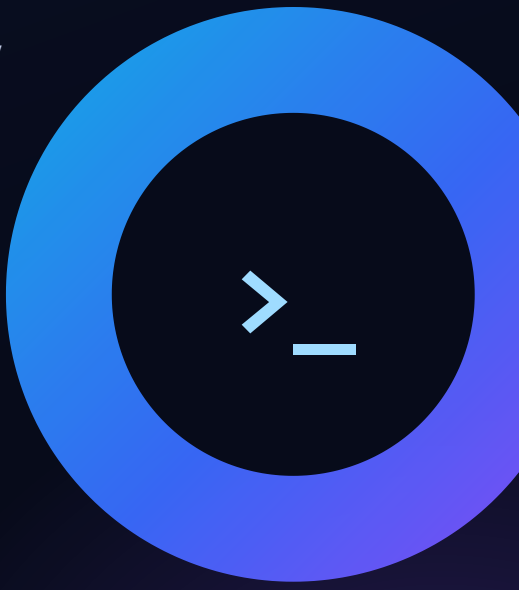
NexHand RemoteManager

KUNDENDOKUMENTATION

BEST PRACTICE FÜR DEN BETRIEB BEIM KUNDEN

Verfahrensbeschreibungen

Einrichtung und Ausscheiden von Technikern, Hinterlegung des Master-Passworts, Datensicherung, Übertragung, Geräteverlust, geänderte Hostschlüssel, Passwortwechsel, Löschung und Versionswechsel



DOKUMENT-ID	VERSION	STAND	STATUS
NH-VF-01	1.2	28.09.2026	Gültig

BEST PRACTICE – AN DIE EIGENE ORGANISATION ANPASSEN

Die Verfahren beschreiben bewährte Abläufe rund um NexHand RemoteManager. Kunden passen Rollen, Fristen und Ablageorte an ihre Organisation an und übernehmen die Verfahren in ihr Informationssicherheits- oder Datenschutzmanagement.

Bezogen auf Programmversion 1.1.6.

DOKUMENTENKONTROLLE

Dokumentinformationen

Titel	Verfahrensbeschreibungen – Betrieb und Sicherheit
Dokument-ID / Version	NH-VF-01 / 1.2
Stand	28.09.2026 (Programmversion 1.1.6)
Hersteller	Michael Kappe
Klassifizierung	KUNDENDOKUMENTATION
Adressaten	Leitung Technik, IT-Administration, Informationssicherheit, Datenschutz
Bezug	NH-TOM-01 (TOM) · NH-ADM-01 (Administratorhandbuch) · NH-BH-01 (Benutzerhandbuch)
Überprüfung	bei organisatorischen Änderungen, nach jedem Sicherheitsvorfall, spätestens jährlich

Änderungshistorie

VERSION	DATUM	ÄNDERUNG
1.2	28.09.2026	Bezug auf Programmversion 1.1.1; Programmversion und Quellcodestand werden automatisch eingesetzt
1.1	28.09.2026	Einordnung als Best Practice (Deckblatt, Status „Gültig“); Inhalte unverändert
1.0	28.09.2026	Erstfassung: Verfahren VF-01 bis VF-10

Freigabe beim Kunden

Mit der Unterschrift werden die angepassten Verfahren für die eigene Organisation in Kraft gesetzt.

Leitung – Name, Datum, Unterschrift

Informationssicherheit / Datenschutz – Datum, Unterschrift

ÜBERSICHT

Inhaltsverzeichnis

ABSCHNITT 1

Zweck und Rollen

NexHand RemoteManager hält Zugänge zu vielen Systemen an einem Ort. Das ist bequem – und macht jeden Rechner mit NexHand zu einem lohnenden Ziel. Die folgenden Verfahren regeln, wie Zugänge entstehen, gesichert, übertragen und wieder entzogen werden.

ROLLE	AUFGABEN
Leitung Technik	genehmigt Einrichtung und Entzug von Zugängen, entscheidet über Maßnahmen bei Vorfällen
IT-Administration	installiert NexHand, verwaltet Lizenzen, Sicherungen und den Referenzbestand
Techniker	nutzt NexHand, schützt Master-Passwort und Gerät, meldet Vorfälle sofort
Informationssicherheit / Datenschutz	wird bei Vorfällen (VF-05, VF-07) beteiligt, prüft Meldepflichten nach Art. 33 DSGVO

Jedes Verfahren nennt Auslöser, Verantwortliche, den Ablauf und den Nachweis, der aufzubewahren ist.

