Funraisin Security Overview

funraisin

Document Reference	**Funraisin Security**
Date	**2nd April 2024**
Version	**2.8**
Reviewed by	**Peter Kurtis, BGP group**
Last Reviewed Date	**February 2024**

Operational Security
- Data storage and processing locations
- Security policies
- Awareness and training

Physical Security
- Data center controls
- Data center compliance

Application Security
- Security testing
- Security controls
- Secure code development
- Data encryption
- User access
- SSL/TLS access
- Code monitoring
- Patch management (Server)
- Code deployment

Application Technology
- Server firewall configuration
- Server and Database access

Backups
- Data storage
- Data Removal & Destruction

Monitoring
- Server Monitoring
- Site Monitoring

- Uptime monitoring

Disaster Recovery and Business Continuity
- Emergency Response Team
- Assumptions
- Disaster Definition
- Team member responsibilities
- Instructions for using the business continuity plan
  - Invoking the plan
  - Disaster declaration
  - Notification
  - Emergency management procedures
- PCI Compliance
- Accepting payments

Funraisin is committed to securing our customers' data to the highest degree. Funraisin services more than 4,000,000 transactions annually for many of the world's leading Not for Profits, that's why trust is the foundation of our privacy and data security promise to our customers, and their supporters.

Operational Security

We have a dedicated security team responsible for the security of the application, identifying vulnerabilities and responding to security events. This service is provided to us by BGP Group. See https://bgpgroup.com.au/

Data storage and processing locations

We store data in data centres based in Australia, USA, Canada and the EU depending on our client's location. We use RackSpace and AWS content delivery networks for content caching. Network mapping for these networks can be found at https://support.rackspace.com/how-to/rackspace-cdn-geography-mapping/ and https://www.cdnplanet.com/cdns/cloudfront/#network.

Security policies

We have a suite of security guidelines with supporting procedures which have been aligned with the ISO 27001 and PCI-DSS standards. Our security documentation is frequently reviewed and updated to reflect changes to our processes made in response to newly identified threats, as well as our commitment to continuous improvement.

We use the NIST Cyber Security Framework to measure our ability to identify, protect, detect, respond and recover from security events.

Awareness and training

All staff and contractors go through a vetting process where they are subject to background checks and confidentiality agreements.

We provide an ongoing program of security awareness training designed to keep *all* members of staff informed and vigilant of security risks. This includes regular assessment of comprehension to measure the program's effectiveness.

Physical Security

We implement physical controls designed to prevent unauthorized access to, or disclosure of, customer data.

Data center controls

We only use state-of-the-art data centres and Cloud providers. Our data centres are monitored 24×7 for all aspects of operational security and performance. They are also equipped with state-of-the-art security such as biometrics, sensors for intrusion detection, keycards, and around-the-clock interior and exterior surveillance.

In addition, access is limited to authorized data centre personnel; no one can enter the production area without prior clearance and an appropriate escort. Every data centre employee undergoes background security checks.

Data center compliance

Our data center provider is certified to the following compliance standards: HIPAA, PCI-DSS, SOC 1 Type 2, SOC 2 Type 2, ISO 27001 and FISMA/NIST.

Our Cloud provider has the following certifications: PCI-DSS, ISO 27001, SOC 1 / 2 / 3, IRAP, ISO 27018 and ISO 9001.

AWS Security & Compliance
https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf

RackSpace Security & Compliance
http://bd905956a42f6ed96c17-a6046798c661ed27e3d4fdfd1b3c5e5a.r62.cf1.rackcdn.com/whitepapers/security/Rackspace_Security.pdf

Application Security

Our application has been designed with a focus on security by leveraging OWASP-aligned security principles for software engineering, encryption technologies and security assurance.

Security testing

We use a combination of regular scheduled scans of our application as well as penetration testing and bug bounty programs to ensure that every area of our application has undergone rigorous security testing.

Our scheduled vulnerability assessment scans simulate a malicious user while maintaining integrity and security of the application's data and its availability.

Security controls

We never give, rent, or sell access to your data to anyone else, nor do we make use of it ourselves for any purpose other than to provide our services.

We store each customer's data within their own database, which is used to retrieve data via the application or the API only. Each request is authenticated and logged.

Secure code development

We follow industry best practices and standards such as OWASP and SANS. We have separate environments and databases for different stages of the application development. We do not use production data in our test and development environments.

