Office Timeline Security FAQ

Overview
Our business runs on our software. We depend on it to manage software development sprints, roadmaps, IT projects and for all cross-organization planning. We also use it to communicate with external teams, clients, executives and other important stakeholders. As such a heavy consumer of Office Timeline ourselves, we understand how important the security of our software is to our customers.

We have focused on implementing a holistic and comprehensive security discipline across all parts of our business. The following Security FAQ will provide information on how we practice security across our business. It will cover:

- App security and infrastructure
- Data Center and Disaster Recovery
- Methodologies
- Certifications / Attestations

To help deliver the software and services our customers require, we work with a small group of trusted vendors. Each of these vendors – such as Stripe or Microsoft Azure – have been carefully selected for meeting a high-standard of security. Our Security FAQ does not address the security practices of these vendors. For a list of our trusted vendors and links to their security pages, please see our privacy statement.

App security and Infrastructure

How do users get and manage their passwords?
Depending on the type of license they purchase, some Office Timeline users will set up user accounts. These users will set their password at registration from our website or inside the Office Timeline Online app, and they have several options to change it if needed:

1. *Clicking the Forgot Password link at login.* The system will email the user a reset link that will allow them to set a new password securely.
2. *Changing it from their Account Settings page once logged in.* To prevent unauthorized access, the user will need to re-enter the old password to be able to save the new one.
3. *Contacting our support team.* In this case, our support representative will initiate the reset and create a temporary password, which the user will be requested to change as soon as they sign in to their account.

Does the application enforce minimum password security requirements?
Yes. The minimum password security requirements we enforce are:

- The passwords should have between 8 and 64 characters
- It can't be a single repeated character (e.g. aaaaaaaa, 11111)
- It can't be a series of consecutive characters (e.g. 12345678, abcdefgh)

Additionally, the user interface provides a strength meter that presents the reliability of their chosen password based on length and the character classes included. The password is encrypted in our database using 256-bit encryption.

Do sessions automatically timeout after a specified period of inactivity? If yes, how long is the session timeout?
Yes. Both on the main website and in the Office Timeline Online app, the session timeout is set at 8 hours. If the user doesn't access the site or the web app before this period expires, they will be automatically logged out of their account.

How is the traffic between clients and servers protected?
We use SSL/TLS for communication channel encryption, and we are protected against XSS (cross-site scripting) attacks. In addition, customer data & credit card data are validated in a Stripe plugin for an additional layer of security.

Do you maintain secure coding guidelines and conduct security code reviews on the source code?
Yes. Our technical security expert maintains the security coding standards, which are applied by developers, testers, and team leaders when uploading code on the repository. Every team receives ongoing training on security code policies.

How do you detect code security defects prior to production?
We have a testing process for the source code (including automated tests, unit and integration tests and automated source code analysis tools), which is used, reviewed and maintained constantly by our developers and security manager. This process gives testing requirements the same priority as functional requirements in development cycles, so we can quickly identify any risks early.

Do you protect against Cross-Site Scripting?
Yes. Our website uses the default mechanism from ASP.NET Core (anti-forgery token) against Cross-Site Scripting attacks. This mechanism is the safest method currently available for web applications.

Are your systems configured to log security-relevant events, such as authentication, data access, payments etc.?
Yes. We have a comprehensive internal audit system which logs all application events containing data related to users, orders, payments, invoices, emails, etc. These logs, along with errors, are saved, tracked and reported (on website and by email) via alerting and error tools from Kibana and Rollbar.

Does your website or online app require certain browser plugins to work correctly?
No. Our website and application do not require any plugin; however, you will need to have JavaScript enabled in your browser.

If any form of cryptography is used in your application, please describe the algorithms that are used.

We use the data protection code base package Microsoft.AspNetCore.Cryptography.KeyDerivation. It includes the default hashing algorithm from .NET Core (HMAC-SHA1, 128-bit salt, 256-bit subkey) which is to protect passwords, tokens, and other data in our system.

Does your Software as a Service use transport encryption?
Yes. Both the Office Timeline Online app and the main website are accessible over HTTPS, and the communication channel is encrypted with SSL/TLS, to provide high levels of integrity and confidentiality.

What type of events are logged and monitored?
We have defined and provisioned a suite of security related alerts that are triggered via Microsoft Azure's monitoring service. For example, these events include website crashes, database availability, CPU/memory load threshold, or other services down alerts. Our administrators and security managers are notified by email and SMS whenever an alert is triggered.

Have you experienced a customer data breach in the past two years?
No. Our customer data has been safely protected since our company's formation, and we are working hard to keep it safe.

Does your company use firewalls and/or network zoning to restrict traffic into and out of your network at strategic points?
Yes. We use Microsoft Azure's Web Application Firewall (WAF) and DDoS Protection to stop network and application layer attacks at the edge, as well as to control, log, filter and block traffic to our backend. In addition, we have a process in place to ensure only authorized personnel can access it. We also utilize network zoning to provide an additional layer of security – where each edge component is in its own network, and the internal networks communicate through VPN, allowing only desired traffic through.

Is encryption protection in place for internal network traffic that potentially carries customer-sensitive information?
Yes. Customer-sensitive data and the application credentials, SSL certificates, and encryption keys are managed, stored, and transmitted securely through the Azure Management Portal in adherence to Azure Data Security and Encryption Best Practices. Additionally, access to the management portal is restricted and requires specific permission, which is logged and recorded in a secure manner.

