NXG Forensics Solution

Security Controls and Processes

Version: 1.1

This document details the security, controls and processes associated with the NXG Forensics Solution.

Prepared for:
Fiscal Technologies customers.

FISCAL TECHNOLOGIES

1. Contents

1 INTRODUCTION

FISCAL Technologies receive security questionnaire requests on a regular basis from potential and existing customers who wish to use the NXG Forensic Solution or are going through the renewal process.

This document is the collated responses from previous security questionnaires and should provide answers for the majority of questions asked in relation to the development and operational running of NXG Forensics Solution.

It outlines the security protocols and protection undertaken by FISCAL Technologies to secure the safety of customer data and explain the robustness of the NXG Forensics solution. It will answer queries your organisation may have prior to undertaking or renewing a relationship with FISCAL Technologies.

2 COMPANY INFORMATION

2.1 BUSINESS ADDRESSES

EMEA Headquarters	**North America Headquarters**
FISCAL Technologies Ltd	FISCAL Technologies, Inc.
448 Basingstoke Road	PO Box 99551
Reading, RG2 0LP	Raleigh
United Kingdom	NC37625

2.2 COMPANIES HOUSE REGISTRATION

FISCAL TECHNOLOGIES LTD.

Company number: 04801836

2.3 VAT REGISTRATION DETAILS

FISCAL Technologies Ltd is a VAT registered company.

UK VAT number: 815382334 or GB815382334

2.4 ICO REGISTRATION DETAILS

ICO Registration Number: ZA115827

2.5 SECURITY COMPLIANCE CERTIFICATIONS

ISO/IEC 27001:2013 Information Security Management System

Scope: The provisioning and management of FISCAL's SaaS delivered financial software from the Reading facility and the associated data centres.

Cyber Essentials

Scope: Only FISCAL Technologies Ltd and its NXG Forensics SaaS solution excluding all else.

3 PRODUCT OVERVIEW

NXG Forensics is an AI-powered risk analysis system which interrogates supplier transaction and employee data, searching for potential risks, anomalies, and fraud.

4 APPLICATION DESIGN & ARCHITECTURE

4.1 REFERENCE ARCHITECTURE

NXG Forensics is a SaaS (Software as a Service) solution hosted using Microsoft Azure's cloud PaaS (Platform as a Service) and IaaS (Infrastructure as a Service) accessed by a web front end.

Each resource is secured according to the best practise for that resource, communications between the components are all secured with TLS 1.2 or greater.

The original NXG Forensics architecture is based on the following Microsoft Azure cloud architecture:

https://docs.microsoft.com/en-us/azure/architecture/

NXG Forensics also utilises an AKS cluster which is used primarily for the purpose of running SOLR.

4.2 DATAFLOW DIAGRAM

The diagram below illustrates the key dataflows between users and the NXG Forensics solution.