VF-01

Einrichtung eines neuen Technikers

Auslöser	Neue Mitarbeiterin oder neuer Mitarbeiter in der Technik, neuer Rechner
Verantwortlich	IT-Administration; Genehmigung durch Leitung Technik
Nachweis	Übergabeprotokoll (Anhang A)

1. Leitung Technik legt fest, welche Projekte der Techniker benötigt.
2. IT-Administration prüft den Rechner: BitLocker aktiv, Bildschirmsperre, aktuelles Windows, persönliches Konto (NH-ADM-01, Anhang B).
3. NexHand installieren; Lizenz aktivieren oder Free-Version nutzen.
4. Referenzbestand übernehmen (NH-ADM-01, Abschnitt 5) – nur mit den freigegebenen Projekten. Nicht benötigte Projekte vorher im Referenzbestand entfernen oder einen eigenen Teilbestand erstellen.
5. Techniker ändert das Master-Passwort und hinterlegt es nach VF-02.
6. Windows-Kopplung nach der Regel des Unternehmens einschalten oder nicht.
7. Einweisung anhand des Benutzerhandbuchs, insbesondere Hostschlüssel (VF-07) und unsichere Protokolle.
8. Übergabeprotokoll unterschreiben lassen.

VF-02

Hinterlegung des Master-Passworts

Auslöser	Einrichtung (VF-01), Änderung des Master-Passworts
Verantwortlich	Techniker; Aufbewahrung durch Leitung Technik
Nachweis	Eintrag im Hinterlegungsverzeichnis (Datum, Person, Ort – nicht das Passwort)

Ohne Master-Passwort sind die gespeicherten Zugangsdaten verloren; der Hersteller kann sie nicht wiederherstellen. Eine Hinterlegung verhindert Stillstand, wenn ein Techniker ausfällt.

1. Techniker legt ein Master-Passwort mit mindestens 12 Zeichen fest, das er nirgends sonst verwendet.
2. Hinterlegung wahlweise
   - im Passwortmanager des Unternehmens in einem Tresor, auf den nur Leitung Technik zugreifen kann, oder
   - im versiegelten Umschlag im Tresor; Siegel mit Datum und Unterschrift.
3. Eintrag im Hinterlegungsverzeichnis.
4. Bei jeder Änderung wird die alte Hinterlegung vernichtet und die neue angelegt.
5. Öffnen einer Hinterlegung nur mit Genehmigung der Leitung Technik; Anlass dokumentieren und den Techniker informieren. Danach ändert der Techniker das Master-Passwort.

VF-03

Datensicherung und Aufbewahrung

Auslöser	regelmäßig (Empfehlung: wöchentlich) und vor jedem Versionswechsel oder Import
Verantwortlich	Techniker (eigener Bestand), IT-Administration (Referenzbestand)
Nachweis	Sicherungsdateien mit Datum im Namen

1. Einstellungen → „Datensicherung & Übertragung“ → Sicherung erstellen.
2. Datei auf ein verschlüsseltes Netzlaufwerk oder in einen Sicherungsordner mit Rechten nur für den Techniker und die IT-Administration verschieben.
3. Aufbewahrung: die letzten vier wöchentlichen und die letzte monatliche Sicherung; ältere löschen.
4. Einmal im Quartal eine Rücksicherung testen: auf einem Testrechner oder mit getrenntem Datenordner (`TECHTOOL_DATA_DIR`) wiederherstellen und mit dem hinterlegten Passwort entsperren.

> **WARUM AUCH ALTE SICHERUNGEN GEFÄHRLICH SIND**
>
> Eine Sicherung enthält die Passwörter zum Zeitpunkt der Sicherung, verschlüsselt mit dem damaligen Master-Passwort. Wurde ein Master-Passwort bekannt, sind auch alle damit erstellten Sicherungen betroffen (VF-05).

