Cloud Security

# Attachment A
# ISO 27001:2017

| Attachment A - ISO 27001:2017<br>The Security aspects of the Aruba Group's Cloud | | | |
|---|---|---|---|
| **Control Area** | | **Our controls** | **Tools and features available to the Customer** |
| **A.5** | **Information security policies** | **Information Security Management System Policies (**ISMS) - The Aruba Group has defined the approach adopted by the organization for managing its Information Security objectives in a specific Company Policy. This document has been approved by Management and published on the company intranet. In support of the abovementioned Policy there are additional policies and procedures for specific issues that define the Aruba Group's Information Security Management System. | |
| **A.6** | **Organization of information security** | **Roles and Responsibilities** - Within the scope of its responsibilities as a cloud service provider, as defined in the page dedicated to the shared responsibility model, the Aruba Group has defined the personnel, roles, skills and responsibilities connected with the processes, in accordance with the principles of the Segregation of Duties, Least Privilege and Dual Control.<br><br>**Segregation of Duties (SoD)** - Within the scope of the operational processes of the Services, different procedures are carried out by different people, so that no single person has control of the entire process.<br><br>**Least Privilege** - Permissions to access premises, equipment, data, functions, etc., are granted to the personnel assigned to services, in accordance with the "least privilege" principle, i.e. to the extent necessary for these resources to carry out the tasks assigned to them, but no more.<br><br>**Dual Control** - The most critical procedures from a security perspective involve the participation of at least two people. | **Roles and Responsibilities** - The general description of the service can be found in the Knowledge Base (KB), on the page dedicated to the general description of the service, together with the service delivery locations table and the table showing the model for responsibilities shared between the Aruba Group as Cloud Service Provider and its customers. |
| **A.7** | **Human resources security** | **Personnel Training** - Service personnel have adequate skills and experience, and are provided with specific training for each important system update.<br><br>**Awareness** - Periodically, staff are made aware of security issues, cybercrime in general and the best practices to be adopted, through specific training courses.<br><br>**Non Disclosure Agreement (NDA)** - Newly hired personnel are required to sign a confidentiality | **Training and Awareness** – The Aruba Group provides a Knowledge Base containing information about cloud services. It contains information on the services, guides, tutorials, documentation on the Application Programming Interfaces (API), glossary and Changelog of the services. |

| Attachment A - ISO 27001:2017<br>The Security aspects of the Aruba Group's Cloud | | | |
|---|---|---|---|
| **Control Area** | | **Our controls** | **Tools and features available to the Customer** |
| | | agreement in order to protect the company's know-how and other confidential information. | |
| **A.8** | **Asset management** | **Asset Inventory** - There is an updated inventory of the assets, which includes a record of the virtual and physical equipment providing the services and their physical location within the Aruba Group's infrastructure.<br><br>The asset inventory is updated following each installation of new equipment in the infrastructure. In addition, to check for any deviations, automatic scans of the networks are carried out on a daily basis to detect any new assets.<br><br>The inventory contains a description of the assets in which the corresponding characteristics are described: for example, the type of equipment (virtual or physical), the infrastructure to which it belongs, internal ownership, etc.<br><br>**Handling of Assets** - There are also internal procedures that define and formalize the activities relating to the preparation of new equipment and its management (e.g. how to make a change, how to update the systems etc.).<br><br>**Configuration Management** - The list of System components is defined so as to allow the identification of the individual hardware and software components and their model or version respectively.<br><br>**Maintenance and Support**- The most important hardware (HW) components for the continuity of the Service is covered by maintenance contracts guaranteeing repair or replacement within a sufficiently rapid timeframe by the supplier, or the availability of identical stored components which can be deployed if required. Regarding commercial software (SW), there are appropriate support contracts that guarantee the supplier's technical support in the event of malfunctions.<br><br>**Disposal** - The Aruba Group guarantees that specific procedures are adopted for the disposal and destruction of hardware components that are no longer used both for foreign colocation data centers and for proprietary data centers in order to ensure that for each storage component that has reached the end of its life and needs to be replaced | **Asset ownership** - In accordance with the principle of shared responsibility, for each service the Aruba Group has identified the respective attributions of ownership, with regard to infrastructure, licences, IP addresses, software provided by the Aruba Group, software, data and content entered by the customer.<br><br>The information about ownership of the assets for the services is available to customers within the public KB on the dedicated page.<br><br>**Data erasure** - Using the disk wipe technique in the Cloud environment, for VPS (Smart), PRO and Private Cloud services, the customer has the option of permanently deleting the data contained on their equipment and making it impossible for it to be recovered. The KB dedicated page sets out the operational steps.<br><br>**Labelling** - The Aruba Group's services allow customers to name and classify assets under their control. The guides published in the Knowledge Base provide precise instructions on how to perform these operations and what the constraints are. |

