

SICHERHEITSBESTIMMUNGEN FÜR EXTERNE ANWENDER VON INFORMATIONSSYSTEMEN

23.04.2026 / Version 1.0

INHALT

1.0	PRÄAMBEL	3
2.0	GELTUNGSBEREICH	3
3.0	SICHERHEITSBESTIMMUNGEN	3
3.1	Zulässige Nutzung von Informationssystemen	3
3.2	Schutz vor unbefugtem Zugriff	3
3.3	Kommunikations- & Anwendungssicherheit	4
3.4	Umgang mit IT-Sicherheitsvorfällen & Schwachstellen	4
3.5	Überwachung der Einhaltung & Folgen bei Missachtung	4

1.0 PRÄAMBEL

Als Betreiber kritischer Infrastruktur (KRITIS) trägt TransnetBW eine besondere Verantwortung für den Schutz von Informationen und Daten. Die Aufrechterhaltung eines angemessenen Informationssicherheitsniveaus ist daher fest in den Unternehmenszielen von TransnetBW verankert.

Externe Anwender, die auf TransnetBW-Informationssysteme zugreifen, tragen in besonderem Maße zur Sicherheit der Systeme bei. Die Einhaltung der in diesem Dokument beschriebenen Regelungen stellt daher eine Voraussetzung für die sichere Nutzung dieser Systeme dar.

2.0 GELTUNGSBEREICH

Die folgenden Regelungen richten sich an alle externen Anwender (nachfolgend „Anwender“) der TransnetBW GmbH (nachfolgend „TransnetBW“), die mit TransnetBW-Informationssystemen umgehen, insbesondere das Personal von Auftragnehmern.

Der Begriff „Informationssystem“ schließt im Folgenden jede Art von Software oder Hardware ein, die dem externen Anwender zu einem vereinbarten Nutzungszweck bereitgestellt wird.

3.0 SICHERHEITSBESTIMMUNGEN

3.1 ZULÄSSIGE NUTZUNG VON INFORMATIONSSYSTEMEN

- a. Die Nutzung von TransnetBW-Informationssystemen ist ausschließlich zu den vereinbarten Zwecken (z. B. Erbringung einer vertraglich geschuldeten Leistung) gestattet.
- b. Soweit möglich sind ausschließlich die von TransnetBW zur Verfügung gestellten Informationssysteme zu nutzen, um den vereinbarten Nutzungszweck zu erfüllen.
- c. Die Privatsnutzung von TransnetBW-Informationssystemen ist für externe Anwender grundsätzlich untersagt.
- d. Der Anwender hat seinen Ansprechpartner bei TransnetBW unverzüglich darüber zu informieren, wenn die Nutzung von TransnetBW-Informationssystemen durch ihn nicht mehr erforderlich ist.
- e. Der Anwender hat Lizenzbedingungen für Software einzuhalten und im Umgang mit fremderstelltem Material geistige Eigentumsrechte zu wahren.
- f. Dem Anwender ist es im Umgang mit TransnetBW-Informationssystemen untersagt, strafbare Inhalte einzubringen, Sicherheitsmaßnahmen zu manipulieren, Schwachstellen auszunutzen, Informationssysteme zu penetrieren oder sie auf andere Weise missbräuchlich zu verwenden.

3.2 SCHUTZ VOR UNBEFUGTEM ZUGRIFF

- a. Persönliche Zugangsdaten (z. B. Passwörter, PINs, Tokens) sind durch den Anwender geheim zu halten und vor unbefugtem Zugriff zu schützen.

- b. Der Anwender muss sicherstellen, dass die Eingabe von Zugangsdaten und die allgemeine Nutzung von TransnetBW-Informationssystemen unbeobachtet erfolgt (z. B. mithilfe einer Blickschutzfolie am Bildschirm).
- c. Personalisierte Benutzerkonten dürfen ausschließlich durch den jeweiligen Anwender verwendet werden. Die Nutzung nicht-personalisierter Benutzerkonten bedarf einer Ausnahmegenehmigung durch TransnetBW.
- d. Für den Zugriff auf TransnetBW-Informationssysteme sind sichere Passwörter zu wählen, die einzigartig, angemessen lang und komplex sind.
- e. Anwender müssen sich von TransnetBW-Informationssystemen abmelden oder die Bildschirmsperre aktivieren, bevor sie sich von dem Endgerät entfernen.

3.3 KOMMUNIKATIONS- & ANWENDUNGSSICHERHEIT

- a. Die eigenständige Installation von Software durch den Anwender ist untersagt.
- b. Externe Informationssysteme dürfen nur über die von TransnetBW bereitgestellten Schnittstellen (z. B. Gäste-WLAN, Remote-Desktop-Lösungen) mit dem TransnetBW-Netzwerk verbunden werden.
- c. Die automatisierte Weiterleitung der Kommunikation von TransnetBW-Kommunikationseinrichtungen an externe Empfängerstellen (z. B. E-Mails, Chat-Nachrichten, Anrufe) ist nicht zulässig.
- d. Externe Anwender müssen sich bei der Kommunikation mittels TransnetBW-Kommunikationseinrichtungen als solche zu erkennen geben (z. B. durch einen deutlichen Hinweis in der Signatur).
- e. Vertrauliche Informationen sind vor dem Versand an externe Empfängerstellen durch den Anwender zu verschlüsseln (z. B. über die Verschlüsselungsfunktion in Outlook). Bei Kommunikation innerhalb von TransnetBW ist eine Verschlüsselung durch den Anwender nicht erforderlich.

3.4 UMGANG MIT IT-SICHERHEITSVORFÄLLEN & SCHWACHSTELLEN

- a. Stellt der Anwender im Umgang mit TransnetBW-Informationssystemen ungewöhnliche Ereignisse oder Schwachstellen fest, welche die Sicherheit der Systeme beeinträchtigen könnten, hat er dies unverzüglich seinem Ansprechpartner bei TransnetBW zu melden.
- b. Bei einem IT-Sicherheitsvorfall hat der Anwender auf weitere Anweisungen durch TransnetBW zu warten. Eigenständige Versuche, den Vorfall zu bewältigen, sind zu unterlassen.

3.5 ÜBERWACHUNG DER EINHALTUNG & FOLGEN BEI MISSACHTUNG

- a. Um die Sicherheit von TransnetBW-Informationssystemen zu gewährleisten, können Benutzeraktivitäten im Einklang mit den geltenden datenschutzrechtlichen Vorgaben protokolliert und überwacht werden.
- b. Die Missachtung dieser Sicherheitsbestimmungen stellt eine Verletzung vertraglicher Regelungen zwischen TransnetBW und dem externen Geschäftspartner dar. Verstöße können rechtliche Konsequenzen nach sich ziehen.

- c. TransnetBW behält sich vor, dem Anwender infolge einer Pflichtverletzung den Zugang zu TransnetBW-Informationssystemen zu verwehren. Die Rechte von TransnetBW gegenüber dem Vertragspartner bleiben davon unberührt.