CHECKLISTE · STAND 07.11.2026

# Checkliste für Ihre IT

> Technische Angaben nach den Dokumentationen von Anthropic und Microsoft. Keine Rechtsberatung. Nicht anwaltlich geprüft.

**So nutzen Sie die Checkliste:** Für den Testtag braucht es nur die fünf Schritte und drei kurze Punkte aus Teil 1. Was erst vor dem Dauerbetrieb dazukommt, steht in Teil 3, was auf Wunsch möglich ist in Teil 4. Die Erläuterungen stehen auf der Seite Für Ihre IT. Technische Angaben nach den Dokumentationen von Anthropic und Microsoft, abgerufen am 01.11.2026; maßgeblich ist deren aktueller Stand.

**Das System:** Die KI-Mitarbeiterin ist Claude Code von Anthropic als Erweiterung für Visual Studio Code, mit dem Regelwerk von Illig Automatisierung. Sie läuft auf einem eigenen Rechner Ihrer Firma („KI-PC“) – empfohlen ein virtueller Rechner in Ihrem Microsoft-Azure-Konto, sonst ein PC im Büro – unter einem Windows-Standardkonto ohne Administratorrechte und braucht nur ausgehende HTTPS-Verbindungen.

## 1. Vor dem Testtag

| Schritt | Was zu tun ist | Wer | Erledigt |
|---|---|---|---|
| 1 · KI-PC | Rechner nur für die KI-Mitarbeiterin. Empfohlen: virtueller Rechner in Ihrem Microsoft-Azure-Konto – Ihre IT legt ein Azure-Abo an und lädt Illig als Gast mit der Rolle „Mitwirkender“ für eine eigene Ressourcengruppe ein; zwei Schritte, die diese Rolle nicht darf – Ressourcenanbieter registrieren und dem Startplan eine Rolle auf den Rechner geben –, erledigt Ihre IT im Termin mit Illig; Illig legt den Rechner dann aus der Ferne an (Windows 11 Enterprise, 4 Kerne, 16 GB, Rechenzentrum in der EU, für Firmen in der Schweiz auch in Zürich, eingehend gesperrt (Remotedesktop nur bei Bedarf für Illigs Adresse); eingeschaltet Mo–Fr 6:30–15:30 Uhr: bei Microsoft etwa 50 € netto im Monat, rund um die Uhr etwa 140 €, in Zürich rund 10 % mehr). Laufen Programme nur im Büronetz: VPN vom Azure-Rechner in Ihr Netz – Ihr vorhandenes VPN mit eigenem Zugang für die KI-Mitarbeiterin (verbindet ohne Bestätigung am Handy, nur zu den nötigen Servern) oder ein fester Tunnel von Azure zu Ihrem Router (bei Microsoft ab etwa 27 € netto im Monat). Ein PC im Büro nur, wenn ein Programm über VPN zu langsam ist (etwa Daten direkt auf einem Netzlaufwerk): Windows 11 (Windows 10 geht, bekommt aber nur noch über das kostenpflichtige ESU-Programm Sicherheitsupdates), 8 GB Arbeitsspeicher, besser 16 GB; am Stromnetz; Uhrzeit und Zeitzone richtig; feste Bildschirmauflösung, ohne Monitor mit HDMI-Dummy-Stecker; in einem Raum, den nur Befugte betreten (Pflicht laut Vereinbarung, weil der Bildschirm entsperrt bleibt). Eine VM auf Ihrem Server geht auch: über die Konsole im Basismodus, nicht in der erweiterten Sitzung. Kein normaler Cloud-PC: Windows 365 Business schließt Bots aus | Ihre IT (Azure-Rechner: Ihre IT und Illig) | ☐ |
| 2 · Zugänge | Windows-Konto als Standardbenutzer, in keiner Administratorgruppe; eigenes Konto für Mail und Teams mit „(KI)“ im Anzeigenamen, lizenziert mit „Microsoft 365 E3 – Unattended“ (Microsofts Lizenz für Software, die ohne Menschen Windows oder Office bedient; enthält Postfach und Office, Teams je nach Variante), berechtigt nur für das, was sie braucht. Den zweiten Faktor bestätigt Ihre IT bei der Anmeldung im Termin; eine generelle Ausnahme ist nicht nötig. Fragt Ihre Anmelderichtlinie am KI-PC regelmäßig neu nach, eine Regel nur für diesen Rechner abstimmen (z. B. bedingter Zugriff für ein vertrauenswürdiges Gerät oder einen Standort) | Ihre IT | ☐ |

