FÜR IHRE IT

Was Ihre IT für die KI-Mitarbeiterin vorbereitet – in fünf Schritten.

Kurz gesagt: Die KI-Mitarbeiterin ist Claude Code von Anthropic mit meinem Regelwerk. Sie braucht einen eigenen Rechner: am einfachsten einen virtuellen Rechner in Ihrem Microsoft-Azure-Konto, den ich als Gast mit einer Rolle für seine Ressourcengruppe aus der Ferne aufsetze (zwei Schritte mit mehr Rechten erledigt Ihre IT im Termin mit mir) – per VPN auch für Programme, die nur in Ihrem Büronetz laufen –, oder einen PC in Ihrem Büro mit einem Windows-Standardkonto für sie. Ihre IT stellt eigene Zugänge für Mail und Teams bereit, hebt für ihr Konto die Bildschirmsperre auf und erlaubt ausgehendes HTTPS. Den Rest richte ich per Fernzugriff in einem gemeinsamen Termin ein; am PC im Büro braucht mein Einrichtungsskript dafür keine Administratorrechte. Was sie liest und auf ihrem Bildschirm sieht, verarbeitet Claude bei Anthropic. Für den Testtag braucht Ihre Firma kein eigenes Claude-Konto; im Betrieb läuft sie über das Abo „Claude Team“ Ihrer Firma. Was sie erreichen kann, bestimmen die Rechte, die Ihre IT vergibt; anhalten kann Ihre IT sie jederzeit, ohne mich.

STAND	07.11.2026, Quellen mit Abrufdatum
FÜR	IT-Verantwortliche und Ihr Systemhaus
ANBIETER	Illig Automatisierung – Nick Illig, Einzelunternehmen, Müllheim (Baden)
SOFTWARE	Claude Code von Anthropic als Erweiterung für Visual Studio Code, mit meinem Regelwerk; unter Windows
KI-MODELL	Claude von Anthropic. Am Testtag über mein Geschäftskonto bei Anthropic, im Betrieb über das Abo „Claude Team“ Ihrer Firma; die KI-Mitarbeiterin meldet sich mit ihrem Konto in Ihrer Team-Organisation an, ohne API-Schlüssel.

WAS IHRE IT TUN MUSS

Fünf Schritte vor dem Testtag.

Mehr braucht es für den Testtag nicht. Was erst vor dem Dauerbetrieb dazukommt und was auf Wunsch möglich ist, steht darunter.

1

Ein Rechner nur für sie. Am einfachsten ein virtueller Rechner in Ihrem Microsoft-Azure-Konto: Windows 11 Enterprise, 4 Kerne, 16 GB (B4as_v2), Rechenzentrum in der EU, für Firmen in der Schweiz auch in Zürich, eingehend gesperrt (Remotedesktop nur bei Bedarf und nur für meine Adresse). Ihre IT legt ein Azure-Abo an und lädt mich 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 sie im Termin mit mir. Den Rechner richte ich dann aus der Ferne ein. Läuft er montags bis freitags von 6:30 bis 15:30 Uhr (er schaltet sich dafür selbst ein und aus), kostet er bei Microsoft etwa 50 € netto im Monat, rund um die Uhr etwa 140 € (in Zürich rund 10 % mehr). Jeder meiner Eingriffe über Azure – dass ich einen Befehl ausführe, neu starte oder den Remotedesktop öffne – steht in Ihrem Azure-Aktivitätsprotokoll; was ich dabei auf dem Rechner tue, steht in meinem Sitzungsprotokoll. Den entsperrten Bildschirm sehen nur Konten mit Rechten auf diesen Rechner, denn er hat keinen Monitor. In unserer Azure-Testumgebung arbeitet sie so seit dem 04.11.2026 – Neustarts, Netzausfall, Freigaben und Alarm geprüft –, bei einem Kunden noch nicht. Laufen Programme nur im Büronetz, verbinde ich den Azure-Rechner per VPN mit Ihrem Netz, wie den Laptop eines Mitarbeiters im Homeoffice: mit Ihrem vorhandenen VPN – ein eigener Zugang für sie, der ohne Bestätigung am Handy verbindet und nur die nötigen Server erreicht – oder mit einem festen VPN-Tunnel von Azure zu Ihrem Router (bei Microsoft ab etwa 27 € netto im Monat). Diesen Weg haben wir in der Testumgebung noch nicht geprüft; wir richten ihn mit Ihrer IT ein und prüfen ihn vor dem Testtag. Ein PC im Büro ist nur nötig, wenn ein Programm über VPN zu langsam arbeitet, etwa weil es seine Daten direkt auf einem Netzlaufwerk hält. Dann: Windows 11, 8 GB Arbeitsspeicher, besser 16 GB, am Stromnetz, mit richtiger Uhrzeit und fester Bildschirmauflösung – ohne Monitor mit einem HDMI-Dummy-Stecker. Weil ihr Bildschirm entsperrt bleibt, steht der PC in einem Raum, den nur Befugte betreten – so sieht es die Vereinbarung zur Auftragsverarbeitung vor. Eine VM auf Ihrem Server geht auch, dann über die Konsole im Basismodus, nicht in der erweiterten Sitzung. Sie bedient Maus und Tastatur wie ein Mensch; arbeitet gleichzeitig jemand am selben Bildschirm, kommen sich beide in die Quere. Nicht geeignet ist ein normaler Cloud-PC (Windows 365 Business): Microsoft schließt Bots dort aus. Windows 10 geht, bekommt aber nur noch über das kostenpflichtige ESU-Programm von Microsoft Sicherheitsupdates.

