Quantum Terms & Conditions

Contents

SUPPORT TERMS **3**

1) SUPPORT OPERATING HOURS **4**

2) SERVICE LEVEL AGREEMENT **4**

3) SUPPORT OPERATIONAL PRACTICES **6**

4) COMMERCIAL TERMS **9**

5) INFORMATION SECURITY DATASHEET **10**

6) PRIVACY & DATA SECURITY **11**

A. DATA COLLECTION & PROCESSING 11

7) TECHNICAL OVERVIEW **12**

A. ARCHITECTURE & PLATFORM OVERVIEW 12
B. API 13
C. HTTP://EA.AZURE.COM/ ENTERPRISE AGREEMENT SUBSCRIPTION BILLING API 13
C. READ-ONLY ACCESS 13
D. APPLICATION READER PERMISSIONS 13
E. API KEY OWNERSHIP 13
F. DATA & ANALYSIS REFRESH CADENCE 14

8) DATABASE & APPLICATION SECURITY **14**

A. DATA ENCRYPTION 14
B. DATA SEGREGATION 14
C. DATABASE ACCESS 14
D. DATA BACKUP & RECOVERY 14
E. WEB APPLICATION SECURITY 15
F. PENETRATION/VULNERABILITY TESTING AND REMEDIATION 15
G. USER ACCESS CONTROL 15
H. SYSTEM AND AUDIT LOGGING 15
I. DATA PROCESSING AND TRANSFER POLICY 15

9) SURVEIL (QUANTUM) SOFTWARE AS A SERVICE (SAAS) END USER TERMS AND CONDITIONS **16**

Support Terms

Summary

Bytes shall grant access to the Bytes Service Desk for the purpose of reporting incidents and logging service requests. This will allow Bytes to deliver remote support for the in-scope applications, providing access to application specific experienced/expert technicians.

Bytes will provide telephone and portal-based support for break/fix incidents and service requests for in-scope platform and applications in accordance with these Support Terms. Providing access to application specific experienced/expert technicians, the management and coordination of escalation to the 3rd line support services and consistent and clear communication between all interested parties.

Exclusions:

- The Quantum support specifically excludes: Technical or advisory support for Microsoft Azure and M365 environments.
- Storage and network configuration and monitoring support.
- Desktop support.
- Network and firewall support.
- Recommendations or best practices used to solve how-to scenarios that take advantage of Microsoft products.
- Changes to the Customer Cloud and On-premise environments.
- Generation of keys or application IDs.
- On site technical support.
- Licensing Support.
- Commercial Optimisation Support.

Dependencies:

The Quantum support has the following Customer dependencies. Failure to comply with these requirements may result in Bytes being unable to provide support:

- All users must have access to the supported in scope applications.
- All support incidents must be raised via the Bytes Service Desk portal.
- To raise/manage tickets via the Bytes portal, users must create an account when prompted.
- To optimise the support experience, users should raise tickets according to the Bytes portal user guide provided at time of registration.

1) Support Operating Hours

Operating Hours

Support Cycle	Service Desk Available	Operating Times
Core Business Hours	Yes	Weekdays, excluding bank holidays, 0900 to 1730
After Hours (Weekdays)	No	n/a
Out of Hours (Weekends & Bank Holidays)	No	n/a

2) Service Level Agreement

Support Incidents

Bytes will provide a response to an Incident within the periods of Operating Hours and use reasonable endeavours in meeting Target Response Time.

The service desk may downgrade the severity level if the customer is not able to provide adequate resources or responses to enable the service desk to provide continuous problem resolution efforts.

Priority Level	Priority Definition	Bytes Target Response Time SLA	Update Frequency
*Priority 1	**Complete loss of business-critical systems** Critical business impact. Complete service failure or inaccessibility of critical functionality. No acceptable workaround available.	2 Hours	24 hours
Priority 2	**Partial loss or degradation of a supported service.** Serious business impact. Widespread degradation of a service or failure of functionality of critical system. No acceptable workaround available.	4 Hours	48 Hours
Priority 3	**Low impact; business-critical systems unaffected, more than one user affected.** Partial/intermittent application degradation or loss of functionality. Typically impacting a subset of users. No direct impact on services availability. A workaround is available.	8 Hours	72 hours
Priority 4	**Minimal impact to non-critical systems.** Application or personal procedure unusable. A workaround is available, or a repair is possible. Threshold breaches with no impact on service.	24 Hours	72 Hours

Service Requests

Bytes will provide a response to a Service Request within the periods of Operating Hours and apply reasonable endeavours in meeting Target Response Time.

Priority Level	Priority Definition	Response Time SLA	Update Frequency
All Service Requests	**Standard Request** Standard service requests are for planned activity and will have no or limited business impact if they are not completed within accelerated timescales An example would be: User account creation/deletion; backup recoveries for auditing purposes.	24 hours	5 Days

3) Support Operational Practices

Incident Resolution Management

Ticket Resolution is defined as the rectification of an issue or service request. The severity level of a ticket may change during the resolution process. Bytes will exercise commercially reasonable efforts to resolve tickets.

Where Bytes is unable to resolve a ticket directly, and the ticket can be raised with a third-party support vendor, Bytes will facilitate the escalation.

A ticket will be deemed resolved as follows:

- The Customer has advised Bytes that the issue has been resolved.
- Where Bytes has received no reply from the Customer following three (3) attempts to contact the Customer about a ticket.
- Where, after commercially reasonable efforts of all parties, neither party is able to demonstrate definitively to both parties' mutual satisfaction that the tickets logged arises from the supported technology rather than any other technology, product or service including any third-party products.
- Appropriate answers to questions have been provided.
- Recommending a suitable workaround that corrects the problem temporarily without negatively impacting the environment. In this instance the workaround would be used until a long-term resolution can be delivered.
- In some instances, a long-term fix resolution may not be available at which point the workaround will be deemed a solution until a hot fix or similar becomes available.

In some circumstances, a fix may not be possible in the current version of the supported technology. In this instance, Bytes may log a feature request against to enhance the supported technology where this is commercially viable and prudent to do so.

Incident Management

For the purposes of reporting service desk performance, the following shall apply when tracking incidents and service request responses and resolutions. SLA timer is paused during the following ticket statuses:

- Escalated to Third Party/Vendor; or
- On-Hold; or
- Pending Customer Response; or
- Force Majeure Event; or
- Resolved.

Escalation Management

If customers are not satisfied with the handling of their case, they can request that case is escalated using the Bytes Services Support portal.

All requests for escalation assistance will be triaged for urgency and impact before being assigned to an appropriate Manager, who will coordinate with the customer, and internally to develop an action plan to remediate the escalation.

