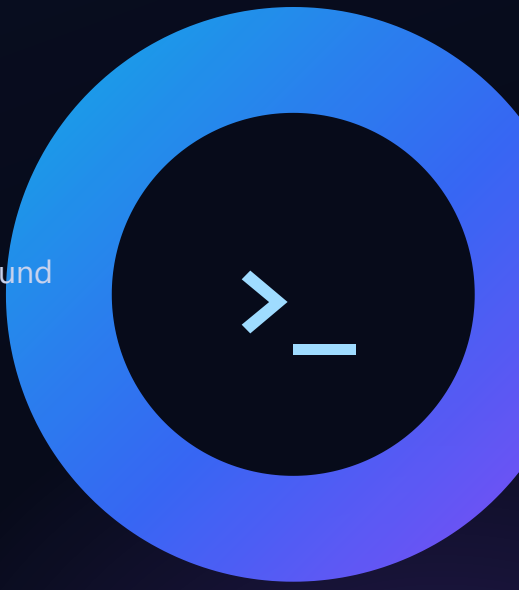
NexHand RemoteManager

KUNDENDOKUMENTATION

DATENSCHUTZ DURCH TECHNIKGESTALTUNG · ART. 25 UND 32 DSGVO

Technische und organisatorische Maßnahmen

Schutzmaßnahmen im Produkt NexHand RemoteManager: verschlüsselter Tresor für Zugangsdaten, Windows-Kopplung, Sitzungen über SSH, SFTP, Remotedesktop, VNC, Telnet, seriell und Web, Datensicherung, Lizenzprüfung und Löschung



DOKUMENT-ID	VERSION	STAND	STATUS
NH-TOM-01	1.7	28.09.2026	Zur Freigabe

HINWEIS FÜR KUNDEN

Dieses Dokument beschreibt die Maßnahmen, die NexHand RemoteManager als Software mitbringt. Kunden setzen die Software in eigener Verantwortung ein; die hier beschriebenen Eigenschaften können sie in ihre eigene TOM-Dokumentation und ihr Verzeichnis von Verarbeitungstätigkeiten übernehmen. Organisatorische Maßnahmen beim Kunden (Abschnitt 9) bleiben Aufgabe des Kunden.

Bezogen auf Programmversion 1.1.6. Bei neueren Versionen gilt die jeweils beiliegende Fassung dieses Dokuments.

DOKUMENTENKONTROLLE

Dokumentinformationen

Titel	Technische und organisatorische Maßnahmen – NexHand RemoteManager
Dokument-ID / Version	NH-TOM-01 / 1.7
Stand	28.09.2026 (bezogen auf Programmversion 1.1.6, Quellcodestand `9e568b7`)
Hersteller	Michael Kappe
Klassifizierung	KUNDENDOKUMENTATION
Adressaten	Kunden und deren Datenschutzbeauftragte; IT-Verantwortliche, die über den Einsatz entscheiden
Bezug	NH-ADM-01 (Administratorhandbuch) · NH-BH-01 (Benutzerhandbuch) · NH-VF-01 (Verfahrensbeschreibungen)
Überprüfung	Bei jeder Programmversion, die Tresor, Verschlüsselung, Datenablage, Sitzungsprotokolle, Lizenzprüfung oder Datensicherung verändert; spätestens jährlich

Änderungshistorie

VERSION	DATUM	ÄNDERUNG
1.7	28.09.2026	Abschnitt 7: direkt an einer Verbindung eingegebene Zugangsdaten werden mit der Verbindung gelöscht
1.6	28.09.2026	Abschnitt 10 und 11: RDP-Test mit echtem Server bestanden
1.5	28.09.2026	Bezug auf Programmversion 1.1.1; Programmversion und Quellcodestand werden automatisch eingesetzt
1.4	28.09.2026	Abschnitt 8: RDP-Diagnoseprotokoll (nur Zeitpunkte, Ereignisse und Codes)
1.3	28.09.2026	Abschnitt 4.6: automatische Beantwortung der HTTP-Anmeldung (Basic Auth)
1.2	28.09.2026	Abschnitt 4.6: Ausfüllen von Web-Anmeldeformularen nur auf dem Ursprung der Verbindung; Öffnen im Standardbrowser
1.1	28.09.2026	Abschnitt 4.2 korrigiert: manuelle Sperre über Menü und Statusleiste (nicht über den Infobereich); Sperren trennt alle offenen Sitzungen
1.0	28.09.2026	Erstfassung für Programmversion 1.1.0: Tresor und Schlüsselableitung, Windows-Kopplung, Sitzungsprotokolle, Hostschlüsselprüfung, Datensicherung, Lizenzprüfung mit Datenübermittlung an den Lizenzserver, Löschkonzept, Restrisiken

Freigabe

Mit der Unterschrift wird bestätigt, dass die beschriebenen Maßnahmen dem ausgelieferten Programmstand entsprechen.