2 **Eigene Zugänge mit knappen Rechten.** Ein Windows-Konto als Standardbenutzer ohne Administratorrechte und ein eigenes Konto für Mail und Teams mit „(KI)“ im Anzeigenamen, lizenziert mit der Lizenz, die Microsoft für Software verlangt, die ohne Menschen Windows oder Office bedient („Microsoft 365 E3 – Unattended“, enthält Postfach und Office; Teams je nach Variante), berechtigt nur für das, was sie braucht. Persönliche Konten von Beschäftigten nutzt sie nicht. Den zweiten Faktor bestätigt Ihre IT bei der Anmeldung im Termin; eine generelle Ausnahme von der Mehrfaktor-Anmeldung brauchen wir nicht. Fragt Ihre Richtlinie am KI-PC regelmäßig neu nach, steht sie, bis ein Mensch bestätigt – dann stimmen wir eine Regel nur für diesen Rechner ab, etwa bedingten Zugriff für ein vertrauenswürdiges Gerät oder einen Standort.

3 **Bildschirm nicht sperren.** Bei gesperrtem Bildschirm sieht sie nur den Sperrbildschirm und steht. Heben Sie deshalb für ihr Konto die Sperr-Richtlinien auf, etwa die Sperre nach Inaktivität oder einen erzwungenen Bildschirmschoner. Energie und Bildschirmschoner stellt mein Einrichtungsskript selbst ein, und es meldet, was noch sperrt. Bitte nicht per Remotedesktop auf ihr Konto verbinden: Beim Trennen bleibt die Sitzung gesperrt, und sie steht. Für Fernwartung eignet sich ein Werkzeug, das die Konsole zeigt. Auf dem Azure-Rechner richte ich eine Aufgabe ein, die die Sitzung nach dem Trennen binnen Sekunden an die Konsole zurückgibt.

4 **Ausgehend HTTPS erlauben.** Port 443 zu Anthropic und zu den Installationsquellen; die Hostnamen stehen in der Checkliste. Einen eingehenden Port braucht sie nicht. Nutzen Sie einen Proxy (SOCKS unterstützt Claude Code nicht), TLS-Prüfung, Virenschutz oder EDR, Anwendungssteuerung wie AppLocker oder eine Ausführungsrichtlinie für PowerShell, oder dürfen Standardbenutzer keine geplanten Aufgaben anlegen, sagen Sie es mir bitte vorher.