| Schritt | Was zu tun ist | Wer | Erledigt |
|---|---|---|---|
| 3 · Bildschirm nicht sperren | Sperr-Richtlinien für ihr Konto aufheben (Sperre nach Inaktivität, erzwungener Bildschirmschoner mit Anmeldung). Energie und Bildschirmschoner stellt das Einrichtungsskript selbst ein und meldet, was noch sperrt. Nicht per Remotedesktop auf ihr Konto verbinden: Beim Trennen bleibt die Sitzung gesperrt, und sie steht (auf dem Azure-Rechner gibt eine Aufgabe die Sitzung binnen Sekunden an die Konsole zurück) | Ihre IT | ☐ |
| 4 · Netz | Ausgehend HTTPS, Port 443, zu den Zielen aus Teil 2; kein eingehender Port. Vorher nennen: Proxy (kein SOCKS), TLS-Prüfung, Virenschutz oder EDR, Anwendungssteuerung (AppLocker, WDAC), Ausführungsrichtlinie für PowerShell per Gruppenrichtlinie, ein Verbot geplanter Aufgaben für Standardbenutzer, gesperrten USB-Speicher | Ihre IT | ☐ |
| 5 · Einrichtung | Gemeinsamer Termin per Teams und Fernzugriff: Ihre IT meldet die Programme einmal unter ihrem Konto an. Installiert werden Python 3.12, VS Code mit der Erweiterung „Claude Code“ und, nur für das Browser-Werkzeug, Node.js und Chrome (oder das vorhandene Edge); verteilt Ihre IT Software selbst, bringt sie diese mit, sonst bestätigt sie die Installation, falls Windows nach Administratorrechten fragt. Illig überträgt das Regelwerk per Fernzugriff (auf Wunsch per USB-Stick) und richtet es unter `C:\KI-Mitarbeiter-Kit` ein (nicht in OneDrive, nicht auf einem Netzlaufwerk). Das Einrichtungsskript braucht keine Administratorrechte und legt die Windows-Aufgabe „KI-Mitarbeiter Aufpasser“ an (bei der Anmeldung und alle 5 Minuten, ohne erhöhte Rechte). Den Azure-Rechner setzt Illig als Administrator selbst auf (Software, automatische Anmeldung, Bildschirmsperre aus, Update-Neustarts außerhalb der Arbeitszeit, Rückgabe der Sitzung an die Konsole); ihr Windows-Konto bleibt Standardbenutzer. Zum Schluss den Not-Aus gemeinsam testen | Ihre IT und Illig | ☐ |
| Daten am Testtag | Auf Wunsch Kopien oder Exporte statt Direktzugang; eine aktuelle Datensicherung Ihrer Programme bestätigen | Ihre IT | ☐ |
| Claude-Konto am Testtag | Läuft über das Geschäftskonto von Illig bei Anthropic; Illig bedient die KI-Mitarbeiterin selbst (per Fernzugriff, auf Wunsch vor Ort) und meldet sie am Ende des Testtags ab | Illig | ☐ |
| Not-Aus | Verantwortliche Person und Vertretung für den Testtag benennen | Sie | ☐ |