| Attachment A - ISO 27001:2017<br>The Security aspects of the Aruba Group's Cloud | | | |
|---|---|---|---|
| **Control Area** | | **Our controls** | **Tools and features available to the Customer** |
| | | and disposed of, the complete, data contained therein is completely and permanently deleted. | |
| **A.9** | **Access control** | **Logical Access Management** - Before accessing internal systems, authorized personnel will be asked to identify and authenticate themselves (via username, password and/or smartcard). Once authenticated, Aruba Group personnel can only access the resources (e.g. systems, data) for which they have been explicitly authorized, according to the actual needs of the position they hold. Users are managed through Active Directory (AD) domain controllers. To guarantee the "Segregation of Duty" principle, logical access to the production environment is managed via AD on a dedicated domain, within which there are users with different privileges and permissions in line with the job-role of the person in question, and in compliance with the principle of least privilege. All users are named individuals, so there are no group and/or shared users and they are periodically subject to independent verification by the Security Department.<br><br>**Password Policy** - Consistent with group security policies and in compliance with privacy legislation ("minimum measures", provisions of the Data Protection Authority), a secure password management policy is applied.<br>Following the creation of a user, the password must be changed at the first login and it must then be changed periodically after a defined period of time. | **Logical Access Management** - It is possible at all times for the customer to register, modify, suspend, reactivate and delete their user profiles, as well as manage the associated commercial aspects (credits, thresholds, associated profiles, etc.). In terms of permissions, it is possible for each customer to manage their assets from an administrative point of view by setting security levels and managing access privileges. In particular, depending on the service, it is possible for customers to:<br>• Assign one or more VMs to its users, relying on the accounting system within the virtual machine.<br>• For Cloud Object Storage and Cloud Backup services, it is possible to create unique credentials to be assigned to independent resource groups.<br>• For the Private Cloud service, it is possible to create sets of technical users within the technical control panel with different permissions.<br>• For partner customers, it is always possible to define the sets of operations permitted to users through appropriate profiling rules.<br><br>The Permissions are organized on a hierarchical basis: there are "parent" Permissions and "child" Permissions; the "parent" Permission automatically guarantees all "child" Permissions while the "child" Permission only guarantees itself and can be activated even without the "parent" Permission. |
| **A.10** | **Encryption** | **TLS Secure Channel** - All data flows from/to the sensitive systems of the systems under analysis, in particular the servers exposed on the Internet, are protected by a TLS secure channel, by means of appropriate configuration on the servers, so as to ensure: | **Encryption Checks** - We suggest that customers adopt a risk-based approach and implement additional encryption checks in the areas for which they are responsible (see Responsibility Matrix) in the event that the data processed within the Aruba Group service is particularly sensitive. |

| Attachment A - ISO 27001:2017<br>The Security aspects of the Aruba Group's Cloud | | | |
|---|---|---|---|
| **Control Area** | | **Our controls** | **Tools and features available to the Customer** |
| | | • server authentication;<br>• session encryption with a symmetric encryption algorithm considered sufficiently secure.<br><br>This applies both to flows originating interactively (web browsing) and to those generated automatically (e.g. Web Services query).<br><br>Until now AES has mainly been used as a symmetric encryption algorithm.<br><br>The enabled version of TLS is as high as possible, taking into account the capabilities of the software clients.<br><br>SSL Server certificates installed on servers exposed on the Internet are issued by a CA recognized as reliable by the main browsers and operating systems.<br><br>The details of the certificates in use on the cloud control panels and the protocols used on the public network are available in the KB on the page dedicated to the certificates in use on Cloud Control Panels.<br><br>**Data at Rest Encryption** - The most security-critical data "at rest", such as passwords, OTP token seeds and other data that must remain confidential to ensure the reliability of processes, are stored using symmetric encryption, using what is considered to be a sufficiently secure algorithm.<br><br>As for the protection of credentials more specifically, passwords are stored within the repository in non-reversible "hashed" mode (fingerprint or digest of the data), using the SHA-512 hashing algorithm. | **Cloud Backup – Encryption** - The Cloud Backup service offers the option to encrypt backed-up data before it is even transferred with a strong password (AES-256 standard). |
| **A.11** | **Physical and environmental safety** | **Data Centers** - The systems for delivering the Cloud Service are located at the "IT1" and "IT2" Data Centers in Arezzo, at Via Gobetti 96 and at Via Ramelli 8 respectively, and the "IT3" data center in Ponte San Pietro (BG) at Via San Clemente 53. In addition to the Italian data centers, the Aruba Group has an international infrastructure network, both proprietary and belonging to qualified partners:<br><br>• CZ1 data center in Ktiš, in the Czech Republic, belonging to the international network of data centers owned by the Organisation; | |

