Fiche de cybersécurité

ElecTrace · contrôle des appareils électriques mobiles (SNG 482638)

Version de l'application : 1.2.2 · Novembre 2026

ElecTrace est un logiciel Windows de suivi des contrôles périodiques des appareils électriques mobiles. Il est conçu pour fonctionner localement, sans compte en ligne ni service cloud. Cette fiche résume les points habituellement demandés lors d'une évaluation de sécurité fournisseur.

1. Architecture et connectivité

- Application de bureau pour Windows, installée sur chaque poste. Les données sont stockées dans un dossier choisi par l'entreprise : poste local ou dossier réseau interne (serveur, NAS).
- Aucun compte en ligne, aucun service cloud, aucune télémétrie, aucune publicité. Aucune donnée de l'entreprise n'est envoyée à l'éditeur ni à un tiers.
- Les scripts de l'interface n'ont pas le droit d'ouvrir de connexion réseau (politique de sécurité du contenu).
- Aucune connexion sortante vers Internet : l'application ne contacte aucun serveur externe, pas même pour son affichage (les polices sont intégrées au programme). Elle fonctionne de la même manière avec ou sans Internet ; le seul accès réseau éventuel est celui vers le dossier partagé interne choisi par l'entreprise.
- Les seuls échanges de données sont volontaires : export et import manuels de fichiers de sauvegarde ou Excel. Le lien de support (Paramètres › À propos) prépare un e-mail contenant la version d'ElecTrace, le nom et l'identifiant de l'entreprise : il s'ouvre dans la messagerie de l'utilisateur, qui décide lui-même de l'envoyer.

2. Stockage et protection des données

- Le parc d'appareils, l'historique des contrôles, les instruments de mesure, le logo de l'entreprise et, en mode multi-clients, les fiches clients sont enregistrés dans des fichiers situés dans le dossier de données de l'entreprise. L'éditeur n'y a techniquement pas accès.
- L'application n'a pas de comptes utilisateurs : l'accès aux données repose sur les droits du dossier (Windows, serveur, NAS), gérés par l'entreprise.
- Les fichiers de données ne sont pas chiffrés par l'application. Pour une protection au repos, il est recommandé de s'appuyer sur le chiffrement du disque ou du NAS de l'entreprise.
- Protection contre la perte de données : écriture en deux temps (fichier temporaire, puis remplacement), détection d'un fichier endommagé ou incomplet (l'enregistrement est alors bloqué, rien n'est écrasé), avertissement si un autre poste a modifié les données entre-temps (aucun écrasement silencieux) et sauvegarde automatique optionnelle à la fermeture.

3. Licence

- La clé de licence est signée numériquement (signature asymétrique ECDSA, courbe P-256, SHA-256). L'application ne contient que la clé de vérification ; la clé de signature reste exclusivement chez l'éditeur. Une clé ne peut donc ni être fabriquée ni être modifiée sans être rejetée. Seules les clés signées au format actuel sont acceptées.
- La licence est liée à l'identifiant unique de l'entreprise : une clé copiée dans le dossier de licence d'une autre entreprise est refusée.
- Le fichier de licence enregistré sur le disque est chiffré (AES-256-GCM) et protégé par un contrôle d'intégrité. La vérification est entièrement locale, sans appel à un serveur.

4. Durcissement de l'application

- L'interface est isolée du système : bac à sable (sandbox) de Chromium, isolation de contexte activée, accès direct à Node.js désactivé, outils de développement désactivés. Basée sur une version d'Electron maintenue (correctifs de sécurité à jour).
- L'interface ne peut ni ouvrir de nouvelle fenêtre, ni naviguer vers une autre page, ni obtenir de permission (caméra, micro, localisation…).
- L'accès aux fichiers est contrôlé par le processus principal : uniquement dans les dossiers que l'utilisateur a lui-même choisis via la fenêtre Windows, uniquement des fichiers ElecTrace (noms autorisés), sans possibilité pour l'interface d'élargir cette zone. Les liens externes autorisés se limitent aux liens e-mail (mailto).
- Toutes les données relues depuis le disque (dossiers partagés, sauvegardes importées) sont contrôlées et remises au format attendu avant usage, et tout texte affiché est échappé : un fichier modifié ou piégé ne peut pas injecter de code. Les certificats d'étalonnage (PDF vérifiés) s'ouvrent dans le lecteur PDF de Windows.
- Import Excel limité (10 Mo, 10 000 lignes, contrôle de l'archive avant lecture) contre les fichiers démesurés ou piégés.
- Le lancement automatique au démarrage de Windows (vérification des échéances) n'est jamais activé sans l'accord de l'utilisateur.
- Une politique de sécurité du contenu (CSP) restreint les ressources que l'interface peut charger : aucun domaine externe, aucun script en ligne. Seul le code du programme peut s'exécuter, ce qui bloque un éventuel code injecté. Un test automatique vérifie avant chaque version que toute donnée affichée est neutralisée.
- Aucun code n'est téléchargé ni exécuté dynamiquement. Les mises à jour ne sont jamais installées automatiquement.