Does your network have protections against ARP spoofing?
All our networks leverage Azure's advanced security services, which include protection against Man-in-the-middle attacks such as Address Resolution Protocol (ARP) and Flooding. As an additional layer of security, networks can only be accessed through user authentication with strong password requirements.

Data Center & Disaster Recovery

Who is your data center provider? Are they certified against a compliance theme? (e.g., TIA-942, ISO 27001, SSAE-16, etc.)

Our data center provider is Microsoft Azure, which meets a broad range of international and industry-specific compliance standards, from ISO27001, HIPAA, and FedRAMP, to SOC 1 and SOC 2. Rigorous third-party audits verify Azure's adherence to the strict security controls mandated by these standards. Azure's compliance reports are available on Microsoft's Service Trust Portal.

Do you sync data to a different environment other than the database?
Yes. We use Elasticsearch clusters to sync data for reports, to log emails sent by the system, and for internal data auditing purposes. In addition, we also use Kibana for logs and errors (please see our FAQ on logging security-relevant events).

Do you back up data?
Yes. All data is saved in the cloud and it is backed up every minute using Azure cloud back-up services. Our back-up and recovery architecture uses geo-redundant storage (RA-GRS) to ensure that the backups are preserved even if the data center is unavailable. Backups are automatically kept for 35 days.

Do you store backups on removable media or in off-site facilities?
Yes. We back up regularly and store these back-ups with Azure. Additionally, we regularly back up to removable media, which are stored at off-site facilities. All backup data is encrypted.

Do you have an auditable process in place for granting and revoking physical access to data centers?
Azure is composed of globally distributed datacenters that are strictly controlled to reduce risk of unauthorized users gaining physical access. We do not have physical access to them.

Do you have disaster recovery and business continuity procedures in place?
Yes. We have a business continuity and disaster recovery (BCDR) process that covers disaster recovery procedures and best practices to ensure business continuity. It addresses disruptions in the service we provide customers, to keep our applications running during unplanned downtimes. Additionally, it leverages Azure recovery services (auto-healing, auto-restart servers, machine replication, geo replication etc.) to ensure business recoverability during outages.

Is there a manual backup and restoration process?
Backups are done automatically through Azure and retained for 35 days. Additionally, we back up data offsite – these backups are automatic as well. As for restoration, this is done manually by authorized staff.

Do you have procedures in place for notifying clients when business disruptions occur?
Yes. Depending on the severity of the business disruption, we may send notifications explaining the issue and letting users know the impact, restoration times and any temporary alternative solutions. To ensure maximum visibility, such notifications may also be posted on all our social media channels.

Has your company ever experienced a major disruption (i.e. catastrophic natural disaster, fire, technology disruption, denial of service attack, material financial loss)?
No, we haven't experienced any major disruptions.

Methodologies

Has your company selected an individual or team to be responsible for managing the information security and privacy program?
Yes. We have a dedicated security professional who oversees secure architecture and practices, and we have a technical security expert who is responsible for specific, code-related data and secure software development processes. Both receive ongoing information security training and stay current with the latest technologies, and threats, applicable to our applications.

Is there a Software Development Life Cycle (SDLC) process?
Our development and delivery process is based on the Agile methodology. We use Continuous Integration and Continuous Delivery for our build and release process to ensure that we can deploy changes quickly and in a sustainable way. Our teams work in iterations and cycle through processes of planning, design, development, testing and deployment, and tasks are adjusted as the situation demands. This practice allows us to detect problems early, reduce risks, and easily adapt to changes in requirements.

How are changes tested?
Development teams create unit and integration tests and also perform manual testing for code changes before deploying to a Development server. Then, the testers create and execute automated and manual tests on both the Development and Testing servers. When the testing teams certify and approve code changes, they are deployed to a Staging server and re-tested simulating a Live environment. The final phase is to swap Staging with Live and re-test in the Live environment.

How are they reviewed and approved?
We have a managed development process. When a developer has finished working on a task, that work is submitted for review and approval from a reviewer board. The code will be merged into the main branch (repository) only when the work is approved.

Is production data used for development and/or testing?
No, real customer data (emails, Stripe customer ID, etc.) is never used for development or testing. We have a mock database which is used for development and testing.

Do developers have access to deploy into production?
No. Once the testing team certifies and approves code changes, a small group of key DevOps staff follow a carefully managed methodology to deploy new code into production.

Do you use an automated source-code analysis tool to detect code security defects prior to production?
Yes, we use tools for automated source-code analysis. These tools are developer productivity extensions for Microsoft Visual Studio that provide continuous code analysis and immediate detection of errors and problems. Our development teams use them to find runtime and compiler errors, code smells, and redundancies as they code. They are also used to scan existing code to ensure compliance with the most current coding standards.

Certifications / Attestations

Is Office Timeline SOC 2® compliant?
Yes, Office Timeline is SOC 2 compliant. We've received our SOC 2 Type 2 Report, which provides an external audit that demonstrates we are meeting the security commitments we have made to our customers. We use Drata's automation platform to continuously monitor 100+ internal security controls across the organization against the highest possible standards. Automated alerts and evidence collection allows us to confidently prove our security and compliance posture any day of the year, while fostering a security-first mindset and culture of compliance across the organization.

If you believe you've discovered a bug in Office Timeline's security, please get in touch at security@officetimeline.com. Our security team promptly investigates all reported issues.

For more information about our security policies, please contact us at security@officetimeline.com.