Hersteller – Name, Datum, Unterschrift	Prüfung – Name, Datum, Unterschrift

ÜBERSICHT

Inhaltsverzeichnis

1 Zweck, Adressaten und Geltungsbereich 5
2 Systemüberblick 6
3 Verarbeitete Daten 7
4 Technische Schutzmaßnahmen im Einzelnen 8
4.1 Tresor und Verschlüsselung der Zugangsdaten 8
4.2 Entsperren, Windows-Kopplung und automatische Sperre 8
4.3 Umgang mit Geheimnissen im Arbeitsspeicher 8
4.4 SSH, SFTP und Hostschlüsselprüfung 9
4.5 Remotedesktop (RDP) 9
4.6 VNC, Telnet, serielle Verbindungen und Web 9
4.7 Anwendungshärtung 10
4.8 Import aus Royal TS 10
4.9 Lizenzprüfung 10
5 Empfänger und Übermittlungen 12
6 Datensicherung und Wiederherstellung 13
7 Lösch- und Aufbewahrungskonzept 13
8 Protokollierung 14
9 Organisatorische Maßnahmen beim Kunden 15
10 Verifikation 15
11 Restrisiken und offene Punkte 16
A Anhang A – Parameterübersicht 17
B Anhang B – Zuordnung zu den Schutzzielen des Art. 32 DSGVO 18

ABSCHNITT 1

Zweck, Adressaten und Geltungsbereich

NexHand RemoteManager ist ein Werkzeug für die Fernwartung. Technikerinnen und Techniker verwalten darin Projekte, Verbindungen und Zugangsdaten und öffnen Sitzungen zu Servern, Arbeitsplätzen und Geräten. Dieses Dokument beschreibt, wie die Software die dabei anfallenden Daten schützt.

Adressaten

Kunden, die NexHand RemoteManager einsetzen, und deren Datenschutzbeauftragte. Die Kunden sind Verantwortliche im Sinne des Art. 4 Nr. 7 DSGVO für das, was ihre Mitarbeiterinnen und Mitarbeiter mit der Software verarbeiten. Das Dokument setzt kein Programmierwissen voraus; die technischen Parameter sind in Anhang A zusammengefasst.

Geltungsbereich

BEREICH	INHALT
Produkt	NexHand RemoteManager 1.1.6 für Windows 10 und 11 (64 Bit). Desktop-Anwendung, die lokal auf dem Rechner der Technikerin oder des Technikers läuft.
Funktionen	Projekte, Ordner und Verbindungen · Credentials (Benutzername, Passwort, SSH-Schlüssel mit Passphrase) mit Vererbung · Sitzungen über SSH, SFTP, RDP, VNC, Telnet, seriell und Web · Import aus Royal TS · Datensicherung und Wiederherstellung · Lizenzierung
Betriebsmodell	Einzelplatz. Alle Daten liegen im Benutzerprofil des angemeldeten Windows-Kontos. Es gibt keinen Cloud-Dienst und keine zentrale Datenhaltung beim Hersteller. Einzige Verbindung zum Hersteller ist die Lizenzprüfung (Abschnitt 4.9).
Nicht erfasst	Die Zielsysteme selbst und was dort während einer Sitzung geschieht · die Netzwerkstrecke zu den Zielsystemen (VPN, Firewall) · der Lizenzserver als Betriebssystem des Herstellers (eigene Dokumentation) · die Sicherheit des Windows-Arbeitsplatzes (Abschnitt 9)

Leitprinzipien

- **Lokal statt Cloud:** Zugangsdaten verlassen den Rechner nur in der jeweiligen Sitzung zum Zielsystem und in einer vom Benutzer selbst angelegten Datensicherung.
- **Verschlüsselung auf Feldebene:** Jedes Geheimnis ist einzeln verschlüsselt und an seinen Datensatz gebunden. Die Datenbankdatei allein verrät keine Passwörter.
- **Datenminimierung** (Art. 5 Abs. 1 lit. c DSGVO): keine Telemetrie, keine Nutzungsstatistik, keine Absturzberichte, keine Protokollierung von Sitzungsinhalten.
- **Sichere Voreinstellungen** (Art. 25 Abs. 2): Hostschlüsselprüfung, Netzwerkebenen-Authentifizierung bei RDP, keine Laufwerksweiterleitung, Zertifikatsprüfung im Web – Abweichungen nur bewusst je Verbindung.

ABSCHNITT 2

Systemüberblick

Die Anwendung besteht aus einer Oberfläche (WebView2) und einem Programmkern in Rust. Nur der Programmkern hat Zugriff auf Datenbank, Tresor und Netzwerk; die Oberfläche fordert Aktionen über eine fest definierte Befehlsschnittstelle an und erhält ein Passwort nur, wenn der Benutzer es ausdrücklich anzeigen lässt.

