Disclosure Policy

–

Guidance for Handling Potential Vulnerabilities

Purpose and Principle

The security of our IT systems, data, and services is of the highest priority to us. With this Disclosure Policy, we describe how we handle reported potential IT vulnerabilities, suspicious activities, or threat situations, hereinafter also referred to briefly as “vulnerabilities”, and how we ensure responsible cooperation with reporting persons.

We expressly welcome reports on security-relevant matters and consider them an important contribution to improving general IT security.

Scope

This Disclosure Policy applies, with regard to its subject matter, to:

- Reports of suspected, potential, and confirmed IT vulnerabilities, suspicious activities, or threat situations affecting
    - our websites,
    - web applications,
    - IT systems and digital services,
- regardless of whether the reports are submitted by internal or external persons.

The geographical scope of this Disclosure Policy covers the entire Stadtwerke Bielefeld Group, including all subsidiaries and affiliated companies.

Please note that reports concerning vulnerabilities with only minor security impact, such as missing HTTP headers, unverified results from automated scans, matters outside the sphere of influence and responsibility of the Stadtwerke Bielefeld Group, and reports that do not meet the requirements listed below will not be taken into account.

Reporting Channel

Vulnerabilities should be reported using the **reporting form** provided on the website.

The reporting form can be found at

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

As part of the report, the following information should be provided where possible:

- Description of the vulnerability
- Affected systems or URLs
- Time of discovery
- Possible impact
- Steps to reproduce, if applicable

How We Handle Reported IT Vulnerabilities

After receiving a report, we proceed as follows:

1. **Acknowledgement of Receipt**
   We generally confirm receipt of the report promptly.
2. **Initial Assessment and Analysis**
   The reported information is reviewed and assessed by our IT security officers and, where personal data is affected, by Data Protection and the Compliance Officer.
3. **Remediation and Measures**
   Confirmed vulnerabilities are prioritized and remediated according to their criticality.
4. **Communication**

   We keep the reporting person informed about progress and provide final feedback on the measures taken.

Responsible Disclosure

We ask reporting persons to observe the principles of responsible disclosure:

- A designated contact person will contact the reporting person after the initial report.
- Details may be shared with third parties before or after remediation of the vulnerability has been completed only after prior substantive coordination with the contact person of the SWB Group.
- Do not exploit vulnerabilities beyond what is necessary for reporting.

Version: 06/08/2026

- Do not impair the availability, integrity, or confidentiality of systems or data.
- Do not conduct social, physical, or technical attacks against employees or infrastructure.

These principles serve to protect all parties involved and to ensure risks are remediated quickly.

Legal Framework / Fair Play

Provided that the report:

- is made in good faith,
- remains within the scope of this Disclosure Policy, and
- does not involve any intentional unlawful use of the vulnerability,

we will not initiate legal action against the reporting person. Any existing statutory reporting obligations to public authorities, such as data protection authorities, the BSI, or the Federal Network Agency, remain unaffected.

If the report constitutes a report under the German Whistleblower Protection Act (HinSchG), or if the report falls within the protection of that Act, we will take into account the protective measures pursuant to Sections 33 et seq. HinSchG, in particular the prohibition of reprisals.

In particular, this Policy does not cover:

- intentional damage,
- data exfiltration,
- denial-of-service attacks,
- social engineering or similar attacks.

Feedback / Recognition

There is **no obligation** to grant remuneration, a bonus, or any other benefit to the reporting person; any recognition of the report is at the sole discretion of the company affected by the report.

Data Protection and Confidentiality

Personal data processed as part of a report will be treated confidentially and used exclusively for the purpose of handling the vulnerability in accordance with the applicable data protection regulations. Personal data will be deleted as soon as the purpose of storage no longer applies. In the case of reportable incidents, the data must be retained for a period of three years after completion of the report (Section 195 German Civil Code, BGB).

Changes to the Disclosure Policy

We reserve the right to amend this Disclosure Policy at any time in order to reflect legal, technical, or organizational requirements.