FeedbackFruits Security Practices

Information security is a key priority for FeedbackFruits: we've designed our practices & procedures based on guidance from the ISO/IEC 27000 standardisation series, NIST Cyber Security Framework, SOC2 Trust Service Principles and Center for Internet Security (CIS) Controls. Our COO, CTO and security team work closely together to establish strong security practices both on an organizational level (through policy & education) and on a technical level (through coding standards & infrastructure/application security).

FeedbackFruits approaches security as a layered challenge - in this document we go over the various layers and the mechanisms that we have in place to ensure the data of our customers remains secure.

Physical security

FeedbackFruits does not operate its own physical infrastructure, but works closely with cloud vendors to deliver its services. Microsoft Azure is our preferred cloud platform: we rely on their services for most of our offerings.

Microsoft Azure documents their physical security practices in high detail, see: https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security for an overview of their measures, and https://docs.microsoft.com/en-us/compliance/regulatory/offering-home for details on Microsoft Azure standards compliance.

Microsoft on Azure physical security compliance:

> *We design and manage the Azure infrastructure to meet a broad set of international and industry-specific compliance standards, such as ISO 27001, HIPAA, FedRAMP, SOC 1, and SOC 2. We also meet country- or region-specific standards, including Australia IRAP, UK G-Cloud, and Singapore MTCS. Rigorous third-party audits, such as those done by the British Standards Institute, verify adherence to the strict security controls these standards mandate.*

Personnel security

As part of our onboarding process and on an annual basis afterwards, employees are instructed on our security policies. This includes instructions on how to work with our company-wide password/secret management, what encryption is, how work

devices should be managed and how to handle customer data if their role requires them to be involved. Employees are highly aware of the risks of phishing/social engineering attacks, know how to report suspicious communications and get exposed to training phishing emails as part of our penetration testing engagements.

Third-party security

As a Software-as-a-Service company, FeedbackFruits focuses on the development of its own application and works with third party vendors to deliver our services to our customers. Before working with third parties, FeedbackFruits assesses their conformance to our security standards.

As mentioned above, Microsoft Azure is our primary cloud vendor. For aspects of our services not covered by Microsoft Azure offerings, we work with alternative vendors. Our focus is always to reduce the exposure to customer data as much as possible: before incorporating a new third party into our offerings, we assess how we can minimize externalized data.

Cloud vendor (Microsoft Azure) security

The FeedbackFruits applications and databases are hosted on the Microsoft Azure cloud infrastructure, one of the leading cloud infrastructure providers worldwide. Over the years, Azure infrastructure has proven to be highly stable, fault-tolerant and secure. For more details on Microsoft cloud infrastructure security practices, refer to the Azure security documentation: https://docs.microsoft.com/en-us/azure/security/fundamentals/overview.

Regions

FeedbackFruits offers hosting in these regions on Microsoft Azure:

- West Europe (Netherlands)
- East US (Virginia)
- Australia East (New South Wales)
- Canada Central (Toronto)

The customer chooses which region is used upon setup.

Network and systems security

Being a cloud hosted platform, FeedbackFruits does not maintain any physical systems or private networks. All systems and networks are maintained by Microsoft Azure, for more information see:

https://docs.microsoft.com/en-us/azure/security/fundamentals/network-overview

Network security is a core aspect of security at FeedbackFruits. All network connections, both inbound and outbound use secure protocols only, for example TLS 1.3.

Each FeedbackFruits hosting region is separated, with independent access control and encryption keys. Deployment is automated, with a select group of technical personnel having full access to our cloud infrastructure and most technical personnel having programmatically limited access through our development platform.

Application security

All FeedbackFruits services are developed using secure coding techniques and with awareness of secure standards. All developers are required to have sufficient knowledge of security standards, defined by for example the Open Web Application Security Project (OWASP). Most common security issues are prevented by using secure frameworks and libraries.

To ensure the quality of the application after each change, we run automated tests (unit & integration) as well as manual tests. All developers write automated tests for new functionality, and we aim to have a 100% test coverage on all services.

Manual Quality Assurance is executed for each functional change and for each release. This includes a full validation of existing functionality as well as a thorough walkthrough of new functionality.

Data security

For a detailed overview of the different kinds of data that FeedbackFruits processes, see https://feedbackfruits.com/privacy.

Access to customer data by employees is regulated using strict policies. An internal administrative tool is accessible for employees on a need-to-have basis, for example for support staff. An employee can request access with a motivation for why access

is needed. The access can only be approved by a select group of admins. Access to this tool can be withdrawn at any time, and this is done automatically when an employee leaves FeedbackFruits.

Direct access to the production infrastructure is only granted to a very select group of engineers that need this access in order to maintain the infrastructure. A list of people with access can be retrieved at any time, and the access can be withdrawn at any time.

Vulnerability management and security audits

The code and its dependencies are continuously scanned for vulnerabilities on every change, and checked for potential risks against the Common Vulnerabilities and Exposures database, see https://cve.mitre.org. Next to that, static analysis is applied to the codebase on every change, using linting tools. These processes are facilitated by our development platform, GitHub.

Most security related patches are handled by our cloud provider, for example on the operating system or cluster layer. Vulnerabilities detected in our own application or within dependencies are assessed in their potential impact and mitigated appropriately. Patches get included in the next scheduled release for non-critical issues, hotfixes are made within a workday and can be rolled out without incurring any downtime to our services.

Monitoring of network requests on production services is in place to detect malicious activity and potential attacks.

A full security audit is executed by an external party on a yearly basis, a summary with the outcomes of the last audit can be provided on request. This includes a penetration test and expert review of security practices.

Incident response policy and plan

No organization is impenetrable. Therefore, FeedbackFruits has a clear incident response policy and plan to act effectively when a security incident presents itself. We aim to meet or exceed all institutional requirements, governmental statutes/regulations and industry standards relevant to our customers in relation to system and data security.

In the event of unauthorized data exposure (either proven or reasonably believed to have been disclosed/exposed to an unauthorized party), our security team, lead by the CTO & COO, enacts our security incident response plan.

First, the scope of the security breach is assessed: is the activity still ongoing or was the breach temporary? Which data was involved, from which sources, and which customers/regions does this leak affect?

Based on the findings, an incident response team with expertise in the relevant systems/fields is assembled. This team works to mitigate any ongoing leaks, makes a comprehensive overview of the leaked data and writes preliminary advice for future prevention of similar events.

Together with our partner teams, the incident response team will notify relevant and affected parties, with an initial notification sent out within 24 hours, and a comprehensive overview reported within 48 hours. Based on our agreements with institutions/partners, we alert key stakeholders first and work with them on a strategy for notifying end users.

After initial assessment of the breach, the assembly and work by the incident response team to fully understand & mitigate the event, notifying our partners and when relevant end users, we write out a post-mortem report to be shared within two weeks of the event happening. This post-mortem report lists next steps to prevent similar events in the future, evaluates the effectiveness and timeliness of our response and invites affected institutions to share their reflections.

FERPA Compliance

FeedbackFruits products comply with the US Family Educational Rights and Privacy Act (FERPA), to allow our US partner institutions to comply with the provisions of the FERPA relevant to them and fulfill their responsibilities according to its requirements.

General Data Protection Regulation (GDPR)

With the European Union General Data Protection Regulation (GDPR), the processing of personal data of individuals in the EU is safeguarded. FeedbackFruits complies with the GDPR and is committed to help our customers to be compliant with its provisions themselves. More information is available in our Data Processing Agreement upon request and as executed with our customers.