Mitigate ESG Platform Security Policy

v1.1. , 02.2024

Table of Contents

Introduction 2
Scope 2
The Platform high-level architecture 2
Data Security & Privacy 3
User Access Control 3
Access Logging and Monitoring 4
Secure API 4
Infrastructure Security 5
Security Audits 5
Third-Party Security 6
Acceptance and Compliance 6
Incident Response 6
Policy Review and Update 6

Prepared by Mitigate: esg@mitigate.dev

Introduction

This Security Policy outlines the measures and protocols in place to ensure the security and integrity of the Mitigate ESG Platform. The policy is designed to protect the platform, its data, and its users from unauthorized access, disclosure, alteration, and destruction.

Scope

This policy applies to all clients, employees, contractors, and third-party service providers who have access to the Mitigate ESG Platform or its data.

The Platform high-level architecture

Mitigate ESG Platform is a Ruby on Rails (used by companies like Airbnb, GitHub, and Shopify) and React (used by Bloomberg, Facebook, Salesforce, Microsoft, and Uber) cloud software application offering a GraphQL API for integrations. We store all customer data in secure PostgreSQL database instances on Amazon Web Services (AWS), ensuring regular data backups and security monitoring. All data in our platform is fully encrypted, both while being transferred and when stored.

Our web infrastructure is hosted on a world class PaaS service Heroku and resources are hosted within the EU region. This setup gives us strong security, the ability to adapt to different needs, and the capacity to grow with our customers across various regions. Please read more about Heroku's security here: https://www.heroku.com/policy/security .

We focus on secure web application development, actively working to prevent issues like back-door access, cross-site scripting (XSS), cross-site request forgery (CSRF), SQL injection, clickjacking, and unauthorized cross-origin scripts. We also enforce SSL/HTTPS for all communications within our app.

The physical infrastructure is hosted and managed within Amazon's secure data centers and utilizes the Amazon Web Service (AWS) technology. Amazon continually manages risk and

undergoes recurring assessments to ensure compliance with industry standards. Amazon's data center operations have been accredited under:

- ISO 27001
- SOC 1 and SOC 2/SSAE 16/ISAE 3402 (Previously SAS 70 Type II)
- PCI Level 1
- FISMA Moderate
- Sarbanes-Oxley (SOX)

Additionally, we are committed to compliance with the GDPR. More about GDPR and compliance read here: https://devcenter.heroku.com/articles/gdpr .

Data Security & Privacy

- **Data Encryption:** All data transmitted to and from the platform is encrypted using industry-standard protocols.
- **Data Backup:** Regular backups of the platform data are performed and stored securely. Backup integrity is tested periodically to ensure data can be effectively restored.
- **Data Handling:** All data collected, stored, processed, and shared by the Mitigate ESG Platform will comply with relevant data protection laws and regulations, including GDPR, to ensure the privacy and protection of user data.
- **Data Usage:** Data will only be used for purposes explicitly consented to by the users or as required for the provision of the platform's services.
- **Data Disclosure:** User data will not be disclosed to third parties without user consent, except where required by law.

User Access Control

- **Authentication:** All users must access the platform using a unique username and password. Passwords must meet the platform's complexity requirements, including minimum length, and the use of both alphanumeric and special characters.

- **Authorization:** User access levels are strictly enforced based on role-specific requirements. Users are granted the least privileges necessary to perform their duties.
- **Account Review:** User accounts are reviewed quarterly to ensure that access levels are appropriate and that dormant accounts are disabled.

Access Logging and Monitoring

- **Access Logs:** The platform will maintain comprehensive logs of all user access and activities. These logs will be regularly reviewed to identify and investigate any suspicious activities or potential security breaches.
- **Monitoring Systems:** Continuous monitoring systems will be implemented to detect and alert on unusual activities that could indicate security incidents or vulnerabilities.
- **Incident Investigation:** In the case of suspected or actual security incidents, detailed investigations will be conducted, leveraging access logs and monitoring data to understand the scope and impact.

Secure API

- **Endpoint Authentication:** We ensure that all our API endpoints require secure authentication, safeguarding against unauthorized access and ensuring that only authenticated users can interact with our platform.
- **Rate Limiting:** We implement rate limiting to prevent abuse and ensure that our services remain available and responsive, protecting against potential denial-of-service attacks.
- **Input Validation:** We rigorously validate all input through our APIs to prevent malicious data processing, effectively reducing the risk of injection attacks and other vulnerabilities.
- **Data Encryption:** We enforce TLS encryption for all communications with our APIs, ensuring that data transmitted to and from our platform is secure and protected from potential eavesdropping or tampering.
- **Version Control:** We maintain strict version control for our APIs, ensuring compatibility and secure evolution of our API infrastructure, enabling us to respond swiftly and effectively to emerging security challenges.

Infrastructure Security

- **Shared Responsibility Model:** In line with Heroku's shared responsibility model, while Salesforce ensures the security of the Heroku infrastructure, Mitigate ESG Platform is responsible for securing the application layer and managing access to its Heroku account and resources effectively.
- **Heroku Security Features:** The platform will utilize Heroku's security features to enhance its security posture, including Heroku's customer-configurable features to maintain secure deployments.
- **Compliance and Certifications:**
    - **PCI:** Salesforce's Attestation of Compliance as a PCI Level 1 Service Provider is acknowledged, with Heroku Shield Services being utilized for PCI compliance.
    - **HIPAA:** For healthcare-related applications, engagement with Heroku's sales team for a Business Associate Addendum is required for HIPAA compliance.
    - **GDPR:** The platform will adhere to GDPR regulations, ensuring the protection of data for users within the EU.
    - **ISO 27001, 27017, and 27018:** Recognition of Salesforce's certifications against these standards ensures adherence to recognized security management best practices and protection of PII.
    - **SOC 1, 2, and 3:** Salesforce's SOC reports are noted, confirming the design and effectiveness of Heroku's controls relevant to the security, availability, and confidentiality of customer data.

Security Audits

- **Regular Audits:** Security audits are planned to be conducted regularly to assess the platform's compliance with this policy and to identify potential vulnerabilities.
- **Audit Response:** Findings from security audits are addressed in a timely manner, with corrective actions implemented to mitigate identified risks.

Third-Party Security

- **Vendor Assessment:** Third-party service providers, including Heroku, are assessed for compliance with relevant security standards and best practices.
- **Data Sharing:** Data shared with third-party service providers is limited to what is necessary, and agreements are in place to ensure they adhere to equivalent security standards.

Acceptance and Compliance

All users of the Mitigate ESG Platform are required to acknowledge and comply with this security policy. Violations of the policy may result in disciplinary action, up to and including termination of access to the platform.

Incident Response

- **Incident Detection:** The platform implements monitoring tools to detect potential security incidents.
- **Incident Response:** In the event of a security incident, a predefined incident response plan is activated. This includes containment, eradication, recovery, and post-incident analysis.
- **Communication:** Stakeholders are informed about significant security incidents in accordance with the platform's communication protocol.

Policy Review and Update

- **Review Cycle:** This security policy is reviewed annually or following significant changes to the platform or its hosting environment.
- **Updates:** The policy is updated as necessary to address new security challenges and to reflect changes in best practices.