Cybersecurity Posture Documentation for Wepay

This document outlines the cybersecurity posture of **Wepay**, a leading fintech company providing digital payment solutions. As a fintech organization, we prioritize protecting sensitive financial data and ensuring compliance with relevant regulations. We maintain a comprehensive set of documents and reports to monitor and improve our cybersecurity posture, helping us safeguard our systems, data, and customer trust.

1. Cybersecurity Frameworks and Assessments

At **Wepay**, we follow industry-recognized cybersecurity frameworks to guide our security practices. Our primary framework is the **NIST Cybersecurity Framework (CSF)**, which we have tailored to meet the specific needs of the fintech industry. We also comply with other standards such as **ISO 27001** and **PCI DSS** to ensure that our security controls are aligned with global best practices and regulatory requirements.

As part of our ongoing efforts, we conduct regular risk assessments across all business units, ensuring that potential vulnerabilities and threats are identified and mitigated.

2. Security Policies and Procedures

Our security policies are designed to protect both our infrastructure and the sensitive data of our users. These policies include:

- **Information Security Policy**: Outlines our organizational commitment to cybersecurity, specifying roles, responsibilities, and the approach to managing risks.
- **Incident Response Plan**: Defines the process for responding to cyber incidents, including breach detection, containment, mitigation, and communication strategies.
- **Data Protection and Privacy Policies**: Ensures compliance with global data protection regulations such as **GDPR** and **CCPA**, outlining the steps taken to secure customer information and protect their privacy.

3. Security Audit and Compliance Reports

As part of our commitment to maintaining a strong security posture, **Wepay** undergoes annual security audits by both internal and external auditors. These audits assess the effectiveness of our cybersecurity controls and help us identify areas for improvement.

We also maintain compliance with the following industry standards:

- **PCI DSS**: To ensure secure handling of cardholder data and mitigate the risk of fraud.
- **ISO 27001**: To maintain an Information Security Management System (ISMS) that meets the highest global standards for security.

4. Cybersecurity Risk Register

The **Cybersecurity Risk Register** is central to our risk management process. It helps us track identified cybersecurity risks and categorize them based on their potential impact on the organization. This register includes the following key components:

- **Risk Identification**: Detailed descriptions of the risks associated with our systems, services, and third-party vendors.
- **Risk Assessment**: An analysis of the likelihood and impact of each identified risk.
- **Risk Mitigation**: Specific measures taken to reduce or eliminate risks, including the implementation of security controls and monitoring systems.

5. Vulnerability Management and Patch Management Logs

At **Wepay**, we have a robust vulnerability management process in place to ensure the security of our systems. This includes:

- **Vulnerability Scanning**: Regular vulnerability scans are conducted to identify potential weaknesses in our applications and infrastructure.
- **Patch Management**: We have a dedicated team that ensures critical patches and updates are applied promptly to all systems, minimizing the window of vulnerability.

6. Security Posture Reports

Our **Security Posture Reports** provide a comprehensive overview of our cybersecurity health, including:

- **Control Implementation**: A record of the cybersecurity controls in place and their status across various business units.

- **Incident History**: A log of past security incidents, including details on the cause, impact, and remediation actions taken.

- **Metrics and Monitoring**: Continuous monitoring of security metrics such as network traffic, authentication attempts, and threat detection, ensuring proactive management of security risks.

7. Control Implementation Documents

The implementation of cybersecurity controls is critical for protecting our infrastructure. At **Wepay**, we have detailed documentation on how each control is applied across our systems, including:

- **Control Configuration**: Detailed guidelines on configuring security controls like firewalls, encryption standards, and access management systems.

- **Operating Procedures**: Standard procedures for maintaining and updating these controls, ensuring their effectiveness against evolving threats.

8. Threat Intelligence Reports

To stay ahead of emerging threats, **Wepay** integrates **threat intelligence** from various sources, providing insights into potential vulnerabilities and attacker TTPs (Tactics, Techniques, and Procedures). These reports include:

- **Emerging Threats**: Regular updates on new attack techniques targeting the fintech industry, including phishing, malware, and ransomware attacks.

- **Threat Analysis**: A detailed breakdown of attacks targeting financial institutions and methods used by cybercriminals to exploit weaknesses.

- **Mitigation Strategies**: Recommended actions and security controls to prevent or minimize the impact of these threats.