5 **Ein gemeinsamer Termin, per Teams und Fernzugriff.** Ihre IT meldet die Programme einmal unter ihrem Konto an; sie selbst gibt keine Passwörter ein. 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. Mein Regelwerk übertrage ich per Fernzugriff, auf Wunsch per USB-Stick vor Ort. Mein Einrichtungsskript braucht keine Administratorrechte, ändert nichts an Firewall und Virenschutz und richtet keinen Dienst ein; es legt nur die Windows-Aufgabe „KI-Mitarbeiter Aufpasser“ an, die ohne erhöhte Rechte läuft. Den Azure-Rechner setze ich als Administrator selbst auf: Software, automatische Anmeldung ihres Kontos, Bildschirmsperre aus, Neustarts für Updates außerhalb der Arbeitszeit und die Aufgabe, die die Sitzung an die Konsole zurückgibt; ihr Windows-Konto bleibt ein Standardkonto. Zum Schluss testen wir gemeinsam den Not-Aus.

Am Testtag reichen Kopien oder Exporte statt Direktzugang zu Ihren Programmen. Vorher bestätigen Sie mir kurz eine aktuelle Datensicherung und wer den Not-Aus auslösen darf. Das Claude-Konto für den Testtag stelle ich, und ich bediene die KI-Mitarbeiterin selbst, per Fernzugriff oder auf Wunsch vor Ort.

Vor dem Dauerbetrieb – nach dem Testtag, gemeinsam

- **Abo „Claude Team“ Ihrer Firma:** Ihre Firma bucht es direkt bei Anthropic, mit mindestens zwei Plätzen (einer für die KI-Mitarbeiterin) und einem Ausgabenlimit für Organisation und Konto der KI-Mitarbeiterin. Was das voraussichtlich kostet, sage ich Ihnen vorher schriftlich.
- **Schnittstellen zuerst:** Bietet ein Programm eine Schnittstelle, etwa die REST-Schnittstelle Ihres ERP, prüfe ich mit Ihnen, ob ich die KI-Mitarbeiterin darüber anbinde – mit einem eigenen Zugang nur mit den Rechten, die der Ablauf braucht. Heute bedient sie Mail, Teams und Programme über die Oberfläche, mit ihrem eigenen Benutzer.
- **Fachprogramme:** ein eigener Benutzer „KI“ mit knappen Rechten, im Banking nur zum Ansehen – ohne Zahlungs- und Unterschriftsrechte.
- **Neustart:** ob sich ihr Konto nach einem Neustart automatisch anmeldet. Ohne automatische Anmeldung arbeitet sie erst wieder, wenn sich jemand anmeldet. Auf dem Azure-Rechner richte ich sie ein; an seinen Bildschirm kommt nur, wer in Azure Rechte auf diesen Rechner hat.
- **Betrieb:** der Weg für die Fernwartung (nur auf den KI-PC – beim Azure-Rechner über meine Rolle in Ihrem Azure, sonst am liebsten mit Ihrem Werkzeug, kein

Auf Wunsch

- Schreibschutz für den Ordner meines Regelwerks per NTFS – nötig erst, wenn sie Mails nach festen Hausregeln selbst versenden soll.
- Eine Regel im Mailserver: Kopie jeder Mail nach außen an ein Postfach Ihrer Firma, oder Senden nach außen für ihr Konto ganz sperren. Das ist die einzige harte Grenze für Mails, auch für Outlook im Web.
- Kamera und Mikrofon des KI-PCs abschalten; in Teams für ihr Konto Aufzeichnung und Transkription aus, und wenn sie es nicht braucht, auch den Austausch mit Teams-Nutzern außerhalb Ihrer Firma.
- Den KI-PC in ein eigenes Netzsegment stellen und intern nur die Ziele freigeben, die sie braucht, etwa Mail und Ihr Fachprogramm. Am Testtag mit Kopien reicht meist der Internetzugang.
- Den Webzugriff in Firewall oder Proxy auf eine abgestimmte Liste begrenzen.
- Festplattenverschlüsselung, etwa BitLocker – empfehle ich, weil Verläufe und Protokolle im Klartext liegen.

Remotedesktop), wer im Betrieb den Not-Aus auslöst, Windows-Updates, Datensicherung, Löschfristen (nach der Frist lösche ich Journal und Protokolle monatlich von Hand).

