TH-POL-003: Cybersecurity Policy and Approach

Overview

Accessibility, privacy, and data security are of the utmost importance at Townhall. Thus, we utilize a Secure Software Development Life Cycle (SSDLC) approach, as detailed further in TH-SOP-001. Townhall deploys consistent, secure, and compliant readiness across development, staging and production environments. We utilize proven and well-regarded 3rd party cybersecurity vendors to audit, observe and repair vulnerabilities immediately. Resulting in a robust, compliant and secure software application lifecycle development, deployment and in production.

Townhall Data Management

Townhall's core value of Respect elegantly captures our approach to data management. We take a minimalist approach to data collection through our strategy of serving as a 'plug-in' to existing Unified Communications as a Service (UCaaS) platforms such as Zoom, Microsoft Teams or WebEx. In essence, we simply read limited user data provided to these platforms and store optional data that is provided to us (e.g. email address, social media accounts, etc.). For further detail, please see our Privacy Policy (https://www.townhall.pro/privacy-policy).

Cybersecurity Posture

Townhall applies a 'secure first' philosophy, which means we integrate security at the initial onset of development in the SSDLC process all the way through production. We utilize a proven and trusted 3rd party platform, to manage assets, user access, architecture design, secrets, vulnerabilities, and activity history to deliver a robust and secure software application. Our approach is secure first, compliance readiness for a handful of industry best practices i.e. NIST, ISO, etc.

A. The software development pipeline is secured by a unified, centralized 3rd party platform, which allows Townhall to build proactive and protective application environments leveraging industry best practices, such as ISO and NIST. To facilitate compliance, Townhall proactively integrates compliance requirements from the beginning of development. This 'secure first' approach minimizes overall costs and improves reliability since we are continually auditing our environments for compliance throughout the SSDLC process.

B. Unique asset management identifiers are issued for every Townhall environment deployed. In production environments, Townhall utilizes observing and detecting tools to assign unique identifiers, which allow for easy asset management.

C. Role Based Access Control (RBAC) methodologies are utilized for Townhall developers. The proven RBAC model assigns access to developers based on hierarchy and product technical requirements. In any instance where we Add, Modify, or Delete users or developers throughout the SSDLC process, we record these actions in the centralized 3rd party platform. Thus, we have documentation and activity history for any user or developer of the Townhall Application.

D. Secure architecture design is utilized for the Townhall application. Microservices, and modern architecture best practices are used to achieve security and compliant readiness from development/staging to production environments.

E. Personal Identifiable Information management (PII): Townhall uses standard industry best practice encryption methods to prevent PII data from being exposed. Access controls systems, highlighted in item C above, enable proper handling and control of PII data.

F. Secrets management: Townhall uses in transit and at rest encryption best practices to properly secure data. Townhall utilizes a secure vault to secure access passwords and other cloud provider issued keys. Further, a key rotation system is integrated to ensure access keys are refreshed within a specific time period and in the case of exposure, exposed keys are quickly removed from use in the application.

G. Vulnerability management utilizes both a protective build secure approach, and a continual scanning process to observe and detect vulnerabilities. This allows Townhall to identify the best security configuration practice that can be proactively installed in our production environments, plus it allows Townhall to continually scan and observe operations for introduction of new vulnerabilities. If any new security vulnerability is announced, Townhall can remediate effectively and efficiently. Further, if any vulnerability is identified, our operational team performs a root cause analysis and either accepts, denies, or fixes the vulnerability through our Change Management Process.

H. Our Change Management process is consistently applied across operations if any change or vulnerability is identified. A unique ID and alert ticket is created for each vulnerability and assigned to the Change Management board for review to either accept, deny or fix. The disposition decision for each vulnerability is based on organizational risk factors and customer requirements.

Townhall Zoom App OAuth Integration

This section outlines the security measures and protocols implemented by Townhall, a Zoom App, during the OAuth 2.0 integration process with Zoom's platform.

OAuth 2.0 Protocol

Townhall uses the OAuth 2.0 authorization framework to enable secure authorization between Zoom's platform and the Townhall app. This standard ensures that user data is securely transferred and that permissions are granted explicitly by the user.

Authorization Flow

1. Authorization Request: A user is redirected to a Zoom authorization page when they choose to integrate Townhall with their Zoom account.
2. User Consent: Townhall connects to the user's Zoom account only after the user approves a permission request.
3. Authorization Code: Post-approval, Zoom generates an authorization code and redirects the user back to a Townhall's specified Uniform Resource Identifier (URI).
4. Exchange Code for Token: The Townhall back-end service then exchanges the authorization code for an access token by making a server-to-server request to Zoom's token endpoint.
5. Access Token Retrieval: Upon successful validation, Zoom's server returns an access token.
6. API Access: Townhall uses the access token to make authorized API calls to Zoom's platform on behalf of the user.

Security Measures

- TLS Encryption: All data transferred during the OAuth flow is encrypted using TLS.
- Token Expiry: The access tokens have expiration dates and Townhall refreshes these regularly to improve security and limit exposure to potential compromise.
- Limited Scopes: Townhall only requests permission to the scopes essential to Townhall functionality. This reduces the amount of data accessed and eliminates unnecessary security risks.
- Secure Storage: All sensitive data (e.g. access tokens) are stored in a secure database.
- Server-to-Server Requests: Code-to-token exchange occurs through server-to-server communication delivering a secure authorization process.

Revision History

Revision	Comments / Changes	Date
1	Initial release	Feb 2023
2	Updated sections C, E	July 2023
3	Added the OAuth integration section	Aug 2023