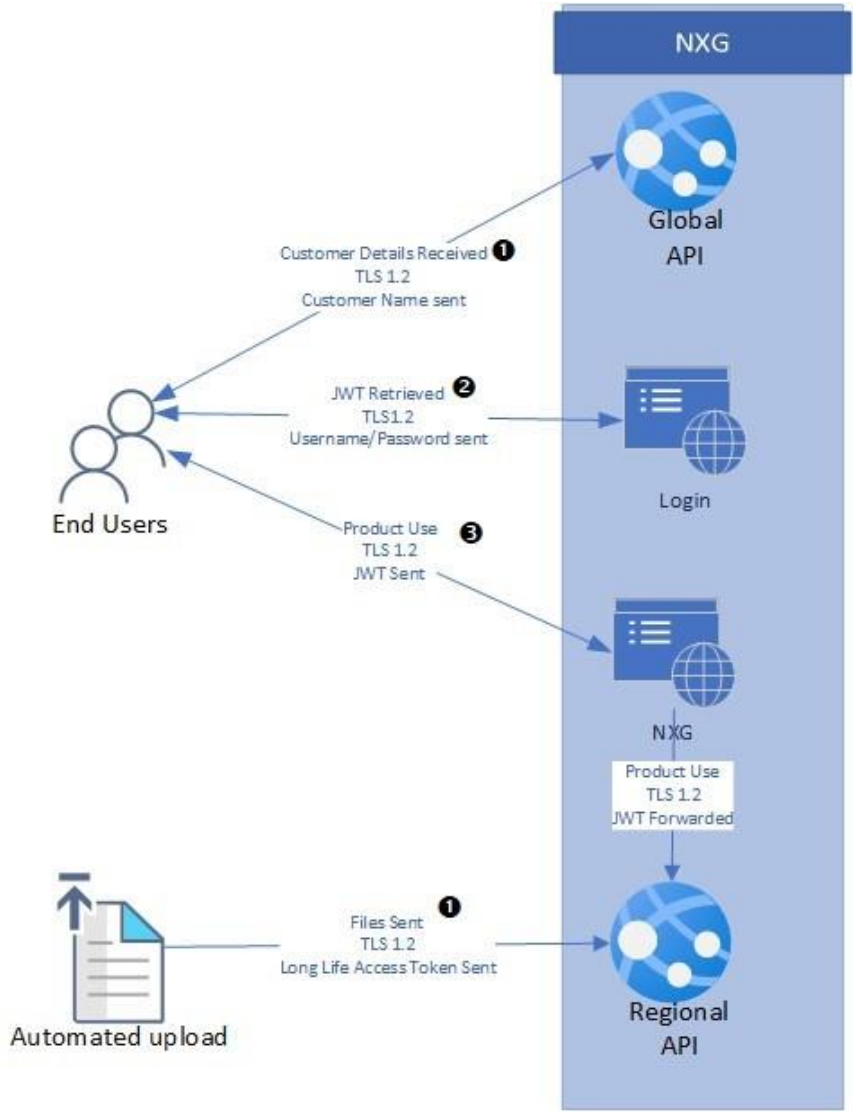

Figure 1 -Dataflows Between Users & NXG Forensics Solution

4.3 HIGH LEVEL ARCHITECTURE DIAGRAM

The diagram below provides an overview of the core NXG Forensics components and their interactions.