| Attachment A - ISO 27001:2017<br>The Security aspects of the Aruba Group's Cloud | | | |
|---|---|---|---|
| **Control Area** | | **Our controls** | **Tools and features available to the Customer** |
| | | • FR1 data center, in Paris, France, belonging to the network of partner data centers;<br>• DE1 data center, in Frankfurt, Germany, belonging to the network of partner data centers;<br>• UK1 data center, in London, in the UK, belonging to the network of partner data centers;<br>• PL1 data center, in Warsaw, Poland, belonging to the network of partner data centers.<br>**Earthquake-resistant Buildings** - The Aruba Group's Data Centers comply with the earthquake-resistance regulations.<br>**Control of Physical Access** - Access to the buildings is only possible for those who actually need it, after signing in at reception, and access to the technical rooms is permitted only for authorized personnel, following identification with a pass and corresponding PIN. The access control system includes the option to allow and disable individual swipe cards for specific areas, times and other criteria, guaranteeing complete security and ease of access.<br>**Anti-intrusion systems** - At the Data Centers and Offices, grilles, bulletproof glass, armoured doors, motorized gates (passive anti-intrusion systems) are deployed, and CCTV and/or VMD systems (active anti-intrusion systems) are installed. The anti-intrusion alarm system in the various zones is fully automatic.<br>The Data Centers are divided into several zones, monitored by anti-intrusion systems. In addition, motion sensors are installed in all areas capable of detecting the presence of people; in sensitive areas (data rooms, Power Centers, warehouses) there are also sensors that detect the opening of doors and a pass is used for entry and exit.<br>**Fire-fighting system** - This system is designed to comply with the law and with the relevant technical standards. Fire detection sensors are present on all floors of the buildings.<br>**Anti-flooding system** - Liquid and anti-flood detection systems are installed. The buildings are also located in flat areas and in a surveyed position with respect to ground level. | |

| Attachment A - ISO 27001:2017<br>The Security aspects of the Aruba Group's Cloud | | | |
|---|---|---|---|
| **Control Area** | | **Our controls** | **Tools and features available to the Customer** |
| | | **Power Supply System** - This system is present in the Data Centers, and is redundant at all levels (substations, power centers, UPS, generators, switchboards, etc.) to guarantee the continuity of the power supply in all foreseeable conditions. It also includes appropriate measures to contain the effect of atmospheric electric discharges, mains spikes, etc.<br><br>**Ventilation and Air Conditioning System (HVAC)** - The system is capable of ensuring optimal climatic conditions for the smooth operation of servers hosted at Data Centers.<br><br>**Internet connectivity** - Redundant connectivity is present in buildings, with a capacity at least twice the minimum necessary.<br><br>**Network Operation Center (NOC)** - The Data Centers are manned 24/7, 365 days a year, by qualified systems personnel, which ensures constant monitoring of the infrastructure and services and timely intervention if needed.<br><br>**Insurance** - The company has entered into an insurance contract to cover risks not mitigated by other security measures. | |