5. Traçabilité et diagnostic

- Un journal technique local, horodaté, enregistre les actions significatives (par ex. modification de données, activation de licence) pour le dépannage.
- Le journal est consultable dans une section protégée par mot de passe et n'est jamais transmis automatiquement. Le mot de passe est modifiable et n'est conservé que sous forme d'empreinte (SHA-256) ; il est recommandé de le changer à la mise en service.

6. Protection des données personnelles

- Les données nominatives sont saisies par l'entreprise elle-même : les noms des contrôleurs, le nom de l'entreprise et, en mode multi-clients, les coordonnées des clients (nom de la personne de contact, téléphone, e-mail). Aucune catégorie de données sensibles au sens de la loi fédérale sur la protection des données (LPD) n'est collectée.
- Ces données restent sous le contrôle exclusif de l'entreprise, sur sa propre infrastructure.

7. Mises à jour et signalement

- Le programme d'installation est signé numériquement au nom de Philippoz Solutions (certificat de signature de code) : Windows affiche l'éditeur vérifié et toute modification du fichier est détectée.
- Les mises à jour sont fournies manuellement par l'éditeur sous forme d'un nouveau programme d'installation ; elles ne s'installent que sur action de l'entreprise.
- Toute vulnérabilité constatée peut être signalée directement à l'éditeur (contact ci-dessous).

CONTACT ÉDITEUR
Philippoz Solutions · support@electrace.ch

Informationsblatt Cybersicherheit

ElecTrace · Kontrolle ortsveränderlicher elektrischer Geräte (SNG 482638)

Version der Anwendung: 1.2.2 · November 2026

ElecTrace ist eine Windows-Software zur Verwaltung der periodischen Kontrollen ortsveränderlicher elektrischer Geräte. Sie ist so konzipiert, dass sie lokal arbeitet, ohne Online-Konto und ohne Cloud-Dienst. Dieses Informationsblatt fasst die Punkte zusammen, die bei einer Sicherheitsbeurteilung von Lieferanten üblicherweise verlangt werden.

1. Architektur und Konnektivität

- Desktop-Anwendung für Windows, auf jedem Arbeitsplatz installiert. Die Daten liegen in einem vom Unternehmen gewählten Ordner: lokaler Rechner oder internes Netzlaufwerk (Server, NAS).
- Kein Online-Konto, kein Cloud-Dienst, keine Telemetrie, keine Werbung. Es werden keine Unternehmensdaten an den Hersteller oder an Dritte gesendet.
- Die Skripte der Benutzeroberfläche dürfen keine Netzwerkverbindungen öffnen (Content Security Policy).
- Keine ausgehende Verbindung ins Internet: Die Anwendung kontaktiert keinen externen Server, auch nicht für die Darstellung (die Schriften sind im Programm integriert). Sie funktioniert mit und ohne Internet identisch; der einzige mögliche Netzwerkzugriff erfolgt auf den vom Unternehmen gewählten internen Freigabeordner.
- Datenaustausch findet nur freiwillig statt: manueller Export und Import von Sicherungs- oder Excel-Dateien. Der Support-Link (Einstellungen › Über) bereitet eine E-Mail mit der ElecTrace-Version, dem Firmennamen und der Unternehmenskennung vor: Sie öffnet sich im E-Mail-Programm des Benutzers, der selbst entscheidet, ob er sie sendet.

2. Speicherung und Schutz der Daten

- Gerätepark, Kontrollverlauf, Messinstrumente, Firmenlogo und im Mehrkundenmodus die Kundendatenblätter werden in Dateien im Datenordner des Unternehmens gespeichert. Der Hersteller hat technisch keinen Zugriff darauf.
- Die Anwendung kennt keine Benutzerkonten: Der Datenzugriff richtet sich nach den vom Unternehmen verwalteten Ordnerberechtigungen (Windows, Server, NAS).
- Die Datendateien werden von der Anwendung nicht verschlüsselt. Für den Schutz ruhender Daten empfiehlt sich die Verschlüsselung des Datenträgers oder des NAS des Unternehmens.
- Schutz vor Datenverlust: zweistufiges Schreiben (temporäre Datei, dann Ersetzen), Erkennung beschädigter oder unvollständiger Dateien (das Speichern wird dann gesperrt, nichts wird überschrieben), Warnung, wenn ein anderer Arbeitsplatz die Daten zwischenzeitlich geändert hat (kein stilles Überschreiben), sowie optionale automatische Sicherung beim Schliessen.

