RESPONSIBLE DISCLOSURE POLICY

FiberCop

FIBER INFRASTRUCTURE PARTNER
OF MILANO CORTINA 2026

MILANO CORTINA 2026

MILANO CORTINA 2026

FIBERCOP – RESPONSIBLE DISCLOSURE POLICY

The security of the networks, systems, and data of our customers and users is a priority for FiberCop. We recognize that, despite security measures in place, vulnerabilities may still emerge. For this reason, we encourage responsible, collaborative, and good-faith reporting of any such issues.

SCOPE

This Policy applies exclusively to vulnerabilities identified in FiberCop's official digital services, websites, and applications, clearly identifiable as such, including digital systems and platforms, applications and online services, as well as externally exposed software components and interfaces.

Reports relating to standard configurations or security best practices without tangible, exploitable impact are out of scope, including, by way of example:

- Missing or suboptimal configuration of HTTP security headers (e.g., CSP, HSTS, X-Frame-Options), unless associated with exploitable vulnerabilities;
- Use of TLS versions or configurations considered weak but not exploitable in the specific context;
- Exposure of banners or version information without demonstrable security impact;
- Purely informational or hardening-related findings.

Vulnerabilities related to Artificial Intelligence–based systems are considered within scope only where they result in concrete and demonstrable impacts on information security (e.g., data exposure, unauthorized access, or security control bypass).

HOW TO REPORT A VULNERABILITY

Please send your report to: cirt[@]fibercop[.]com

The report should include, where possible:

- Description of the vulnerability;
- Affected system or URL;
- Steps to reproduce the issue;
- Any supporting technical evidence.

Reports may also be submitted anonymously or under a pseudonym.

To encrypt vulnerability reports submitted via email, you can use this **PGP Public Key**.

EXPECTED CONDUCT

We ask that you:

- Do not exploit the vulnerability or issue you have discovered for any benefit or advantage;
- Do not perform any activity that could harm us or our users, disrupt the affected system or service, or result in the unauthorized disclosure of data.

- Take all reasonable steps to avoid privacy violations (loss of confidentiality, integrity, or availability of data) and/or service degradation or disruption;
- Respect the privacy of our users and/or customers: accessing or using personal data, even if incidentally encountered during testing, is strictly prohibited except where strictly necessary to identify, validate, report, or help remediate the vulnerability and protect our users.
- If the vulnerability involves an actual or potential personal data breach, promptly notify dpo.fibercop[@]fibercop[.]com and cirt[@]fibercop[.]com;
- Do not modify systems or applications;
- Do not perform Denial of Service (DoS) or brute-force attacks;
- Do not execute aggressive automated scanning;
- Do not use social engineering techniques against our employees or suppliers;
- Do not carry out physical security attacks;
- Do not introduce backdoors into systems, as this would further compromise their security;
- Provide sufficient information to reproduce the issue so that it can be resolved as quickly as possible. Typically, the IP address or URL of the affected system and a description of the vulnerability are sufficient; however, additional details may be required for complex cases;
- Do not disclose vulnerability details to third parties until the vulnerability has been remediated, and coordinate with us in advance regarding any communication or publication related to the vulnerability;
- Maintain responsible behavior even after a fix has been released, carefully considering the type of information disclosed, always with the aim of protecting our users and their data.

FIBERCOP COMMITMENTS

FiberCop commits to:

- Acknowledge receipt of the report;
- Provide an initial response within 7 business days, including our assessment and an expected resolution timeline;
- Keep all received information confidential;
- Process personal data in compliance with applicable regulations.

This Policy does not authorize unlawful activities and does not override applicable laws. We reserve the right to manage and take action against reports and notifications that do not comply with the criteria set out in this Responsible Disclosure Policy and applicable laws.

RECOGNITION

Any public acknowledgment or inclusion in a “Hall of Fame” will only occur with the explicit consent of the reporter. At present, no financial compensation is provided for reported vulnerabilities.

FINAL NOTES

This Policy:

- Does not constitute a contract or a public offer;
- Does not guarantee specific timelines or outcomes;
- May be amended or updated by FiberCop at any time.