An escalation will be considered closed if it meets one or more of the following requirements:

- The initially agreed objectives have been achieved.
- A satisfactory monitoring period has elapsed without problem recurrence.
- The escalation has been reviewed and agreement reached to downgrade the case severity level.
- The customer has agreed that the issue is resolved.
- A mutually accountable decision has been made that the issue is resolved.

Bytes Responsibilities

Bytes shall;

- provide required personnel that are appropriately skilled and knowledgeable to deliver the services detailed within this Statement of Work.
- use reasonable endeavours to identify and resolve issues.
- use reasonable endeavours to ensure continuity of its personnel assigned to this agreement.
- provide a Service Desk and escalation facility for all reported level 2 and 3 incidents and request for information.
- provide a Self-Service Portal for approved Customer IT staff to lodge and track incidents and Service Requests.
- provide an email address for approved Customer IT staff to lodge incidents and service requests.
- capture and redirect out-of-scope Incidents and Service Requests.
- track, manage and report Service Token utilisation.
- identify, filter, and classify incidents to a priority level and handle according to agreed-upon incident response procedures.
- troubleshoot and diagnose incidents for all in scope service components.
- escalate incidents to the appropriate next-level service group within the Customer, or the Customer to manage Third Party as soon as it is clear that the incident is unable to be resolved without external assistance.
- maintain current and historical records of all tickets and the resolution of those calls for the life of the contract and provide reporting and trend capabilities.
- actively review the status of in scope open and unresolved incidents, and the progress being made to resolve them.
- upon resolution of a Bytes assigned Incident, carry out closure of the ticket by confirming with the Customer.
- receive and action incidents and requests from nominated Customer IT representatives.
- action reviewed and approved service requests.
- monitor and track service request progress through to final closure and record/update service request record status as appropriate.

Customer Responsibilities

The Customer shall;

- co-ordinate internal key personnel and attend meetings and conference calls relating to the Service.
- provide Bytes with all necessary co-operation in relation to this SoW.
- maintain a level of Service Tokens with Bytes to ensure anticipated use of the Service can be maintained.
- carry out all Customer responsibilities in a timely and efficient manner.
- use Bytes ITSM Toolset for Incident and Service Requests.
- provide Level 1 Service Desk support, triaging and assistance for inquiries about the features and usage of hardware and software defined within the scope of services.
- provide and maintain escalation contact list(s) for the Customer and Third-Party contacts.
- receive and action incidents and requests from Customer's end users.
- raise Major Incidents P1 to the Service Desk via telephone in addition to normal channels.
- approve Customer IT representatives raise service requests to Bytes for action.

Exclusions

Bytes are not obliged to resolve or work around any incident arising from or caused by:

- any factor external to the Services, such as third-party network outages.
- any modification (whether by way of alteration, deletion, addition or otherwise) made to any part of the Service by anyone other than Bytes.
- any equipment or third-party software or service used in connection with the Service and not supplied by Bytes.
- the failure to follow Bytes reasonable instructions in respect of the Services; or
- make any enhancements of, additions to, or customizations of, the functions and features of the Services.

Dependencies

Where remote access is required to investigate or correct an Incident, the Customer shall:

- provide Bytes with remote access connection and logon details.
- or host a web-based session through which Bytes can gain sufficient access to adequately undertake required investigation, analysis, and corrective work.
- unless otherwise agreed, all equipment required to perform the Service will be provided by the Bytes.
- where direct access is required to Customer systems, the Customer will provide any required IT equipment and credentials to facilitate such access to support the delivery of the Service.
- access to relevant Systems will be provided by the Customer as required for the sole purpose of delivery of support.

Assumptions & Constraints

The Customer will work with Bytes to be available during call resolution based on the severity of the case. If these response times cannot be met, the severity will be lowered, and the Customer will be advised.

Any recommended resolutions to cases will be implemented by the Customer in accordance with the Customer's change control processes.

The Customer authorises Bytes to escalate cases to the Vendor on behalf of the Customer although this does not make Bytes an agent of the Customer.

Bytes will not be responsible for any resolution or impact to the Customer's environment where cases are raised directly with the Vendor by the Customer.

Bytes will provide support only for Supported Product(s). Requests for support on products outside of support will be handled on a best endeavours basis and will not be governed by any SLAs.

Modifications to Support Terms

Bytes may update these Support Terms at any time, but in no event will Bytes materially degrade these Support Terms during the applicable Product Term for which Fees have been paid.

4) Commercial Terms

Pricing Notes for Quantum 365

The following outlines how the Quantum 365 SaaS (service) fees are calculated, the billing process, the procedure for service termination and payment terms.

Total Licensed Accounts: Accounts with assigned M365 Licenses. Excl. AD identities that do not have any M365 licences assigned against them.

Fees: Fees will be based on the "Total License Accounts" held within each associated tenant at the start of the service.

Billing Period: The billing period is end of calendar, monthly in arrears.

Billing Cycle: The number of licensed accounts reconciled monthly. If the actual number of licensed accounts is less than the number of licensed accounts determined at the start of the contract, the Customer will still be billed for the original quantity. Should the number exceed the original quantity, the Customer will be billed accordingly ("No True Down")

Unit Price: Unit Price is fixed for 12-month period.

Pricing Notes for Quantum Azure

The following outlines how the Quantum Azure SaaS (service) fees are calculated, the billing process, the procedure for service termination and payment terms.

Fees: The fees for the Service are calculated based on a percentage of the customer's monthly Microsoft Azure spend per customer tenant.

Billing Period: The billing period is end of calendar, monthly in arrears.

Billing Cycle: Customers will be charged for a full month regardless of the specific day the service start date. Invoices are generated at the end of each billing period.

e.g. If a customer subscribes to the service on any day of the month, they'll be charged for the entire month and then subsequent invoices will be generated at the end of each billing period. This ensures that billing is consistent and predictable for both Bytes and the Customer.

Payment Terms

Payment terms are in accordance with standard service provider payment and credit terms.

Service Termination

Either party may terminate the Service for any reason upon thirty (30) days written notice to the Bytes Account Manager. Upon termination, Customer shall immediately cease all use of the Service and Bytes will revoke all access and delete all customer data.

5) Information Security Datasheet.

Governance & Risk Management

Bytes operate an Information Security Management System ("ISMS") which, being externally audited on an annual basis, has achieved accreditation to the ISO27001 international standard.

The Bytes Group Head of IT, Kevin Beadon, is the owner/administrator of the accredited ISMS and is responsible for reporting on compliance and governance to the Bytes Executive Committee.

All activities related to the development, management and delivery of Quantum Azure are governed by the policies and procedures which form the basis of the accredited ISMS. The monitoring of compliance with required policies and procedures is continuous.

