joyous

Joyous Security and Privacy

Overview of Framework and Policies

This document is intended to be **customer-facing**. It serves as the top of our security and privacy documentation tree and is used during onboarding for all new Joyous staff.

Introduction - Our customers' data is important to us

Our customers trust us with a significant amount of sensitive employee data and we recognise that Joyous' security practices are important to them. This document provides an overview of our policies and the mechanisms used to enable them.

Protection from Data Loss/Corruption

All data is **continuously mirrored** in a database cluster, so that operation continues without data loss in the event of a server failure. In addition, data is **backed up off site every minute**.

Stored data ('**data at rest**') in our databases is encrypted automatically via transparent disk encryption. In addition to the storage system level encryption, data is also encrypted at the storage device level with AES-256 on solid state drives (SSD) using a separate key.

All parts of the Joyous application and website, including login pages, pass data via TLS which means that all **data in transit** is encrypted at all times.

Application Level Security

We implement **multiple layers** of logic that **segregate the data of different organizations**, including the obligatory use of standard 'factory' methods that ensure that a user's organization is always confirmed before reading from or writing to the database.

Joyous maintains a security test plan for its software, including **automated testing** of each part of its API to test access controls, permissions, organizational separation and logging.

Joyous **passwords are hashed and can't be read by our own staff**. If a password is lost it can't be retrieved - it must be reset. The creation, storage and use of passwords and other secrets internal to Joyous are described in our **Identity, Access and Secrets Policy**.

Joyous **controls remote access** to critical systems by using one-time-passwords, network encryption and IP-whitelisting so that access is only allowed from specified locations.

Employees and Education

We **continuously train employees** on best security practices, including how to identify social engineering, phishing scams, and hackers. All new staff are provided security orientation training in their first week of employment. Employees that have may access to customer data (engineers, analysts and support) undergo **criminal history background checks**.

Joyous assigns **clear roles and responsibilities** *(*Security Roles and Responsibilities*)* for information security. Access to data and underlying hosts is restricted solely to Joyous operational personnel who have been **granted express access by senior management** and have a work need to access systems. Permissions and entitlements are **periodically audited**, and our **exit process** ensures termination of access when an employee leaves Joyous.

Employee laptops are updated with the latest upgrades, patches and hot-fixes as they become available. We do not provide employees other personal computing devices. Joyous maintains a policy (Laptop Security Policy) governing the downloading and installation of software by employees. Each laptop runs an end-user agent that enables verification of installed applications and centralised management of anti-malware.

Privacy and Data Retention

Our **Privacy Policy** is described at joyoushq.com/privacy.

Joyous complies with the requirements of the General Data Protection Regulation (EU) 2016/679 (GDPR). The legal basis of activities performed outside the EU is as follows:

- Data analysis. In New Zealand, based on Article 45 Adequacy.
- Cloud services. Based on EU Model Contract Clauses.

Joyous supports the privacy features expected by employees and required by modern privacy regulations (including the GDPR) such as the ability to edit and permanently delete feedback and the ability for an employee to request their full record.

Joyous maintains a strong separation between production and development/QA systems. Data moving from production to development/QA is automatically anonymized to enable robust testing while maintaining privacy.

Data Retention.

- Joyous does not persist or archive data unnecessarily.
- Deleted feedback is permanently deleted.
- If an employee is removed from an organization (e.g. via a people data integration) their personal data will be archived and their feedback retained. This enables a person to rejoin the organization or to join in a different capacity (e.g. changing status from employee to contractor). It also enables analytics that include relevant historical data.
- If an employee requests that their data be deleted it will be deleted, including feedback.

Disclosure, Response, Assurance and Review

Joyous maintains a documented **Incident Management and Response** process. If we become aware of a vulnerability or incident we notify the customer(s) affected.

Joyous automates **Security Assurance** including:

- **Vulnerability Management** to ensure newly discovered vulnerabilities in code dependencies are automatically identified and remediated.
- **Endpoint Protection** (including anti-virus/anti-malware) with central control/reporting so that all Joyous employee's laptops are protected and their configuration validated.
- **Penetration Testing** to detect potential Internet-facing attack vectors. This includes manual penetration testing by a qualified external firm at least annually, combined with automated weekly testing.

Service Providers

Our applications servers, databases, storage and backups are hosted exclusively on Google Cloud Platform (GCP) and Amazon Web Services infrastructure. This applies to both Joyous application servers and the MongoDB Atlas service which hosts our databases. Google and AWS data centers implement DDOS mitigation and comply with a very broad range of physical security and information security standards.

All Joyous data is stored using the MongoDB Atlas service which has achieved both ISO27001 and SOC2 Type 2 certification. Mongo's ISO27001 certification is public, and we have an NDA in place with Mongo to periodically review other external audit results which have always been excellent.

Our acquisition process for new Service Providers ensures that any addition(s) are compatible with our security requirements.