3. Lizenz

- Der Lizenzschlüssel ist digital signiert (asymmetrische Signatur ECDSA, Kurve P-256, SHA-256). Die Anwendung enthält nur den Prüfschlüssel; der Signaturschlüssel verbleibt ausschliesslich beim Hersteller. Ein Schlüssel kann daher weder gefälscht noch verändert werden, ohne abgelehnt zu werden. Es werden nur im aktuellen Format signierte Schlüssel akzeptiert.
- Die Lizenz ist an die eindeutige Kennung des Unternehmens gebunden: Ein in den Lizenzordner eines anderen Unternehmens kopierter Schlüssel wird abgelehnt.
- Die auf dem Datenträger gespeicherte Lizenzdatei ist verschlüsselt (AES-256-GCM) und durch eine Integritätsprüfung geschützt. Die Prüfung erfolgt vollständig lokal, ohne Serveraufruf.

4. Härtung der Anwendung

- Die Oberfläche ist vom System isoliert: Chromium-Sandbox, Kontextisolierung aktiviert, direkter Node.js-Zugriff deaktiviert, Entwicklerwerkzeuge deaktiviert. Basiert auf einer unterstützten Electron-Version (aktuelle Sicherheitskorrekturen).
- Die Oberfläche kann weder neue Fenster öffnen noch zu einer anderen Seite navigieren noch Berechtigungen (Kamera, Mikrofon, Standort…) erhalten.
- Der Dateizugriff wird vom Hauptprozess kontrolliert: nur in den Ordnern, die der Benutzer selbst über das Windows-Auswahlfenster gewählt hat, nur ElecTrace-Dateien (zugelassene Namen), ohne dass die Oberfläche diesen Bereich erweitern kann. Externe Links sind auf E-Mail-Links (mailto) begrenzt.
- Alle vom Datenträger gelesenen Daten (Freigabeordner, importierte Sicherungen) werden vor der Verwendung geprüft und in das erwartete Format gebracht, und jeder angezeigte Text wird maskiert: Eine veränderte oder präparierte Datei kann keinen Code einschleusen. Kalibrierzertifikate (geprüfte PDF) werden im PDF-Programm von Windows geöffnet.
- Excel-Import begrenzt (10 MB, 10 000 Zeilen, Prüfung des Archivs vor dem Lesen) gegen übergrosse oder präparierte Dateien.
- Der automatische Start beim Hochfahren von Windows (Prüfung der Fälligkeiten) wird nie ohne Zustimmung des Benutzers aktiviert.
- Eine Content Security Policy (CSP) schränkt ein, welche Ressourcen die Oberfläche laden darf: keine externe Domain, keine Inline-Skripte. Nur der Programmcode darf ausgeführt werden, was eingeschleusten Code blockiert. Ein automatischer Test prüft vor jeder Version, dass alle angezeigten Daten maskiert werden.
- Es wird kein Code dynamisch heruntergeladen oder ausgeführt. Aktualisierungen werden nie automatisch installiert.

5. Nachvollziehbarkeit und Diagnose

- Ein lokales, mit Zeitstempel versehenes technisches Protokoll erfasst wichtige Aktionen (z. B. Ändern von Daten, Lizenzaktivierung) für die Fehlerbehebung.
- Das Protokoll ist in einem passwortgeschützten Bereich einsehbar und wird nie automatisch übermittelt. Das Passwort ist änderbar und wird nur als Prüfsumme (SHA-256) gespeichert; es wird empfohlen, es bei der Inbetriebnahme zu ändern.

6. Datenschutz

- Personendaten werden vom Unternehmen selbst erfasst: die Namen der Kontrollpersonen, der Firmenname und im Mehrkundenmodus die Kontaktangaben der Kunden (Name der Kontaktperson, Telefon, E-Mail). Es werden keine besonders schützenswerten Personendaten im Sinne des Bundesgesetzes über den Datenschutz (DSG) erhoben.
- Diese Daten bleiben ausschliesslich unter der Kontrolle des Unternehmens, auf dessen eigener Infrastruktur.

7. Aktualisierungen und Meldung von Schwachstellen

- Das Installationsprogramm ist auf Philippoz Solutions digital signiert (Code-Signing-Zertifikat): Windows zeigt den verifizierten Herausgeber an, und jede Veränderung der Datei wird erkannt.
- Aktualisierungen liefert der Hersteller manuell als neues Installationsprogramm; sie werden nur auf Veranlassung des Unternehmens installiert.
- Festgestellte Schwachstellen können direkt dem Hersteller gemeldet werden (Kontakt unten).