| Attachment A - ISO 27001:2017<br>The Security aspects of the Aruba Group's Cloud | | | |
|---|---|---|---|
| **Control Area** | | **Our controls** | **Tools and features available to the Customer** |
| **A.12** | **Equipment** | **Operating procedures** - The procedures that prescribe operational behaviors are documented, made available and acknowledged by the personnel concerned.<br><br>**Server Hardening** - The servers that host components critical for the security of services undergo systemic interventions designed to reduce the area of attack, such as: removing unnecessary software, disabling unnecessary services/protocols, installing security patches recommended by vendors, applying policies for the complexity of passwords, enabling security logs, etc.<br><br>**Distributed Denial of Service (DDoS) protection–** A system is implemented that analyzes incoming data, detecting abnormal traffic and, where possible, blocking potentially dangerous packages.<br><br>**Logging** - The logs of the infrastructure servers for privileged access to the systems are collected and stored in compliance with legal requirements. These logs are periodically verified by the Security Team through internal audits. The application logs of the operations carried out during use of the services are made available to customers.<br><br>Likewise, the work of System Administrators is subject to verification by the data controllers at least once a year, in order to check compliance with the organisational, technical and security measures concerning the processing of personal data, provided for under current regulations.<br><br>**Monitoring and Alerts** - The critical systems of the Service are controlled by a continuous monitoring system. The system has the ability to generate "alerts", in the form of email or SMS messages, which allow you to promptly inform the personnel in charge of a potential accident or disruption, so that the necessary actions can be implemented as soon as possible.<br><br>**Backup (where the Aruba Group is responsible)** - The functional components for delivering the service, user management and other architectural components of the service follow the backup procedures defined at company level, which are periodically verified and tested. | **Backup** - The cloud services offered by the Aruba Group allow customers to create and set up their own automated backups through the Cloud Backup and Bare Metal Backup solutions, choosing their own policies in terms of encryption, frequency, type (complete or incremental) and other specific needs.<br><br>The optional **Disaster Recovery as a Service (DRaaS)** also allows you to test the failover procedures without any interruptions.<br><br>All the procedures for managing the backup and restore services are performed independently by the users and are described in the service's Knowledge Base (KB) on the dedicated page, where the various methods that can be used to backup data are also described.<br><br>No other backup copy of the data is made other than those independently defined by the users.<br><br>**Logging** – The Aruba Group provides customers with the application logs they produce when using the services.<br><br>• Cloud PRO: the user can view logs for operations on virtual machines such as creating, deleting, storing, restoring, turning on, turning off, resetting, changing passwords, changing features, creating, deleting and restoring snapshots.<br>• Cloud VPS (SMART): the user can view logs for operations on virtual machines such as creating, deleting, turning on, turning off, resetting and upgrading.<br>• Virtual Switches: the user can view logs for operations on Virtual Switches such as purchase and removal and feature changes.<br>• Public IPs: the user can view logs for operations on Public IPs such as purchasing and removing a public IP, managing and changing the reverse DNS.<br>• Balancers: the user can view logs for balancer operations such as creating a balancer, editing a balancer, balancer |

| Attachment A - ISO 27001:2017<br>The Security aspects of the Aruba Group's Cloud | | | |
|---|---|---|---|
| **Control Area** | | **Our controls** | **Tools and features available to the Customer** |
| | | **Antivirus** - All devices in the Aruba Group's network are controlled, monitored and protected by EDR systems. EDR (Endpoint Detection and Response) technology monitors known and unknown threats across all endpoints and company servers in real-time and proactively. A dedicated group with 24-hour coverage is responsible for analyzing anomalous events and intervening promptly.<br><br>**Vulnerability Management process** - The entire Aruba Group perimeter is regularly scanned by automated tools and by qualified industry professionals in order to identify any possible or potential vulnerabilities. Any critical issue identified is immediately reported to the competent group, thereby starting a problem resolution cycle that may end with a new release or with a mitigation (e.g. virtual patching). Finally, to verify its effectiveness, another scan is performed to make sure that the system has recovered from the vulnerability.<br><br>**Capacity Management and Change Management** - In order to ensure proper delivery/provision of the service, the Aruba Group believes that it is essential to monitor available resources, to analyze capacities and to adopt appropriate precautions for their optimal exploitation and to ensure the normal use of services.<br><br>The levels of connectivity, the levels of resource occupation, disk space and the sizing of the infrastructure are monitored with specific tools by the group of operators belonging to the Network Operation Center (NOC), 24/7/365, whose task also extends to monitoring any anomalous event.<br><br>The monitoring tools allow the setting of specific controls for each service, detecting anomalies and making it possible to anticipate the need for change.<br><br>The changes made necessary by the monitoring and capacity management activities are managed in a controlled manner so that the results can be verified and to keep track of the activities carried out.<br><br>**Updates and Patching** - All systems are periodically updated and patched using centralized tools and following internal procedures that require testing first in the development environments. Once this | deletion, enabling or disabling a balancer, adding, editing and removing rules.<br>• Unified Storage: the user can view logs for operations on the Virtual Switches such as purchase and removal and feature changes.<br>• FTP service: the user can view logs for operations on FTP accounts such as activating and removing and editing space.<br>• Private Cloud: the user can view logs for operations on their Private Cloud such as creation, deletion and changes to resources.<br>• Cloud Backup: the user can view logs for operations on their backup accounts related to creating, deleting and changing the plan, changing or resetting passwords.<br>• Cloud Monitoring: the user can view logs for operations on their monitoring services and related controls such as creating a monitoring plan or adding a new control, deleting a monitoring or control plan, changing the monitoring plan or a single check.<br>• Cloud Object Storage: the user can view logs for operations on their Object Storage accounts in connection with creating, deleting and changing the plan, changing or resetting passwords.<br>• Domain Center: you can view logs for operations on your domains and DNS in connection with adding a new domain, domain deletion and changes to domain data, DNS creation, DNS deletion, changes to any DNS records.<br>• Jelastic Cloud: the user can view logs for operations on their Jelastic Cloud accounts in connection with creating, deleting and changing the plan, changing or resetting passwords.<br>• Database as a Service (DBaaS): the user can view logs for operations on their "Database as a Service" accounts relating to creating, deleting and changing the plan, changing or resetting passwords, |