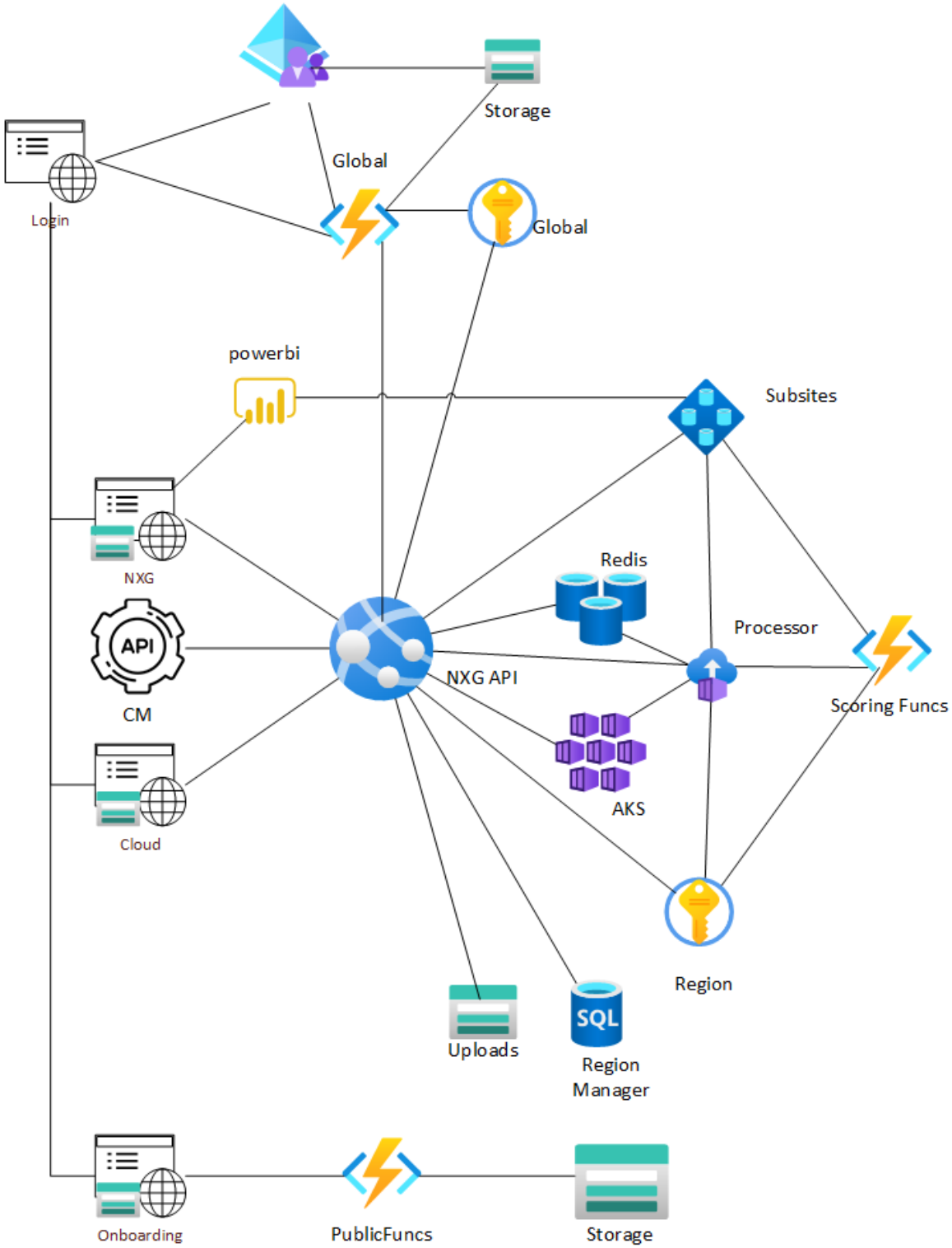

Figure 2 - Core NXG Forensics Components & Interactions

5 APPLICATION DEVELOPMENT

5.1 DEVELOPMENT APPROACH

NXG Forensics is developed on the Microsoft .NET platform using Agile software development techniques, Scrum, Test Driven Development, Pair Programming, Continuous Integration and Continuous Delivery.

- Separate test and production environments are housed on Microsoft Azure
- Identified changes to the code base are tracked and must have a work item assigned to them.
- Modifications are carried out in 2 week sprints and are made in separate branches.
- At the end of each two-week sprint, all verified changes will be promoted to a release.
- A pre-release meeting will be held with the CAB who will review and approve the release.
- Release is deployed to the live production environments via an automated pipeline.

5.2 SECURITY BY DESIGN

NXG Forensics is developed using a "security by design" approach and adhering to OWASP principles.

Security is considered throughout the NXG Forensics development process, from design through to final sign off for the release.

- All tasks are evaluated on creation, to determine whether they will have a potential impact on the security of the solution.
- If a task is identified with a potential security impact, any mitigation will be addressed during the design phase and verified during the review stages.
- Any tasks flagged as having a security impact are reviewed by the CAB in the release readiness meeting to ensure that they have been addressed prior to deployment.

5.3 DEVELOPMENT TEAM

The NXG Forensics Solution development is carried out by permanent employees located in the United Kingdom. At this time, no work is outsourced to third parties.

FISCAL Technologies requires members of the development team to take GDPR, ISO 27001 and OWASP awareness training on an annual basis.

Employee duties are segregated within the development, and infrastructure support functions, but due to the nature and size of FISCAL Technologies there is some overlap between these roles. For example, there is a single development team responsible for solution development and verification with some engineers occasionally required to assist with operational support.

5.4 DEVELOPMENT ENVIRONMENT

NXG Forensics development and test environments are deployed to the Microsoft Azure cloud on separate sites. All resources are hosted on unique services in Azure for each environment.

