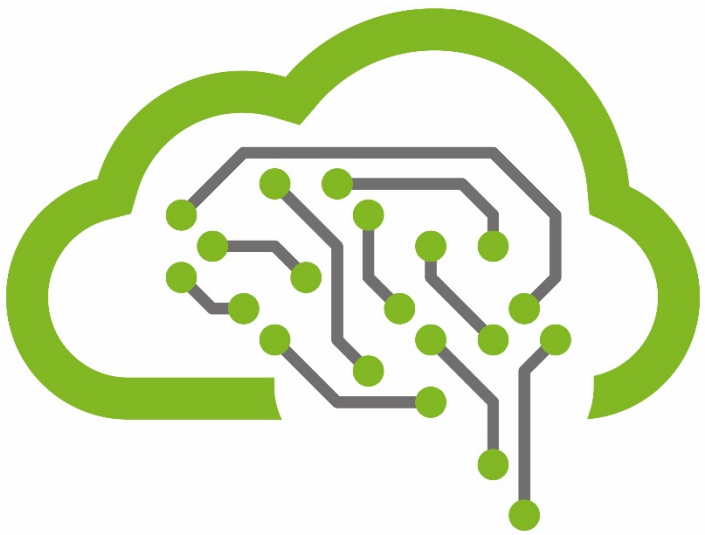
NetFM UK



IT INFRASTRUCTURE AND DATA MANAGEMENT

December 2021
Version 2.0

IT INFRASTRUCTURE AND DATA MANAGEMENT

CONTENTS:

1. **GENERAL DISCLOSURE**
2. **INFORMATION SECURITY MANAGEMENT PRACTICES**
3. **PLATFORM ARCHITECTURE AND SECURITY CONTROLS**
   - 3.1 Architecture
   - 3.2 Server, Logins and Mobile Devices
   - 3.3 GitLab Communication
   - 3.4 Cloud Hosting
   - 3.5 Audit Trail
   - 3.6 Availability and Performance
   - 3.7 Network Security
   - 3.8 Security Monitoring
   - 3.9 Authentication
   - 3.10 Compliance
4. **DATA MANAGEMENT AND SECURITY CONTROLS**
   - 4.1 Data Storage, Deletion and Decommission
   - 4.2 Data Backup and Disaster Recovery
   - 4.3 Data Security
   - 4.4 Access Control
5. **SUPPORT SERVICES**
   - 5.1 Customer Success
   - 5.2 Customer Support
   - 5.3 Issue Reporting
   - 5.4 Response Protocol

IT INFRASTRUCTURE AND DATA MANAGEMENT

1. GENERAL DICLOSURE

NetFM was founded in 1997 by David Herring with the company mission to design and deliver intuitive, cost-effective and dynamic software systems, tailoring core software to meet clients' diverse business requirements, working practices and internal policies. The company ethos has always been to use highly skilled UK based individuals to achieve this mission.

2. INFORMATION SECURITY MANAGEMENT PRACTICES

Information Security Management policies and procedures have been developed and include administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. All employees fully support and enforce initiatives for following information security best practices.

Autonomous environments are maintained for development, staging, and production. All software releases are performed using our CI/CD tool chain under the control of the lead development team.

3. PLATFORM ARCHITECTURE AND SECURITY CONTROLS

3.1 Architecture

NetFM's cloud-based architecture has been designed with performance, availability, and scalability in mind.

3.2 Server, Logins and Mobile Devices

For server logins, NetFM uses Google Authenticator running on a separate, pre-approved device. NetFM operates a BYOD policy for smartphones and laptops for Account Managers (admin users) accessing the systems themselves. NetFM Admin Logins are restricted to the dedicated Account Manager and Lead Developer for that client and mobile devices are regulated by the NetFM Mobile Device Policy.

3.3 GitLab Communication

NetFM uses the DevOps platform GitLab for managing all employee interactions relating to client systems. All actions carried out within client systems are logged and monitored. Clients are provided restricted access to the platform in order to raise tickets for development work or highlighting issues within their system.

3.4 Cloud Hosting

All of NetFM's hosting is done through OUH, a TÜV certified business, which draws 100% of its energy from CO2-free hydropower, one of the cleanest energy sources available.

To access the NetFM hosting platform for OS updates and administration, NetFM only uses laptops running Linux OS with built-in password policies and have a two-factor authentication access policy using a one-time password generator on a separate, pre-approved device.

3.5 Audit Trail

NetFM uses standard Linux accounting to record all server access. For client systems access, NetFM records user ID, time/date, pages visited, actions carried out, device and OS used.

IT INFRASTRUCTURE AND DATA MANAGEMENT

3.6 Availability and Performance

NetFM's development engineers monitor the health of the platform using industry standard tools to detect adverse events before they can impact the availability or performance of the production site. The architecture has been designed to handle spikes in usage and has the ability to be scaled in order to address increased volume. The system architecture and monitoring processes allow NetFM to provide its platform with 99.9% availability or higher, on a monthly basis.

