KiviCare Telemedicine Addon – Security & Compliance Policies

---

1. Vulnerability Management Policy

Detection
We employ automated security testing throughout the development lifecycle. Static Application Security Testing (SAST) is performed on every commit using **PHP_CodeSniffer (PHPCS)** with the **WordPress-Extra ruleset**. Dynamic Application Security Testing (DAST) is conducted using **OWASP ZAP** against staging environments prior to major releases.

Remediation
Identified vulnerabilities are classified based on severity using the **CVSS scoring model**. Any vulnerabilities rated **Critical** or **High** immediately block production deployment until resolved.

Patching
Verified security fixes are released to customers within **72 hours** of confirmation.

---

2. Data Retention & Protection Policy

Data Minimization
We strictly limit stored data to what is necessary for core functionality:

- **Zoom OAuth Tokens:** Stored securely in the WordPress `wp_usermeta` table
- **Meeting Metadata:** Limited to Meeting ID and Join URL, stored in the custom `wp_kc_appointment_zoom_mappings` table
- **No Media Storage:** The application does **not** access, process, or store Zoom video, audio recordings, or meeting transcripts

Encryption & Access Control
All communication with Zoom APIs is encrypted using **TLS 1.2 or higher**. Database access is restricted to authenticated WordPress administrators with appropriate permissions.

Deletion / Right to be Forgotten

- **OAuth Tokens:** When a Doctor selects the “Disconnect” option in the dashboard, the `disconnect_doctor()` function immediately removes all stored OAuth tokens from the database
- **Meeting Metadata:** When an appointment is deleted, all related Zoom meeting metadata is removed via the `deleteAppointment` controller logic

---

3. Privacy Policy (Zoom-Specific)

User Consent
Doctors explicitly grant access through **OAuth 2.0 authorization** before any Zoom integration is enabled.

Data Sharing
Patient names and email addresses are transmitted to Zoom **only** when required for meeting invitations (if enabled) or for populating the Zoom meeting topic. This information is **not shared with any third parties**.

Cookies
The plugin relies solely on standard WordPress session cookies for administrative authentication. No tracking or analytics cookies are used for patients joining Zoom meetings.

---

4. Incident Management & Response Policy

Reporting
In the event of a confirmed security incident involving Zoom credentials or patient-related data, we commit to notifying the **Zoom Security Team within 72 hours**.

Containment & Mitigation
Immediate response actions include revoking compromised API keys and secrets and forcing a reset of all Doctor OAuth tokens by clearing the associated WordPress usermeta entries.

---

5. Infrastructure & Dependency Management Policy

Dependency Management
PHP dependencies are managed using **Composer**. The `composer.lock` file ensures consistent and reproducible dependency versions across all environments.

Security Updates
Dependencies are reviewed **monthly** for known CVEs (Common Vulnerabilities and Exposures) and updated as required.

Environment Security
The application operates within the customer's WordPress environment. We provide documented minimum server requirements, including **PHP 8.0 or higher** and **SSL-enabled hosting**, to ensure baseline infrastructure security.