VF-04

Übertragung auf einen anderen Rechner

Auslöser	Rechnertausch, zusätzlicher Einsatzrechner (z. B. Laptop für Außeneinsätze)
Verantwortlich	Techniker; IT-Administration bei Lizenzen
Nachweis	Lizenzverwaltung (Gerät freigegeben bzw. aktiviert)

1. Auf dem alten Rechner Sicherung erstellen (VF-03).
2. Datei auf verschlüsseltem Weg übertragen: Netzlaufwerk mit Rechten, verschlüsselter USB-Stick. Nicht per E-Mail oder über öffentliche Cloud-Dienste.
3. Auf dem neuen Rechner NexHand installieren und die Sicherung übernehmen; mit dem Master-Passwort der Sicherung entsperren.
4. Wird der alte Rechner nicht mehr genutzt: Lizenz dort freigeben, Daten löschen (VF-06, Schritt 4).
5. Lizenz auf dem neuen Rechner aktivieren.
6. Übertragungsdatei vom Übertragungsmedium löschen.

Bei zwei parallel genutzten Rechnern entwickeln sich die Bestände getrennt. Ein automatischer Abgleich ist in Version 1.1 nicht enthalten.

VF-05

Verlust oder Diebstahl eines Geräts

Auslöser	Rechner mit NexHand verloren, gestohlen oder unbefugt benutzt; Verdacht auf Schadsoftware; Master-Passwort bekannt geworden
Verantwortlich	Techniker meldet sofort; Leitung Technik steuert; Informationssicherheit/Datenschutz bewertet
Frist	Meldung unverzüglich; Bewertung der Meldepflicht an die Aufsichtsbehörde binnen 72 Stunden (Art. 33 DSGVO)
Nachweis	Vorfallprotokoll

Bewertung

LAGE	RISIKO FÜR DIE ZUGANGSDATEN
Gerät aus, BitLocker aktiv, keine Windows-Kopplung	gering – Datenbank verschlüsselt, Geheimnisse zusätzlich mit dem Master-Passwort geschützt
Gerät aus, BitLocker aktiv, Windows-Kopplung aktiv	mittel – wer das Windows-Passwort kennt oder errät, kann den Tresor öffnen
Gerät entsperrt oder im Standby mit angemeldetem Benutzer	hoch – Tresor möglicherweise offen
Ohne BitLocker	Projekt- und Hostnamen lesbar; Geheimnisse weiter durch das Master-Passwort geschützt, sofern keine Windows-Kopplung
Schadsoftware oder Master-Passwort bekannt	hoch – alle gespeicherten Zugangsdaten gelten als bekannt

Ablauf

1. Techniker meldet den Vorfall sofort an Leitung Technik und Informationssicherheit.
2. Windows-Konto des Technikers sperren bzw. Kennwort zurücksetzen (macht auch die Windows-Kopplung wertlos).
3. Falls möglich: Gerät per Geräteverwaltung sperren oder löschen.
4. Lizenz des Geräts in der Lizenzverwaltung freigeben lassen.
5. Aus der letzten Sicherung ermitteln, welche Zugangsdaten auf dem Gerät gespeichert waren.
6. Je nach Bewertung: Passwörter und Schlüssel der betroffenen Zielsysteme ändern (VF-08), beginnend bei den kritischsten (Domänen-Administratoren, Firewalls, Root-Zugänge). Öffentliche SSH-Schlüssel des Geräts auf den Servern entfernen.
7. Betroffene Kunden informieren, soweit vertraglich vereinbart.
8. Meldepflicht prüfen und Vorfall dokumentieren.

VF-06

Ausscheiden eines Technikers

Auslöser	Austritt, Wechsel in einen Bereich ohne Fernwartung
Verantwortlich	Leitung Technik, IT-Administration
Nachweis	Übergabeprotokoll (Anhang A), Liste der geänderten Zugangsdaten

1. Letzten Arbeitstag abstimmen. Bis dahin angelegte Verbindungen und Credentials per Sicherung übernehmen, falls sie im Referenzbestand fehlen.
2. Rechner zurücknehmen. Lizenz freigeben.
3. Hinterlegtes Master-Passwort vernichten (VF-02).
4. Daten löschen: `%APPDATA%\com.techtool.app`, Sicherungen des Technikers, Übertragungsdateien. Bei Weitergabe des Rechners: Datenträger vollständig löschen oder neu aufsetzen.
5. Windows- und Firmenkonten des Technikers sperren.
6. Gemeinsam genutzte Zugangsdaten, die der Techniker kannte oder im Tresor hatte, ändern (VF-08). Persönliche Konten auf den Zielsystemen deaktivieren, SSH-Schlüssel des Technikers entfernen.

