MIB Navigate Security Overview

FINAL Version 2.0 – Updated for VS&TD Release

03 October 2025

1 Security

This document provides an overview of the security measures implemented as part of the Navigate programme. Using the ShiftLeft methodology we have embedded security and privacy by design at the start of the application development process. We have adopted a holistic approach that covers industry standards such as OWASP, ISO 27001, as well as data protection requirements, including the GDPR.

1.1 Infrastructure Security

Security controls, including tools, are in place to secure all our resources across our environment with a robust security framework enabling us to prevent, detect, and respond quickly to threats. Our security platform receives dynamic security intelligence updates from global threat databases to provide extra defence against threats like zero day vulnerabilities. We have a robust environment with segregations primed to receive or send files from 3rd parties which undergo rigorous security scans, safeguarding against potential threats.

1.2 Network Security

Access to our environment is restricted via WAF protecting applications, API from exploits and vulnerabilities, and Firewall with IDS/IPS capabilities using security protocols like SSL encryption and TLS. Our default security policies restrict use of obsolete/out-dated technologies and ensures secure data transmission via modern security protocols. The environment is matured through Zero-Trust framework with network segregation by limiting communication across the network and denying access to critical segments. Access to our resources from internet are restricted to VPN enabled domain joined corporate devices and cloud-based proxy with firewall access.

1.3 Access and Identity

Industry leading tools are used to implement Identity and Access Management with Role Based Access Control (RBAC) using a Zero Trust Identity model with least privileged principal and Multi-Factor Authentication (MFA) for user login with periodic audits and reviews. Security policies are implemented for password protection, application access, privileged access management and access removals for employee transfer/termination. MIB utilises a VPN and MFA controls for secure access to our corporate network from any outside or unsecured networks.

1.4 Data Security

All data at rest is encrypted with 256-bit AES encryption and is FIPS 140-2 compliant. While anonymisation and pseudonymisation techniques support compliance with data protection laws,

data is classified based on the sensitivity of the data and the access to the data is restricted with RBAC to ensure that data is accessed by internal resources and authorised third party suppliers only.

We have safeguarded our data in transit with encryption and apply present-day protocols such as TLS1.2 or higher, SFTP and HTTPS for all our resources. Data resources are segregated from other resources which also helps to enable ease of data driven traffic within data resources. Threat detection systems and security policies in place generate alerts on suspicious activity and prevent data loss/breach.

1.5 Code Security

Our Secure SDLC methodology integrating OWASP is achieved with ShiftLeft approach where security is always preserved during all stages of the development. The codebase/repositories are embedded with SAST tool which at every step of our development detects vulnerabilities in real-time which are worked upon thus preventing them getting into the application code before release.

1.6 Logging and alerts

Comprehensive real-time secure logging and monitoring with tamper proof policies in place enabled for all our resources and user activities including firewall, WAF and anti-malware tools. Logs collected in a centralised location are analysed with SIEM tools that has advanced threat intelligence and Regulatory compliance auditing and reporting. The SOC team, responsible for monitoring and managing security posture, evaluates the alerts to help eliminate false positives and focus on real attacks, reducing the mean time to remediate real incidents.

1.7 Key management

Security keys are stored and managed in a key management service which is FIPS 140-2 Level 3 NIST validated and security policies are in place to ensure that key rotation and renewals happen periodically. Access to the key management services is highly restricted using privileged access and network segregations.

1.8 Penetration Testing

Periodic internal and annual third-party PEN tests (carried out by CREST accredited testers) validate the security of applications and infrastructure in an effective way to proactively identify potential vulnerabilities, risks, and flaws that provide an actionable remediation plan to plug loopholes before they are exploited.

1.9 Third Party Risk Management

The MIB Third-Party Risk Management framework includes an integrated supplier assurance procedure followed by both the Information Security and Data Privacy teams. All third parties are processed through the onboarding procedure review in accordance with criticality and risk posture. A cyclical process for review is in place determined on criticality of service provision and risk.

1.10 Security Incident Response

MIB operates a Security Incident Management Policy supported by Information Security, the BCP Management Framework and Data Privacy. The Security Incident Management Policy and Plans are reviewed at least annually supported with scheduled scenario-based testing including DR, BCP, Ransomware and Breach events for assurance purposes. All policies and plans are signed off at Executive level and communicated business wide.

1.11 Business Continuity Plan (BCP) – Disaster Recovery (DR)

MIB are certified to ISO22301 for Business Continuity Management Systems. Similar to Security Incident Response, there are policy, plans and playbooks in place based on scenario testing and lessons learned, which are reviewed and updated at least annually.

We have set up our primary and secondary locations in the UK as our business continuity and disaster recovery (BCDR) strategy, where all the resources and data are replicated between these two UK sites. The tested failover from primary region to secondary happens within the accepted SLA to ensure that our business applications are online during planned and unplanned outages.

1.12 Certifications

MIB is certified to ISO 27001, the international standard for information security management systems, and ISO 22301, the standard for business continuity management systems. These certifications reflect our commitment to maintaining strong security controls and ensuring resilience against operational disruptions.