# SECURITY BRIEF

MOMINT

# OVERVIEW

The following security document provides an overview of the security standards and guardrails instilled within Momint. This will serve to highlight the current security posture in accordance to the technologies, processes, data and regulatory requirements encompassing the organisation. The areas that will be covered include:

- Security policy: Application and Infrastructure protection
- Security policy: Privileged access and user management
- Security policy: Data protection
- Security policy: Smart contracts and transaction protection
- Security policy: Continuous assurance and third-party reviews

# APPLICATION AND INFRASTRUCTURE PROTECTION

The Momint solution is built upon the MEAN stack which includes a combination of MongoDB, expressJS, Helmet, AngularJS and Node.js all hosted in Microsoft Azure.

## Application Protection

To ensure deployed applications (web, mobile and APIs) meet security best practices a number of controls have been embedded adhering to OWASP Top 10 and SANS 25 application controls.

As a base standard, users are required to have a minimum password length of twelve characters including a mixture of uppercase, lowercase and special characters. Additionally by default, multifactor action is required where one-time-pins (OTPs) are sent to an out of band channel using either Google authentication or Microsoft authenticator applications.

All user session management is managed through json web tokens (JWTs), that governs strict authorisation management and includes a session timeout period of 30 minutes for all users.

From an external perspective, Momint's application is protected by Azure Front Door, which provides a web application firewall (WAF) and protection for DoS and DDoS based attacks. The Azure WAF has been configured to contain rule sets both from OWASP and SANS institute to negate any client or server-side attacks such as cross-site scripting (XSS) and local file inclusion (LFI). Sentry has also been deployed as an application monitoring agent, to detect any anomalies that may not present as regular user behavior when utilising Momint.

In the event Azure's WAF is able to be bypassed, Momint has included both client side and server controls, where each request is validated or rejected by downstream applications. Safety mechanisms for smart contracts have also been embedded using mutlisig that can pause or disable Momints smarts contract in the event of compromise.

## Infrastructure Protection

As the Momint application is hosted in Microsoft Azure using Azure app service. This ensures all hosting infrastructure is kept up to date, as containers images are patched against any public exploits through automated updates by Microsoft. As an additional layer, Microsoft Defender is used  on all hosting infrastructure, where any security concern discovered is highlighted in Azure Security Center for remediation.

In relation to secret management used to connect to hosting infrastructure, all secrets used in Momint's cloud estate are stored in Azure key vault adhering to the principle of least privilege for security principals (users, groups and service principals).

The MongoDB used for storage is segregated in Momint's internal network and encrypted at rest. To ensure data redundancy and failover, daily backups are conducted.

# PRIVILEGED ACCESS AND USER MANAGEMENT

Momint's standard across all infrastructure enforces only two administrator roles. Internal staff access rights are managed through role based access control (RBAC) in Azure and Github. Momint also uses Github's enterprise license to further add granular access rights in development pipelines. All user access to servers is further conducted in Momint's internal network with a requirement of multifactor authentication.

# DATA PROTECTION

As data is sent from client applications to the web server, all communication channels are encrypted using TLS 1.2 where symmetric encryption uses a **key length of X and asymmetric encryption uses X.**

All data at rest is encrypted and all private keys used in the estate are encrypted to military standards using AES256 bit encryption.

Personally identified information (PII) is protected using data masking on the MongoDB to ensure standard database users are unable to view PII such as telephone numbers, email address or card numbers.

<ADD/DELETE IF YOU HAVE ANY DLP IN YOUR ESTATE>

<DLP TOOL> has been provisioned in Momint's estate to prevent any sensitive data loss. DLP(data loss prevention) ensures that sensitive data such as PII is not lost, misused or accessed by unauthorised users. The <DLP tool> classifies confidential and business data and identifies any violations under Momint's defined policies. This allows Momint to be both GDPR and POPIA compliant.

# SMART CONTRACTS AND TRANSACTION PROTECTION

Smart contract and transaction processes conducted by Momint are in line with the Proceeds of Crime Act 2002, Anti Money Laundering (AML) policies and producers. Full details pertaining to the policies provisioned by Momint adhering to AML are available from Momint's AML policy document. As a summary of this document, the following are included:

- Employee Obligations: All Momint staff are required and held accountable for all suspicious money laundering actions.

- AML Officer Obligations: Momint is required to have at least one AML officer who is required to disclose and report any breach of AML policies.
- Customer Due Diligence: Customer due diligence is conducted adhering to KYC through having requirements for creators and collectors.
- Transaction Monitoring: All transactions are monitored and facilitated in the Momint platform through preconfigured risk scores for all users.
- Record Keeping: All transaction histories and any relevant financial data is kept for five years.

## CONTINUOUS ASSURANCE AND THIRD PARTY REVIEWS

Momint contains two security champions that perform continuous internal security engagements to identify and provide security recommendations for all deployed applications and cloud environments. Where both of these security champions are accredited by the EC Council achieving the Certified Ethical Hacker (CEH) certification. Since the inception of Momint, two internal audits have been conducted. In addition to this, an external audit has been conducted encompassing the Momint application.

As security audits only provide a snapshot of the current security posture of an organisation, Momint has further procured security tooling to provide continuous assurance within development pipelines. Presently, Momint uses dependabot in GitHub, to ensure all development dependencies used in the application are kept up to date. Furthermore, Momint uses GitHub’s enterprise license that provides environment protection for code repositories and credential scanning. Static code analysis tooling is also used to ensure development code meets security best practices.