VF-07

Geänderter Hostschlüssel

Auslöser	NexHand meldet „Hostschlüssel hat sich geändert!“
Verantwortlich	Techniker; bei unklarer Ursache Informationssicherheit
Nachweis	Ticket oder Notiz mit Ursache

1. Nicht verbinden. Dialog mit „Abbrechen“ schließen.
2. Ursache klären: Wurde der Server neu installiert, getauscht, die IP-Adresse neu vergeben? Nachfrage beim Kunden bzw. Serverbetreuer.
3. Ist die Ursache bekannt: Fingerabdruck auf dem Server selbst ermitteln (z. B. `ssh-keygen -lf /etc/ssh/ssh_host_ed25519_key.pub` über die Konsole) und mit der Anzeige vergleichen. Nur bei Übereinstimmung „Trotzdem vertrauen“.
4. Ist die Ursache unbekannt: Informationssicherheit informieren, weder verbinden noch Zugangsdaten eingeben. Ein untergeschobener Server könnte das Passwort mitlesen.

VF-08

Passwortwechsel auf Zielsystemen

Auslöser	regelmäßiger Wechsel nach Vorgabe, VF-05, VF-06, Kundenwunsch
Verantwortlich	Techniker des Projekts
Nachweis	Ticket mit Datum und betroffenen Systemen (ohne Passwörter)

1. Neues Passwort auf dem Zielsystem setzen.
2. In NexHand das zugehörige Credential öffnen und das neue Passwort eintragen. Durch die Vererbung gilt es sofort für alle Verbindungen, die dieses Credential nutzen.
3. Verbindung testen.
4. Andere Techniker mit demselben Credential informieren und den Referenzbestand aktualisieren. Neue Sicherung erstellen.

VF-09

Ende eines Kundenprojekts und Löschung

Auslöser	Vertragsende, Ende der Auftragsverarbeitung, Kundenwunsch
Verantwortlich	Leitung Technik; Ausführung durch IT-Administration und alle Techniker mit dem Projekt
Nachweis	Löschbestätigung je Rechner

1. Liste der Rechner erstellen, auf denen das Projekt vorhanden ist (Referenzbestand, Techniker).
2. Auf jedem Rechner das Projekt löschen (Rechtsklick → „Löschen“). Passwörter, Schlüssel und Passphrasen der Projekt-Credentials werden dabei sofort überschrieben; Namen und Hosts bleiben als gelöschte Datensätze in der Datenbank (NH-TOM-01, Abschnitt 7).
3. Globale Credentials prüfen, die nur für diesen Kunden genutzt wurden, und löschen.
4. Sicherungen, die das Projekt enthalten, laufen nach der Aufbewahrungsfrist aus (VF-03). Verlangt der Kunde eine sofortige Löschung, die Sicherungen löschen und neu erstellen.
5. Löschung bestätigen und dem Kunden auf Anfrage mitteilen.

VF-10

Versionswechsel

Auslöser	neue Programmversion des Herstellers
Verantwortlich	IT-Administration
Nachweis	Freigabevermerk mit Version und Datum

1. Versionshinweise und aktualisierte TOM des Herstellers lesen; Änderungen an Schutzmaßnahmen bewerten.
2. Herkunft und Prüfsumme des Pakets prüfen.
3. Test auf einem Referenzrechner mit Kopie eines echten Bestands (`TECHTOOL_DATA_DIR`).
4. Techniker erstellen eine Sicherung (VF-03).
5. Verteilung (NH-ADM-01, Abschnitt 8); eigene TOM-Dokumentation bei Bedarf aktualisieren.

ANHANG A

Vorlage Übergabeprotokoll

Anlass	☐ Einrichtung (VF-01) ☐ Ausscheiden (VF-06) ☐ Rechnertausch (VF-04)
Techniker	
Rechner / Rechnername	
BitLocker / Bildschirmsperre	☐ geprüft
Programmversion	
Freigegebene Projekte	
Lizenz	☐ aktiviert ☐ freigegeben ☐ Free-Version
Master-Passwort	☐ geändert und hinterlegt (VF-02) ☐ Hinterlegung vernichtet
Windows-Kopplung	☐ ein ☐ aus
Daten gelöscht	☐ Datenordner ☐ Sicherungen ☐ Übertragungsdateien
Zugangsdaten geändert	☐ nicht erforderlich ☐ erledigt, siehe Ticket
Einweisung erfolgt	☐ Benutzerhandbuch ☐ Hostschlüssel ☐ Vorfallmeldung

Techniker – Datum, Unterschrift

IT-Administration – Datum, Unterschrift