| Attachment A - ISO 27001:2017<br>The Security aspects of the Aruba Group's Cloud | | | |
|---|---|---|---|
| **Control Area** | | **Our controls** | **Tools and features available to the Customer** |
| | | step has been completed, they are applied in the production environment.<br><br>**Synchronisation** - All Cloud systems use the NTP system to synchronise their clocks and maintain event consistency. The authoritative source for clock synchronisation is INRiM (http://www.inrim.it). The time zone on all systems used is CEST, with the exception of UK time where GMT is used. All VMs provided have a CEST-based time zone and use the host on which they are installed as the source for their clock synchronisation<br><br>**Multitenancy and Secure Data Erasure– The Aruba Group** guarantees a multitenancy system that makes it possible to separate requests of individual customers from one another and to separate the customers' requests from those of the Cloud Service Provider.<br><br>The Aruba Group has specifically developed the public cloud control panel as a multitenant solution in accordance with the guidelines for secure programming and, it only allows access and control of the customer's own Cloud Infrastructure. In addition, for PRO, VPS and Private Cloud services, and whenever external software is used, multitenancy is guaranteed directly by the virtualization systems used.<br><br>When the service is closed, or when the credit runs out, as defined in the contract, the Aruba Group will delete and permanently remove the data from the Cloud services as described at https://kb.cloud.it/account-aru/utilizzo-del-credito/cosa-avviene-ad-esaurimento-del-credito.aspx. Depending on the service, deletion can take place through APIs, technical control panels, scripts or specific software.<br><br>The Aruba Group uses a defined process to manage the periodic deletion of temporary files from its cloud systems. | backing up and restoring databases and restarting instances.<br><br>**Capacity Management** - With regard to customer capacity management, the Aruba Group allows the customer to constantly monitor the consumption of the financial and technical resources at their disposal, also allowing forecasting.<br><br>In addition, when purchasing the service, a description is provided of the cases in which there are limits to the expandability of resources.<br><br>**Synchronisation** - When it is believed that clock synchronisation may be difficult for the customer, detailed information is provided in the public Knowledge Base (for example, on the scheduled operations page) or in the control panels.<br><br>**Multitenancy**<br><br>Cloud PRO. Multitenancy is guaranteed:<br><br>• By the public cloud control panel specifically developed as a multitenant solution by the Aruba Group and by the authenticated public APIs. These solutions only allow access to and governance of your Cloud infrastructure.<br>• By the Hyper-V and VMware virtualisation system. The customer only has access to their Virtual Machines (VMs) that the underlying hypervisors keep logically isolated from others. The VMs provided to the customer are installed with access control tools whose credentials are chosen directly by the customer during creation. The login tools that come with the equipment are SSH for Linux environments and RDP for Windows environments. Public networks are shared by customers but on all the equipment made available there is a perimeter firewall for customer use. In addition to this, the customer has the opportunity of purchasing the Virtual Switch service which consists of the provision of a dedicated VLAN not shared with other customers on which the |