KONTAKT HERSTELLER

Philippoz Solutions · support@electrace.ch

Cybersecurity Information Sheet

ElecTrace · inspection of portable electrical equipment (SNG 482638)

Application version: 1.2.2 · November 2026

ElecTrace is Windows software for managing the periodic inspections of portable electrical equipment. It is designed to run locally, with no online account and no cloud service. This sheet summarises the points usually requested in a supplier security assessment.

1. Architecture and connectivity

- Desktop application for Windows, installed on each workstation. Data is stored in a folder chosen by the company: a local PC or an internal network folder (server, NAS).
- No online account, no cloud service, no telemetry, no advertising. No company data is sent to the publisher or to any third party.
- The interface's scripts are not allowed to open network connections (Content Security Policy).
- No outgoing connection to the Internet: the application contacts no external server, not even for its display (the fonts are built into the program). It works identically with or without Internet; the only possible network access is to the internal shared folder chosen by the company.
- Data exchange only happens on the user's initiative: manual export and import of backup or Excel files. The support link (Settings › About) prepares an e-mail containing the ElecTrace version and the company's name and ID: it opens in the user's e-mail program, and the user decides whether to send it.

2. Data storage and protection

- The equipment fleet, inspection history, measuring instruments, company logo and, in multi-client mode, the client records are stored in files in the company's data folder. The publisher has no technical access to them.
- The application has no user accounts: access to the data relies on the folder permissions (Windows, server, NAS) managed by the company.
- The data files are not encrypted by the application. For protection at rest, rely on disk or NAS encryption provided by the company.
- Protection against data loss: two-step writes (temporary file, then replace), detection of damaged or incomplete files (saving is then blocked and nothing is overwritten), a warning if another workstation has changed the data in the meantime (no silent overwrite), and an optional automatic backup on exit.

3. Licence

- The licence key is digitally signed (asymmetric ECDSA signature, P-256 curve, SHA-256). The application contains only the verification key; the signing key stays exclusively with the publisher. A key can therefore be neither forged nor altered without being rejected. Only keys signed in the current format are accepted.
- The licence is bound to the company's unique identifier: a key copied into another company's licence folder is rejected.
- The licence file stored on disk is encrypted (AES-256-GCM) and protected by an integrity check. Verification is entirely local, with no call to any server.

4. Application hardening

- The interface is isolated from the system: Chromium sandbox, context isolation enabled, direct Node.js access disabled, developer tools disabled. Built on a supported Electron version (current security fixes).
- The interface can neither open new windows, navigate to another page, nor obtain permissions (camera, microphone, location…).
- File access is controlled by the main process: only within folders the user has personally chosen in the Windows folder dialog, only ElecTrace files (allowed names), with no way for the interface to widen this area. External links are limited to e-mail links (mailto).
- All data read from disk (shared folders, imported backups) is checked and normalised before use, and all displayed text is escaped: a modified or booby-trapped file cannot inject code. Calibration certificates (verified PDFs) open in the Windows PDF reader.
- Excel import is limited (10 MB, 10,000 rows, archive check before reading) against oversized or booby-trapped files.
- Automatic start with Windows (due-date check) is never enabled without the user's consent.
- A Content Security Policy (CSP) restricts the resources the interface may load: no external domain and no inline scripts. Only the program's own code can run, which blocks any injected code. An automated test checks before each release that all displayed data is escaped.
- No code is downloaded or executed dynamically. Updates are never installed automatically.

5. Traceability and diagnostics

- A local, time-stamped technical log records significant actions (e.g. changing data, licence activation) for troubleshooting.
- The log can be viewed in a password-protected section and is never transmitted automatically. The password can be changed and is stored only as a hash (SHA-256); changing it at commissioning is recommended.

6. Personal data protection

- Personal data is entered by the company itself: the inspectors' names, the company name and, in multi-client mode, the clients' contact details (contact person's name, phone, e-mail). No category of sensitive personal data under the Swiss Federal Act on Data Protection (FADP) is collected.
- This data remains under the company's exclusive control, on its own infrastructure.

7. Updates and vulnerability reporting

- The installer is digitally signed in the name of Philippoz Solutions (code-signing certificate): Windows shows the verified publisher, and any modification of the file is detected.
- Updates are supplied manually by the publisher as a new installer and are installed only on the company's action.
- Any vulnerability found can be reported directly to the publisher (contact below).

PUBLISHER CONTACT

Philippoz Solutions · support@electrace.ch