NetFM UK

SECURITY OVERVIEW

1. DATA STORAGE AND SECURITY

1.1 Accessibility

All Visitor Express backend data is held within a Django-ORM (Object Relational Manager) service to facilitate modern easy access for all web services.

The physical data for the Django-ORM is held in a modern postgres database. The data is held on mirrored SSD disks to provide the fastest access available. The postgres database is configured with a live replication service, so there is full mirroring also at the server level.

Incremental backups are taken hourly and full backups daily to separate disk storage — all held securely and co-located within UK-based OVH data centres.

Where Visitor Express supports Azure SAML login, we support multiple identity providers via SAML and offer AAD Business-2-Business (B2B) capability. The system will comply with the Technology Code of Practice and is fully GDPR compliant.

1.2 Security

Security to the service is maintained through all data being held in a private cloud. The Visitor Express cloud service is protected by two independent firewalls: one at the network edge provided by OVH and a second Linux based firewall installed on all Visitor Express production servers.

Both these firewalls are set to only allow secure encrypted access via HTTPS or SSH. For SSH access we mandate it from a designated Visitor Express known IP address — and for infrastructure access we mandate two-factor authentication using a one-time SMS passcode.

The platform has documented Disaster Recovery and Mirrored Failover processes and the Visitor Express booking system and app meet WCAG 2.1 AA standards.

1.3 Management

The data held for all employees is customisable within Visitor Express to ensure only the minimal data is held.

For Single Sign On, only three employee fields are mapped: name, email and mobile.

These are explicitly targeted for the purposes of:

1. Name: e.g. to display on live desk floor plans where floor plans are integrated.
2. Email: e.g. to provide notifications of visitors and/or bookings related to that user.
3. Mobile: to provide SMS alerts on visitor arrivals and/or bookings related to that user.

This information is cached within the Visitor Express service, with the ability to easily view and remove directly from the admin interface.

There are powerful search filters on the admin interface that allow direct removal of all data pertaining to selected individuals.

All employees have direct access to the data held for them via the Visitor Express app.

SECURITY OVERVIEW

1.4 Storage

The data is only held on UK based servers provided by OVH.

OVH is committed to ensuring optimal security for its infrastructures. This includes implementing a security policy for information systems, and meeting the requirements for multiple standards and certifications (PCI-DSS certification, ISO/IEC 27001 certification, SOC 1 TYPE II and SOC 2 TYPE II certificates, etc.)

We only allow two secure encrypted protocols to access the data HTTPS and SSH. For SSH we mandate the access from a designated set of IP addresses belonging to the Visitor Express staff.

For infrastructure access to the OVH services we mandate two-factor authentication using one time SMS pass codes. The data is held in a modern open source postgres database (currently 12.2) that uses mirrored SSD disks to provide maximum speed and resilience.

The database has both a primary and secondary replication server, so there is also full mirroring at the server hardware level.

Hourly incremental backups and full daily backups are also housed with secure UK based hosting services.

No customer data is held outside of these facilities, and we take great care to use fake data for development and demonstration purposes — unless a client has explicitly authorised us otherwise.

1.5 Penetration Testing

In addition to independent penetration tests, the Visitor Express team also regularly undertakes its own penetration testing programs. These Snort based penetration tests ensure the platform meets the highest security standards.

Full automated static application security tests (SAST) are run on our code using the GitLab continuous integration hooks. We provide GitLab access to customers requiring code level security reviews.

2. HUMAN RESOURCES SECURITY

2.1 Pre-Employment Screening

Pre-employment screening will verify the credentials of job applicants and check that the applicant meets pre-conditions of employment (e.g. that the individual is legally permitted to take up an offer of employment and has no serious relevant criminal history or history of misuse of data.)

2.2 Terms and Conditions of Employment

All employees sign a declaration and non-disclosure agreement as part of their overall agreement. A copy of the *Information Security* and *Data Privacy Employee Declaration Form* can be supplied on request.