| Attachment A - ISO 27001:2017<br>The Security aspects of the Aruba Group's Cloud | | | |
|---|---|---|---|
| **Control Area** | | **Our controls** | **Tools and features available to the Customer** |
| | | | customer can interconnect respective equipment for maximum segregation.<br><br>Cloud VPS (SMART). Multitenancy is guaranteed:<br><br>• By the public cloud control panel specifically developed as a multitenant solution by the Aruba Group and by the authenticated public APIs. These solutions only allow access to and governance of your Cloud infrastructure.<br>• By the VMware virtualisation system. The customer has access only to their VMs which the underlying hypervisors keep logically isolated from the others. The VMs provided to the customer are installed with access control tools whose credentials are chosen directly by the customer during creation. The login tools that come with the equipment are SSH for Linux environments and RDP for Windows environments. Public networks are shared by customers but on all the equipment made available there is a perimeter firewall for customer use.<br><br>Virtual Switch and Hybrid Link: these are resources dedicated to the individual tenant. Multitenancy is guaranteed by the public cloud control panel specifically developed as a multitenant solution by the Aruba Group and by authenticated public APIs. These solutions only allow access to and governance of your Cloud infrastructure.<br><br>Private Cloud. Multitenancy is guaranteed:<br><br>• By the vCloud Director control panel, specifically developed by VMware in multitenant mode. This control panel only allows access to and governance of your Cloud infrastructure.<br>• By the VMware virtualisation system. The customer only has access to their VM Virtual Data Center which the underlying hypervisors keep logically isolated from the others. The VMs provided to the customer are installed with access control tools whose credentials are chosen directly by the |

| Attachment A - ISO 27001:2017<br>The Security aspects of the Aruba Group's Cloud | | | |
|---|---|---|---|
| **Control Area** | | **Our controls** | **Tools and features available to the Customer** |
| | | | customer during creation. The login tools that come with the equipment are SSH for Linux environments and RDP for Windows environments. A perimeter software firewall (NSX Edge) is available on each Virtual Data Center provided, which allows the isolation of its Virtual Data Center from the others and allows the customer to configure the optimal security rules for respective purposes. The customer has the option to independently create dedicated private networks that are not shared by other customers for configuring their own architecture. If required, public networks can also be provided as dedicated networks not shared with other customers.<br><br>Bare Metal Backup. Multitenancy is guaranteed:<br><br>• By the public cloud control panel specifically developed as a multitenant solution by the Aruba Group and by the authenticated public APIs. These solutions only allow access to and governance of your Cloud infrastructure.<br>• By the Veeam control panel. Customers only have access to their own backup dataset and have no way of seeing or controlling other customers' backup systems.<br><br>Disaster Recovery. Multitenancy is guaranteed:<br><br>• By the public cloud control panel specifically developed as a multitenant solution by the Aruba Group and by the authenticated public APIs. These solutions only allow access to and governance of your Cloud infrastructure.<br>• By the Zerto control panel. Customers only have access to their own data set and have no way of seeing or controlling other customers' Disaster Recovery (DR) systems. |

| Attachment A - ISO 27001:2017<br>The Security aspects of the Aruba Group's Cloud | | | |
|---|---|---|---|
| **Control Area** | | **Our controls** | **Tools and features available to the Customer** |
| | | | Cloud Backup (Evault/Commvault). Multitenancy is guaranteed:<br>• By the public cloud control panel specifically developed as a multitenant solution by the Aruba Group and by the authenticated public APIs. These solutions only allow access to and governance of your Cloud infrastructure.<br>• By the Evault or Commvault backup system. Customers only have access to their own backup dataset and have no way of seeing or controlling other customers' backup systems.<br>Cloud Monitoring: Multitenancy is guaranteed by the public cloud control panel specifically developed as a multitenant solution by the Aruba Group and by authenticated public APIs. These solutions only allow access to and governance of your Cloud infrastructure.<br>Cloud Object Storage: Multitenancy is guaranteed:<br>• By the public cloud control panel specifically developed as a multitenant solution by the Aruba Group and by the authenticated public APIs. These solutions only allow access to and governance of your Cloud infrastructure.<br>• By the Scality Identity and Access Management system. Customers only have access to their own storage account and have no way of seeing or controlling other customers' accounts.<br>IaaS for SAP HANA: Multitenancy and segregation are guaranteed thanks to various measures: Through a dedicated SSL VPN that allows the customer to access the platform management system. Through a unique account on the VMware virtualization system that allows access to the customer's VMs only. Through the segregation offered by the dedicated network, made available to the customer and not shared with other customers. Through the internal tools provided with the |