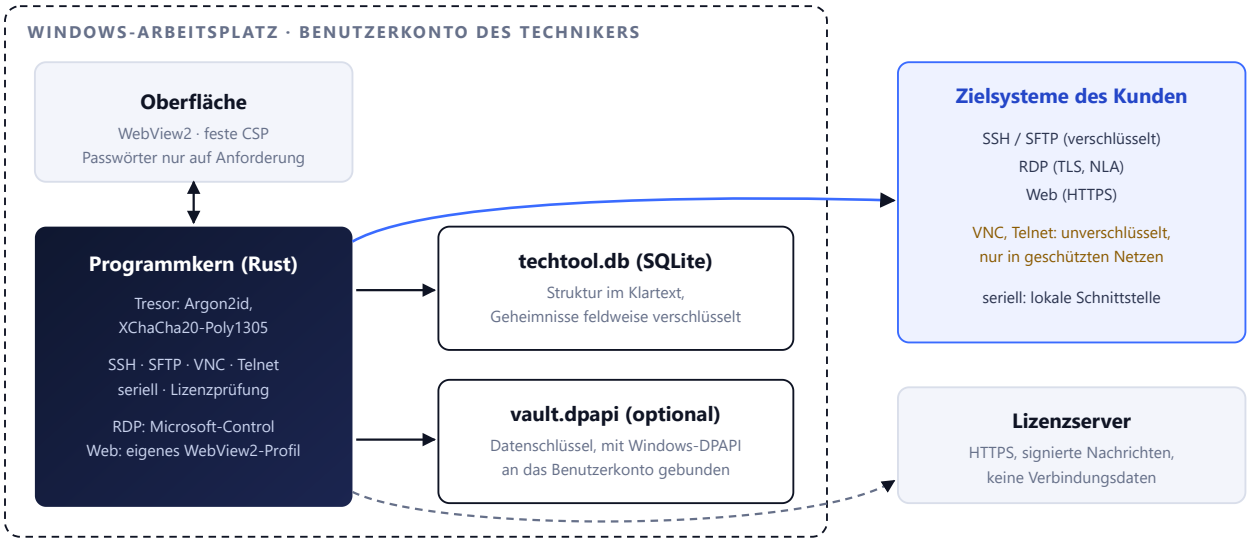


Abbildung 1: Komponenten und Datenflüsse. Durchgezogen: Sitzungen zu den Zielsystemen; gestrichelt: Lizenzprüfung.

Ablageorte

DATEI	ORT	INHALT
`techtool.db`	`%APPDATA%\com.techtool.app\`	Projekte, Ordner, Verbindungen, Credentials (Geheimnisse verschlüsselt), bekannte Hostschlüssel, Änderungsprotokoll, Lizenzdaten
`vault.dpapi`	ebenda	nur bei aktivierter Windows-Kopplung: Datenschlüssel, mit DPAPI verschlüsselt
`web\`, `web-insecure\`	ebenda	Browserprofile der Web-Sitzungen (Cookies, Cache der aufgerufenen Seiten)
Sicherungen	`Dokumente\NexHand-Sicherungen\` oder frei gewählt	Kopie der Datenbank, Geheimnisse weiterhin verschlüsselt
SFTP-Zwischendateien	`%TEMP%\NexHand RemoteManager\`	zum Öffnen heruntergeladene Dateien (Abschnitt 11)

ABSCHNITT 3

Verarbeitete Daten

NexHand RemoteManager verarbeitet in erster Linie Zugangsdaten zu IT-Systemen. Personenbezogen sind vor allem Benutzernamen, Namen in Projekten und Notizen sowie Inhalte, die während einer Sitzung sichtbar werden.

DATENART	BEISPIELE	SCHUTZ
Stammdaten der Struktur	Projekt- und Ordnernamen (häufig Kundennamen), Verbindungsnamen, Hostnamen, IP-Adressen, Ports, Notizen	lokal im Benutzerprofil; Zugriff nur nach Entsperren über die Anwendung
Credentials	Benutzernamen, Domänen	wie Stammdaten
Geheimnisse	Passwörter, private SSH-Schlüssel, Passphrasen	feldweise verschlüsselt (4.1)
Hostschlüssel	SHA-256-Fingerabdrücke der SSH-Server	lokal; Schutz vor untergeschobenen Servern (4.4)
Sitzungsinhalte	Terminalausgaben, Bildschirminhalte, Dateien	werden nicht gespeichert; nur im Arbeitsspeicher, solange die Sitzung offen ist
Lizenzdaten	Lizenzschlüssel, Geräte-Fingerabdruck (Hash), Rechnername, Programmversion	Übermittlung nur an den Lizenzserver (4.9, 5)

KEINE TELEMETRIE

Die Software sendet keine Nutzungsdaten, Absturzberichte, Verbindungslisten oder Hostnamen an den Hersteller oder Dritte. Die einzige Verbindung zum Hersteller ist die Lizenzprüfung mit den in Abschnitt 5 abschließend aufgezählten Daten.

ABSCHNITT 4

Technische Schutzmaßnahmen im Einzelnen

Die Maßnahmen sind im Programmkern umgesetzt und gelten für alle Projekte und Verbindungen. Sie lassen sich von der Oberfläche aus nicht umgehen.

