DATA PROTECTION OPERATIONAL POLICY

This document provides an overview of data protection tools and operational measures taken by Fetch Enterprises to ensure the security and protection of customer data, documentation and system access. The document is meant for partners, clients, consultants and representatives.

1. DATA PROTECTION

1.1 All employees, suppliers and consultants of Fetch Enterprises (Fetch) are required to protect information shared by you and are governed in writing by our policies, specific instructions, service level agreements and confidentiality clauses.

1.2 We ensure that all personnel that have access to, or may have access to customer data, are aware of the sensitivity of it, and are explicitly made responsible for protecting the data where appropriate.

1.3 Furthermore our consultants and outsourced development network, where applicable, have signed terms and conditions similar to those in our license and service agreement with regards to the protection of customer data. These agreements include technical, security and operational measures that protect customer data to at least the same level as our agreement with clients.

2. RESOURCE MANAGEMENT

2.1 Background verification checks on employees, suppliers and consultants involved in the handling, storing, processing or administration of client information, customer data and systems are carried out in accordance with relevant laws, regulons and ethics.

2.2 We ensure that our termination process includes the revoking of access rights and mechanisms to all hardware, software, networks and facilities used to process, transmit or store customer data.

2.3 Employees, suppliers and consultants are contractually and operationally bound to using our internal systems and controls for the storing, sharing, processing and management of customer data files, issuing of credentials and usage of document resources.

2.4 Server, hardware and software inventory is stored and updated in a secure environment hosted by Fetch and backed up for emergency access.

2.5 Client, supplier and consultant information, agreements & statuses are also stored and updated in a secure environment hosted by Fetch and backed up for emergency access.

3. USER ACCESS CONTROL

3.3 We use a centralised authentication mechanism to authenticate system users based on username and password, which are linked to specific individuals and are not shared with colleagues, departments, or job titles.

3.4 For added protection, any system generated password provided to the users in the delivery of their operational responsibilities are changed after the first login.

3.5 Access by employees, suppliers and consultants to client accounts is restricted based on a ‘Need to Know’ basis and authorised in writing by Management.

3.6 Access by employees, suppliers and consultants to the data, information and database systems are removed upon termination of their employment, contract or agreement.

4. OPERATIONAL ACCESS CONTROL

4.1 Every employee, supplier or consultant that accesses and manages any databases, spreadsheets or lists on clients' behalf in the performance of their daily responsibilities follow strict protocol to only store and process data and information using the internal systems and tools hosted by Fetch and made available to them for this purpose. These include:

4.1.1 gofetch.online is the proprietary Customer Data Platform used for the consolidation, data cleansing, customer profiling and distribution of customer data to clients' 3rd party systems.

4.1.2 send.gofetch is a secure facility hosted by for the sharing, revoking, tracking, downloading and uploading of files to ensure that no customer data is saved on hard drives, external storage devices, tablets or phones.

4.1.3 share.gofetch is a secure facility hosted by Fetch for the issuing, revoking and tracking of credentials made available to employees, suppliers and consultants under strict internal protocol and approval.

4.1.4 dev.gofetch is dedicated and secure development environment for developers to develop new features and custom projects, which ensures that they are not granted access to the core system code or live client data.

4.2 Furthermore, end-user terminals, computers and laptops that no longer require access to the information systems, or servers containing the data, are removed from the access control systems and other network systems, where applicable.

5. SECURITY SCANS

5.1 GoFETCh has enabled automated Application Security Scan's on a regular and scheduled bases for all critical applications. The two types of tests being performed, include:

5.1.1 Network Vulnerability Scan – Includes general server node security and is performed on a weekly basis.

5.1.2 Application Vulnerability Scan – Includes security scans at application level and is performed twice a week.

5.2 These scans are in place to identify vulnerabilities at hosting, network and application level and are actively monitored.

5.3 Outcomes are incorporated into our ongoing housekeeping to ensure that GoFETCh maintains its status as a secure and trusted platform provider.

6. INCIDENT MANAGEMENT

6.1 All operational policies, including incident management procedure and disaster recovery planning, are reviewed every 6 months and updated where necessary to ensure that they remain current and are constantly improved.

6.2 Fetch documents management responsibilities for Incident Management and Incident Management Procedures to ensure a quick, effective, and orderly response to information security incidents. We have an established Incident Management Procedure for incident reporting, incident response, escalation and incident resolution that includes the requirement to notify relevant parties of data breaches in accordance with relevant data-compliance regulations.

6.3 The information security incidents that may be included, as a minimum, are the following event types:

- Attempts to gain unauthorised access to systems or data;
- Masquerading, spoofing as authorised users;
- Any targeted attack such as a denial of service or advanced persistent threat attack;
- Unauthorised use of Fetch platforms for the processing, transmitting or storing of customer data by authorised/unauthorised users;
- Unauthorised changes to information systems, hardware, firmware , software or data without the knowledge of Fetch;
- Existence of unknown user accounts;
- Any and all suspected or actual unauthorised disclosure of client and or customer data.