Security Addendum

This Security Addendum describes the technical and organizational security measures implemented, developed, and maintained by Flare Systems, Inc. ("**Flare**") in relation to the services provided, including the Flare Platform. It applies to all Customers, including partners and resellers.

1. **DEFINITIONS**
   - **Customer Data:** Data, information, or materials provided or submitted by Customer while using the services.
   - **Security Incident:** Any event or set of circumstances that compromises or threatens the confidentiality, integrity, or availability of Service Assets, including, unauthorized use and access to Customer Data.
   - **Service Assets**: A collective term referring to both Customer Data and Systems, encompassing all data and systems involved in the provision of services by Flare.
   - **Systems**: All hardware, software, databases, communication systems, electronic data processing tools, and other related infrastructure used to store, process, or transmit Customer Data within the scope of services provided by Flare.

2. **SECURITY GOVERNANCE**
   - **Security Program.** Flare maintains a formally documented security program with clear roles, responsibilities, and processes consistent with industry standards (e.g., ISO 27001). The security program is reasonably designed to address risks to Service Assets and ensure compliance with legal and regulatory requirements.
   - **Annual Review.** Security policies are regularly reviewed and updated to reflect current industry standards and regulatory requirements.
   - **Independent Review.** Flare undergoes independent periodic assessments (e.g., SOC 2 Type II) to ensure the effectiveness of its security controls. Customers may request copies of assessments at security@flare.io.

3. ACCESS CONTROL & IDENTITY MANAGEMENT
   - **Role-Based Access Control (RBAC)**: Access to Service Assets is granted based on job roles and responsibilities, ensuring that individuals only have access to the data and Systems necessary for their duties.
   - **Privileged Access Management:** Accounts with elevated access privileges (e.g., system administrators) are protected by multi-factor authentication (MFA) and follow the principle of least privilege.
   - **Password Management:** Passwords must adhere to strong complexity requirements, be securely stored (hashed and salted), and transmitted using encryption (e.g., SSL, IPSec). Initial passwords are reset upon first use.
   - **Immediate Access Termination:** Access to Service Assets is immediately revoked when personnel leaves Flare or change roles.

4. HUMAN RESOURCES SECURITY
   - **Pre-Employment Screening**: Comprehensive background checks, including criminal checks, are conducted on personnel before granting access to Service Assets.
   - **Ongoing Security Training**: Personnel with access to Service Assets receive regular security awareness training, covering topics like secure software development, data protection, and incident reporting.
   - **Confidentiality Obligations:** All personnel with access to Customer Data are required to sign confidentiality agreements.

5. DATA PROTECTION

- **Data Classification**: Flare classifies data based on sensitivity, ensuring appropriate controls for different data types (e.g., public, confidential, highly confidential). Customer Data is categorized to ensure that higher protections are in place for sensitive information.
- **Segregation of Environments**: Customer Data is only used in production environments. Development and testing environments are separated and do not contain live Customer Data unless it is anonymized.
- **Encryption**: Customer Data is encrypted at rest and in transit using industry-standard encryption technologies (e.g., AS-256). Encryption keys are managed with proper segregation of duties, ensuring that key custodians do not have access to the data being protected.

6. SECURE DEVELOPMENT

- **Secure Coding Standards:** Flare's application development follows secure coding practices based on OWASP guidelines. These practices mitigate common security vulnerabilities such as cross-site scripting (XSS), SQL injection, and other web application threats.
- **Code Reviews:** All code changes undergo peer reviews and automated static analysis to detect vulnerabilities early in the development cycle.
- **Dynamic Security Testing:** Before production deployment, dynamic application security testing (DAST) is conducted. This includes automated vulnerability scans, manual penetration testing, and automated security testing.
- **Change Management**: Flare's platform updates and changes go through a formal change management process, which includes risk assessments for significant changes.
- **Source Code Protection**: Flare uses version control systems to protect source code and employs strict access controls to prevent unauthorized modifications.

7. TECHNICAL TESTING

- **Penetration Testing:** External penetration testing is performed at least annually to identify potential security gaps in the production environment. These tests are conducted by external experts to simulate real-world attacks and identify vulnerabilities that could lead to an incident.
- **Vulnerability Management:** Quarterly automated vulnerability scans are conducted across all critical components of the Flare Platform, including applications, networks, and supporting infrastructure. These scans are used to identify, quantify, and prioritize.
- **Remediation of Vulnerabilities:** Flare follows a strict vulnerability management process, prioritizing and addressing all critical and high-risk vulnerabilities identified during the quarterly scans and annual penetration tests. A remediation plan is developed for each identified vulnerability, and changes are implemented to address them promptly.
- **Patch Management:** Security patches are applied as part of routine maintenance to ensure that Systems are hardened against known security threats. Critical patches are applied when vulnerabilities are discovered, and other updates follow a regular patching schedule.

