovery, selezionando sorgente

Aruba Business srl
Via L. Gulinelli 21/A - 44122 Ferrara, Italy, P.IVA 01497070381
PEC: info@pec.arubabusiness.it - Sito Web: www.arubabusiness.it

Allegato A - ISO 27001 Gli aspetti di Sicurezza del Cloud Aruba			
Area di Controllo		**I nostri controlli**	**Strumenti e funzionalità a disposizione del Cliente**
		center: scelta del sito, aspetti architettonici, sicurezza fisica, sistemi antincendio, impianto elettrico, impianto meccanico e rete dati Un data center di Rating 4 (former Tier 4) ha componenti ridondati sempre attivi, oltre a percorsi multipli di alimentazione e raffreddamento degli hardware. Infine, i data center sono strutturati per sopportare un guasto in un qualsiasi punto dell'impianto senza causare downtime e sono protetti nei confronti degli eventi fisici tra i quali anche le catastrofi naturali (es. incendio, alluvione, terremoto, etc.). I Data Center IT3 DCA e DCB del Gruppo Aruba sono certificati ISO/IEC 22237, standard internazionale di riferimento per l'intero ciclo di vita del data center, dall'ideazione strategica alla realizzazione e messa in esercizio, in linea con le normative ANSI/TIA 942 (standard americano) ed EN 50600 (standard europeo). L'ambiente cloud è composto da una infrastruttura multi-data center, i cui servizi sono interconnessi da una rete IPSEC ad elevata banda e protezione. Essendo la struttura pensata per essere multi-data center è predisposta nativamente al Disaster Recovery in quanto tutti i data center sono indipendenti dal punto di vista logico tra di loro. Le macchine dei clienti virtualizzate non sono sottoposte a Disaster Recovery geografico in quanto vengono forniti ai clienti stessi tutti gli strumenti necessari a costruirsi su misura i sistemi e le procedure di Disaster Recovery.	(sito primario) e destinazione (sito secondario) a scelta tra proprie infrastrutture virtuale VMware on-premise e/o Data Center del Gruppo Aruba abilitati al servizio Virtual Private Cloud.
A.18	**Conformità**	**Protezione dei dati personali** - Tutti i servizi sono erogati nel pieno rispetto della vigente normativa in tema di protezione dei dati personali secondo il Regolamento UE 2016/679 ("GDPR"), il D.lgs. 196/2003, così come indicato dal D.lgs. 101/2018, ed i Provvedimenti dell'Autorità Garante per la protezione dei dati personali. **Revisione** (**auditing**) - Gli eventi registrati col tracciamento, in particolare quelli che potrebbero indicare una minaccia alla sicurezza, sono periodicamente analizzati. **Ispezioni interne** - Il responsabile delle verifiche e delle ispezioni (auditing) assicura lo svolgimento di verifiche di conformità del servizio cloud a quanto previsto nel presente documento e dalle norme vigenti con periodicità perlomeno annuale.	

Aruba Business srl
Via L. Gulinelli 21/A - 44122 Ferrara, Italy, P.IVA 01497070381
PEC: info@pec.arubabusiness.it - Sito Web: www.arubabusiness.it

STORICO VERSIONI

VERSIONE 1.1 DEL 14/04/2023	***NATURA DELLE MODIFICHE: Aggiornati i controlli A.12, A.13, A.17***
VERSIONE 1.0 DEL 01/01/2022	***NATURA DELLE MODIFICHE: Prima emissione***

Aruba Business srl
Via L. Gulinelli 21/A - 44122 Ferrara, Italy, P.IVA 01497070381
PEC: info@pec.arubabusiness.it - Sito Web: www.arubabusiness.it