## 2. Freigaben für die Firewall

Ausgehend, HTTPS, Port 443. Freigeben Sie am besten ganze Hostnamen, nicht einzelne Pfade. Stand 01.11.2026; maßgeblich ist die aktuelle Liste von Anthropic.

```

# Betrieb

api.anthropic.com platform.claude.com

# Anmeldung im Browser am KI-PC und beim Erneuern der Anmeldung

claude.ai claude.com

# nur bei Single Sign-on:

# sso.claude.com

# Einrichtung und kontrollierte Updates

marketplace.visualstudio.com *.gallery.vsassets.io* .gallerycdn.vsassets.io update.code.visualstudio.com vscode.download.prss.microsoft.com *.vscode-cdn.net pypi.org files.pythonhosted.org

# Browser-Werkzeug (Pakete für Node.js)

registry.npmjs.org

# Lebenszeichen im Betreuungsabo – erst nach Ihrer Genehmigung

hc-ping.com

# winget – nur, wenn Ihre IT die Programme nicht selbst verteilt

cdn.winget.microsoft.com www.python.org dl.google.com nodejs.org ```

Dazu Microsoft 365 und Teams wie bei jedem Arbeitsplatz, Ihre Fachprogramme und die Webseiten, die sie für ihre Aufgaben braucht. Nicht nötig und besser gesperrt lassen: Nutzungsstatistik und Fehlerberichte von Claude Code (`http-intake.logs.us5.datadoghq.com`, `browser-intake-us5-datadoghq.com`) und die Connectoren von claude.ai (`mcp-proxy.anthropic.com`) – beides ist in der KI-Mitarbeiterin abgeschaltet – sowie Plugin-Marktplätze (`github.com`), die sie nicht braucht. Für die API nennt Anthropic die festen IP-Bereiche `160.79.104.0/23` und `2607:6bc0::/48`.
```

## 3. Vor dem Dauerbetrieb

| Prüfpunkt | Was zu tun ist | Wer | Erledigt |
|---|---|---|---|
| Abo „Claude Team“ Ihrer Firma | Direkt bei Anthropic zu den gewerblichen Bedingungen (mit DPA): mindestens zwei Plätze (einer für die KI-Mitarbeiterin, einer für eine Person Ihrer Firma), Ausgabenlimit für die Organisation und für das Konto der KI-Mitarbeiterin (ohne gesetztes Limit gilt „Unlimited“); die KI-Mitarbeiterin meldet sich mit ihrem Konto der Team-Organisation an, ohne API-Schlüssel. Was das voraussichtlich kostet, sagt Illig vorher schriftlich | Sie, Illig hilft | ☐ |
| Schnittstellen zuerst | Bietet ein Programm eine Schnittstelle, etwa die REST-Schnittstelle des ERP, prüft Illig mit Ihnen, ob er die KI-Mitarbeiterin darüber anbindet – mit eigenem Zugang nur mit den Rechten, die der Ablauf braucht. Heute bedient sie Mail, Teams und Programme über die Oberfläche, mit ihrem eigenen Benutzer | Ihre IT (Zugang), Illig (Anbindung) | ☐ |
| Fachprogramme | Benutzer „KI“ mit knappen Rechten: lesen, vorbereiten, anlegen; keine Freigaben, keine Stammdaten, keine Zahlungen. Banking nur zum Betrachten von Kontoinformationen | Ihre IT mit Illig | ☐ |
| Neustart | Entscheidung über die automatische Anmeldung ihres Kontos nach einem Neustart (nur bei physisch geschütztem Rechner); ohne sie arbeitet sie erst wieder, wenn sich jemand anmeldet. Nutzungszeit für Windows-Updates auf die Arbeitszeit legen | Ihre IT | ☐ |
| Fernwartung | Nur auf dem KI-PC: beim Azure-Rechner Illigs Rolle in Ihrem Azure (jeder Zugriff über Azure als Vorgang im Aktivitätsprotokoll – was Illig dabei auf dem Rechner tut, steht in seinem Sitzungsprotokoll –, Entzug mit einem Klick), sonst ein Werkzeug, am liebsten das Ihrer IT, das die Konsole zeigt; Verbinden und Trennen einmal testen; kein Windows-Remotedesktop als Arbeitsweg | Ihre IT und Illig | ☐ |
| Updates und Sicherung | Wer Windows-Updates einspielt; wer `job.md` und den Ordner `arbeit\` sichert (Verläufe und Browserprofil besser nicht mitsichern) | gemeinsam | ☐ |