| Attachment A - ISO 27001:2017<br>The Security aspects of the Aruba Group's Cloud | | | |
|---|---|---|---|
| **Control Area** | | **Our controls** | **Tools and features available to the Customer** |
| | | | VM that make it possible to create multiple user and administrative profiles.<br><br>Domain Center: Multitenancy is guaranteed by the public cloud control panel specifically developed as a multitenant solution by the Aruba Group and by authenticated public APIs. These solutions only allow access to and governance of your Cloud infrastructure.<br><br>Jelastic Cloud: Multitenancy is ensured in two ways:<br><br>• By the public cloud control panel specifically developed as a multitenant solution by the Aruba Group and by the authenticated public APIs. These solutions only allow access to and governance of your Cloud infrastructure.<br>• By the Jelastic system: customers have access only to their Jelastic account and have no way of seeing or controlling other customers' accounts.<br><br>Database as a service (DBaaS): Multitenancy is guaranteed by the public cloud control panel specifically developed as a multitenant solution by the Aruba Group and by authenticated public APIs. These solutions only allow access to and governance of your Cloud infrastructure. |
| **A.13** | **Communication security** | **Firewall and IPS** - The web portals provided for the services are protected by the cloud service data center firewall and protected by IPS.<br><br>As far as computing services are concerned, all virtual machines provided by the Aruba Group are modelled and made available in the form of images. These images are produced and tested by Aruba Group technicians and, in particular, after installing the Operating System and carrying out the first configuration, the firewall system is enabled, | **Firewall** - Customers are the administrator of their own server and therefore have the ability to change the firewalling settings. The guides and tutorials in the KB provide information on how to segregate and protect network security and set up a firewall on the customer's own cloud.<br><br>**Virtual Switch** Customers have the option to purchase the Virtual Switch service which includes the provision of a dedicated VLAN |

| Attachment A - ISO 27001:2017<br>The Security aspects of the Aruba Group's Cloud | | | |
|---|---|---|---|
| **Control Area** | | **Our controls** | **Tools and features available to the Customer** |
| | | granting the least possible privileges and opening only the necessary doors.<br><br>**Virtual Private Network (VPN)** - Remote access to the company's network (LAN) is granted only to authorized personnel requiring such access; remote access is possible only through a VPN that ensures: confidentiality of communication, strong server authentication and strong (two-factor) user authentication. | that is not shared with other customers, on which customers can interconnect their machines for maximum segregation, with the ability to independently create dedicated private networks, not shared by other customers, for configuring their own architecture (Private Cloud).<br><br>If required, public networks can also be provided as dedicated networks not shared with other customers.<br><br>**Geographical location of data to guarantee Security and Compliance** - Alternatively, services delivered by the Aruba Group can be activated on the basis of a data center or regionally (which corresponds to a country).<br><br>Customers have the option of specifying the Data Center or Data Centers in which their services are to be activated and their data transferred; for services provided on a regional basis, customers have the option of selecting the country within which to activate the service.<br><br>Under no circumstances does the Aruba Group move systems or content outside of the geographical locations (data center or regions) configured by its customers. |
| **A.14** | **Systems acquisition, development and maintenance** | **Managing Changes** - Changes to the application software are subject to evaluation and approval before they are implemented; they are then tested before proceeding to production, in order to verify the correct implementation of the new features and the absence of regressions. In addition, all the software developed is managed by a versioning system. | **Managing Changes** – The Aruba Group provides customers with a changelog (as described in the dedicated KB page) to inform them of releases, fixes, corrections and updates to the services. |
| **A.15** | **Relations with suppliers** | **Managing Suppliers** - The Aruba Group has a corporate policy that governs relations with suppliers. The policy provides that, for the proper definition and management of relationships with each new supplier, the following aspects, among others, must always be taken into account, with particular attention to information security:<br><br>• risk assessment and preliminary investigations to be carried out for the complete evaluation of the new supplier; | |

