Disclosure Policy

–

Orientierung für den Umgang mit möglichen Schwachstellen

Zweck und Grundsatz

Die Sicherheit unserer IT-Systeme, Daten und Dienste hat für uns höchste Priorität. Mit dieser Disclosure Policy beschreiben wir, wie wir mit gemeldeten, möglichen IT-Schwachstellen, verdächtigen Aktivitäten oder Bedrohungslagen (nachfolgend auch kurz „Schwachstellen“) umgehen und wie wir eine verantwortungsvolle Zusammenarbeit mit meldenden Personen sicherstellen.

Wir begrüßen Hinweise auf sicherheitsrelevante Themen ausdrücklich und sehen diese als wichtigen Beitrag zur Erhöhung der allgemeinen IT-Sicherheit.

Geltungsbereich

Diese Disclosure Policy gilt sachlich für:

- Meldungen von vermeintlichen / potentiellen und nachgewiesenen IT-Schwachstellen, verdächtigen Aktivitäten oder Bedrohungslagen für
    - unsere Webseiten,
    - Webanwendungen,
    - IT-Systeme und digitale Dienste,
- unabhängig davon, ob die Meldungen durch interne oder externe Personen erfolgen.

Der räumliche Anwendungsbereich dieser Disclosure Policy betrifft die gesamte Stadtwerke Bielefeld-Gruppe mit allen Tochter- und Beteiligungsgesellschaften.

Bitte beachten Sie, dass Meldungen zu Schwachstellen mit lediglich geringfügigen Sicherheitsauswirkungen (z. B. fehlende HTTP-Header), nicht verifizierten Ergebnissen automatisierter Scans, Sachverhalten außerhalb des Einfluss- und Verantwortungsbereichs der Stadtwerke Bielefeld-Gruppe sowie Meldungen, die nicht den nachfolgend aufgeführten Anforderungen entsprechen, nicht berücksichtigt werden.

Meldeweg

Schwachstellen sollen über das auf der Webseite bereitgestellte **Meldeformular** gemeldet werden.

Stand: 06.08.2026

Das Meldeformular ist zu finden unter

➔ https://www.stadtwerke-bielefeld.de/privatkunden/services/kontakt/it-sicherheitshinweise/

Im Rahmen der Meldung sind – soweit möglich – folgende Informationen bereitzustellen:

- Beschreibung der Schwachstelle
- betroffene Systeme oder URLs
- Zeitpunkt der Feststellung
- mögliche Auswirkungen
- ggf. Schritte zur Reproduktion

Unser Umgang mit gemeldeten IT-Schwachstellen

Nach Eingang einer Meldung gehen wir wie folgt vor:

1. **Bestätigung des Eingangs**
   Wir bestätigen den Eingang der Meldung in der Regel zeitnah.
2. **Erstbewertung und Analyse**
   Die gemeldeten Informationen werden durch unsere IT-Sicherheitsverantwortlichen sowie – sofern personenbezogene Daten betroffen sind - den Datenschutz und den Compliance-Beauftragten geprüft und bewertet.
3. **Behebung und Maßnahmen**
   Bestätigte Schwachstellen werden gemäß ihrer Kritikalität priorisiert und behoben.
4. **Kommunikation**

   Wir halten die meldende Person über den Fortschritt auf dem Laufenden und geben eine abschließende Rückmeldung zu den getroffenen Maßnahmen.

Verantwortungsvolle Offenlegung (Responsible Disclosure)

Wir bitten meldende Personen, die Grundsätze der verantwortungsvollen Offenlegung zu beachten:

- Eine anzusprechende Person setzt sich nach initialer Meldung mit der meldenden Person in Kontakt.

Stand: 06.08.2026

- Weitergabe von Details gegenüber Dritten vor oder nach Abschluss der Behebung der Schwachstelle nur nach vorheriger inhaltlicher Abstimmung mit der Kontaktperson der SWB-Gruppe.
- Keine Ausnutzung von Schwachstellen über das zur Meldung notwendige Maß hinaus
- Keine Beeinträchtigung von Verfügbarkeit, Integrität oder Vertraulichkeit von Systemen oder Daten
- Keine sozialen, physischen oder technischen Angriffe auf Mitarbeitende oder Infrastruktur

Diese Grundsätze dienen dem Schutz aller Beteiligten und einer schnellen Behebung von Risiken.

Rechtlicher Rahmen / Fair Play

Sofern die Meldung:

- in gutem Glauben erfolgt,
- im Rahmen dieser Disclosure Policy bleibt und
- keine vorsätzliche rechtswidrige Nutzung der Schwachstelle beinhaltet,

werden wir keine rechtlichen Schritte gegen die meldende Person einleiten. Eine etwaig bestehende, gesetzliche Meldepflicht gegenüber staatlichen Stellen (z.B. gegenüber Datenschutzbehörden, BSI, Bundesnetzagentur) bleibt davon unberührt.

Sofern es sich bei der Meldung um einen Hinweis nach dem Hinweisgeberschutzgesetz (HinSchG) handelt bzw. die Meldung vom Schutz dieses Gesetzes umfasst ist, werden wir die Schutzmaßnahmen gem. §§ 33 ff. HinSchG, insbesondere das Verbot von Repressalien, berücksichtigen.

Nicht von dieser Policy gedeckt sind insbesondere:

- absichtliche Schädigungen,
- Datenabflüsse,
- Denial-of-Service-Angriffe,
- Social Engineering oder ähnliche Angriffe.

Rückmeldung / Anerkennung

Es besteht **keine Verpflichtung** zur Gewährung einer Vergütung, Prämie oder sonstigen Leistung gegenüber der meldenden Person; eine etwaige Anerkennung der Meldung erfolgt nach freiem Ermessen der von der Meldung betroffenen Gesellschaft.

Datenschutz und Vertraulichkeit

Personenbezogene Daten, die im Rahmen einer Meldung verarbeitet werden, behandeln wir vertraulich und ausschließlich zum Zweck der Bearbeitung der Schwachstelle gemäß den geltenden Datenschutzbestimmungen. Personenbezogene Daten werden gelöscht, sobald der Zweck der Speicherung entfallen ist. Bei meldepflichtigen Vorfällen sind die Daten für einen Zeitraum von drei Jahren nach Abschluss der Meldung aufzubewahren (§195 BGB).

Änderungen der Disclosure Policy

Wir behalten uns vor, diese Disclosure Policy jederzeit anzupassen, um rechtlichen, technischen oder organisatorischen Anforderungen Rechnung zu tragen.

Stand: 06.08.2026