| Prüfpunkt | Was zu tun ist | Wer | Erledigt |
|---|---|---|---|
| Löschfristen | Fristen für Journal und Protokolle festlegen (Vorschlag: drei Monate). Nach der Frist löscht Illig sie von Hand, monatlich per Fernwartung oder vor Ort, mit Löschprotokoll; Ihre IT kann jederzeit selbst löschen. Von selbst löschen sich nur Bildschirmfotos (nach drei Tagen) und Verläufe, die 14 Tage nicht benutzt wurden | Sie (Frist), Illig (Löschung) | ☐ |
| Not-Aus und Störungen | Wer im Betrieb den Not-Aus auslöst und wo Beschäftigte eine Störung melden. Störungen zeigt der KI-PC vor Ort an (Datei `ALARM.txt`, Hinweisfenster). Im Betreuungsabo richtet Illig zusätzlich ein Lebenszeichen zu sich ein – erst nach Ihrer Genehmigung in Textform: Der KI-PC ruft regelmäßig eine feste Adresse beim Überwachungsdienst healthchecks.io auf, ohne Namen oder Inhalte; dafür `hc-ping.com` freigeben (Teil 2) | Sie, Ihre IT | ☐ |

## 4. Auf Wunsch

| Maßnahme | Was zu tun ist | Wer | Erledigt |
|---|---|---|---|
| Schreibschutz | Ordner des Regelwerks per NTFS schreibschützen (Rezept von Illig); nötig erst, wenn sie Mails nach festen Hausregeln selbst versenden soll | Ihre IT mit Illig | ☐ |
| Mails nach außen | Regel im Mailserver: Kopie jeder Mail ihres Kontos an Externe an ein Postfach Ihrer Firma – oder Senden nach außen für ihr Konto ganz sperren. Das ist die einzige harte Grenze, auch für Outlook im Web | Ihre IT | ☐ |
| Kamera, Mikrofon, Teams | Kamera und Mikrofon des KI-PCs abschalten; Aufzeichnung und Transkription in Teams für ihr Konto aus; wenn nicht gebraucht, auch den Austausch mit Teams-Nutzern außerhalb Ihrer Firma | Ihre IT | ☐ |
| Netzsegment | KI-PC in ein eigenes Netzsegment stellen und intern nur die Ziele freigeben, die sie braucht (z. B. Mail, Fachprogramm); am Testtag mit Kopien reicht meist der Internetzugang | Ihre IT | ☐ |
| Webzugriff | Freigabeliste in Firewall oder Proxy abstimmen – sie begrenzt auch PowerShell, eigene Skripte und den Browser | Ihre IT mit Illig | ☐ |

| Maßnahme | Was zu tun ist | Wer | Erledigt |
|---|---|---|---|
| Verschlüsselung | Festplattenverschlüsselung, etwa BitLocker – Verläufe und Protokolle liegen im Klartext | Ihre IT | ☐ |