8. OPERATION SECURITY

- **Anti-Malware Protection:** Anti-malware solutions are implemented across all Systems, with regular updates applied to defend against evolving malware threats. Scanning for malicious software is conducted periodically, and automated alerts are triggered if malware is detected.
- **Firewall and Network Controls:** Flare employs network firewalls to block unauthorized access, applying strict security rules to limit exposure to external threats. Firewall configurations are regularly reviewed to ensure alignment with security policies. A VPN is used for network segmentation to isolate resources and mitigate risks associated with network-level attacks.
- **Intrusion Detection and Prevention:** Flare utilizes adequate tools, including Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) to monitor network traffic for suspicious activities and automatically block unauthorized access attempts.
- **Log Monitoring:** Flare uses centralized logging systems to collect and store security events affecting the Service Assets. The relevant logs are continuously monitored for suspicious activities.

Based on predetermined rules, anomalies or unusual behaviours trigger alerts for further investigation.
- **Threat Monitoring and Intelligence:** Flare performs continuous online threat monitoring of monitored sources, including for data leaks.

9. PHYSICAL AND ENVIRONMENTAL SECURITY

- **Access Control:** Our data centres are equipped with comprehensive physical access control systems, including security personnel, biometric scanning, keycard access, and video surveillance to monitor and control the entry.
- **Redundant Systems:** Our data centres have redundant power supplies, cooling systems, and other environmental controls to maintain continuous operations and ensure availability of Flare services.
- **Environmental Protections:** Our data centres are also protected against natural disasters and environmental risks, such as fire, floods, and seismic activity, through sophisticated detection and mitigation systems.
- **Clear Desk Policy:** All employees, whether working from home or in-office, are required to adhere to a clear desk policy. This ensures that sensitive materials, including Customer Data or printed reports, are securely stored or disposed of at the end of each workday.
- **Secure Workstations:** Employees working from home must ensure their workstations are physically secure. This includes locking devices when not in use and preventing unauthorized access by using strong authentication methods (e.g., password protection and MFA).
- **Confidentiality in Shared Spaces:** Employees are prohibited from discussing or displaying sensitive information in public or shared spaces (e.g., coffee shops or co-working spaces) where unauthorized individuals may observe or overhear confidential materials.
- **Device Security:** Company-issued devices, such as laptops, are protected by encryption and endpoint protection software. Employees are required to use only company-approved devices for accessing Flare systems and Customer Data.

10. INCIDENT MANAGEMENT

- **Incident Response Plan (IRP):** Flare maintains a formal, documented Incident Response Plan (IRP) outlining procedures for the detection, analysis, containment, eradication, and recovery from Security Incidents. The IRP is regularly reviewed and updated based on evolving threats and industry best practices.
- **Customer Notification:** Flare will notify affected Customers without undue delay, and no later than 48 hours after becoming aware of a Security Incident. The notification will include an initial assessment of the incident, the nature of the incident, its scope, and the measures taken to mitigate the impact. Additional updates will be provided as more information becomes available.
- **Forensic Investigation:** Flare conducts a forensic investigation to identify the root cause and attack vectors involved in significant Security Incidents. When necessary, Flare will collaborate with Customer to provide summaries or detailed reports of the Security Incident for compliance purposes, or internal review.
- **Remediation Plan:** Flare will implement a remediation plan to prevent the reoccurrence of a Security Incident.

11. BUSINESS CONTINUITY AND DISASTER RECOVERY

- **BCMS.** Flare maintains a formal Business Continuity Management System ("**BCMS**") designed to ensure the continuous availability of services during disruptive events. The BCMS framework is periodically reviewed and updated to address new risks and changes in the operational landscape.
- **Disaster Recovery Plan (DRP):** Flare implements a Disaster Recovery Plan (DRP) to ensure the restoration of critical systems and Customer Data in the event of a significant disruption, such as natural disasters, cyberattacks, or system failures.

- **Backup and Recovery Procedures:** Critical systems and Customer Data are regularly backed up, with procedures in place to ensure data integrity and secure restoration in case of a system outage. Backups are securely stored in multiple locations to ensure redundancy.
- **Testing and Updates:** The BCMS and DRP are regularly tested through simulation exercises and drills. These tests are conducted to ensure that recovery procedures are effective, and personnel are familiar with their roles. Flare continuously reviews and updates the plans to address new challenges and improve recovery capabilities.

12. COMPLIANCE AND AUDITS

- **Independent Third-Party Audits:** Flare undergoes periodic independent third-party audits, including annual SOC 2 Type II assessments, to validate the effectiveness of its security controls and provide assurance to customers. Customers may request a summary or results of the latest audit by contacting security@flare.io.
- **Customer Audit Rights:** Once annually, Customers have the right to request audit information relating to Flare's compliance with its security obligations under this addendum. Flare will provide relevant audit reports, such as SOC 2 Type II, and other certifications, upon written request. Any additional audit requests will be subject to mutually agreed terms and may involve reasonable limitations and costs borne by the Customer.
- **Remediation:** If any non-compliance or areas for improvement are identified through audits or assessments, Flare will promptly implement a remediation plan to address the findings and enhance its security posture. Customers will be informed of any significant findings that may impact the security of their data.

Flare reserves the right to update or modify this Security Addendum from time to time to reflect changes in our security practices, legal requirements, or industry standards. Any adverse material changes will be communicated to Customers at least 30 days prior to their effective date. If you disagree with the change, you can contact us at security@flare.io within this delay, otherwise, continued use will be interpreted as acceptance.