The catalogue of policies which form the basis of the ISMS have been communicated to all Bytes personnel and are freely available in an internal network location at all times.

All Bytes personnel are screened prior to employment in accordance with the requirements of the latest version of the BS7858 standard with the addition of the collection of character and employment references. This process is comprehensive and includes applicant, financial, employment and criminal checks.

All Bytes personnel receive periodic training in Information Security and have provided written confirmation that they have; completed the training, have read the policies and that they are aware of/accept their responsibilities as imposed by the ISMS. Non-compliance/breach of these responsibilities is a defined disciplinary matter.

All Bytes personnel have signed a legally binding confidentiality agreement. Non-compliance/breach of this agreement is a defined disciplinary matter.
Where a third-party trusted partner is engaged to provide development or support resource, the partner will operate an accredited ISMS (equivalent or greater than ISO27001), will operate policies and procedures which are the direct equivalent of those operated by Bytes and must maintain Microsoft ISV Gold certification.

Bytes leverage various policies and controls, such as in-transit and at-rest data encryption, tight access controls and strong authentication, network/infrastructure/application-layer security, and incident response.

What frameworks/standards does Bytes have in place?

Framework	**Status**
Cyber Essentials/Cyber Essentials Plus	Certified Organisations - Iasme Search: Bytes Software Services
IASME (Level 1)	
ISO Certifications (9001,14001,27001)	ISO Certification | Bytes
ICO Registration	Z6191945
CREST Certified	https://www.crest-approved.org/member_companies/bytes-software-services-ltd

6) PRIVACY & DATA SECURITY

Our data and privacy governance is supported by our privacy policy: Privacy Policy | Bytes

a. DATA COLLECTION & PROCESSING

What customer data does Quantum ingest for processing?
The platform needs read-only access to a number of types and categories of personal data for processing. In summary, they cover the following data types: identity, business contact, financial, transaction, technical, profile, usage, marketing and communication, plus aggregated data. No sensitive or special categories of personal data is required, ingested, or processed.

What is the purpose of collecting this data?
Quantum Azure is used to monitor and analyse public cloud consumption and costs to support effective cost management and drive savings.

For how long will data be collected and processed?
Processing will continue for the full term of the engagement as defined in the *Work Order* between the *Customer* and *Bytes*.

How does Quantum ingest customer data?
Customer data is ingested via read-only integration with Microsoft APIs. Following the onboarding process (via unique link), customers are guided through a very simple four-step procedure which requires Global Administrator credentials to authenticate.
Whilst onboarding via link is the preferred method, manual onboarding can also be undertaken when and if required.

Where is customer data stored and processed?
All application components and customer data are located within the Microsoft Azure UK South datacentre and are geo-locked to the UK only - for high-availability/failover purposes.

When and how is customer data deleted?
A Customer may, at any point during the engagement, request that their data be deleted from Quantum Azure storage by submission of request to the Bytes Service Desk. This request will be actioned within two (2) working days of receipt of the request and written confirmation of the deletion will be sent.
After thirty (30) calendar days have passed following the expiry of an engagement – where no renewal of service has occurred and/or where no renewal activity is taking place – all Customer data will be deleted from Quantum Azure storage and written confirmation of the deletion will be sent.
Data will be securely deleted following the documented Bytes ISMS procedure.
When Bytes receives a Subject Access Request directly from the Customer, we endeavour to process all requests within one month of receipt.

For all questions or queries related to data should be sent to: GDPR@bytes.co.uk.

7) TECHNICAL OVERVIEW

a. ARCHITECTURE & PLATFORM OVERVIEW

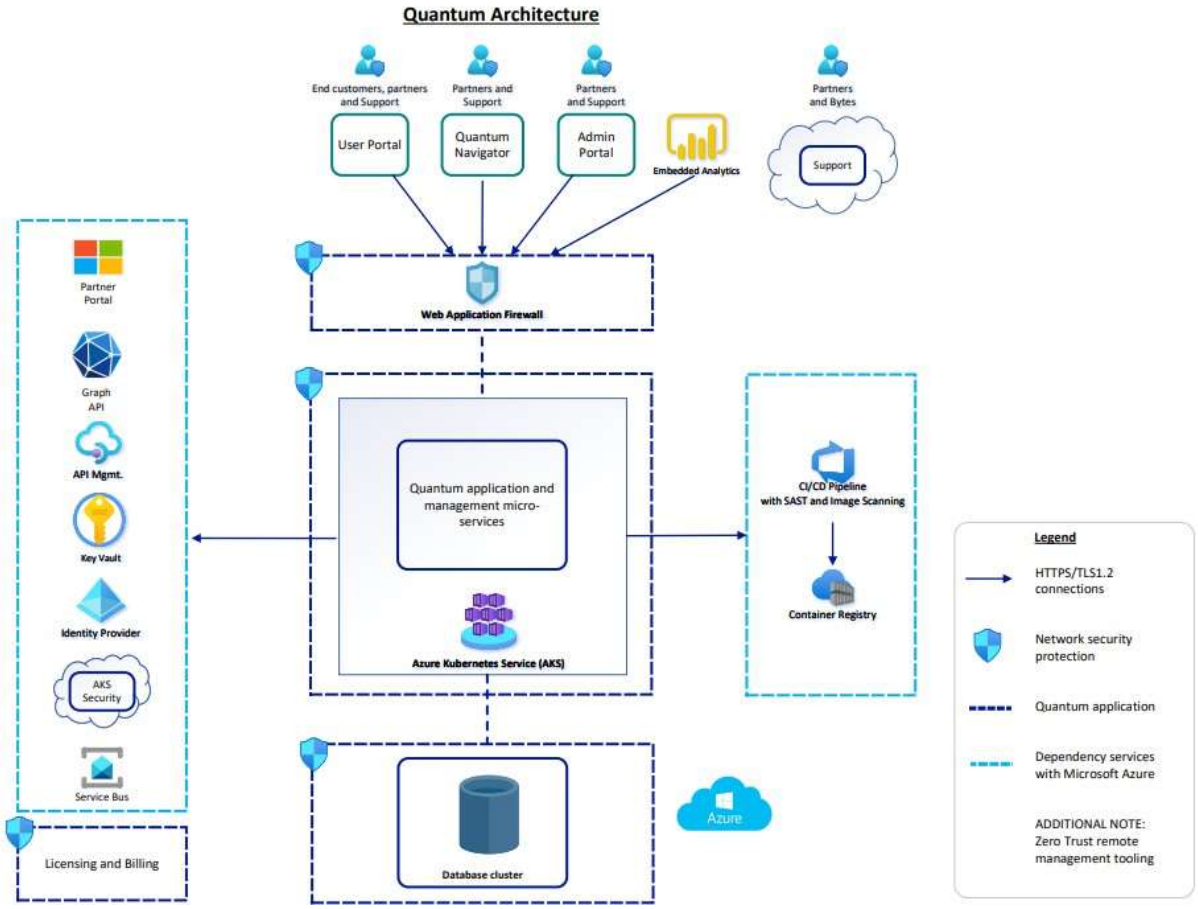
What network, infrastructure, and system security measures are in place?

