



Omella Security Overview

Omella is built to enrich student and member experiences by allowing organizers to focus on what they love and do best - leading their organization.

This white paper provides a current overview of the policies and practices that comprise our security approach. Along with the practices outlined below, Omella works with school and district administrators, third-party auditors, and expert policy advisors to continually strengthen our investments across all aspects of security.

At the school and district levels, this requires complying with regulations like FERPA and COPPA. As part of our commitment to privacy in the school environment, Omella complies with all applicable privacy laws. To meet these program guidelines as well as our own rigorous standards, Omella employs two kinds of security features: those that are user-facing, and those that are embedded in the service.

When users pay for goods, services and charity, their payment method data is collected by Stripe, a 3rd party, PCI compliant payment processor and is therefore not stored by Omella or accessible to organizers, such as teachers or school administrators. We have also adopted advanced cloud computing practices and strict internal policies to ensure the integrity of the data we manage.

Overview

Organizations and their members trust Omella with important and sensitive information. Our security approach consists of seven critical components that allow us to maintain data security and integrity for entry, transfer, storage and access.

- Corporate governance
- Logical security

- Physical security
- Environment security
- Software security
- Privacy principles
- Regulatory principles

Each of these components are described in more detail below.

Corporate governance

Omella has adopted our practices to meet the criteria set forth in the [NIST Cybersecurity Framework V1.1](#), which advances our ability to safeguard sensitive information.

- All Omella employees receive privacy and security training at least annually.
- All Omella employees and contractors sign agreements that require them to preserve and protect the confidentiality of sensitive information they may access while doing their jobs.
- Information security controls are measured, monitored, and tested for their effectiveness to support continuous improvement.

Logical security

Omella implements technical controls to prevent the inadvertent exposure of user information.

- Sensitive information is protected at rest and in transit across untrusted networks using strong encryption.
- Omella's physical infrastructure is hosted and managed within Amazon's secure data centers through Heroku 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)

For more information please see:
<https://aws.amazon.com/security/>

- Employees are required to enable two-factor authentication in every internal and external service where two-factor authentication is made available and practical.

Physical security

Omella applies layered physical access controls to safeguard employees and protect systems that access, store, transmit or process user information.

- Omella is hosted in a data center facility with rigorous physical security controls including a non-descript location, security staff, layered electronic access controls from all building ingress points to interior zones, intrusion detection, and surveillance monitoring.

Environmental security

Omella uses Amazon Web Services (AWS) and other third-party services in the AWS environment to host and operate our service.

- AWS's environmental protections reduce the risks associated with fire, loss of power, flood, humidity, and temperature changes in their facilities.
- Data center facilities are strategically located in regions that are less commonly affected by natural disasters.
- Cloud-based information storage is protected from environmental threats using fault-tolerance and redundancy.
- The AWS cloud infrastructure has been designed and managed in compliance with regulations, standards, and best practices, including HIPAA, SOC 1/SSAE 16/ISAE 3402 (formerly SAS70), SOC 2, SOC 3, PCI DSS Level 1, ISO 27001, FedRAMP, DIACAP and FISMA, ITAR, FIPS 140-2, CSA, CMMC, NIST, and MPAA.

Learn more about Amazon's security and environmental protection policies [here](#).

Software security

Omella's software is delivered using industry-tested technology with privacy, end-user safety, and security in mind.

- Vulnerabilities discovered in our applications are prioritized and remediated swiftly
- All Omella clients use TLS/SSL when communicating with our servers.
- Omella follows an industry standard secure development process that considers privacy by design and aims to avoid common security exposures.

Privacy principles

Omella has adopted modern practices with respect to handling personal information.



- Omella maintains a [Privacy Notice](#) in a clear and conspicuous location on our website to inform consumers about how personal information is used, collected, and shared.
- The processing of personal information is limited to the purposes identified by a commercial agreement and never repurposed.
- Omella does not disclose personal information to any third party without authorization unless that disclosure is necessary in order to comply with the law or a valid request from public authorities.
- Omella will never sell, trade, barter, or exchange for value consumers' personally identifiable information or personal data.
- In the case of a security incident resulting in a data breach or the unauthorized disclosure of personal information, as defined by a state, federal or other regulation, Omella will promptly notify impacted parties and authorities.

Omella has designated a Security Incident Response Manager, Felipe Rodrigues, who is responsible for coordinating the response to consumer data breaches with members of our executive leadership, security, and legal teams. The Security Incident Response Team can be reached at security@omella.com.

Regulatory compliance

Omella works with policy advisors to ensure that our products and practices remain compliant with relevant mandates and regulations.

- Omella maintains PCI compliance through reliance on 3rd party vendors under the "PCI validation: SAQ A".

- Omella maintains KYC compliance with every organization that uses the service to collect money.
- Omella helps schools comply with federal FERPA regulations.

Additional information

Omella's approach to security was developed to help organizations, such as schools, districts, nonprofits and others, remain confident in the integrity and security of their data, so they can focus on their mission and helping their members.