QUALIS FLOW LIMITED

TECHNICAL NOTE

1.0 Purpose

The purpose of this document is to provide an overview of Qualis Flow Limited's information security management for the development, testing, deployment, configuration, support and hosting of software for materials and waste data capture, auditing and management.

2.0 Software as a service

2.1 Information security

Qflow is provided as Software as a Service on a secure cloud environment. This section details our security policies.

2.1.1 Data storage and integrity

All of our production data including client information is hosted in Microsoft Azure. All customer data is stored using redundant storage replicated across geographically separated locations, in the UK.

All customer data is encrypted in-transit and at rest.

Data is encrypted at rest using AES 256
Data is encrypted in transit using TLS1.3

2.1.2 Secure configuration

Platform configuration is managed by Terraform scripts. The scripts are tracked and version controlled in our Git repo. The scripts do not contain any sensitive data. Any sensitive data such as passwords are stored in Azure key vaults. No connection string, password or key values are stored with the code in version control.

2.1.3 Managing user privileges

Access to production data is restricted to the platform Owner (Jade Cohen) and our core developers.

Our Owner has global access. Our core developers have global access. No other user has access to any production backend resource.

Access to customer data is restricted to:

- Our ticket-processing team have access to customer data for processing
- Customer Success Managers have access to customer data only for accounts they manage

2.1.4 Platform security

The system presents 3 APIs: a public API, a logistics API and a core API. The public API allows our customers to read the data we hold for them, and to import images for processing. The logistics API supports our mobile app. The core API supports our end user web portal.

The public API is secured using credentials that Customer Success Managers maintain, which callers use to obtain a bearer token that must be passed to each call to the API.
All of our Core API endpoints require authentication with our Azure B2C platform. Unauthenticated users may not use any of our endpoints. Logistical API, which is used for the mobile app, requires authentication via our hosted IdentiftyServer4 app.

All endpoint to access layer transitions is screened using our own logic to determine if a user may access that data.
Users are not able to delete records. Users may only toggle soft deletions. We have data versioning in place which can allow us to restore records to previous states if needed. Mass update operations are also restricted to specific fields.

We use Azure Defender to enforce our security policies and audit security.

2.1.5 Incident management

Our policy is to report all criminal incidents to the police; we have never had such an incident.

Any security or data loss incidents shall be immediately reported to the Owner. These include: attempted breaches (whether or not successful) of any company systems; data loss (or near misses), whether accidental or deliberate; loss of any company IT equipment, or personal equipment used for company business.

2.2 Mobile application

The Qflow mobile app is hosted on Google Play and the App Store, and is accessed via a secure, project- or user-specific set of credentials.

2.3 Disaster Recovery and Business Continuity

Our primary mechanism for maintaining business continuity in the face of business failures is georeplication of services and data. By maintaining redundant versions of services and data, we are robust to a wide range of individual system failures, e.g. hardware failure.

In addition, we use offline backups to protect against problems which are not handled by georeplication.

2.3.1 Hosting

Our service is hosted in Microsoft Azure in two geographically separate locations (both in the UK).

Data is live-georeplicated between our two sites, providing us with resilience against physical disasters at either location. Our RPO matches the RPO of the underlying infrastructure; < 5 minutes for hardware failures.

2.3.2 Backup

We have daily backups.

2.3.3 Disaster recovery

We have the ability to bring up servers in either of our locations, or a new Azure location. Our RTO is 2 hours within office hours.

2.3.4 Future Enhancements

The following enhancements are planned for H1 2023:

- Off-site backups of data
- Disaster recovery drills, including restore from backup
- Increased automation of our disaster recovery process
- Improving our RTO when services need to be rebuilt from scratch, by making the disaster recovery process the same as our regular release process.

These measures are designed to improve our resilience to physical destruction of systems, e.g. datacentre fire, and malicious action, e.g. ransomware action.

2.4 Software development

All software development occurs in-house using Scrum methodology, allowing for regular updates to the application. All source code is securely stored and managed using Git, which is administered using Microsoft Azure DevOps.

We operate multiple separate testing and development environments to that of our primary infrastructure. These are of matched specification to the primary, allowing the development and testing teams to extensively validate software before upload to the production environment.

All systems are developed in accordance with our Test Policy. All new code is covered by automated unit and acceptance tests.

2.5 Software Support

Support is provided by Customer Success Managers, who will be designated prior to deployment. Contact details for your Customer Success Manager will be provided, with response times covered in our standard Terms and Conditions.