Quantum runs as a container-based application on the Azure Kubernetes Service (AKS) platform, with segmentation applied between running micro-services internally and externally, from the front-end web application firewall, through network security groups (NSG) and API integrations, to accessing the database layer.

The application is fully hosted in the Microsoft Azure public cloud infrastructure allowing it to be completely scalable and to ensure high availability.

Hotfixes and feature enhancements are performed over an agreed release cycle without impacting its business operations.

There is both physical and logical data separation between environments (e.g. Test, UAT, Production) within the Microsoft Azure infrastructure. This is further augmented using Microsoft Azure Subscriptions with individual Virtual Networks.



b. API

Quantum Azure has a full set of API data points that can interface to existing systems directly or with minimal integration. It can take feeds from other systems via the API to enhance your experience and improve automation.

c. http://ea.azure.com/ Enterprise Agreement Subscription Billing API

Bytes specifically utilise six (6) of the available Azure EA Billing API data points to collect data for analysis by Quantum Azure:

1. *Balance and Summary API* - offers a monthly summary of information on balances, new purchases, Azure Marketplace service charges, adjustments, and overage charges.
2. *Usage Detail API* - offers a daily breakdown of consumed quantities and estimated charges by an Enrolment. The result also includes information on instances, meters and departments.
3. *Marketplace Store Charge API* - returns the usage-based marketplace charges breakdown by day for the specified Billing Period or start and end dates (one-time fees are not included).
4. *Price Sheet API* - provides the applicable rate for each Meter for the given Enrolment and Billing Period.
5. *Reserved Instance Usage API* - returns the usage of the Reserved Instance purchases.
6. *Reserved Instance Charges API* - returns the billing transactions made.

Where access is no longer available to the EA Portal, Quantum will make use of the Consumption API.

d. READ-ONLY ACCESS

Microsoft API integrations are exclusively read-only via REST XML, with authentication managed on an automated basis using the Azure Key Vault. Quantum Azure, by default, requires read-only access to all environments to obtain sufficient data to deliver the majority of the functionality of the product. Bytes use a proprietary AI engine to add context to the raw data and consequently there is no requirement to make changes in your environments to be able to analyse and present recommendations for optimal financial consumption.

e. APPLICATION READER PERMISSIONS

The Quantum system is configured in a way which does not allow for Azure Reader permissions to be added automatically for Azure subscriptions, and as such, requires the Azure Tenant Administrator to perform some manual actions for this to be achieved. To successfully onboard to Quantum Azure, Bytes will require the following:

- The User Account Name that has Azure AD administrative privileges to your Azure AD.
- The Azure Tenant Administrator should be a Global Admin, but must have the Owner role assigned to each subscription in scope Azure AD (portal.azure.com).
- This role must allow write permissions which will grant the Quantum application read access to the subscriptions in scope
- For EA customers, administrative permission to the EA Subscription(s) and access to your Azure EA Portal (https://ea.azure.com) will also be required.

f. API KEY OWNERSHIP

Provision of the access key for API data access to the Customer's Microsoft Azure tenant – which is required only for Customers accessing Azure through an Enterprise Agreement - is achieved using the Microsoft Azure Tenant (Read-Only). This ensures that the key remains in the full control of the tenant/Customer and can be voided or renewed at any point.

g. DATA & ANALYSIS REFRESH CADENCE

Type	Schedule
Azure Data Sync	01:30AM daily
Alerts Sync	Every four (4) hours
Security Alerts Sync	01:20AM daily
Security Scores Sync	01:25AM daily
Service Status Sync	Every twenty-four (24) hours
Quantum Azure Reports Refresh	Daily (after completion of Data Sync)

8) DATABASE & APPLICATION SECURITY

a. DATA ENCRYPTION

How does Bytes manage data security?
All data is encrypted at rest (with AES) and in transit (TLS 1.2 or above) – including between application and database. By default, access to the user/web interface uses a current version of the Transport Layer Security ("TLS") cryptographic protocol.

Access is controlled via tight technical policies and strong multi-factor authentication (MFA), with row-level data masking available where required, as an advanced custom solution request. Standard backup and data retention practices are in place; component and system status is proactively monitored.

b. DATA SEGREGATION

How is customer data segregated?
In addition to database storage encryption, as well as implementing data segregation and role separation, Quantum Azure leverages Microsoft PowerBI functionality and publishes separate workspaces for each customer for segregation purposes.
Furthermore, when data is collected, the Customer Tenant ID is appended to each record. This is used as a unique identifier/primary key to achieve logical separation for analysis, presentation, and access.

c. DATABASE ACCESS

Who has access to the database?
Only specific Application-related and Administrative IP addresses are permitted to connect to the database.

d. DATA BACKUP & RECOVERY

Quantum is supported by Bytes Backup and Business Continuity Management Policy – copies can be found on our website: GDPR Policies | Bytes

How is Quantum managed in the event of Disaster Recovery?
Data collected by Quantum Azure is only a copy of that maintained in each Customer's Microsoft Azure tenant and therefore loss or corruption of data held by Quantum Azure will not impact the source data which will remain untouched.
In the circumstance of complete/catastrophic loss of the Quantum Azure database, once an authorised API connection is re-established with the Customers Azure tenant, Quantum Azure data will repopulate immediately.
Regardless, backups of the databases are performed nightly to the Microsoft Azure Secure Vault area within the geo-locked region.
The infrastructure and code which deliver Quantum Azure are replicated daily using Microsoft Azure Site Replication functionality with the date being held within the geo-locked region.

e. WEB APPLICATION SECURITY

How is the Quantum web application secured?

The entire environment is front ended with Microsoft Azure Application Gateway and Microsoft Azure Web Application Firewall ("WAF") which leverage the latest Core Rule Sets from the Open Web Application Security Project ("OWASP").

f. PENETRATION/VULNERABILITY TESTING AND REMEDIATION

What are Bytes testing processes?

Annually as well as upon significant change, Bytes Internal CREST certified testing team penetration test the changes.

OWASP testing is completed annually by an independent certified partner. Where future testing identifies risks, they will be categorised in accordance with industry practice.