4.1 Tresor und Verschlüsselung der Zugangsdaten

- **Datenschlüssel:** Beim Einrichten erzeugt die Anwendung einen zufälligen 256-Bit-Schlüssel (Zufallsquelle des Betriebssystems). Er verschlüsselt jedes Geheimnis einzeln.
- **Verfahren:** XChaCha20-Poly1305 – authentisierte Verschlüsselung mit 192-Bit-Zufallsnonce je Vorgang. Eine Veränderung am verschlüsselten Wert wird beim Entschlüsseln erkannt.
- **Bindung an den Datensatz:** Die Kennung des Credentials geht als zusätzliche authentisierte Angabe (AAD) in die Verschlüsselung ein, bei Passphrasen ergänzt um den Zweck. Ein verschlüsselter Wert lässt sich deshalb nicht unbemerkt in einen anderen Datensatz kopieren.
- **Master-Passwort:** Der Datenschlüssel ist mit einem aus dem Master-Passwort abgeleiteten Schlüssel verpackt. Ableitung mit Argon2id (64 MiB Speicher, 3 Durchläufe, 16 Byte Salz), das Verfahren ist speicherintensiv und bremst das Durchprobieren von Passwörtern stark aus. Mindestlänge 8 Zeichen.
- **Passwortwechsel:** verpackt nur den Datenschlüssel neu, mit neuem Salz. Das Master-Passwort selbst wird nirgends gespeichert.
- **Kein Hintertürzugang:** Ohne Master-Passwort (oder die Windows-Kopplung auf dem ursprünglichen Rechner) sind die Geheimnisse nicht wiederherstellbar – auch nicht durch den Hersteller.

4.2 Entsperren, Windows-Kopplung und automatische Sperre

- **Gesperrter Zustand:** Ohne Entsperren zeigt die Anwendung nur den Sperrbildschirm. Der Programmkern verweigert alle Befehle, die Geheimnisse benötigen.
- **Windows-Kopplung (optional):** Auf Wunsch wird der Datenschlüssel mit der Windows-Datenschutz-API (DPAPI) an das Windows-Benutzerkonto gebunden und in `vault.dpapi` abgelegt. Dann entsperrt die Anwendung beim Start ohne Passworteingabe. Die Datei ist auf einem anderen Rechner oder unter einem anderen Konto wertlos. Vor dem Übernehmen wird der Schlüssel gegen einen Prüfwert im Tresor getestet.
- **Abschalten:** In den Einstellungen jederzeit; die Datei wird gelöscht. Nach manuellem Sperren entsperrt die Anwendung bis zum nächsten Start nicht automatisch.
- **Automatische Sperre:** nach einstellbarer Inaktivität (Standard 30 Minuten, 0 = aus). Solange eine Sitzung offen ist, wird nicht gesperrt, um laufende Fernwartung nicht abzubrechen. Bei aktiver Windows-Kopplung ist die Sperre wirkungslos, da sofort wieder entsperrt würde; hier schützt die Sperre des Windows-Arbeitsplatzes (Abschnitt 9).
- **Manuelle Sperre:** Tastenkürzel `Strg` + `L`, Menü „Datei“ oder Statusleiste. Beim Sperren werden alle offenen Sitzungen getrennt, da ohne Tresor keine Zugangsdaten bereitstehen.

4.3 Umgang mit Geheimnissen im Arbeitsspeicher

- Datenschlüssel und entschlüsselte Geheimnisse liegen in Speicherbereichen, die beim Freigeben überschrieben werden (Rust-Bibliothek `zeroize`). Beim Sperren wird der Datenschlüssel verworfen.

- Geheimnisse werden im Programmkern für den Verbindungsaufbau entschlüsselt. Die Oberfläche erhält ein gespeichertes Passwort nur, wenn der Benutzer es im Credential-Dialog über das Augensymbol ausdrücklich anzeigen lässt – und nur bei entsperrtem Tresor. Private SSH-Schlüssel und Passphrasen werden nicht angezeigt.
- Die Anwendung schreibt keine Geheimnisse in Protokolldateien oder temporäre Dateien.

4.4 SSH, SFTP und Hostschlüsselprüfung

- **Transport:** SSH-Protokoll 2 mit der Bibliothek `russh`; nur aktuelle Verfahren für Schlüsselaustausch und Verschlüsselung. SFTP läuft innerhalb derselben verschlüsselten Verbindung.
- **Hostschlüssel:** Beim ersten Kontakt zeigt die Anwendung den SHA-256-Fingerabdruck des Servers und verlangt eine Bestätigung. Bestätigte Schlüssel werden gespeichert. Ändert sich der Schlüssel später, erscheint eine deutliche Warnung; ohne ausdrückliche Zustimmung wird die Verbindung nicht aufgebaut. Das schützt vor untergeschobenen Servern („Man in the Middle“).
- **Anmeldung:** Passwort oder privater Schlüssel (OpenSSH- und PEM-Format), Passphrase aus dem Tresor oder als Abfrage; die Passphrase kann auf Wunsch im Tresor gespeichert werden.
- **SFTP-Dateiexplorer:** Übertragungen nur auf ausdrückliche Aktion (Ziehen, Kopieren, Menü). Kein automatischer Abgleich.