Data encryption

To protect data we encrypt information in transit by supporting TLS 1.2. Sensitive data at rest (such as PII data) is also encrypted using AES-256 encryption.

User access

We put considerable effort into ensuring the integrity of sessions and authentication credentials. Passwords storage and verification are based on a one-way method, meaning passwords are stored using a strong salted hash which cannot be reversed.

Data is either uploaded directly into the application using a web browser or uploaded via the API which uses secure transfer protocols.

SSL/TLS access

All Funraisin sites are served constantly via HTTPS TLS 1.2 unless in test mode.

Code monitoring

Every Funraisin site is monitored daily for code changes by Codeguard (codeguard.com) with daily changes sent to our Head of Technology for review.

Any changes made to the applications code that were not scheduled can be immediately detected and reinstated automatically to the last stable release.

Patch management (Server)

Each Funraisin application receives updates on a weekly basis with all updates tested and reviewed prior to release

All Funraisin servers are managed by BGP Group. Operating System and application platform software is monitored on a daily basis and any security patches are deployed the next Saturday after the patch is released, unless the patch is deemed non essential.

Code deployment

Funraisin code deployment is based on the “Continuous Deployment” methodology whereby features and fixes are rolled out as soon as they become available. This mitigates the risk of bugs and ensures that any issues are found quickly,

All development is carried out in a separate development environment that mirrors the functionality of a production website and that is kept uptodate just as a production site would be.

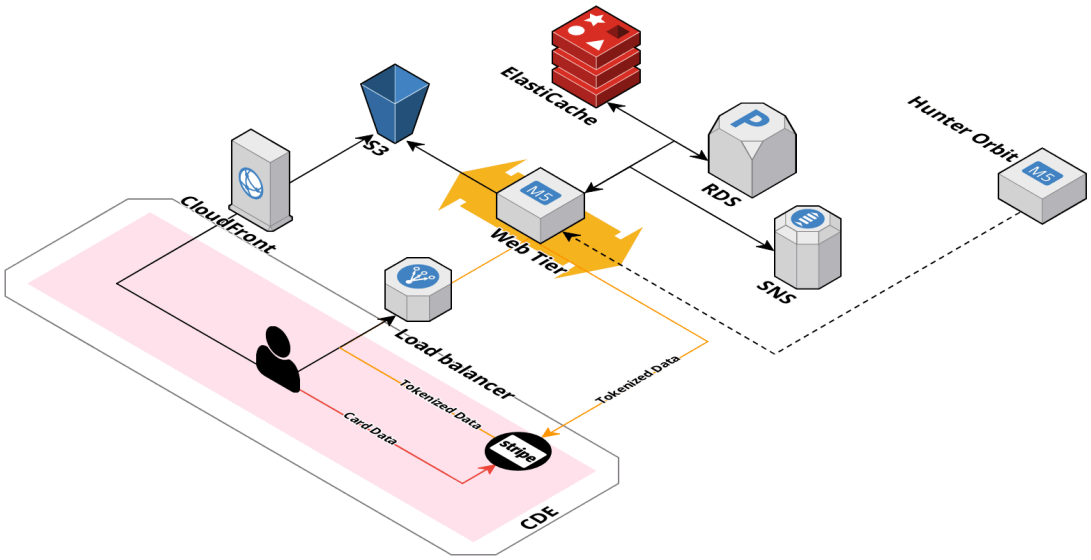
Prior to releasing updates each update is progressed into a “rush box” environment where we are able to test the expected outcome on a live scenario, before they are synced out to the core platforms.

All updates are managed in a GIT repository as is each individual site allowing us to roll back changes at any time.

All issues are logged via issue tracking software, Bugherd.

Application Technology

Every Funraisin powered website is hosted within our Rack Space or AWS based Cloud environment. All servers are currently running Linux & PHP with each individual site sitting behind its own Load Balancer and connecting to a Rack Space or RDS Cloud MySQL Database Server as shown below. Databases do not support remote access.



Server firewall configuration

Each server instance is protected by the a firewall with the following port settings.

TCP Port 80 Accept
TCP Port 443 Accept
TCP Port 12345 Accept

Server and Database access

Each server can only be accessed by a Funraisin employee via SSH or SFTP as well as the Code Guard monitoring agent (see below).

Database access is restricted to connections only from the Funraisin application itself. Remote access is not permitted.