SECURITY OVERVIEW

2.3 Data Security Breach Management

A data security breach incident report form must be completed to report suspected and actual data breach incidents such as data loss. The form can be completed by anyone with knowledge of the incident and should be completed as soon as a data breach has been identified.

A copy of the *Data Security Breach Incident Report Form* can be supplied on request.

For more details of data security breach management, a copy of the *Data Security Breach Management Policy* can be supplied on request.

2.4 Leavers Procedure

Visitor Express is committed to ensuring staff leaving the organisation pass through an efficient and thorough handover process ensuring that the security of Company and Client data is maintained. A copy of the *Leavers Checklist* can be supplied on request.

3. ASSET MANAGEMENT

All our infrastructure assets are managed using industry best practices. We maintain an inventory of our infrastructure via our server provider.

We keep an up-to-date inventory of all the assets that we issue to our employees and these assets are returned to the company when an employee leaves the company.

4. APPLICATION ACCESS CONTROL

All users must use a password that is at least 8 characters to access Visitor Express. User login sessions are valid for 60 days. Users can only join an organisation and register an account through a valid invitation or manual account creation by the organisation owner (the client).

Access to projects is limited by per-user permissions and can be revoked by the project owner at any time. Visitor Express maintains a revision history of each goal within a project allowing changes to be reviewed and reverted if required.

5. SYSTEM AND ACCESS CONTROL

Access to resources within our production servers is limited to a subset of authorised administrators.

Authorised administrators are only permitted to access our servers through SSH from specified IP addresses using public key SSH authentication.

Only authorised administrators are allowed limited access to our infrastructure console and must authenticate using two-factor authorisation. Only the Technical Director of NetFM has access to the root credentials for our infrastructure provider. All other staff use managed accounts with limited privileges.

Access to production data is limited strictly to NetFM and Client Administrators and subject to client authorisation in accordance with NetFM's *Access Control Policy* document.

SECURITY OVERVIEW

As soon as an employee leaves the company, we terminate all access for that employee throughout the organisation.

6. CRYPTOGRAPHY AND ENCRYPTION

Passwords are individually salted and stored using PBKDF2 with HMAC-SHA256 with 65536 iterations, per NIST guidelines on memorized secrets. Visitor Express data is stored at-rest using AES encryption with keys managed by our cloud provider. Clients can only use Visitor Express over TLS, traffic is encrypted between your browser and our load balancer.

7. LOGGING AND MONITORING

Our application logs are aggregated centrally within our VPC. We hold application-level access logs and also maintain system-level logs from our infrastructure. All changes made to our infrastructure are logged by our cloud provider.

8. NETWORK SECURITY

We limit external access to our resources strictly by necessity using security groups. By default, no ports are remotely accessible to our infrastructure. A single bastion host has its SSH port (22) exposed to remote traffic which is only available to authorised administrators with an authorised private key pair.

All public services are exposed internally to a load balancer, which allows requests from the internet to be routed internally to our application servers without directly exposing them to the internet.

9. SECURITY IN DEVELOPMENT AND DEPLOYMENT PROCESSES

Source code for Visitor Express is stored in a private repository on GitLab. Deployments are automatically orchestrated from GitLab-CI, and only privileged engineers have the rights to make pushes to repositories that are deployed to our production environment. Our repository allows us to audit the code that was pushed with each release.

All team members are required to use two-factor authentication. Only authorised administrators are able to make configuration changes to our application servers or the software running on them.

When engineers leave the organisation, their access rights to all and any repositories are revoked.

10. OPERATIONS SECURITY

NetFM have installed anti-virus and anti-malware software on all laptops and desktops used by our employees. In addition, these laptops are password protected and, in most cases, encrypted.

We carry out a quarterly audit on all laptops to make sure they are well protected.

Please refer to NetFM's *Mobile Devices Policy* for further information and guidance.