iQuila Ltd

Product Security Policy

IQ22095r1

This Document Applies to:

iQuila Cloud

iQuila Enterprise

Product Security Policy for iQuila Cloud & Enterprise Product ranges

This document addresses the processing of personal or personal identifiable data by iQuila Ltd.

iQuila Cloud is a hosted connectivity solution based in selected Data Centres which conform to ISO270001 & AICPA – SOC2 regulations. iQuila Cloud does not access or process any data unless it is provided to iQuila by the Customer.

iQuila Enterprise is an on-premise solution and is not hosted or operated by iQuila Ltd. iQuila Ltd does not access or process any data from it unless it is provided to iQuila ltd by the Customer.

Overview of iQuila Capabilities:

iQuila is a unique connectivity software enabling Layer 2 connectivity over standard internet connections. It secures endpoint devices and delivers multiple security services to protect the enterprise. It also provides visibility to devices which are part of the extended LAN network. iQuila Ltd LAN security services include functions such as remote access, Layer 2 Bridging, web security features, and Active Directory protection including end to end military grade encryption.

1. Personal Data Processing.

The table below classifies any personal data used by iQuila Cloud services to carry out the services and the purpose of that data. All data is held in encrypted form and is not accessible by iQuila Ltd, it is used by the customer for connections.

iQuila Enterprise is an on-site solution and does not transmit any data to iQuila Ltd

Personal Data Category	Types of Personal Data	Purpose of Processing
Connection Data	❖ IP Address of user's device ❖ User ID and/or usern a m e ❖ Host ID ❖ MAC Address ❖ User passwords ❖ Destination host name for the applicable firewall.	To create and maintain the end user's connection with the applicable firewall and/or router.

2. Cross-Border Transfers.

The iQuila Enterprise Solution is not hosted or operated by iQuila Ltd, nor does it send data to iQuila Ltd. Accordingly, iQuila Ltd does not make or access cross-border transfers of personal data processed.

The iQuila Cloud Solution is hosted by iQuila Ltd in Data Centres which conform to ISO270001 & AICPA – SOC2 regulations. Customer's select in which jurisdiction they wish their service to be hosted and, as such, no cross-border transfers of personal data are processed.

3. Access Control

The table below lists the personal data used by iQuila Ltd to carry out the service, who can access that data, and why.

Personal Data Category	Who has access	Purpose of the access
❖ Connection Data	❖ Customer	❖ To create and maintain the end user's always on connection.

4. Data Portability.

Customer may export Network Visibility Module Data to a data store controlled by the customer.

5. Data Deletion & Retention.

iQuila Cloud services delete customer connection data upon termination of the service

iQuila Enterprise is an on-premise solution and therefore data deletion and retention is determined and managed by the Customer.

Personal Data Category	Retention Period	Reason for Retention
❖ Connection Data	❖ Only retained while the applicable connection is established. iQuila Cloud does not retain this data once the applicable connection is terminated.	❖ To create and maintain the end user's connection with the applicable firewall and/or router.

6. Third Party Service Providers (Sub-processors).

iQuila Enterprise is an on-premise solution and therefore use of third party service providers or sub- processors is determined by the Customer.

iQuila Cloud Services are based in internationally recognized Data Centers which have the highest security compliance.

7. Information Security Incident Management.

Breach and Incident Notification Processes

iQuila Ltd Security & Trust Team coordinates the Data Incident Response Process and manages the enterprise-wide response to data-centric incidents. The Incident team works directly with the CTO to direct and coordinate iQuila`s personnel including the Incident Response Team and the Advanced Security Group.

The CTO manages the receipt, investigation, and public reporting of security vulnerabilities related to iQuila products. iQuila`s management team details the process for reporting security incidents.

iQuila Ltd customers receive important product and technology information, including security advisories for critical and high severity security vulnerabilities by email. This service allows Customers to choose the timing of compliance. If you have questions or concerns about any product or security notifications, contact your iQuila sales representative.

8. Certifications and Compliance with Privacy Laws.

iQuila Ltd risk and compliance management services ensure security and regulatory compliance in the design of iQuila products and services to meet the obligations under the EU General Data Protection Regulation and other privacy laws around the world.