Octofuse - Security Policy

Last Updated: August 27, 2025

This Security Policy describes the measures implemented by **OMI-TECH LLC** ("OMI-TECH," "Octofuse," "we," "our," or "us"), a company incorporated in the State of Florida, USA, to ensure the confidentiality, integrity, and availability of customer data when using the Octofuse platform, websites, applications, and related services (the "Services").

This Policy applies globally, including jurisdictions such as the United States, Mexico, the European Union, Brazil, and others where Octofuse is used. It is designed to align with leading data protection frameworks, including **GDPR, CCPA/CPRA, LGPD, and LFPDPPP (Mexico)**.

---

1. Purpose and Scope

This Policy defines security standards and practices to protect customer, employee, and company data processed by Octofuse. It applies to: - All OMI-TECH employees, contractors, and third parties handling data on behalf of Octofuse. - All systems, networks, and applications owned, operated, or managed by Octofuse.

---

2. Governance and Responsibility

- The **Octofuse Security Team** oversees implementation, monitoring, and evolution of this Policy.
- Security policies are reviewed at least annually, or as needed due to legal, technical, or business changes.
- All personnel undergo annual security awareness training.

---

3. Access Control and Authentication

- User accounts must use strong passwords and, where available, **multi-factor authentication (MFA)**.
- Access is granted on the **principle of least privilege**.
- Access rights are reviewed regularly and revoked immediately upon termination of employment or contract.

---

4. Data Protection

- **Encryption in transit:** All communications use TLS 1.2 or higher.
- **Encryption at rest:** Data stored is protected with AES-256 encryption.
- **Data segregation:** Production, development, and test environments are separated.

- **Data minimization:** Sensitive categories of data (e.g., health, PCI, biometric) are not permitted unless explicitly authorized in writing.

---

5. Monitoring and Logging

- Systems are monitored for suspicious or unauthorized activity.
- Logs of access, administrative actions, and security events are maintained and periodically reviewed.
- Vulnerability scans and penetration tests are conducted to identify and mitigate risks.

---

6. Incident Response

- Octofuse maintains an **Incident Response Plan** covering preparation, identification, containment, investigation, eradication, recovery, and post-incident review.
- Customers will be notified without undue delay if a data breach affecting their information occurs, in compliance with applicable law (e.g., GDPR, LGPD, LFPDPPP).

---

7. Business Continuity and Disaster Recovery

- Octofuse infrastructure is hosted on **Amazon Web Services (AWS)** and leverages **Cloudflare** for global content delivery, performance optimization, and security services (including DDoS protection).
- Both AWS and Cloudflare maintain industry-leading certifications (ISO 27001, SOC 2, etc.).
- Data is replicated across multiple regions to ensure resiliency.
- Recovery Point Objective (RPO): near zero (≤ 24 hours beyond 7 days).
- Recovery Time Objective (RTO): ≤ 24 hours for systemic disruptions.

---

8. Physical Security

- Octofuse does not operate physical data centers. Instead, it relies on AWS and Cloudflare facilities with industry-leading physical and logical security controls, including biometric access, video monitoring, and 24/7 security staff.

---

9. Personnel and Training

- All employees and contractors must complete security and data protection training annually.
- Personnel are bound by confidentiality obligations.
- Acceptable use rules prohibit introducing malware, sharing accounts, or circumventing security controls.

---

10. Third Parties and Subprocessors

- Third-party providers are vetted for security posture and contractual obligations.
- Subprocessors are required to implement security measures consistent with this Policy.
- Key subprocessors include **Amazon Web Services (AWS)** and **Cloudflare, Inc.**, which provide hosting, networking, and security services.
- A current list of subprocessors is available upon request.

---

11. Customer Responsibilities

While OMI-TECH implements strong security controls, customers are responsible for: - Maintaining the confidentiality of their account credentials. - Using strong passwords and enabling MFA. - Configuring their workspaces and integrations securely. - Maintaining their own backups of critical data when required.

---

12. Limitations of Liability

Octofuse implements industry-standard security measures; however, **no system can guarantee absolute security**. By using the Services, customers acknowledge and accept these inherent risks. OMI-TECH shall not be held liable for security or availability incidents attributable to third-party providers such as AWS or Cloudflare. OMI-TECH’s liability is otherwise limited as described in the **Terms of Service**.

---

13. Updates to this Policy

We may update this Security Policy periodically. If significant changes are made, we will notify users by email or through the Services. Continued use of the Services after changes constitutes acceptance of the updated Policy.

---

14. Contact

For questions or security concerns, contact us at: - **Email:** customer@octofuse.app
- **Mail:** OMI-TECH LLC, 848 Brickell Ave Suite 950, Miami, FL 33131, USA