4.5 Remotedesktop (RDP)

- RDP nutzt das in Windows enthaltene Microsoft-Remotedesktop-Control (`mstscax.dll`). Verschlüsselung, Zertifikatsprüfung und Updates liefert damit Microsoft über Windows Update.
- **Netzwerkebenen-Authentifizierung (NLA/CredSSP)** ist standardmäßig eingeschaltet. Die Serverauthentifizierung steht auf „warnen“: Bei ungültigem Zertifikat fragt das Control nach.
- Anmeldedaten werden dem Control direkt übergeben. Systemdialoge zur Passworteingabe sind abgeschaltet, damit keine Zugangsdaten in der Windows-Anmeldeinformationsverwaltung landen.
- **Weiterleitungen:** Zwischenablage und Audio sind voreingestellt an; Laufwerke und Drucker aus. Jede Weiterleitung lässt sich je Verbindung schalten. Laufwerksweiterleitung gibt dem Zielsystem Zugriff auf lokale Dateien und sollte nur bei Bedarf aktiviert werden.
- Remotedesktop-Gateway wird unterstützt; die Anmeldedaten werden dann für Gateway und Ziel gemeinsam verwendet.

4.6 VNC, Telnet, serielle Verbindungen und Web

PROTOKOLL	SCHUTZ	HINWEIS
VNC	VNC-Passwortverfahren des Servers	Das VNC-Protokoll verschlüsselt die Bildübertragung nicht. Nur in geschützten Netzen oder über VPN/SSH-Tunnel verwenden.
Telnet	keiner	Unverschlüsselt, auch Passwörter. Nur für Altgeräte im lokalen Netz.
Seriell	physischer Zugang	Lokale COM-Schnittstelle, keine Netzwerkübertragung.

PROTOKOLL	SCHUTZ	HINWEIS
Web	HTTPS mit Zertifikatsprüfung (WebView2)	Eigenes Browserprofil getrennt von Edge. „Zertifikatsfehler ignorieren“ ist standardmäßig aus, lässt sich nur je Verbindung einschalten und läuft dann in einem getrennten Profil, damit die Ausnahme nicht auf andere Web-Verbindungen übergreift. Hinterlegte Credentials werden nur auf dem Ursprung der Verbindung (Schema, Host, Port) in das Anmeldeformular eingetragen, nie nach einer Umleitung und nie automatisch abgesendet. Eine HTTP-Anmeldung (Basic Auth) des Webservers beantwortet NexHand nur für denselben Ursprung automatisch; nach einer abgelehnten automatischen Antwort übernimmt der Benutzer (keine Wiederholungsschleife). Bei unverschlüsseltem HTTP gehen diese Zugangsdaten wie bei jedem Browser im Klartext übers Netz. Wahlweise öffnet die Verbindung im Standardbrowser des Benutzers; dann gelten dessen Schutzmaßnahmen, NexHand überträgt keine Zugangsdaten.

4.7 Anwendungshärtung

- **Content Security Policy:** Die Oberfläche darf nur eigene Ressourcen laden und nur mit dem Programmkern sprechen. Fremde Skripte oder Verbindungen sind ausgeschlossen.
- **Befehlsschnittstelle:** Die Oberfläche kann nur fest registrierte Befehle aufrufen. Alle Befehle, die auf Daten, Geheimnisse oder Sitzungen zugreifen, prüfen selbst, ob der Tresor entsperrt ist.
- **Speichersichere Sprache:** Programmkern und Protokolle sind in Rust geschrieben. Eine ganze Klasse von Sicherheitslücken (Pufferüberläufe, Zugriff auf freigegebenen Speicher) ist damit weitgehend ausgeschlossen.
- **Keine eingebetteten Fremdinhalte** in der Oberfläche; Web-Sitzungen laufen als getrenntes WebView ohne Zugriff auf die Befehlsschnittstelle.

4.8 Import aus Royal TS

- Der Import liest die exportierte Datei (`.rtsz`, `.rtsx`) lokal. Es gibt keine Verbindung zu Royal TS oder zu Diensten Dritter.
- Übernommen werden Struktur, Hosts und Benutzernamen. Passwörter liegen in Royal TS verschlüsselt vor und werden nicht übernommen; sie werden beim ersten Verbinden abgefragt und auf Wunsch im Tresor verschlüsselt gespeichert.
- Die Importdatei selbst bleibt unverändert. Nicht mehr benötigte Kopien sollte der Kunde löschen (Abschnitt 9).

4.9 Lizenzprüfung

- Ohne Lizenz läuft die Software als Free-Version mit höchstens 10 Verbindungen. Es findet dann keinerlei Kommunikation mit dem Lizenzserver statt.
- Beim Aktivieren erzeugt die Anwendung ein eigenes Schlüsselpaar (Ed25519). Der private Schlüssel wird mit dem Tresor verschlüsselt gespeichert.
- Anfragen an den Lizenzserver gehen ausschließlich über HTTPS und sind zusätzlich signiert. Antworten und Lizenzzusagen („Leases“) prüft die Anwendung gegen den fest eingebauten öffentlichen Schlüssel des Servers; gefälschte Antworten werden verworfen.
- Die Prüfung arbeitet offline weiter: Eine Lizenzzusage gilt bis zum Ende ihrer Kulanzzeit, auch ohne Serverkontakt. Die Erneuerung läuft im Hintergrund (Prüfung alle 30 Minuten, Kontakt nur bei Fälligkeit).