The solution is developed using the latest technologies to take advantage of built-in protection against several common vulnerabilities, including amongst others SQL injection, XSS attacks, CSRF, HTTP Response attacks.

5.5 VERIFICATION

FISCAL Technologies believes that product quality is the responsibility of the whole team and doesn't have a dedicated QA team.

NXG Forensics test strategy utilises automated testing and FISCAL Technologies has invested in developing a suite of unit tests, automated integration, UI, and performance tests to maintain the quality of NXG Forensics Solution.

Unit tests are created for each code change, and these are run automatically every time the source is built. Testing is further supported by a suite of Playwright tests which run each night.

Changes are peer reviewed, before check-in and all changes are manually checked on the test environment and approved for release.

Weekly performance testing is performed on NXG Forensics using an historical data file of 3 million transactions. Additional load testing is performed when research is required into specific performance issues or when changes are required to improve the scalability of the solution.

Functional and automated testing must be completed successfully prior to the NXG Forensics release.

5.6 SOURCE CONTROL MANAGEMENT

All NXG Forensics code changes are managed by an offsite source repository. This repository is used to identify all the changes that are contained within a particular software release.

5.7 CHANGE MANAGEMENT PROCESS

All changes are peer reviewed, verified, and approved on an internal test environment prior to release. A release readiness meeting is held by the Change Advisory Board (CAB). The CAB consists of the Director of IT and Security, Head of Development, Product Owners, and SCRUM leads from the development team. During this meeting the CAB reviews a pre-list checklist covering Security and Compliance, Operational Excellence, Performance and Stability, Cost optimisation, User Experience, the release is only approved if the list is successfully completed.

Once approved, it is deployed via an automated CI/CD pipeline.

5.8 PRODUCTION UPDATES RELEASE PROCESS

Updates to NXG Forensics live production sites are released via a secure automated CI/CD deployment pipeline once release approved by CAB.

The solution is deployed through a service account using Infrastructure as Code (IaC) to prevent and reduce risk with integrity of the build being compromised, potential malicious intent, remove the need for personnel to have privilege in the production environment. Ensuring the consistency and security of deployment. The release process is automatically applied to the solution without the need for customer intervention.

Product updates are deployed on a continuous basis currently every two weeks; more frequently if required. Where possible these updates will ensure the minimal impact on customers. Any updates that will potentially impact customers are deployed outside of standard working hours. In exceptional circumstances high priority patches may be deployed during working hours, potentially resulting in a minor interruption to the service.

FISCAL Technologies operates a roll-forward approach when updating NXG Forensics. Should an issue be encountered during the deployment, a further update will be released to resolve it, rather than rolling-back the entire update.

NXG Forensics customers are informed of new features via the "What's New" notifications displayed within the product.

6 USER ACCESS

NXG Forensics is hosted in the Microsoft Azure cloud service and users can access it via a supported browser (Google Chrome, Microsoft Edge & Mozilla Firefox).

No part of the solution is hosted at the customer's site & NXG Forensics does not support mobile devices.

6.1 USER AUTHENTICATION

NXG Forensics users are provided with an account utilising their email address as its unique user identifier. Access is secured either by username/password or by using the integrated SSO solution. User accounts and passwords are managed by Azure B2C unless customers have selected the SSO integration option.

Threat management is handled by Azure B2C Smart Lockout. Further information can be found here:

https://docs.microsoft.com/en-us/azure/active-directory-b2c/threat-management

NXG Forensics solution doesn't support CAPTCHA.

Customers are responsible for managing users within their NXG site.

6.2 PASSWORD POLICY

NXG's password policy follows the "Strong" complexity requirements provided by Azure B2C which requires a password between 8 to 64 characters and 3 out of 4 of the following types of characters: lowercase, uppercase, numbers, or symbols.

New users are supplied the URL to their site and are required to change their password the first time they logon.

NXG Forensics users can reset their password by selecting the option on the login page by selecting the "Forgot your password" link to create a new password. This password can be used in conjunction with their email address to access their NXG Forensics user account.

