

VERPFLICHTUNGSERKLÄRUNG

für den Zugang zu IT-Diensten der
NETWAYS GmbH und ihren verbundenen Unternehmen

zwischen

NETWAYS GmbH und ihren verbundenen Unternehmen
Deutschherrnstr. 15-19
90429 Nürnberg

– nachfolgend „NETWAYS“ –

und

Kunde (Organisation)

Firma/Behörde: _____

Straße: _____

Postleitzahl / Ort: _____

Land: _____

sowie der unterzeichnenden natürlichen Person:

Vorname, Nachname: _____

E-Mail-Adresse: _____

Rolle/Funktion beim Kunden: _____

Projekt/Vertragsnummer (falls zutreffend): _____

– nachfolgend „Nutzer“ –

1. PRÄAMBEL

Diese Verpflichtungserklärung regelt die Pflichten des Nutzers im Zusammenhang mit dem Zugang zu und der Nutzung von IT-Diensten der NETWAYS.

Sie gilt für die unterzeichnende natürliche Person, die im Auftrag des Kunden auf IT-Dienste der NETWAYS zugreift.

Der Nutzer verpflichtet sich, die nachfolgenden Sicherheits-, Datenschutz- und Vertraulichkeitsvorgaben während des Zugriffs auf IT-Dienste der NETWAYS einzuhalten.

2. GELTUNGSBEREICH UND ZWECK DER NUTZUNG

(1) Die Verpflichtung gilt für alle IT-Dienste, die NETWAYS dem Kunden zur Verfügung stellt und zu denen der Nutzer einen personenbezogenen oder technischen Zugang erhält. Hierzu zählen insbesondere:

☐ Request-Tracker (rt.netways.de)

☐ GitLab (gitlab.netways.de)

☐ Sonstige IT-Dienste: _____

(2) Die Nutzung der IT-Dienste erfolgt ausschließlich zur Erfüllung der zwischen NETWAYS und dem Kunden vereinbarten Leistungen und nur im hierfür erforderlichen Umfang.

(3) Eine private Nutzung der IT-Dienste sowie jede Nutzung zu anderen als den vereinbarten geschäftlichen Zwecken ist untersagt.

3. PASSWÖRTER UND AUTHENTIFIZIERUNG

- (1) Passwörter müssen mindestens 14 Zeichen lang sein.
- (2) Passwörter sind mindestens einmal jährlich sowie nach der ersten Verwendung zu ändern.
- (3) Die letzten fünf Passwörter dürfen nicht erneut verwendet werden.
- (4) Passwörter müssen aus einer Kombination von Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen bestehen.
- (5) Standardpasswörter dürfen nicht verwendet werden.
- (6) Sofern für einen IT-Dienst eine Mehr-Faktor-Authentifizierung vorgesehen ist, wird der Nutzer diese verwenden und die hierfür erforderlichen Faktoren ebenso vertraulich behandeln wie Passwörter.
- (7) Die dem Nutzer zugeordneten Benutzerkennungen sind personalisiert und nicht übertragbar; eine gemeinsame Nutzung von Accounts ist untersagt.

4. WEITERE SICHERHEITSVERPFLICHTUNGEN

- (1) Anmeldeinformationen (z.B. Benutzername, Passwort, Token, Recovery Codes) sind sicher aufzubewahren und nicht an Dritte weiterzugeben.
- (2) Der Nutzer trifft geeignete Vorkehrungen, um unbefugten Zugriff auf die IT-Dienste zu verhindern (z.B. Sperren des Arbeitsplatzes bei Abwesenheit, aktueller Virenschutz, sichere Systemkonfiguration).
- (3) Es ist untersagt, Sicherheitsmechanismen (z.B. Passwort-Richtlinien, Session-Timeouts, Zugriffsbeschränkungen) zu umgehen oder zu manipulieren.
- (4) Bei einem Sicherheitsvorfall oder dem Verdacht auf eine Kompromittierung der Zugangsdaten ist NETWAYS unverzüglich zu informieren.
Meldeweg:
E-Mail: info@netways.de
Telefon/Hotline: +49 911 928850
- (5) Wenn der Zugriff des Nutzers nicht länger benötigt wird, teilt der Nutzer dies sofort dem Kunden bzw. den zuständigen Stellen mit, damit der Zugriff beendet werden kann.
- (6) Beim Ausscheiden des Nutzers aus der Organisation des Kunden bzw. unmittelbar nach Beendigung seiner Tätigkeit ist der Zugriff zu melden und zu beenden.