3.7 Network Security

NetFM deploy ClamAV on the servers to continuously scan for virus threats. NetFM also uses security scanning within all build processes, ensuring no security leaks are present before any code is pushed live to production servers. Additionally, NetFM uses a number of in-house tools, e.g. Wapiti, to regularly scan all production servers for security vulnerabilities.

3.8 Security Monitoring

NetFM updates servers weekly, on a service window between 6am and 7am on a Tuesday morning to ensure the servers always have the latest OS security updates. We use this same window to carry out application upgrades on the production servers — only after the upgrade has been available on a staging server for prior customer testing.

3.9 Authentication

Two factor authentication is used for all access to code repositories, databases and access to the company email platform. Only specified IP addresses (managed and confirmed by the Technical Director) have direct access to client databases.

3.10 Compliance

NetFM is hosted on a cloud platform, OVHcloud, that aligns with common industry certifications and standards, including ISO/IEC 27701, ISO/IEC 27001, ISO/IEC 27017 and ISO/IEC 27018.

4. DATA MANAGEMENT AND SECURITY CONTROLS

4.1 Data Storage, Deletion and Decommission

All data and servers are held within private, secure UK-based data centres with strict access control procedures. Data is deleted on an automated, script-based basis within the application. Any inactive user accounts are automatically deleted after 12 months and any historic user data after seven years. Server disks are destroyed after a server is decommissioned. Video evidence of this is recorded and supplied for end customer evidence.

4.2 Data Backup and Disaster Recovery

NetFM has a full disaster recovery and back-up solution for the entire platform. This allows the manual fail-over of all and any of the servers on the platform to a remote location. In addition, NetFM can recover individual files intuitively through a web-based interface whilst working on the platform. The platform currently consists of four servers and associated network infrastructure, sited within a single, secure rack enclosure.

We use mirrored SSD disks on all production servers for maximum availability and response time with 0.2sec for all web servers. Our databases our mirrored in a mast/slave configuration - so all transactions are written to two non-volatile data stores on each completed transaction. Databases are backed up daily with incremental backups to a third non-volatile store.

4.3 Data Security

NetFM is ICO registered, registration number: ZB049295. All security threats and responses are shared with all employees on a private discord server. The action response is discussed there by all senior developers to ensure a quick and thorough response has been actioned to policy processes and guidelines.

Copies of NetFM's *Data Security Breach Management Policy* and *Data Security Breach Management Action Plan Workflow* can be emailed on request.

4.4 Access Control

NetFM only allows production server access to senior developers (three people). This is controlled by Ubuntu SSH access controls. Login to client systems is restricted to senior developers and the dedicated Account Manager (as the designated System Administrator). NetFM uses Linux accounting to monitor all server access and also uses hosting platform-based firewalls to give an independent access control layer to the firewalls built into Linux.

Privileged Access accounts are unique to each designated user and access to source code restricted to key staff. Account access and password complexity requirements are regularly reviewed, with passwords requiring change every 90 days.

Linux standard highly secure sudo is used for all privileged commands at server level. Access to all systems is password protected to password policy complexity and restricted to designated users. There are no shared credentials. NetFM User IDs/passwords are managed by the relevant user. Access to the NetFM email platform is protected by two-factor authentication.

Password policies are built into the Linux OS. For access to the Hosting Management platform, NetFM uses a two-factor authentication that uses a one-time password generator on a separate device.

For server login, NetFM uses Google Authenticator running on a separate mobile device.

For front-end system access, NetFM are required to choose a password of minimum 10 characters with three of four uppercase, lowercase, integer and special characters. Users are locked out of the system after three unsuccessful login attempts and must be reset by Admin/SysAdmin. Passwords are required to be updated every 90 days. Access to all NetFM systems is revoked by the Technical Director beginning two weeks before any employee's employment end date.

IT INFRASTRUCTURE AND DATA MANAGEMENT

5. SUPPORT SERVICES

5.1 Customer Success

At NetFM we are dedicated to the success and support of our customers. Each customer has a dedicated point of contact throughout their lifecycle to ensure they are supported for maximum value realisation.

5.2 Customer Support

NetFM provides customer-facing WhatsApp channels for product and service availability updates in near real-time. Customers also have access to GitLab where tickets can be raised to highlight development requests or technical issues.

5.3 Issue Reporting

NetFM uses a priority labelling reporting system through GitLab. Each report is labelled by either a P1, P2 or P3.

- A P1 label requires immediate attention as in this scenario, the customer cannot operate
- A P2 label requires timely attention, although the customer is still able to operate
- A P3 label usually requires development for a “would like to have” feature

5.4 Response Protocol

Any request for changes will be responded to by the account manager on GitLab within 24 hours providing an initial response. Development feedback for none P1 issues will be added to the communications network, GitLab within one working week. Releases happen thereafter at the scheduled release times unless otherwise stated. Scheduled release times are Tuesday mornings between 6am and 8am weekly. Changes will be on the staging server for a minimum of one week (low impact), longer for testing more complex issues.