- ✓ **Störungen** zeigt der KI-PC vor Ort an, in der Datei `ALARM.txt` und mit einem Hinweisfenster. Im Betreuungsabo richte ich zusätzlich ein Lebenszeichen zu mir ein – erst nach Ihrer Genehmigung in Textform: Der KI-PC ruft regelmäßig eine feste Adresse beim Überwachungsdienst healthchecks.io auf; bleibt das aus oder meldet er eine Störung, bekomme ich eine E-Mail. Übertragen wird nur dieses Signal, ohne Namen oder Inhalte. Dafür braucht der KI-PC ausgehend `hc-ping.com`.

Quellen: Microsoft, „Extended Security Updates (ESU) program for Windows 10“ (learn.microsoft.com) · Anthropic, „Enterprise network configuration“ (code.claude.com) – abgerufen 01.11.2026 · Microsoft, „Microsoft 365 Unattended License“ (microsoft.com) – abgerufen 04.11.2026 · Microsoft, „Windows 365 Service Description“ (learn.microsoft.com) · Microsoft, Azure-Preise (azure.microsoft.com): B4as_v2 in Germany West Central 0,155 € je Stunde, Standard-SSD 128 GB 8,62 € und öffentliche IP-Adresse 3,29 € im Monat, netto; Bürozeiten mit rund 200 Stunden im Monat und Speicherzugriffen gerechnet – abgerufen 05.11.2026; B4as_v2 in Switzerland North (Zürich) 0,171 € je Stunde – abgerufen 06.11.2026. Angaben zum Regelwerk aus meiner Einrichtungsanleitung.

SCHUTZ UND EHRLICHE GRENZEN

Was technisch gesperrt ist – und was nicht.

Ein Schutz-Hook meines Regelwerks prüft jeden Werkzeugaufruf, bevor Claude Code ihn ausführt. Die harte Grenze bleiben die Rechte, die Ihre IT vergibt.

Technisch gesperrt

- **Mails:** Versand per SMTP, Outlook-Automatisierung oder Send-MailMessage sperrt mein Regelwerk. „Senden“ in Outlook geht über ihre Bildschirm-Werkzeuge nur mit einem Einmal-Schlüssel für einen Klick, der 10 Minuten gilt. Für Empfänger außerhalb Ihrer Firma gibt es ihn nur zu einer Freigabe, die sie mit Name und Wortlaut der eingetragenen Person einträgt – nachvollziehbar, aber nicht fälschungssicher. Für interne Empfänger stellt sie ihn selbst aus, und an wen die Mail im Fenster geht, prüft das Werkzeug beim Klick nicht. Mails nach festen Hausregeln selbst zu versenden, ist ab Werk aus.
- **System:** Eingriffe in System, Netz, Konten, Virenschutz, Dienste, Autostart und geplante Aufgaben; in der Standardeinstellung auch Installationen; Zugriffe auf gespeicherte Passwörter und Browser-Anmeldungen auf den üblichen Wegen; das Löschen ganzer Laufwerke, System- und Benutzerordner. An ihren eigenen Regeln kann sie nichts ändern. Fällt die Prüfung aus, wird gesperrt statt durchgelassen.
- **Sensible Fenster:** kein Bildschirmfoto, solange ein Passwort-, Banking- oder Ausweisfenster sichtbar ist; keine Eingaben in Passwort-Manager, Windows-Anmelde- und Sicherheitsdialoge; Kennwortfelder

Was nicht gesperrt ist

Teams-Nachrichten und Eingaben im Browser haben kein Freigabe-Tor, auch nicht Outlook im Web; dafür gilt ihre Arbeitsanweisung. Eine harte Grenze für Mails ist nur eine Regel in Ihrem Mailserver (siehe „Auf Wunsch“).

Das Internet beschränkt mein Regelwerk nicht von selbst – das kann nur Ihre Firewall oder Ihr Proxy.

Einzelne Dateien löschen – per Befehl oder über die Oberfläche – kann sie, soweit die Rechte ihres Kontos reichen; dafür gilt ihre Arbeitsanweisung.