- Das Gerät wird über einen Fingerabdruck erkannt: Die Windows-`MachineGuid` wird mit einem produktspezifischen Schlüssel (HMAC) gehasht. Die Kennung selbst verlässt den Rechner nicht.

ABSCHNITT 5

Empfänger und Übermittlungen

Die Software übermittelt Daten nur an die Zielsysteme, die der Benutzer selbst aufruft, und – bei aktivierter Lizenz – an den Lizenzserver des Herstellers.

EMPFÄNGER	DATEN	ANLASS
Zielsysteme des Kunden	Benutzername, Passwort bzw. Schlüsselnachweis, Tastatur- und Mauseingaben, übertragene Dateien	nur beim Öffnen einer Sitzung durch den Benutzer
Lizenzserver des Herstellers	Lizenzschlüssel · öffentlicher Client-Schlüssel · Geräte-Fingerabdruck (HMAC-Hash) · Rechnername (`COMPUTERNAME`) · Programmversion · Betriebssystem („windows“)	Aktivieren, Erneuern, Freigeben der Lizenz
Microsoft	keine durch NexHand veranlasste Übermittlung	WebView2 und das RDP-Control werden über Windows Update aktualisiert; deren eigene Diagnoseeinstellungen richten sich nach der Windows-Konfiguration des Kunden

> **NICHT ÜBERMITTELT**
>
> Verbindungslisten, Hostnamen, IP-Adressen der Zielsysteme, Benutzernamen, Passwörter, Projektnamen, Notizen und Sitzungsinhalte werden nie an den Hersteller übermittelt.

Der Rechnername dient dazu, dass der Kunde seine aktivierten Geräte in der Lizenzverwaltung erkennen und gezielt freigeben kann. Eine Übermittlung in Drittländer findet durch die Software nicht statt; Standort und Betrieb des Lizenzservers beschreibt die Dokumentation des Lizenzservers.

ABSCHNITT 6

Datensicherung und Wiederherstellung

Die Datensicherung ist eine konsistente Kopie der Datenbank. Geheimnisse bleiben darin mit dem Master-Passwort verschlüsselt; wer die Sicherungsdatei findet, erhält ohne Master-Passwort keine Zugangsdaten.

- **Anlegen:** nur bei entsperrtem Tresor, über Einstellungen → Datensicherung. Standardordner `Dokumente\NexHand-Sicherungen`, Dateiname mit Datum und Uhrzeit.
- **Prüfen vor dem Einspielen:** Die Anwendung öffnet die Datei, prüft Aufbau und Tresor und zeigt Anzahl der Projekte, Verbindungen und Credentials.
- **Wiederherstellen:** Vorher wird der aktuelle Bestand automatisch gesichert (`techtool-vor-wiederherstellung-…db`). Danach wird der Tresor gesperrt und die Windows-Kopplung entfernt, da sie zu den alten Daten gehört. Entsperrt wird mit dem Master-Passwort der Sicherung.
- **Übertragung auf einen anderen Rechner** (z. B. Techniker-Laptop): über dieselbe Funktion. Die Lizenzaktivierung ist an das Gerät gebunden und wird auf dem neuen Rechner ungültig; dort ist eine eigene Aktivierung nötig.

> **AUFGABE DES KUNDEN**
> Die Software sichert nicht automatisch. Sicherungsrhythmus, Aufbewahrungsort (z. B. verschlüsseltes Netzlaufwerk) und Aufbewahrungsdauer legt der Kunde fest (Verfahren in NH-VF-01).

ABSCHNITT 7

Lösch- und Aufbewahrungskonzept

OBJEKT	BEIM LÖSCHEN	VERBLEIB
Credential	Passwort, Schlüssel und Passphrase werden sofort überschrieben (auf leer gesetzt)	Name und Benutzername bleiben als gelöschter Datensatz in der Datenbank
Verbindung, Ordner	als gelöscht markiert, nicht mehr sichtbar; direkt an der Verbindung eingegebene Zugangsdaten werden mitgelöscht und ihre Geheimnisse überschrieben	Datensatz bleibt in der Datenbank
Projekt	mit allen Ordnern, Verbindungen und Credentials als gelöscht markiert; Geheimnisse der Credentials überschrieben	wie oben
Gesamter Bestand	Deinstallation mit Option „Daten entfernen“ oder Löschen des Ordners `%APPDATA%\com.techtool.app`	Sicherungen außerhalb dieses Ordners bleiben erhalten
Lizenz	„Freigeben“ im Lizenzdialog löscht Aktivierung und Client-Schlüssel lokal und gibt den Platz beim Server frei	Serverseitige Aufbewahrung nach Dokumentation des Lizenzservers

Gelöschte Datensätze werden aufbewahrt, damit ein späterer Abgleich zwischen mehreren Geräten Löschungen erkennen kann. Sie enthalten keine Geheimnisse, aber weiterhin Namen, Hostnamen und Notizen (Restrisiko, Abschnitt 11).

