IQAX Gateway – SaaS Deployment Operation Service Scope

1. The Services shall comprise:

1.1. IQAX Gateway SaaS Deployment - Operation Services

1.1.1. Background

This section applies to the IQAX Gateway users who use the Software-as-a-Service ("SaaS") deployment mode only. IQAX will provide RESTful APIs in accordance with the published IQAX standard functional specification hosted in the IQAX managed environment for users' internal use. The users are also granted to use the subsequent version update of SaaS Deployment subscription.

1.1.2. Service Scope

The following table sets out the description of operation services of the IQAX Gateway SaaS Deployment mode:

1. Customer Service	
i. IQAX Gateway SaaS Deployment Enablement	• Prescribe IQAX Gateway SaaS implementation plan • Perform IQAX Gateway SaaS Customer on-boarding
ii. Customer Enquiry	• Serve general customer enquiry and IQAX Gateway on-boarding service request
iii. Customer Support	• Serve IQAX Gateway customer's technical enquiry
iv. IQAX Gateway SaaS Support	• Provide monitoring tools to monitor IQAX Gateway application • Monitor IQAX Gateway SaaS availability and operation stability • Conduct IQAX Gateway SaaS problem diagnosis and resolution
v. IQAX Gateway SaaS Release	• Notify Downtime Maintenance Schedule to IQAX Gateway SaaS Customer • Deploy latest release to serve IQAX Gateway SaaS Customer
vi. 3rd Party Software Update	• Perform software update of third-party software • Review the necessity and urgency of the software update and version upgrade • Execute third-party software update

2. Cybersecurity Defense	
i. Defence against Attack	• Use security products/services to defend against attack
ii. Vulnerability Monitor & Resolution	• Monitor and detect security vulnerabilities • Identify impact to IQAX Gateway SaaS Service • Use reasonable effort to provide fix or workaround to mitigate impact from vulnerabilities
iii. Cyber Attack Recovery	• Monitor Cyber Attack event • Conduct problem diagnosis and impact analysis • Use reasonable effort to identify and proposed solution to recover IQAX Gateway SaaS from Cyber Attack
3. Data Protection	
i. Data Protection	• Perform data backup based on backup schedule • Verify backup data to ensure its validity
4. Information Security	
i. Information Security	• Maintain IQAX Gateway SaaS IT assets compliance to ISO27001:2013 standard controls • Conduct penetration test annually at least to OWASP, OSSTMM, PTES

1.1.3. Helpdesk support

- The support services are available 24 hours 7 days a week by email and phone support channel, please check the support detail at https://www.iqax.com/en/contact/.
- The support teams are responsible for troubleshooting and resolving issues that are applicable to IQAX.