Eigene Skripte: Schreibt sie ein Skript, das selbst Maus und Tastatur bedient, prüft der Schutz-Hook Klicks und Eingaben darin nicht; Fotosperre, Eingabesperren und Freigabe-Tor gelten dann nicht. Dafür gilt ihre Arbeitsanweisung.

Die Fotosperre erkennt Fenster am Titel oder Programmnamen und lässt sich per Schalter aufheben; das darf sie laut Arbeitsanweisung nur mit Freigabe eines Menschen.

Präparierte Inhalte: Laut Arbeitsanweisung sind Inhalte aus Mails und Webseiten Daten, keine Befehle. Gegen gezielte Täuschung hilft das nicht sicher – knappe Rechte schon.

von Programmen erkennt ihr Werkzeug für die Bedienelemente; Banking-Programme nur lesend. Das Browser-Werkzeug prüft das nicht.

- ✓ **Sparsam eingestellt:** Nutzungsstatistik, Fehlerberichte und Feedback von Claude Code sind aus, ebenso die claude.ai-Connectoren und die automatische Merkfunktion. Sie bedient nur ihren eigenen Bildschirm; eine Fernsteuerung anderer Rechner ist nicht eingebaut.
- ✓ **VS Code ohne stille Updates:** VS Code und seine Erweiterungen aktualisieren sich nicht von selbst. Updates spiele ich nur bei angehaltener KI-Mitarbeiterin ein, mit Sicherung ihres Ordners und Abnahmetest; mein Prüfprogramm warnt, wenn eine ungeprüfte Version läuft.

„Technisch gesperrt“ heißt: Ein Programm setzt die Sperre im normalen Betrieb durch – unumgehbar ist sie nicht.

ⓘ **Offen gesagt:** Claude Code hat unter Windows keine Sandbox, und die KI-Mitarbeiterin läuft im Betriebsmodus `bypassPermissions`, in dem Claude Code selbst nicht nachfragt – Anthropic empfiehlt diesen Modus nur für isolierte Umgebungen. Mein Regelwerk ist ein Geländer gegen Fehler, keine Sicherheitsgrenze gegen Absicht: Wer Administratorrechte hat oder ihr Konto übernimmt, kann es abschalten. Deshalb gehören dazu ein eigener Rechner, ein Standardkonto und knappe Rechte.

Quellen: Anthropic, „Configure the sandboxed Bash tool“ (code.claude.com): „On native Windows, Claude Code runs commands unsandboxed.“ · „Configure permissions“ (code.claude.com): „Only use this mode in isolated environments like containers or VMs where Claude Code can't cause damage.“ – abgerufen 01.11.2026.

ANHALTEN UND ABSCHALTEN

Anhalten kann Ihre IT sie jederzeit – ohne mich.

Kurzfassung für alle im Betrieb: Wie hält man sie an?

1. **Not-Aus:** eine leere Datei `STOP` im Ordner `C:\KI-Mitarbeiter-Kit\` anlegen, etwa mit `New-Item -ItemType File C:\KI-Mitarbeiter-Kit\STOP`. Dann hält sie vor ihrem nächsten Schritt an: Lesen bleibt erlaubt, handeln nicht; ein Befehl, der gerade läuft, läuft zu Ende. Weiter geht es erst, wenn ein Mensch die Datei löscht. Sie selbst kann STOP weder anlegen noch löschen, und der Aufpasser startet sie so lange nicht.

2. **Abschalten ohne Datei:** den PC herunterfahren (den 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; im Betrieb ihr Konto aus Ihrer Claude-Organisation entfernen – laut Anthropic verliert sie damit sofort den Zugang. Am Testtag melde ich sie am Ende selbst ab.

3. **Was nicht reicht:** die Stopp-Taste im Chatfenster oder VS Code zu schließen – der Aufpasser macht nach etwa 5 Minuten weiter. Ganz aus ist sie, wenn Ihre IT den Aufpasser in einer PowerShell als Administrator mit `Disable-ScheduledTask -TaskName "KI-Mitarbeiter Aufpasser"` ausschaltet und danach VS Code schließt.

