Vulnerability Disclosure Policy

LAST UPDATED: September 29, 2025

Temperature Superstore is committed to protecting our customers, data, and systems. We appreciate the role of the security community in helping us maintain a safe and secure environment.

This policy outlines our approach to handling unsolicited vulnerability reports. While we do not actively solicit feedback or operate a formal bug bounty program, we take all valid reports seriously and investigate them thoroughly.

Reporting Security Issues

If you believe you've found a security vulnerability in a Temperature Superstore system or asset, please report it by emailing us at website.security@briskheat.com.

When reporting, please:

- Respect privacy – If you access someone else's data (e.g., usernames, passwords, or personal information), stop immediately and report it. Do not save, share, or transmit this data.
- Act in good faith – Submit your report without any conditions or demands.
- Collaborate responsibly – Report your findings promptly. Stop testing after identifying the first issue and request permission before continuing. Allow us reasonable time to investigate and resolve the issue before any public disclosure.

Please do not:

- Exfiltrate data. Use a proof of concept to demonstrate the issue instead.
- Exploit the vulnerability to disable or bypass security controls.
- Engage in social engineering (e.g., phishing or impersonation).
- Use automated tools or scanners without prior authorization.

Post-Report Process

Once we receive a report, Temperature Superstore will:

1. Maintain confidentiality – We ask that all communications regarding the vulnerability remain private.
2. Verify the issue – We will investigate and confirm the validity of the report.
3. Remediate – If confirmed, we will address the vulnerability and implement a fix or mitigation.
4. Communicate – We will acknowledge your report within 10 business days and provide status updates as appropriate.
5. After resolution, BriskHeat may, at its sole discretion, choose to publicly acknowledge the reporter's contribution. This decision is made following internal review and is based on factors such as, but not limited to, the nature of vulnerability, its impact, and alignment with our internal policies.

Please note: Temperature Superstore does not operate a formal bounty program. Any recognition is discretionary and determined on a case-by-case basis, based on factors such as severity, impact, and alignment with internal criteria.

Important Note

This policy is intended to align with current security best practices. However, Temperature Superstore does not actively solicit vulnerability reports through public platforms or outreach. Any time, effort, or resources invested in evaluating our systems are done at the sole discretion of the reporter.

We appreciate the efforts of those who choose to report responsibly and help us improve our security posture.

Policy Updates

Temperature Superstore reserves the right to modify or update this Vulnerability Disclosure Policy at any time without prior notice. We encourage reporters and researchers to review the policy periodically to stay informed of any changes.