Risks which are identified as being in either "Critical" or "High" category will be remediated by application of patch/hot fix within two (2) weeks of the receipt of the test findings.

Risks which are identified as being either "Medium" or "Low" category will be assessed for impact and necessary remediation will be prioritised accordingly or else the risk will be logged and monitored as part of the periodic ISMS governance procedures.

Bytes conducts annual CE+ certification and vulnerability scans the internal and external estate.

Bytes conducts a CHECK ITHC on an annual basis that tests aspects of the whole estate including red team testing on the internal infrastructure - this is by an externally certified CREST and CHECK provider.

g. USER ACCESS CONTROL

How is user access to the platform granted and controlled?

Access to Quantum Azure is achieved using Microsoft Azure AD authentication – every user must have an Office365 account registered with their organisations Microsoft Azure AD implementation. Quantum Azure does not have access to nor does/can it store passwords.

If a Customer removes a user record from their Azure AD, access to Quantum Azure will automatically be removed.

During the initial onboarding into Quantum Azure, Customers will be asked to provide a list of authorised users who will then be provisioned with access. In addition, Bytes will provision access to necessary technical support resources and to the Bytes Account Manager/Director. Additional resources will only be provisioned access and have access removed upon receipt of specific authorisation.

h. SYSTEM AND AUDIT LOGGING

All activities, including usage, within the front-end and supporting database are logged and saved in an Audit Log.

Access to the tool is logged by the application and is similarly monitored and logged by Microsoft Azure AD and associated tools.

Irregular account behaviour is also monitored and logged using the functionality of the Microsoft Azure Security Centre suite of services.

i. DATA PROCESSING AND TRANSFER POLICY

All data collection, processing and transfer is aligned with Bytes Data Privacy Policy: Privacy Policy | Bytes

If further documentation is required and is not available on the website, please contact services@bytes.co.uk or log via the portal https://services.bytes.co.uk.

9) Surveil (Quantum) Software as a Service (SaaS) End User Terms and Conditions

1 **Terms and conditions**

1.1 Acceptance of terms and conditions:

(a) The Customer accepts the terms and conditions in effect at the time of supply of the SaaS.

(b) The Supplier may update these terms and conditions at any time and the current version of the terms and conditions as published on itexactglobal.com will apply to and be incorporated into all Agreements except that where a Fixed Term applies the updated terms and conditions will not apply for the remainder of the current Fixed Term but will apply for the renewal of that Fixed Term (if any) and any ongoing use beyond the end of the current Fixed Term (as applicable). Supplier will provide one month's written notice of any material change to these terms and conditions.

(c) Without limiting clause 1.1(b), the Customer's continued use of the SaaS confirms the Customer's acceptance to be bound by the latest terms and conditions.

(d) Any additional or different terms that the Customer may stipulate or state in any communication with the Supplier will not be binding on the Supplier or included in the Agreement unless expressly agreed in writing by the Supplier.

1.2 The 'Agreement' comprises the Customer Information, Selected Options, Relevant Pricing, these terms and conditions (as updated from time to time under clause 1.1(b) above) and the Support Schedule.

1.3 These terms and conditions apply to customers that purchase SaaS (or on whose behalf SaaS is purchased) and if there is a trial period available, these terms and conditions also apply to that trial period.

1.4 The SaaS is available from the Supplier directly and from Authorized Partners and is available at various Purchase Locations. Regardless of where the purchase is made, these terms and conditions apply as between the Supplier and the Customer.

1.5 All capitalized terms used in these terms and conditions have the meanings given to them in the definition section in clause 19.

1.6 Where someone other than the Customer purchases SaaS on behalf of the Customer that person is deemed to have authority to accept these terms and conditions for the Customer.

2 Trial

2.1 If a Trial is available to the Customer and the Customer elects to use the SaaS for a Trial, the Customer acknowledges that use of SaaS for the Trial is subject to these terms and conditions.

2.2 Trial period

(a) The Trial will commence when the Trial SaaS is made available to the Customer. In order for the Trial SaaS to be available to the Customer, the Customer will need to follow the steps outlined to the Customer by the Supplier, the Authorized Partner or at the Purchase Location, and accept these terms and conditions. The Customer acknowledges that the Trial is for the version of SaaS made available under the free trial offer, as hosted by the Supplier. The free trial will end on expiration of the Trial

Period, unless terminated earlier under these terms and conditions.

2.3 Provisioning for Trial

(a) The Supplier will provide the Trial SaaS to the Customer in accordance with these terms and conditions. The Supplier will:

i. provide the Customer with access to the Trial SaaS;

ii. provide assistance with use of the SaaS as reasonably requested by the Customer (or the Supplier will procure the Authorized Partner to provide assistance). The assistance will be available from the Customer during the hours notified by the Supplier, or the hours notified by the Authorized Partner or at the Purchase Location (as applicable). If no hours are notified, the Supplier or relevant Authorized Partner will use reasonable endeavours to provide assistance during their working day.

2.4 Common terms apply: Except for clauses 3, 5 and 6, all clauses of these terms and conditions apply to Trials (in addition to this clause 2).

3 SaaS

3.1 Provision of SaaS: The Supplier will provide the SaaS to the Customer in accordance with the Agreement. The SaaS is provided to the Customer on a non-exclusive basis and the Customer's right to use the SaaS is not transferable. The Supplier will provide log on access to the Customer to enable the Customer to access and use the SaaS.

3.2 SaaS Hosting and Availability: The Supplier provides the SaaS bundled with the Hosting. The Supplier's commitment to SaaS availability is the Monthly Uptime Commitment, which applies subject to the Exception Factors. Where emergency maintenance is necessary or where unplanned outages occur, this will be notified to the Customer as soon as possible after coming to the Supplier's attention. Where the Supplier does not meet the Monthly Uptime.

3.3 Commitment, and the failure to meet the Monthly Uptime Commitment is not due to any of the Exception Factors:

(a) a Service Credit may apply; and

(b) the Customer may submit a Claim to the Supplier.

If the Supplier, following its assessment of the Claim, determines that the Monthly Uptime Commitment was not met in the relevant period (and that this was not due to any Exception Factors), a Service Credit will apply (Service Credits are not available for every SaaS, refer definition of 'Service Credit' in clause 19).

SaaS Availability: The availability of the SaaS is dependent on factors outside of the Supplier's control and as such the Supplier cannot and does not warrant that the SaaS will be continuously available or available without interruption.