ABSCHNITT 8

Protokollierung

- **Änderungsprotokoll:** Die Datenbank führt je Änderung einen Eintrag mit Objektart, Kennung, Vorgang (anlegen, ändern, löschen) und Zeitpunkt. Inhalte, insbesondere Geheimnisse, werden nicht protokolliert.
- **Keine Sitzungsaufzeichnung:** Terminalausgaben, Tastatureingaben und Bildschirminhalte werden nicht gespeichert.
- **Keine Anmeldeprotokolle beim Hersteller:** Welche Verbindung wann geöffnet wurde, bleibt ausschließlich auf dem Rechner und wird auch dort nicht gesondert protokolliert.
- **RDP-Diagnoseprotokoll:** Zur Fehlersuche schreibt NexHand die Ereignisse des Remotedesktop-Controls in `logs\rdp.log` im Datenordner: Zeitpunkt, eine zufällige Sitzungskennung, Ereignisnummer und Code. Verbindungsname, Host, Benutzername und Zugangsdaten werden nicht aufgezeichnet. Die Datei wird ab 512 KB neu begonnen und verlässt den Rechner nicht.
- Kunden, die eine Nachweisführung über Fernwartungszugriffe benötigen, nutzen die Protokolle der Zielsysteme (Anmeldeprotokolle von SSH, Windows-Ereignisanzeige) oder eines Jump-Hosts.

ABSCHNITT 9

Organisatorische Maßnahmen beim Kunden

Die Software schützt die Daten nur so gut, wie der Arbeitsplatz geschützt ist, auf dem sie läuft. Die folgenden Maßnahmen liegen in der Verantwortung des Kunden; sie sind als Empfehlung formuliert.

BEREICH	EMPFEHLUNG
Arbeitsplatz	Festplattenverschlüsselung (BitLocker) · aktuelles Windows mit automatischen Updates · Virenschutz · Bildschirmsperre nach kurzer Inaktivität · persönliches Windows-Konto je Techniker
Master-Passwort	mindestens 12 Zeichen, nur für NexHand verwendet · nicht weitergeben · Hinterlegung für den Notfall (versiegelter Umschlag, Passwortmanager der Firma) nach NH-VF-01
Windows-Kopplung	nur auf Rechnern mit Festplattenverschlüsselung und gesperrtem Windows-Konto aktivieren; auf gemeinsam genutzten Rechnern ausschalten
Credentials	persönliche statt gemeinsamer Konten auf den Zielsystemen, wo möglich · SSH-Schlüssel mit Passphrase · regelmäßiger Passwortwechsel auf den Zielsystemen
Unsichere Protokolle	Telnet und VNC nur in abgeschotteten Netzen oder über VPN; Zertifikatsfehler im Web nicht dauerhaft ignorieren
Datensicherung	regelmäßig, auf verschlüsselten Datenträgern; alte Sicherungen nach festgelegter Frist löschen
Importdateien	nicht mehr benötigte Kopien von Royal-TS-Dokumenten nach dem Import löschen
Geräteverlust	Passwörter der betroffenen Zielsysteme ändern, Lizenz freigeben (Verfahren NH-VF-01)
Ausscheiden	Laptop zurücknehmen, Datenbestand löschen, gemeinsam genutzte Zugangsdaten ändern

ABSCHNITT 10

Verifikation

PRÜFUNG	METHODE	ERGEBNIS
Tresor: Einrichten, Entsperren, falsches Passwort, Passwortwechsel	automatisierte Tests des Programmkerns	BESTANDEN
Bindung verschlüsselter Werte an den Datensatz	automatisierter Test: vertauschter Wert wird abgewiesen	BESTANDEN
DPAPI-Kopplung	automatisierter Test (Ver- und Entschlüsseln), manueller Test Autostart	BESTANDEN
Löschen überschreibt Geheimnisse	automatisierter Test, Kontrolle der Datenbank	BESTANDEN

PRÜFUNG	METHODE	ERGEBNIS
Hostschlüssel: erster Kontakt, geänderter Schlüssel	manueller Test gegen lokalen SSH-Testserver	BESTANDEN
Sicherung und Wiederherstellung	automatisierter Test, manueller Test mit getrenntem Datenordner	BESTANDEN
Lizenz: Free-Version, Aktivierung, Erneuerung, Freigabe, gefälschte oder fremde Antworten, Widerruf, Lease eines fremden Geräts	automatisierte Tests gegen simulierten Server	BESTANDEN
Lizenz: Ablauf der Kulanzzeit, zurückgestellte Uhr	Code-Prüfung; eigener automatisierter Test geplant	AUSSTEHEND
RDP mit Anmeldung an einem echten Server (Windows Server 2019): Anzeige, Tastatur, Maus, Größenanpassung, Zwischenablage, Zertifikatsabfrage	manueller Test mit Version 1.1.1	BESTANDEN