## 5. Abnahme vor dem Dauerbetrieb (am Testtag nur Not-Aus und Freigabe-Tor)

| Prüfpunkt | Was zu tun ist | Wer | Erledigt |
|---|---|---|---|
| Prüfprogramm | `python kit\diagnose.py` im Ordner des Regelwerks unter ihrem Konto: keine Meldung „FEHLER“ | Illig, Ihre IT sieht zu | ☐ |
| Aufpasser | `python kit\aufpasser.py --nur-pruefen` zeigt, dass sie läuft | Illig | ☐ |
| Not-Aus | Datei `STOP` anlegen, eine Aktion wird verweigert; Datei löschen, sie arbeitet weiter | Not-Aus-Verantwortliche, Ihre IT | ☐ |
| Freigabe-Tor | Illig führt vor, dass „Senden“ in Outlook ohne Freischaltung nicht geht | Illig, Ihre IT sieht zu | ☐ |
| Wecken | Teams-Nachricht an ihr Konto; sie reagiert binnen weniger Minuten | Sie | ☐ |
| Neustart | Rechner neu starten und prüfen, was passiert – mit automatischer Anmeldung läuft sie wieder, ohne steht sie | Ihre IT | ☐ |

## 6. Abschalten und Abbau

| Prüfpunkt | Was zu tun ist | Wer | Erledigt |
|---|---|---|---|
| Sofort anhalten | Leere Datei `STOP` in `C:\KI-Mitarbeiter-Kit\` anlegen; weiter geht es erst, wenn ein Mensch sie löscht | Not-Aus-Verantwortliche, Ihre IT | ☐ |
| Abschalten ohne Datei | PC herunterfahren (Azure-Rechner: im Azure-Portal „Beenden“ – er startet am nächsten Arbeitstag nach Plan wieder; dauerhaft zusätzlich seinen Startplan abschalten), ihr Windows-Konto sperren und sie abmelden oder ihren Internetzugang sperren, ihr Konto aus Ihrer Claude-Organisation entfernen. Das Chatfenster oder VS Code zu schließen reicht nicht | Ihre IT | ☐ |

| Prüfpunkt | Was zu tun ist | Wer | Erledigt |
|---|---|---|---|
| Aufpasser aus | In einer PowerShell als Administrator: `Disable-ScheduledTask -TaskName "KI-Mitarbeiter Aufpasser"`, danach VS Code schließen; endgültig `Unregister-ScheduledTask -TaskName "KI-Mitarbeiter Aufpasser"` | Ihre IT | ☐ |
| Zugänge sperren | Ihr Konto aus der Claude-Organisation entfernen, in VS Code „Claude Code: Logout“; Konten sperren: Windows, Microsoft 365 und Teams, Fachprogramme, Fernwartung | Ihre IT, Illig | ☐ |
| Daten übergeben und löschen | Übergeben, was Sie behalten möchten; dann löschen: `.zustand\`, den Ordner `%USERPROFILE%\.claude` ihres Kontos (Verläufe, Vorher-Kopien, Eingabeverlauf, Einstellungen) und den Ordner des Regelwerks | Illig mit Ihrer IT | ☐ |
| Einstellungen zurück | VS-Code-Einstellungen aus der Sicherungskopie zurückholen; Energieeinstellungen nach Wunsch; einen NTFS-Schreibschutz, falls eingerichtet, vorher aufheben | Ihre IT, Illig | ☐ |
| Programme und Konto | Programme deinstallieren (Python, VS Code, ggf. Node.js und Chrome) und das Windows-Konto löschen – oder den Rechner neu aufsetzen | Ihre IT | ☐ |
| Bestätigung | Löschbestätigung in Textform – nach dem Testtag ohne Folgeauftrag binnen 5 Werktagen, nach Vertragsende binnen 10 Werktagen | Illig | ☐ |

## Ansprechpartner

| | Ihre Firma | Illig Automatisierung |
|---|---|---|
| Name | [Name] | Nick Illig |
| Rolle | [IT-Verantwortliche Person oder Systemhaus] | Einrichtung und Betreuung |
| E-Mail | [E-Mail] | nick@illig-automatisierung.com |
| Telefon | [Telefon] | +49 176 55734716 (auch WhatsApp) |
| Not-Aus-Verantwortliche | [Name, Vertretung] | – |