3.4 Exception Factors: The Exception Factors are:

(a) Planned Maintenance;

(b) lack of availability or outages of telecommunications networks (Supplier to provide evidence);

(c) a network or device failure external to the Supplier's or its third party provider's data centers, including at Customer's site or between the Customer's site and the Supplier's or third party's data centers;

(d) issues resulting from the Customer's use of infrastructure (including IaaS), software or services (other than the SaaS) including issues related to dependencies on the Customer's Integrated Services and Products;

(e) any third party act, omission or circumstance which results in unavailability of the SaaS, whether malicious or not (other than where the third party is a subcontractor engaged by the Supplier); and

(f) a Force Majeure Event.

3.5 Security Breach

(a) Without limiting any other legal obligations that the Supplier may have in the event of a security breach, the Supplier represents that it has used and will continue to use reasonable endeavours in designing and/or utilizing the SaaS Systems and in operating and managing the SaaS so as to minimize the risk of a Security Breach.

(b) In the event of any Security Breach:

i. the Supplier will, subject to all applicable laws, notify the Customer as soon as practicable after the Supplier becomes aware of the Security Breach;
ii. the Customer will notify the Supplier as soon as practicable, but no later than 24 hours after the Customer becomes aware of the Security Breach;

(c) subject to all applicable laws, immediately following notification of a Security Breach under clause 3.4(a) or (b) above, the parties will coordinate with each other to investigate the Security Breach. The Supplier will cooperate with the Customer in the Customer's handling of the matter, including, without limitation by assisting with any investigation, providing the Customer with physical access to the facilities and operations affected to the extent reasonably practical, facilitating interviews with the Supplier's employees and others involved in the matter and making available all relevant records, logs, files, data reporting and other materials required to comply with applicable law, regulation, industry standards or as otherwise reasonably required by Customer.

3.6 Data

(a) The Customer warrants that the Customer has the right and authority to deal with the Data in the manner contemplated by the Agreement.

(b) The Customer is responsible for:

i. all Data entry requirements; and
ii. except as expressly provided otherwise in the Agreement, for all aspects of the Customer's access and use of the SaaS; and
iii. managing the Permitted Users in respect of their use of the SaaS and managing any changes to the Permitted Users;
iv. ensuring that Permitted Users keep all login details for the SaaS confidential and do not share their login details; and
v. ensuring that, in using the SaaS, the Customer and all Permitted Users comply with all applicable laws. To the extent permitted by law, the Supplier accepts no responsibility for ensuring that use of the SaaS will result in the Customer complying with applicable laws or enable the Customer to comply with applicable laws (including for example and without limitation, laws requiring records to be stored in a particular jurisdiction).

(c) Nothing in the Agreement transfers ownership of the Data to the Supplier or to any Authorized Partner.

(d) All Data is available to the Customer:

i. for the term of the Agreement, via the SaaS;
ii. on request to the Supplier at any time during the term of the Agreement and for a period of 1 Month following expiration or termination of the Agreement.

3.7 Support: The Supplier or Authorized Partner will provide assistance in resolving issues in respect of the Customer's access or use of the SaaS, in accordance with the Support Schedule.

3.8 Common terms apply: Except for clause 2, all clauses of these terms and conditions apply to the SaaS (in addition to this clause 3).

4 SaaS Dependencies

4.1 The Customer acknowledges that the SaaS is or may be dependent on proper implementation and availability and correct functioning of the Customer's Integrated Services and Products.

4.2 Neither the Supplier nor any Authorized Partner has any responsibility or liability to the Customer, and in any event no obligation to refund or reduce amounts paid by the Customer, for incorrect or unexpected functioning, or failure, of the SaaS where that incorrect or unexpected functioning, or failure, is directly or indirectly due to incorrect or inappropriate implementation or incorrect functioning, or lack of availability of the Customer's Integrated Services and Products.

5 Charges and payment

5.1 The Customer will pay the Relevant Pricing for the SaaS to the Supplier, the Authorized Partner or via the Purchase Location (as applicable) in accordance with the timing agreed in writing between the Customer and the Supplier, between the Customer and the Authorized Partner or as accepted by the Customer at the Purchase Location.

5.2 All applicable value added taxes will be charged and payable in addition to the Relevant Pricing.

5.3 Subject to clause 5.4, the Customer will pay all invoices in full, without setoff, counterclaim or deduction of any kind, on or before the due date.

5.4 If the Customer wishes to dispute an invoice, it must notify the Supplier in writing within 14 days of the date of the invoice and provide details of the dispute. The Customer may withhold payment of the disputed part of an invoice only and must pay that part (or any amount subsequently agreed or determined to be the correct amount owing) promptly on resolution of the dispute.

5.5 Without the Supplier waiving any other right or remedy it may have, if any amount due is not paid by the Customer by the due date, the Supplier may:

(a) charge the Customer interest calculated at 1.5% on the balance of the amount due by the Customer from the due date until payment is received in full by the Supplier; and/or

(b) charge the Customer all collection costs reasonably incurred by the Supplier in collection of the amount outstanding (including solicitor and/or collection agency fees); and/or

(c) suspend supply of the SaaS until the outstanding amount is paid in full. The Supplier will give 10 Working Days' notice in writing of its intention to suspend delivery under this clause.

5.6 The Relevant Pricing may be changed by the Supplier on the Supplier giving at least six weeks' written notice (by email) to the Customer of the new charges that will apply except that where a Fixed Term applies, the new pricing will not apply until expiration of the current Fixed Term.

6 Term

6.1 The Agreement commences (and provision of the SaaS and Support Services commences) when the Customer purchases the SaaS and the Agreement will continue:

(a) where there is no Fixed Term, until terminated under clause 6.2 or clause 11;

(b) where there is a Fixed Term, for the Fixed Term unless terminated under clause 6.3 or clause 11.

6.2 In addition to the parties' rights of early termination under the Agreement or otherwise at law, where there is no Fixed Term the Agreement may be terminated by the Customer at any time:

(a) on written notice to the Supplier, or where the purchase was made from an Authorized Partner on written notice to that Authorized Partner; or

(b) through the termination processes at the Purchase Location,

with the termination taking effect at the end of the month in which the Supplier or Authorized Partner (as applicable) confirms receipt of the Customer's termination request.

6.3 In addition to the parties' rights of early termination under the Agreement or otherwise at law, where a Fixed Term applies (including where the Customer selects a Fixed Term at the Purchase Location as a Selected Option (where available)), the Agreement will continue until expiration of the Fixed Term. On expiration of the Fixed Term the Agreement will, subject to clause 5.4, automatically continue for further periods each of the duration of the Fixed Term (or such shorter period as may apply following the initial Fixed Term) on the same terms and conditions (unless updated as provided for under clause 1.1(b)) unless at least one month prior to the expiration of the current Fixed Term one party notifies the other party in writing that the Agreement is to

terminate on expiry of the current Fixed Term.