FISCAL's internal password policy requires a minimum 14 characters with complexity requirements. Passwords have a maximum age of 180 days and minimum of 1 days. Passwords cannot be reused remembering the last 24 passwords. Account lockouts are in place with a 15-minute lockout duration following 10 invalid attempts in a 15-minute window. We also require MFA be used where possible. Multi-factor authentication is required by to access the live production and administration tools. By default, MFA is required for all user accounts, regardless of privilege level.

Multi-factor authentication is required to access the live production NXG Forensics administration tools.

6.3 SSO INTEGRATION

NXG Forensics provides an option to integrate with the customers own SSO solution. This option allows the customer to manage items such as password expiry / reset, multi-factor authentication requirements, and lockout policies, using the customers own authentication policies.

The list of currently supported SSO providers can be found on the NXG Forensics on-boarding pages, by following the link - https://onboarding-uswest.apfnxg.com/sso/overview

6.4 USER PERMISSIONS

NXG Forensics provides the ability for customers to restrict which areas of the solution their users can access via the Access Permissions feature.

Customers can restrict user access in the following areas: file upload, create access token, user administration, actions, employees, and unit access.

6.5 SESSION MANAGEMENT

NXG Forensics Solution maintains user sessions and manages them using Microsoft Azure B2C, which determines when the session identifier is no longer valid.

User sessions currently timeout after one hour. This timeout is not customer configurable.

The system allows multiple user sessions for the same user.

7 INFORMATION SECURITY

7.1 DATA UPLOADS

Customers must upload their transaction, supplier and employee data files to the NXG Forensics Solution via an API for processing and analysis.

The system only accepts valid files of a specific type and size limits are enforced. The files are parsed as text files and are not executable. Once uploaded the files are not available for download.

Documentation on the uploads API can be found here:

https://onboarding.apfnxg.com/uploads/why

NXG Forensics does not actively connect to the customer's network and therefore does not require a dedicated network connection.

All website certificates use SHA256 with either 2048-bit RSA or 256-bit ECDSA keys.

7.1.1 Single Point of Failure

The NXG Forensics processor is the only known single point of failure. The processor is used when uploading data and therefore does not affect the daily reviewing of risks and suppliers. In the rare event of the processor failing, the Engineering team receives an alert allowing them to investigate and restart the service.

7.2 DATA TYPES

NXG Forensics processes invoices and master-supplier data held in ERP / accounting systems. Additionally, if a customer has the Employees option, then they also will need to upload employee data.

NXG Forensics:

- Does not require any personally identifiable data, but it is possible the supplier information will contain names, phone numbers and email addresses. It is also possible that some suppliers will be individuals and so will be recognisable by "supplier name" and address information.
- Does not store any Protected Health Information (PHI) data.
- Does not store any financial data considered to be "in-scope" for Payment Card Industry Data Security Standard (PCI-DSS) or Sarbanes-Oxley (SOX) regulations.

7.3 DATA USAGE

Data is used within the solution to enable it to identify patterns and find future potential risks.

As per the contract, customer data may be used for development and test purposes to improve the effectiveness of the solution and ensure that the most appropriate risks are identified. Customer data is Anonymised prior to use.

7.4 DATA LOCATION

NXG Forensics is hosted in the Microsoft Azure cloud and customer sites are available in the UK, EU, and the US Azure regions.

A small amount of metadata resides in the EU region.

7.5 METADATA

Product usage metrics are collected as Metadata to help improve customer service and is stored in the EU region. This data includes:

- Page visits
- Processing metrics
- Authentication attempts
- Login information
- Permissions
- Audit logs

It is not possible to opt out of this functionality as this data is required to ensure that the service is running effectively.

7.6 DATA SEPARATION

NXG Forensics segregates each customer's data into separate customer databases.

7.7 ENCRYPTION

During customer data uploads NXG Forensics utilises a RESTful API connection secured with JWT (JSON Web Token) bearer authentication and HTTPS/TLS 1.2 or higher (AES 256) encryption.