ABSCHNITT 11

Restrisiken und offene Punkte

RESTRISIKO	BEWERTUNG UND UMGANG
Kompromittierter Arbeitsplatz	Schadsoftware mit Zugriff auf das Benutzerkonto kann bei entsperrtem Tresor Eingaben und Speicher mitlesen. Keine Software kann das vollständig verhindern; Gegenmaßnahmen nach Abschnitt 9.
Windows-Kopplung	Wer sich am Windows-Konto anmelden kann, kann den Tresor öffnen. Bewusste Komfortentscheidung, abschaltbar; Empfehlung in Abschnitt 9.
Metadaten unverschlüsselt	Projekt- und Verbindungsnamen, Hostnamen und Notizen liegen im Klartext in der Datenbank, damit die Anwendung ohne Entsperren starten und suchen kann. Schutz durch Festplattenverschlüsselung.
Gelöschte Datensätze	bleiben ohne Geheimnisse erhalten (Abschnitt 7). Geplant: endgültiges Bereinigen nach einstellbarer Frist.
SFTP-Zwischendateien	Zum Öffnen heruntergeladene Dateien bleiben im Temp-Ordner, bis Windows ihn bereinigt. Geplant: Löschen beim Beenden.
Unverschlüsselte Protokolle	VNC und Telnet übertragen ungeschützt; die Protokolle werden für Altgeräte angeboten. Einsatz nur nach Abschnitt 9. Geplant: Hinweis in der Oberfläche beim Anlegen solcher Verbindungen.
Codesignatur	Der Installer ist noch nicht signiert; Windows SmartScreen warnt beim ersten Start. Bezug nur über die offizielle Quelle des Herstellers. Geplant: Signatur mit Code-Signing-Zertifikat.

ANHANG A

Parameterübersicht

Stand 28.09.2026, Programmversion 1.1.6.

PARAMETER	WERT	WIRKUNG
Datenschlüssel	256 Bit	zufällig, Zufallsquelle des Betriebssystems
Verschlüsselung	XChaCha20-Poly1305	authentisiert, 192-Bit-Nonce, AAD = Kennung des Datensatzes
Schlüsselableitung	Argon2id v1.3	64 MiB, 3 Durchläufe, 1 Thread, 16 Byte Salz
Master-Passwort	mind. 8 Zeichen	empfohlen 12 und mehr
Windows-Kopplung	DPAPI, Benutzerkonto	mit zusätzlicher Entropie; optional
Automatische Sperre	30 Minuten	einstellbar, 0 = aus; nicht bei offenen Sitzungen
Hostschlüssel	SHA-256	Bestätigung beim ersten Kontakt, Warnung bei Änderung
RDP	NLA an	Serverauthentifizierung „warnen“; Laufwerke und Drucker aus
Free-Version	10 Verbindungen	ohne Kontakt zum Lizenzserver
Lizenzsignatur	Ed25519	Anfragen, Antworten und Leases signiert; Transport HTTPS (rustls)
Lizenzerneuerung	Prüfung alle 30 min	Kontakt nur bei Fälligkeit; offline bis Ende der Kulanzzeit
Geräte-Fingerabdruck	HMAC-SHA-256	aus der Windows-MachineGuid, Kennung verlässt den Rechner nicht
Telemetrie	keine	–

ANHANG B

Zuordnung zu den Schutzzielen des Art. 32 DSGVO

SCHUTZZIEL	MASSNAHMEN (ABSCHNITT)
Vertraulichkeit Art. 32 Abs. 1 lit. b	Feldweise Verschlüsselung und Argon2id (4.1) · Sperre und Windows-Kopplung (4.2) · Speicherbereinigung (4.3) · SSH, NLA, HTTPS (4.4–4.6) · CSP und Befehlsschnittstelle (4.7) · keine Telemetrie (3, 5)
Integrität Art. 32 Abs. 1 lit. b	Authentisierte Verschlüsselung mit Datensatzbindung (4.1) · Hostschlüsselprüfung (4.4) · signierte Lizenznachrichten (4.9) · Änderungsprotokoll (8)
Verfügbarkeit und Belastbarkeit Art. 32 Abs. 1 lit. b	Lokaler Betrieb ohne Abhängigkeit von Cloud-Diensten (1) · Lizenzprüfung offline bis Ende der Kulanzzeit (4.9) · automatische Wiederverbindung bei RDP (4.5)
Rasche Wiederherstellbarkeit Art. 32 Abs. 1 lit. c	Datensicherung mit Prüfung und automatischer Sicherung vor dem Einspielen (6)
Überprüfung und Evaluierung Art. 32 Abs. 1 lit. d	Automatisierte Tests je Version (10) · Überprüfung dieses Dokuments je Version (Dokumentinformationen)
Datenminimierung / Speicherbegrenzung Art. 5 Abs. 1 lit. c, e; Art. 25	Keine Sitzungsaufzeichnung (8) · Rechnername und Fingerabdruck-Hash als einzige Gerätedaten (5) · Überschreiben von Geheimnissen beim Löschen (7) · sichere Voreinstellungen (1)