7 Data Protection

7.1 Where Data Protection Laws apply, the Data Protection Schedule attached to these terms and conditions applies. Where Data Protection Laws do not apply, the Data Protection Schedule may not be attached or if it is attached in any event does not apply.

8 Intellectual Property

8.1 All Intellectual Property in:

(a) the SaaS; and

(b) the software, processes, methodology and know-how used by the Supplier in its performance of the Agreement;

is the property of the Supplier (or its licensors) and nothing in the Agreement operates to change that ownership.

8.2 The Customer must not, nor may the Customer permit any other person to do any of the following, or attempt to do so:

(a) copy, alter, modify, reverse assemble, reverse compile, reverse engineer or enhance the SaaS Systems; or

(b) permit or enable users other than Permitted Users to access or use the SaaS; or

(c) provide the SaaS to any users through operation of a bureau or like service; or

(d) resell, rent, lease, transfer, sublicense or otherwise transfer rights to use the SaaS; or

(e) use the SaaS in any way that could damage or interfere with the SaaS Systems in any way;

(f) use the SaaS otherwise than in the manner in which the SaaS is designed to be used;

(g) use the SaaS in any way that could interrupt, damage or otherwise interfere with use of the SaaS by any other customers;

(h) do any act which would or might invalidate or be inconsistent with the Supplier's Intellectual Property rights.

8.3 The Customer must notify the Supplier of any actual, threatened or suspected infringement of any Intellectual Property right and of any claim by any third party that any use of the SaaS infringes any rights of any other person, as soon as that infringement or claim comes to the Customer's notice. The Customer must (at the Supplier's expense) do all such things as may reasonably be required by the Supplier to assist the Supplier in pursuing or defending any proceedings in relation to any such infringement or claim.

8.4 The Customer indemnifies the Supplier against any loss, costs, expenses, demands or liability whether direct, indirect or otherwise, and whether arising in contract, tort (including negligence), equity or otherwise, arising out of a claim by a third party alleging infringement of that third party's Intellectual Property rights if such claim arises from infringement, suspected infringement or alleged infringement due to:

(a) use of the SaaS in a manner or for a purpose or in combination with any other SaaS or product not reasonably contemplated or authorized by the Supplier; or

(b) a breach by the Customer of clause 8.2.

9 Confidential Information

9.1 The parties recognise and acknowledge the confidential nature of the Confidential Information.

9.2 Neither party may use or disclose any Confidential Information other than:

(a) to its employees, directors or contractors to the extent necessary in the performance of the Agreement; or

(b) with the express prior written consent of the other party; or

(c) to its professional advisers.

10 Warranties

10.1 Each party warrants to the other that it has authority to enter into and perform and the ability to perform its obligations under the Agreement.

10.2 With the exception of the warranties given under clauses 10.1, all warranties, terms and conditions (including without limitation, warranties and conditions as to fitness for purpose and merchantability), whether express or implied by statute, common law or otherwise are excluded to the extent permitted by law.

10.3 Any warranties made to the Customer under the Agreement extend solely to the Customer.

11 Termination

11.1 The Supplier or the Customer may terminate the Agreement immediately on written notice to the other party if the other party:

(a) breaches any of its obligations under the Agreement and fails to remedy the breach within 20 days of receiving notice requiring the breach to be remedied; or

(b) ceases business or becomes insolvent or goes into liquidation or has a receiver or statutory manager appointed over its assets or ceases to carry on business or makes any arrangement with its creditors.

11.2 On termination of the Agreement:

(a) all amounts due to the Supplier or relevant Authorized Partner will become immediately due and payable;

(b) the Supplier will cease to provide the SaaS to the Customer, and the Customer will cease to have any entitlement to use the SaaS;

(c) the provisions of the Agreement that are by their nature intended to survive termination will remain in full force.

12 Liability

12.1 This limitation does not apply to claims by the Customer for bodily injury or damage to real property or tangible personal property where the Supplier is legally liable for that injury or damage.

12.2 The Supplier's liability under this Agreement is limited to direct loss only, to the amount paid by the Customer in the 12 month period preceding the event giving rise to the claim.

12.3 In no event is the Supplier liable for any indirect loss or for any loss of profits, lost savings, lost revenue, loss of data, business interruption, incidental or special damages, or for any consequential loss.

13 Dispute resolution

13.1 In the event of any dispute arising between the parties in relation to the Agreement, no party may commence any proceedings relating to the dispute (except where the party seeks urgent interlocutory relief) unless that party has complied with the procedures in this clause 13.

13.2 The party initiating the dispute ("the first party") must provide written notice of the dispute to the other party ("the other party") and nominate in that notice the first party's representative for the negotiations. The other party must within fourteen days of receipt of the notice, give written notice to the first party naming its representative for the negotiations ("Other Party's Notice"). Each nominated representative will have authority to settle or resolve the dispute. The parties will co-operate with each other and endeavour to resolve the dispute through discussion and negotiation.

13.3 If the dispute is not resolved within one month following the date of the Other Party's Notice (or such longer period agreed by the parties in writing), either party may utilize any other legal remedies available to it in seeking to resolve the dispute.

14 Consumer guarantees

14.1 The Customer acknowledges that where it is acquiring the SaaS for the purposes of a business, to the extent permitted by the relevant legislation, any statutory consumer guarantees or legislation that are intended to apply to non-business consumers only will not apply.

15 Force majeure

15.1 The Supplier may suspend its obligations to perform under the Agreement if it is unable to perform as a direct result of a Force Majeure Event. Any such suspension of performance must be limited to the period during which the Force Majeure Event continues.

15.2 Where the Supplier's obligations have been suspended under clause 15.1 for a period of 90 days or more, the Customer may immediately terminate the Agreement by giving notice in writing to the Supplier.

16 General

16.1 Entire agreement: The Agreement constitutes the complete and exclusive statement of the agreement between the parties, superseding all proposals or prior agreements, oral or written, and all other communications between the parties relating to the subject matter of the Agreement.

16.2 Waiver: No exercise or failure to exercise or delay in exercising any right or remedy by a party will constitute a waiver by that party of that or any other right or remedy available to it.

16.3 Partial invalidity: If any provision of the Agreement or its application to any party or circumstance is or becomes invalid or unenforceable to any extent, the remainder of the Agreement and its application will not be affected and will remain enforceable to the greatest extent permitted by law.

16.4 Independent contractor: The Supplier is an independent contractor to the Customer and is in all respects independent of the Customer. Nothing in the Agreement constitutes either party a partner, agent, employee or joint venture of the other.

16.5 Suspension: The Supplier may suspend performance of its obligations under the Agreement for so long as it is unable to perform for reasons outside of its control.