All data at rest is secured using AES-256 encryption.

NXG Forensics is hosted in Microsoft Azure. Publicly accessible endpoints all require authentication and authorisation and where applicable firewalls are deployed to further restrict access.

7.8 DATA RETENTION

Historical data is kept within the system to aid in risk finding activities. Data is retained for the life of the customer contract, regardless of length. The more data available to the NXG Forensics Solution the more accurate the analysis.

NXG Forensics does not provide an archiving capability.

7.9 DATA DESTRUCTION

If a customer should terminate their contract with FISCAL Technologies, NXG Forensics securely removes all associated data from the customer's account leading to the destruction of their data and backups within 30 days.

Custom scripts are used to remove NXG Forensics platform elements from Microsoft Azure. Azure security processes are then utilised to remove the data from their PaaS (Platform as a Service) and IaaS (Infrastructure as a Service) offerings, (https://servicetrust.microsoft.com/).

Details of Microsoft Azure's disposal of equipment can be found in the Equipment Disposal section in the attached link:

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

7.10 DATA BACKUPS

Customer backups are created frequently (every 10 - 15 minutes for transaction logs, dailies every 24 hours, and full weekly backups) that allow a point in time recovery for any backups. Backups are kept on a rolling 7 days as part of the Microsoft Azure cloud solution and can be restored to a new site should NXG Forensics encounter a catastrophic failure.

Backups are stored on a separate site in the same geographical location as the customer's main site.

7.11 DATA ACCESS

Access to NXG Forensics customer data is restricted to FISCAL employees required to investigate specific customer issues raised via the FISCAL customer helpdesk.

8 APPLICATION SECURITY

8.1 VULNERABILITY MANAGEMENT

FISCAL Technologies use a variety of tools to minimise the impact of security vulnerabilities. Packages used by NXG Forensics are reviewed and updated regularly to reduce the opportunity of running against outdated components.

Vulnerability scans are run against NXG Forensics infrastructure on a weekly basis. When issues are identified they are evaluated, and resolutions are scheduled based on severity. Issues are resolved during NXG Forensics two-week release cycle, but high priority issues can be deployed as hot fixes in between scheduled releases. Critical and high-risk vulnerabilities are resolved or remediated within 14 days of a remedy becoming available.

Microsoft Azure functionality includes:

- B2C which has inbuilt defences to defend against session replay and man-in-the-middle attacks.
- Key Vault which secures secrets.
- The platform manages file integrity monitoring.
- SQL Transparent Data Encryption (TDE) manages the keys for this multi-tenant solution
- Further information can be found at here:

https://docs.microsoft.com/en-us/azure/active-directory-b2c/threat-management

The NXG Forensics Solution:

- is developed following OWASP security principles.
- uses a combination of Entity Framework & parameterised queries for data access to protect against SQL injection attacks.
- UI is created using React, which comes with built-in mechanisms to protect against XSS attacks.
- Uses React route templating to ensure URLs follow a certain pattern. If the URL is manipulated, the user will either be redirected back a valid page which they are authorised to access or an error page.

The API:

- uses bearer tokens for authentication. This prevents CSRF from being an applicable attack vector.
- uses ASP .NET core which has built-in protection against HTTP Response Splitting attacks. It makes minimal use of HTTP response headers, and no user untrusted values are use in HTTP response headers.
- uses ASP .NET core authentication, with middleware running for all requests to enforce authentication. The API is also configured so that by default endpoints will return a forbidden

response until the endpoint explicitly specifies what permissions are required to access that resource.

- has a top-level exception handler which returns no detail in the event of an unhandled exception when running in production.

Microsoft Defender for the Cloud is enabled on our cloud environment and is reviewed on a regular basis to ensure that latest security recommendations are reviewed and implemented as appropriate so that the platform is secure.

Risk assessments are performed on third-party packages and libraries, which include reviewing the justification for using the package and the results of a vulnerability scan security assessment.

To prevent data leakage via error messages, NXG Forensics standard error handler only returns HTTP status codes.

