NetFM UK - Information Security Policy

1. Human Resources Security

1.1. Screening

We have the necessary processes in place to do background verification checks of certain employees if the customer requires this. These checks are compliant with the local laws and regulations of the place where the employee is based.

1.2. Terms and Conditions of Employment

All employees, sub-contractors and suppliers have to sign a confidentiality and non-disclosure agreement with us as part of their overall agreement. Also, we communicate the need for confidentiality to all our employees and hold them properly accountable for it.

2. 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 back to the company when an employee leaves the company.

3. 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.

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.

4. 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 Access Control Policy document.

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

5. Cryptography and Encryption

Passwords are individually salted and stored using PBKDF2 with HMAC-SHA256 with 65536 iterations, per NIST guidelines on memorised 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.

6. 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.

7. Network Security

Visitor Express is deployed in a private server. Our infrastructure provider (OVH) manages physical security of the infrastructure and security of the network and virtualisation layers on which Visitor Express operates.

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.

None of our resources are directly accessible from the internet, which is enforced using security groups. 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.

8. 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.

9. Operations Security

NetFM have anti-virus and anti-malware software installed on all the laptops 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.