16.6 Assignment: The Customer is not permitted to assign its rights under the Agreement.

17 Notices

17.1 Notices from the Supplier to the Customer under the Agreement will be sent to the Customer at the Customer's contact details specified in the Customer Information. The Customer may notify the Supplier of a change to the contact details specified in the Customer Information, on seven days' notice in writing to the Supplier. Notices from the Customer to the Supplier under the Agreement must be sent to the Supplier at the Supplier's relevant office, details included on the Supplier's website.

17.2 Notices sent by email will be deemed received on sending, provided that the sender does not receive an automatic delivery failure notification. Notices sent by post will be deemed received:

(a) on the third day following posting if sent and received locally (not internationally); and

(b) on the tenth day following posting if posted internationally.

18 Governing law and jurisdiction:

18.1 The Agreement is governed by the laws of England and Wales. The parties hereby submit to the non-exclusive jurisdiction of the courts of England and Wales.

19 Definitions: In these terms and conditions:

"Agreement" has the meaning given to that term in clause 1.2 above;

"Authorized Partner" means a third party that has been authorized by the Supplier to sell the SaaS;

"Claim" means a claim, submitted by the Customer to the Supplier in writing, that the Monthly Uptime Commitment has not been met (claims are subject to the Supplier determining whether or not an Exception Factor applied);

"Confidential Information" means any proprietary information, know-how and data disclosed or made available by one party to the other party but does not include any information which:

(a) is in the public domain without any breach of the Agreement;

(b) on receipt by the other party is already known by that party;

(c) is at any time after the date of receipt by the other party, received in good faith by that party from a third party;

(d) required by law to be disclosed by the other party;

"Customer" means the customer named in the Customer Information;

"Customer Information" means the customer name, email address and any other contact information submitted by or on behalf of a customer:

(a) to the Supplier or Authorized Partner in the course of agreeing to purchase (or agreeing to a Trial) of the SaaS;

(b) at a Purchase Location in the course of agreeing to purchase (or agreeing to a Trial) the SaaS;

"Customer's Integrated Services and Products" means services or products (including third party services or products) which are integrated (in any way) by or for the Customer with the SaaS, regardless of who undertakes that integration work or how it is undertaken;

"Data" means the Customer's data that is entered by the Customer and processed in the course of provision of the SaaS and includes where the context permits, the 'Personal Data' (as defined in the attached GDPR and Data Protection Schedule);

"Data Protection Legislation" means all applicable data protection and privacy legislation in force from time to time in the UK and EU including without limitation the UK GDPR, the EU GDPR, the Data Protection Act 2018 (and regulations made thereunder (DPA 2018), and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended; and all other legislation and regulatory requirements in force from time to time which apply to a party relating to the use of personal data.

"EU GDPR" means the General Data Protection Regulation (EU) 2016/679;

"Exception Factors" means factors the existence of which mean the Supplier cannot ensure availability of the SaaS, as described in clause 3.3;

"Fixed Term" (if any) means:

(a) the fixed term for supply of the SaaS, agreed in writing between the Supplier or relevant Authorized Partner and the Customer; or

(b) the fixed term selected by the Customer in the Selected Options;

"Force Majeure Event" means any war, riot, third party strike, natural disaster or other circumstance of a similar nature that is outside of the control of the affected party;

"Hosting" means the Standard Hosting or if applicable, the Selected Hosting and is subject to the Monthly Uptime Commitment;

"Intellectual Property" includes all copyright, trademarks, designs, patents, domain names, concepts, know-how, trade secrets, logos and all other similar property and rights whether registered or unregistered;

"Monthly Uptime Commitment" (where applicable) means the monthly uptime commitment made by the Supplier for the SaaS, relevant to the Hosting, as notified in writing by the Supplier or Authorized Partner or by written notification at the Purchase Location, prior to purchase;

"Permitted Users" means:

(c) employees, directors or contractors of the Customer; and

(d) where the Selected Options include options for selecting the number of permitted users, not more than the number of employees, directors or contractors selected;

"Planned Maintenance" means maintenance on all or any part of the SaaS Systems and if applicable to the Agreement will be undertaken at times notified to the Customer in writing;

"Purchase Location" means any internet site from which the SaaS is available for purchase;

"Relevant Pricing" means the pricing for the SaaS that is notified in writing to the Customer by the Supplier or by the relevant Authorized Partner prior to the purchase by the Customer or made available at the Purchase Location, and:

(a) includes Standard Hosting or Selected Hosting as applicable;

(b) where Selected Options apply, means or includes (as applicable) the pricing for the Selected Options;

"SaaS" means the software-as-a-service supplied by the Supplier and selected by the Customer by agreement with the Supplier or an Authorized Partner or at the Purchase Location, as modified from time to time by the Supplier;

"SaaS Systems" means, as the context permits, the software used by the Supplier to provide the SaaS and/or the equipment on which that software is installed (whether this is the Supplier's software or equipment or is third party software or equipment);

"Security Breach" means access or disclosure of the Data to or by anyone other than the Permitted Users where the access or disclosure occurs through bypassing the security mechanisms of the SaaS Systems;

"Selected Hosting" if there are hosting options other than Standard Hosting, means the hosting selected by the Customer from the options offered by the Supplier to the Customer;

"Selected Options" means, if there are options to choose from for provision of the SaaS, the options for provision of the SaaS selected by the Customer by agreement with the Supplier, an Authorized Partner or at the Purchase Location (the options may include for example, the Selected Hosting (if applicable), Support Services options, the maximum number of users or the term for which the SaaS is to be provided);

"Service Credit" means the Supplier's service credits (if any), details of which are available on request from the Supplier or relevant Authorized Partner (as applicable) or specified at the Purchase Location;

"Support Schedule" means the support schedule which is either attached to these End User terms and conditions or separately provided by the Supplier or Authorized Partner or made available at the Purchase Location, prior to purchase;

"Support Services" means the support services provided under the Support Schedule;

"Standard Hosting" means the Supplier's standard hosting offering for the SaaS as notified by the Supplier to the Customer (or if not notified, details are available on request from the Supplier);

"Trial" (where available) means use of the SaaS, free of charge;

"Trial Period" (where applicable) means the trial period notified to the Customer in writing by the Supplier, Authorized Partner or at the Purchase Location, prior to commencement of the Trial;

"Trial SaaS" (if any) means the version of the SaaS made available by the Supplier at its discretion for a Trial.

"UK GDPR" means the EU GDPR as amended and incorporated into English law by the DPA 2018;

19.2 Interpretation: In these terms and conditions:

(a) reference to the plural includes reference to the singular, and vice versa;

(b) headings inserted for convenience of reference only and do not affect the interpretation of the Agreement.