Backups

Each Funraisin site is backed up with the following schedule:

- Daily full server backups with 3 day retention
- Bi-daily full database backups stored offsite + incremental database backups throughout the day
- Daily site files backups, stored off-site

Data storage

All backed up data is stored securely in a private network within RackSpace or AWS. At no time is any data stored within Funraisin's own company network.

Backups can be provided to clients on request.

Data Removal & Destruction

All of our data centers follow best practice when it comes to decommissioning storage media. See section on "Physical Security". All backups are deleted on request.

Monitoring

All Funraisin sites are monitored both at server level and at the individual site level.

Server Monitoring

All Funraisin AWS and RackSpace servers are monitored in real-time using Nagios (https://www.nagios.com/) which monitors server & database health and provides SMS alarms to the Funraisin server team.

Site Monitoring

Each Funraisin site is monitored in real-time via Solarwinds Appoptics application monitoring which provides us with metrics such as but not limited to:

Page views per minute
Server throughput
Server response time
End user time
Error rate

This allows us to monitor all sites in real-time to watch for traffic spikes, bottle necks and any errors users may be experiencing. If an individual site goes over a set threshold of poor performance SMS alarms are sent out to the Funraisin server team to investigate.

Uptime monitoring

Uptime monitoring can be provide for at additional cost via an external monitoring system. We are able to support both Ping monitoring as well as Keyword monitoring. We recommend using (https://www.siteuptime.com/) SiteUptime.

Disaster Recovery and Business Continuity

Emergency Response Team

Name	Company	Mobile
Scott Dilley	Funraisin	+61405171825
Courtney Evans	Funraisin	+61404805326
Luka Maretic	Funraisin	+385 99 4610 394
Peter Kurtis	BGP Group	+614011296674

Assumptions

- Key people (team leaders or alternates) will be available following a disaster.
- A national disaster such as nuclear war is beyond the scope of this plan.
- Each 3rd party organization will have its own plan consisting of unique recovery procedures, critical resource information and procedures.

Disaster Definition

Any loss of utility service (power, water), connectivity (system sites), or catastrophic event (weather, natural disaster, vandalism) that causes an interruption in the service provided by Funraisin operations. The ERT identifies vulnerabilities and recommends measures to prevent extended service outages.

Team member responsibilities

- Each team member will designate an alternate
- All of the members should keep an updated calling list of their work team members' work, home, and cell phone numbers both at home and at work.
- All team members should keep this plan for reference at home in case the disaster happens after normal work hours. All team members should familiarize themselves with the contents of this plan.

Instructions for using the business continuity plan

Invoking the plan

This plan becomes effective when a disaster occurs. Normal problem management procedures will initiate the plan, and remain in effect until operations are resumed at the original location or a replacement location and control is returned to the appropriate functional management.

Disaster declaration

The senior management team, with input from the ERT, is responsible for declaring a disaster and activating the various recovery teams as outlined in this plan.

In a major disaster situation affecting multiple business units, the decision to declare a disaster will be determined by Funraisin senior management. The ERT will respond based on the directives specified by senior management.

Notification

Regardless of the disaster circumstances, or the identity of the person(s) first made aware of the disaster, the plan must be activated immediately in the following cases:

- Two or more systems and/or sites are down concurrently for three or more hours
- Five or more systems and/or sites are down concurrently for one or more hours
- Any problem at any system or network facility that would cause either of the above conditions to be present or there is certain indication that either of the conditions are about to occur

Emergency management procedures

The following procedures are to be followed by system operations personnel and other designated Funraisin personnel in the event of an emergency.

In the event of a natural disaster

1. Notify the ERT
2. Determine risk of outage and possible timeframe
3. Take immediate backups of all critical systems

In the event of a network services provider outage

1. Notify the ERT
2. Determine cause of outage and timeframe for it's recovery
3. If outage is expected to be greater than 6 hours relocate all servers to a new data centre unless the outage is global
4. Notify all platforms and provide instructions

PCI Compliance

All Funraisin sites are compatible with PCI DSS. If you wish to add your Funraisin site to your own PCI Compliance we are able to provide you with our AOC.

Accepting payments

All payments are captured through Stripe, unless by special arrangement. Card data is encrypted using Stripe's client side encryption via their Stripe JS product and then any payment is processed using a secure card token. At no time does any card data touch Funraisin servers. Card data is not stored within any Funraisin application.

This is compliant with the PCI DSS SAQ A-EP guidelines. For more information on Stripe JS visit https://stripe.com/docs/stripe-js