Abbau

- ✓ **Fristen:** Nach dem Testtag ohne Folgeauftrag baue ich sie binnen 5 Werktagen ab, nach Vertragsende binnen 10 Werktagen – jeweils mit Bestätigung der Löschung in Textform.
- ✓ **Bei mir** gibt es keine Kopie Ihrer Daten. Ihre Daten bleiben in Ihren Programmen; Ihr Team arbeitet dort von Hand weiter.
- ✓ **Die einzelnen Schritte** zum Deinstallieren stehen in der Checkliste.

Quelle: Anthropic, „Manage members on Team and Enterprise plans“ (support.claude.com): „They lose access to the organization immediately.“ – abgerufen 01.11.2026.

PROTOKOLLE

Was sie auf dem KI-PC festhält.

Alles liegt auf dem KI-PC, unverschlüsselt und geschützt durch die Dateirechte; öffnen können es ihr Windows-Konto und Ihre Administratoren. Festgehalten werden die Klicks und Tasten ihres Maus- und Tastaturwerkzeugs (Getipptes nur als Zeichenzahl), Freigaben mit Name, Kanal und Wortlaut, freigeschaltete Mails mit Empfänger und Fenstertitel, Eingaben in ihr Chatfenster mit den ersten 80 Zeichen, Sperren mit bis zu 300 Zeichen des Befehls und ihr Gesprächsverlauf mit Claude.

Speicherorte: im Ordner `C:\KI-Mitarbeiter-Kit\` die Protokolle in `.zustand\log`, die Freigabe-Protokolle in `.zustand\freigaben`, die Bildschirmfotos in `.zustand\shots`, das Journal in `arbeit\journal` und die Hinweise in `ALARM.txt`; die Verläufe im Profil ihres Kontos unter `%USERPROFILE%\.claude`.

Löschung: Bildschirmfoto-Dateien löscht ihr Foto-Werkzeug nach drei Tagen, jeweils beim nächsten Foto. Verläufe, die 14 Tage nicht benutzt wurden, löscht Claude Code; den laufenden Verlauf löschen wir nach Absprache, spätestens beim Abbau. Journal und Protokolle bleiben, bis sie nach der vereinbarten Frist gelöscht werden – heute von Hand: Ich lösche sie monatlich per Fernwartung oder vor Ort und vermerke das im Löschprotokoll; Ihre IT kann jederzeit selbst löschen.

Jede Aufzeichnung mit Inhalt, Frist und Leserkreis steht auf der Seite Für Ihren Betriebsrat, die Fristen aus Sicht des Datenschutzes unter Datenschutz & Sicherheit.

Quelle: Anthropic, „Explore the .claude directory“ (code.claude.com): „Transcripts and history are not encrypted at rest. OS file permissions are the only protection.“ – abgerufen 01.11.2026.

TECHNISCHE DETAILS

Auf Anfrage – für Ihr Systemhaus.

Für den Testtag brauchen Sie das nicht. Fragt Ihre IT nach, schicke ich die Angaben mit Herstellerquelle, oder wir besprechen sie in 15 Minuten per Teams.

- **Netz:** alle Hostnamen und IP-Bereiche von Anthropic, VS Code und den Installationsquellen; Proxy mit Anmeldung, TLS-Prüfung mit eigenem Zertifikat
- **Zentrale Vorgaben:** verwaltete Einstellungen für Claude Code per Datei, Registry oder claude.ai – welche sich mit meinem Regelwerk vertragen und welche es lahmlegen
- **Software:** was genau installiert und eingestellt wird, Virenschutz und Anwendungssteuerung, der Ablauf eines Updates

- **Prüfbefehle:** Befehle, die nur lesen, etwa für Anmeldung, Aufpasser und Einstellungen
- **Fernwartung:** Werkzeug, Ablauf einer Sitzung, Protokoll und Entzug; die vertraglichen Regeln stehen unter Datenschutz & Sicherheit, Abschnitt 5
- **Azure-Rechner:** Aufbau, Rollen, An- und Abschaltzeiten, Kosten und Fernwartung im Einzelnen – erprobt in unserer Testumgebung, noch bei keinem Kunden
- **Datenverkehr zum Hersteller:** was Claude Code an Anthropic schickt und was davon abgeschaltet ist

UNTERLAGEN

Die Checkliste für Ihre IT.