8.2 MALWARE PROTECTION

Malware protection is handled by Microsoft's Azure platform. Additionally, weekly vulnerability scans are performed on the third-party packages that are used within the solution.

8.3 PENETRATION TESTING

NXG Forensics Solution is subject to an annual Penetration test performed by an external CREST accredited agency.

This is an external test performed against a test account created on the production environment. This test does not include a source code review, but the external testers are granted access to a user account.

9 PHYSICAL SECURITY

9.1 MICROSOFT AZURE CLOUD COMPUTING SERVICES

The physical security of the NXG Forensics servers is managed by the Microsoft Azure service team. Details of which can be found here:

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

Microsoft Azure meets the following security standards; ISO 27001/27002, SOC1, SOC2

https://docs.microsoft.com/en-us/compliance/assurance/assurance-datacenter-security

10 OPERATIONAL SECURITY

NXG Forensics is a SaaS solution deployed in Microsoft Azure. Where NXG Forensics utilises Microsoft SaaS offerings Microsoft are responsible for the patching and security of these products in line with their compliance requirements and service agreements.

For all other areas of NXG Forensics, FISCAL manages the patching and update as required and deployed using IaC (Infrastructure as Code) techniques.

Details of Microsoft's compliances and audit reports can be found here: https://servicetrust.microsoft.com/

10.1 SECURE ENVIRONMENT

NXG Forensics is a SaaS solution deployed on the Microsoft Azure Cloud platform. This platform provides a secure environment to host the application and allows it to take advantage of the security features provided. Further details of the security features provided by the Microsoft Azure Cloud Computing Service can be found by following the link below:

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

The live production NXG Forensics solution is deployed to a separate environment, segregated from all development and test environments. Access to NXG Forensics live production environments is restricted to only those employees that require it on a least privilege basis and the solution is updated via a secure deployment pipeline.

The solution uses an Azure VPN Gateway to administer the service. The supported cipher suites are documented by Microsoft on the link below under the "What IKE/IPsec policies are configured on VPN gateways for P2S?" and "What TLS policies are configured on VPN gateways for P2S?" sections.

https://docs.microsoft.com/en-us/azure/vpn-gateway/point-to-site-about#what-ikeipsec-policies-are-configured-on-vpn-gateways-for-p2s

NXG Forensics uses a multitude of different technologies to protect customer data, these include, but is not limited to, the use of the following:

- Azure's SQL Transparent Data Encryption (TDE), Azure managed identities, HTTPS, and the Azure Key Vault.
- Cloudflare and Microsoft Azure DDoS Protection provide protection to NXG Forensics from Denial-of-Service attacks.

Network ports used to connect to NXG Forensics are limited and controlled, and additional network restrictions implemented to limit network intrusion.

10.2 **ACCESS MANAGEMENT**

FISCAL Technologies has adopted the principle of least privilege to ensure that access to NXG Forensics live production environments is only available to those that require it. Access to NXG Forensics live production environments is granted to members of the development team on a limited basis, only when required to investigate and diagnose issues. Escalated privileges are removed once the issue has been diagnosed and addressed.

Members of FISCAL Technologies support team are authorised to directly access customer sites via the User Interface once there is an open support ticket and they have requested authorisation from the customer.

An individual incident for a customer will be provided a support ticket, with ticket ID number for reference, communication is primarily through email however also through direct calls to the customer affected (when possible), customer is informed up to the point of resolution and a final satisfaction email is sent upon closure.

It is FISCAL Technologies policy that all operational administration is undertaken from FISCAL supplied equipment.

10.3 **MONITORING**

The NXG Forensics Solution is monitored on a regular basis. Azure Monitor provides the capability to monitor trends and increase capacity where needed. We also utilise the elastic nature of Azure to scale up when needed. When consistent platform issues are identified the resources allocated to the platform are adjusted appropriately.

NXG Forensics sites are monitored to ensure that resources are available to prevent individual customers impacting the performance of other customers in that pool. No specific SIEM tools are deployed.