| Attachment A - ISO 27001:2017<br>The Security aspects of the Aruba Group's Cloud | | | |
|---|---|---|---|
| **Control Area** | | **Our controls** | **Tools and features available to the Customer** |
| | | • the selection of contract clauses, in order to assess whether standard contracts cover the risks identified, or whether it may be necessary to add/amend specific clauses;<br>• control of access to information, to provide access to the supplier in accordance with the "Need-to-know" principle, and thus only to the data and information that are actually required and necessary for the performance of respective activities;<br>• control of access to Aruba Group systems, if the deliverable enables the supplier to access the systems, through specific users, using a Private Network (VPN) and a specific detection response and virtual desktop infrastructure (VDI) system provided by the Aruba Group;<br>• monitoring of non-conformities, for the regular performance of checks, in order to verify the supplier's compliance with agreed contractual requirements, and the security of information.<br>In addition, external supplies necessary for the development, maintenance and provision of the Service are subject to checks designed to mitigate the risk of security incidents caused by non-compliant material or improper actions by suppliers. All providers of professional services are required to sign a non-disclosure agreement (NDA).<br>The contractual models used by the Aruba Group for delivering the service provide for the possibility of the Aruba Group using third parties to carry out its activities. This collaboration is based on the Aruba Group's commitment, stipulated in contracts with any subcontractors, to verify that, based on the type of service provided, they are able to comply with the same requirements and levels of security to which the Aruba Group is committed. The Aruba Group keeps a list of service subcontractors, available to customers on request. Likewise, when new/additional subcontractors are taken on, the Aruba Group undertakes to notify its customers well in advance in order to allow the latter to raise any objections or to withdraw. | |
| **A.16** | **Managing information security incidents** | **Information Security Incident Management Process** - The Aruba Group has identified and documented, within a specific policy, its structured and programmed approach to the management of | |

| Attachment A - ISO 27001:2017<br>The Security aspects of the Aruba Group's Cloud | | | |
|---|---|---|---|
| **Control Area** | | **Our controls** | **Tools and features available to the Customer** |
| | | information security events and incidents that may occur in the context of the operations of the companies of the Aruba Group, applying the ISO 27035 guideline in its information security incident management flow.<br><br>This process is implemented through a specific plan which determines the operational measures that must be implemented in the event of Information Security Incidents.<br><br>An incident management flow has been defined and the responsibilities related to its application have been identified, both in terms of incident management and resolution and in terms of strategic support for the timely adoption of the decisions necessary for dealing with the most relevant Security Incidents (for example Major incidents, Unknown Incidents, Data Breaches).<br><br>Timelines and procedures have also been defined for the preparation and delivery of communications relating to information security incidents to authorities, customers and third parties. | |
| **A.17** | **Information security aspects of managing business continuity** | **Disaster Management Procedure – The Aruba Group** has drawn up a Business Continuity Plan and specific procedures relating to the services that are essential for the operation of the Data Centers (electricity, air conditioning and connectivity).<br><br>Operational continuity is guaranteed by the servers installed at the **Arezzo Data Centers** (IT1 and IT2), on an "online-online" basis. For each component of the service present at the Gobetti IT1 DC, there is a twin within the Ramelli IT2 DC; this guarantees permanent operation, as the twin component is online and the service is usable by both parties. | **Disaster Recovery as a Service (DRaaS) – The Aruba Group** provides the Disaster Recovery solution as a service designed to guarantee business continuity for companies, enabling them to quickly replicate and restore access and functionality for their IT infrastructure after an interruption due to a cyber attack, failure or disastrous event.<br><br>Using a self-service Web Control Panel with a secure connection, customers can create Disaster Recovery guidelines and policies by selecting a source (the Primary Site) and a destination (the Secondary Site) of their choice from their own on-premise VMware virtual infrastructure and Aruba Group data centers with the Private Cloud service enabled. |
| **A.18** | **Compliance** | **Protection of Personal Data** - All services are provided in full compliance with the regulations in force regarding the protection of personal data, in accordance with Regulation (EU) 2016/679 | |

| Attachment A - ISO 27001:2017<br>The Security aspects of the Aruba Group's Cloud | | | |
|---|---|---|---|
| **Control Area** | | **Our controls** | **Tools and features available to the Customer** |
| | | ("GDPR"), Legislative Decree 196/2003, as amended by Legislative Decree 101/2018, and the Provisions of the Data Protection Authority.<br><br>**Auditing** - Events recorded with tracking, particularly those that could indicate a security threat, are periodically analyzed.<br><br>**Internal Inspections** - The auditing and inspections manager makes sure that checks are carried out on the compliance of the cloud service with the provisions of this document and the regulations in force, at least once a year. | |