PRODUCT DATA SHEET

SUPPLEMENTS THE HPE DATA PRIVACY AND SECURITY AGREEMENT SCHEDULE

	Aruba Central
Aruba* performs the following Services:	Services provide Aruba WLAN network management and monitoring. Additional functionalities are offered in forms of various apps running with Central, which includes but is not limited to, guest Wi-Fi access, Wi-Fi users analytics, network health, etc. This is a SaaS solution. For more info check out Aruba Central.
Customer Personal Data	Data collected as part of network management and related applications include: • Device MAC • Device IP • Device Operating System • Device Host-name • User-name • Email (in case of guest self-registration) • Phone (in case of guest self-registration) • Social media identity (in case of guest social login)
Data subjects to whom Customer Personal Data pertains are	Customer's client /end user /employee /contractor and temporary worker
With respect to Customer Personal Data, Customer is acting as	Controller
Aruba shall process Customer Personal Data only as follows:	**Provision of Services:** The information gathered and stored by the product is the minimum required to ensure secure access to the portal, and essential to performing its function. All session logs about a user will be automatically purged after 90 days. **Support Services:** Access to customer environment and data for troubleshooting is provided to Aruba support services based on customer agreements and permissions

* Aruba, a Hewlett Packard Enterprise company, is referred throughout this document as Aruba

	Aruba Central
Security and encryption	**Product Security features:** • **Physical Security:** Aruba Central is hosted in the most widely adopted IaaS platform - Amazon Web Services (AWS) that offers the most comprehensive security and compliance features. AWS has put in place security measures around all critical areas including perimeter, infrastructure, data and environment layers. • **Network Security:** We use services and tools that the IaaS provider offers and some 3rd party solutions to make sure our production environment is as secure as it can be from external threats and internal vulnerabilities. The production instance is deployed in its own Virtual Private Cloud (VPC) on the IaaS providers cloud. • **Application Architecture and Security:** All traffic that is exchanged between the Central application and the outside world is done using HTTPS over SSL. All traffic flow is encrypted using AES encryption technology. Different applications tiers such as web, app and db are designed to operate in a whitelist framework. Only necessary and required communication paths are allowed between tiers. Each instance within a tier is protected by firewall rules to prevent any unauthorized or malicious access. • **Data Security:** All data exchange between the application and devices and users happens using HTTPs. Data is rest is encrypted and stored. Data backup occurs on a regular basis and backup data is stored in a redundant manner. • From an organization perspective we have a devsecops team that manage all security and operational aspect of the app.
Third Party Security Certifications:	None today
Privacy-specific certifications:	None today