5. UMGANG MIT INFORMATIONEN, VERTRAULICHKEIT UND DATENSCHUTZ

- (1) Der Nutzer verpflichtet sich zum vertraulichen und sachgemäßen Umgang mit allen Informationen, zu denen er Zugriff erhält.
- (2) Personenbezogene Daten werden gemäß der Datenschutz-Grundverordnung (DSGVO) und den einschlägigen Datenschutzgesetzen vertraulich behandelt und geschützt.
- (3) Der Nutzer behandelt alle ihm im Rahmen des Zugriffs bekannt werdenden Geschäfts- und Betriebsgeheimnisse von NETWAYS und deren Kunden vertraulich und verwendet sie ausschließlich zu dem vorgesehenen Zweck.
- (4) Lokale Kopien von Informationen (z.B. Exporte, Screenshots, Backups) werden nur erstellt, wenn dies zur Aufgabenerfüllung erforderlich ist und unterliegen denselben Vertraulichkeits-, Schutz- und Löschpflichten wie die Originaldaten.
- (5) Zugangsdaten und sonstige vertrauliche Informationen sind nach Entzug der Berechtigung sicher und vollständig zu löschen, soweit keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

6. PROTOKOLLIERUNG UND KONTROLLE

- (1) Dem Nutzer ist bekannt, dass NETWAYS Zugriffe auf IT-Dienste (z.B. Anmeldevorgänge, Konfigurationsänderungen, Datenexporte) zu Sicherheits-, Betriebs- und Nachweiszwecken protokolliert und ausgewertet.
- (2) Die Protokollierung erfolgt unter Beachtung der geltenden datenschutzrechtlichen Bestimmungen.

7. TECHNISCHE BZW. SYSTEMGEBUNDENE ZUGÄNGE

- (1) Für technische oder systemgebundene Zugänge (z.B. Funktions- oder Service-Accounts), die im Verantwortungsbereich des Kunden genutzt werden, gelten die oben genannten Regeln sinngemäß.
- (2) Für jeden solchen Zugang wird eine verantwortliche natürliche Person benannt. Diese Person stellt sicher, dass:
 - nur berechtigte Personen den Account nutzen,
 - Zugriffe nachvollziehbar dokumentiert und zugeordnet werden können und
 - bei Personalwechsel oder Aufgabenänderung die Berechtigungen unverzüglich überprüft, angepasst oder entzogen werden.

8. DAUER DER VERPFLICHTUNG UND FOLGEN VON VERSTÖßEN

- (1) Diese Verpflichtung gilt ab Unterzeichnung und für die Dauer des Zugriffs des Nutzers auf IT-Dienste der NETWAYS.
- (2) Dem Nutzer ist bewusst, dass Verstöße gegen diese Verpflichtungserklärung zivilrechtliche, arbeitsrechtliche und ggf. strafrechtliche Konsequenzen haben können.
- (3) Unberührt bleiben weitergehende vertragliche Regelungen zwischen NETWAYS und dem Kunden.

9. SCHLUSSBESTIMMUNGEN

- (1) Diese Verpflichtungserklärung ergänzt bestehende Verträge und Vereinbarungen zwischen NETWAYS und dem Kunden, ohne diese zu ersetzen.
- (2) Sollten einzelne Bestimmungen dieser Verpflichtungserklärung unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

Ort, Datum

Ort: _____

Datum: _____

Unterschrift Nutzer

(Unterschrift Nutzer)

Name in Druckbuchstaben: _____

Rolle/Funktion: _____