We aim to provide support with respect to Qflow systems, including training, configuration and set-up, and any problems as they are experienced, supported by our wider Technical Support team. Your Customer Success Manager will also be there to support you in getting the most value out of Qflow for your organisation.

3.0 Accessibility

Our UX focuses on clear, well-structured presentation. We have not recently audited our system against the WCAG2 standard.

4.0 Data protection and GDPR

Qualis Flow complies fully with the General Data Protection Regulation (GDPR) and its principles; lawfulness, fairness and transparency, purpose limitations, data accuracy,

necessity, and processing securely with integrity.

Qualis Flow is the Data Processor, with the various obligations of each party covered in our standard Terms and Conditions.

All Qualis Flow employees are required to adhere to the requirements of current data protection legislation and Qualis Flow's privacy statement.

5.0 Compatibility

Qflow requires no installed components.

Qflow is maintained for use with Microsoft Edge and Google Chrome (v84 or later), is compatible with various Microsoft Office applications and screen resolutions; proactively identified in part through Google Analytics. We also informally endeavour to maintain compatibility with Safari, and Firefox.

We support both Android and iOS devices as well as any modern browser.

6.0 Professional Services

We do not currently use any 3rd party professional services to monitor or audit our systems.

7.0 Data handover and support

The purpose of this section is to provide an overview of Qualis Flow Limited's process for managing access to data and services associated with the Qflow products (Mobile App and Web Platform) upon termination of a client contract.

We are referring to "data" as meaning the following:

- Delivery tickets (images or pdf's)
- Waste tickets (images or pdf's)
- Records data (data which is exported from the Qflow Web Platform, via CSV)
- Dashboard data (visualisations and exported data from the Dashboards within the Qflow Web Platform)

This does not include customer personal data, which is managed under Data Protection and GDPR regulations.

We are referring to "services" as meaning the following:

- Customer Success support from the Qflow team
- Other communications managed with the Qflow team

7.1 Access to data and services during contract

During the contract period with Qualis Flow Limited, users will have access to the Qflow Mobile App, Qflow Web Portal, and subsidiary products as outlined in the terms and conditions (T&Cs)

This means that users can access their data at any time, including export of tickets, raw data from Records, or insights from the Dashboards.

Clients will also be supported by the Qualis Flow Customer Success team, in being appropriately trained to utilise the Qflow products and access the data.

7.2 Access to data and services post contract

When a contract expires or is terminated, users will have access to the Qflow products, and the included data, for 1 month post the contract end date.

Over this month, this means that users will be able to:

- Export data from the Qflow Web Platform (via CSV files)
- Pull data from the Qflow API (where applicable)
- Export data from the Qflow Dashboards (via CSV files)

Users will not be able to:

- Submit more tickets via the Qflow Mobile App, for onwards processing by Qflow
- Submit more tickets via the Qflow email, for onwards processing by Qflow

The Qualis Flow Customer Success team will still be able to support clients throughout this 1 month period, post contract end date. This support will be primarily in respect of helping clients to recover any data they wish to hold on to and helping to address any final data or insights related questions.

7.3 Data retention

A copy of the data will be retained by Qualis Flow indefinitely. However for the customer to access this outside of the 1 month post-contract period, access to this will need to be arranged with a Qualis Flow Customer Success Manager.

As per the Qualis Flow standard terms and conditions, a copy of the data is kept by Qualis Flow for the purposes of training models, improving the Qflow product over time, and providing insights back to the industry on key trends and benchmarks, to benefit the industry in achieving circularity and net zero carbon goals.

7.4 Data protection and GDPR

Qualis Flow complies fully with the General Data Protection Regulation (GDPR) and its principles; lawfulness, fairness and transparency, purpose limitations, data accuracy, necessity, and processing securely with integrity.

Qualis Flow is the Data Processor, with the various obligations of each party covered in our standard Terms and Conditions.

All Qualis Flow employees are required to adhere to the requirements of current data protection legislation and Qualis Flow’s privacy statement.

8.0 Certifications and accreditations

Qualis Flow Limited operates at a high level of management and quality assurance. In line with this, we are certified compliant with Cyber Essentials.

In addition, Qualis Flow has achieved certification against the following management systems:

- An Information Security Management System (ISMS) which is certified to meeting the requirements of ISO 27001:2013
- A Quality Management System (QMS) which is certified to meeting the requirements of ISO 9001:2015

Certificates are available on request