Microsoft Defender for the Cloud is regularly monitored and reviewed on a regular basis to ensure that the latest security recommendations are implemented as appropriate to ensure the platform is secure.

FISCAL Technologies does not currently deploy an Intrusion Detection System or Intrusion Prevention System (IDS / IPS) for NXG Forensics.

11 DISASTER RECOVERY

11.1 SOLUTION RESILIENCE

NXG Forensics Solution infrastructure resilience and redundancy is managed by Microsoft Azure. Details which can be found here:

https://docs.microsoft.com/en-us/azure/security/fundamentals/infrastructure-availability

NXG Forensics is not hosted in a virtual infrastructure and therefore virtual machines may not be restored to a previous point in time and images cannot be downloaded and moved to a new cloud provider.

11.2 SITE AND DATA RECOVERY

Deployment of NXG Forensics is fully scripted and in the event of a catastrophic platform failure, the service can be recreated by re-running the deployment scripts and restoring customer data from backups.

The Recovery Point Objective (RPO) is 24 hours (from incident start), and the Recovery Time Objective (RTO) is 3 business days.

This recovery time of the NXG Forensics Solution failure is dependent on the extent of the failure. In the worst-case scenario that the platform needs to be rebuilt, it could take up to 5 days to rebuild the site and restore all customer data.

11.2.1 Site Recovery Testing

NXG Forensics consists of two platform components, a global service, and regional services. A full test of all components is performed annually as part of a disaster recovery test, but tests of the regional components are run weekly as part of the recreation of testing environments.

Recovery of NXG Forensics is tested by rebuilding a copy of the production environment, uploading test customer data, and validating the results.

12 APPLICATION AUDITING

12.1 LOGGING

NXG Forensics audits a variety of activities, including file uploads, workflow, access token generation, changes to users and permissions and configuration settings, the majority of these logs are held internally. Application logs are retained for over 90 days before deletion.

Users can also add comments when updating workflow, which can be reviewed at any time.

12.2 USAGE

Logs are not routinely monitored but are used by internal support for monitoring the platform, troubleshooting and diagnostics.

NXG Forensics Solution audit logs are not directly accessible to customers, however if required logs relevant to a specific customer can be retrieved. Please note that dependent on circumstances there may be an additional charge for this service.

13 AUDIT ASSESSMENT

FISCAL operates an ISMS programme that is compliant in ISO/IEC 27001 and Cyber Essentials. FISCAL is audited twice yearly for ISO27001 and once yearly for Cyber Essentials compliance.

A summary report may be provided upon request only.

Customers may perform external security assessments (Penetration Testing) on the NXG Forensics Solution, after requesting and receiving consent from FISCAL Technologies. FISCAL Technologies may request a copy of any findings from these assessments.

14 SUPPLIER CHAIN SECURITY

14.1 THIRD-PARTY SUPPLIERS

NXG Forensics Solution utilises the following external third-party services as part of its solution:

- **Microsoft Azure Cloud Computing Services**

  1 Microsoft Way, Redmond, WA, United States

- **Cloudflare**

  101 Townsend Street, San Francisco, CA 94107, United States

  Cloudflare is an American content delivery network and DDoS mitigation company.

  It provides the NXG Forensics solution with DNS and DDOS protection.

- **LexisNexis Risk Solutions**

  UK Head Office, Lexis House, 30 Farringdon Street, London. EC4A 4HH

  LexisNexis is used by NXG Forensics to provide Sanctions and ESG matches.

14.2 THIRD-PARTY SUPPLIER POLICY

FISCAL Technologies have an ongoing persistent contract with the third-party suppliers listed above. They regularly review the solutions, identifying potential risks and either mitigating or accepting them depending on their severity.

FISCAL Technologies assess the risk of any suppliers prior to selection and engagement validating for security, financial, sanctions, ethical requirements to ensure they meet the needs of the business.

Customer data is not available to Microsoft Azure or Cloudflare as it is encrypted and not visible during transit and at rest.