Die fünf Schritte zum Abhaken, die Hostnamen für Ihre Firewall und die Schritte zum Abbau – im Browser lesbar und als PDF.

CHECKLISTE · 8 SEITEN

Checkliste für Ihre IT

Was Ihre IT vor dem Testtag vorbereitet, was vor dem Dauerbetrieb dazukommt, welche Ziele die Firewall freigibt und wie Sie die KI-Mitarbeiterin abbauen.

Im Browser lesen **PDF, 123 KB**

Diese Seite als PDF: herunterladen. Die Vereinbarung zur Auftragsverarbeitung, die technischen und organisatorischen Maßnahmen und alle Unterlagen für Ihren Datenschutzbeauftragten stehen auf der Seite Datenschutz & Sicherheit.

KONTAKT

Fragen Ihrer IT? Schreiben Sie mir.

Gern spreche ich direkt mit Ihrer IT oder Ihrem Systemhaus, per Teams oder am Telefon – 15 Minuten reichen meist. Schreiben Sie mir kurz, wann es passt.

Nick Illig
Prozessautomatisierung (Einzelunternehmen)
Unterm Grasweg 57
79379 Müllheim, Deutschland

E-Mail: nick@illig-automatisierung.com
WhatsApp: +49 176 55734716

Stand dieser Seite: 07.11.2026. Die Webquellen habe ich zwischen dem 01. und 06.11.2026 abgerufen; maßgeblich ist jeweils der aktuelle Stand der Dokumentation von Anthropic und Microsoft.

Verträge, Datenfluss und Löschfristen erklärt die Seite für Ihren Datenschutzbeauftragten, was aufgezeichnet wird die Seite für Ihren Betriebsrat, Fragen zu Haftung, Kosten und Ausfall die Startseite: Datenschutz & Sicherheit · Für Ihren Betriebsrat · Impressum · häufige Fragen

Alle Quellen dieser Seite

1. Extended Security Updates (ESU) program for Windows 10 – Sicherheitsupdates für Windows 10 nur noch kostenpflichtig
2. Microsoft 365 Unattended License (Licensing Guidance) – Lizenz für Software, die ohne Menschen Windows oder Office bedient
3. Windows 365 Service Description – „Robotic Process Automation/bots“: Business nein, Enterprise ja
4. Azure-Preisrechner – Preise für virtuelle Rechner, Festplatten, IP-Adressen und VPN-Gateways (Frankfurt, abgerufen am 05.11.2026; Zürich, abgerufen am 06.11.2026)
5. Claude Code: Enterprise network configuration – Ziele für Proxy und Firewall, Proxy-Variablen, kein SOCKS
6. Claude Code: Configure the sandboxed Bash tool – keine Sandbox unter nativem Windows
7. Claude Code: Configure permissions – Empfehlung, bypassPermissions nur in isolierten Umgebungen zu nutzen
8. Manage members on Team and Enterprise plans (Support) – Konto aus der Claude-Organisation entfernen, „They lose access to the organization immediately.“
9. Claude Code: Explore the .claude directory – Verläufe und Eingabeverlauf; keine Verschlüsselung, nur Dateirechte

Abgerufen zwischen dem 01. und 06.11.2026; maßgeblich ist jeweils der aktuelle Wortlaut der Quelle.

© 2026 Nick Illig · Prozessautomatisierung · Unterm Grasweg 57 · 79379 Müllheim

Diese Website setzt selbst keine Cookies, nutzt kein Tracking und lädt nichts von Drittanbietern.

Mein Angebot richtet sich ausschließlich an Unternehmen. Claude, Anthropic, Amazon Bedrock, Google Cloud, Microsoft Teams und die übrigen genannten Produktnamen sind Marken ihrer jeweiligen Inhaber. Eine Partnerschaft mit diesen Herstellern besteht nicht.