RESPONSIBLE DISCLOSURE POLICY

Version 1.0

Last Updated: 2026-03-09

Blueshift Cybersecurity, Inc. (“Blueshift,” “we,” “us,” or “our”) provides products and services, including the IntelliThreat AI Platform and managed security services, including managed SOC and XDR services. We are committed to maintaining the security, availability, and integrity of our products, services, and infrastructure. We value the efforts of security researchers and members of the security community who help us identify and responsibly report potential security vulnerabilities. This policy describes how to report suspected vulnerabilities to Blueshift and the conditions under which Blueshift may consider certain research activity to be authorized. This policy is provided for informational purposes only, may be modified, limited, or revoked by Blueshift at any time in its sole discretion, and does not create any contractual commitment, waiver, or other legal obligation except as expressly required by applicable law.

This policy applies only to security vulnerabilities discovered in Blueshiftowned and expressly designated systems, software, applications, websites, APIs, and cloud services, including (a) the IntelliThreat AI Platform and related Blueshift-hosted environments and (b) Blueshift-operated infrastructure and internal service-delivery environments used to support managed SOC and XDR services, in each case solely to the extent Blueshift has designated them as in scope. This policy does not apply to customer environments, customer data environments, partner environments, channel partner environments, thirdparty systems, thirdparty services, or any asset, network, domain, application, tenant, endpoint, or environment not expressly owned or designated in writing by Blueshift as in scope for this policy, even if that environment interoperates with, connects to, is monitored by, or otherwise relates to Blueshift products or services. No asset is in scope by implication, inference, course of dealing, or public association with Blueshift.

1. REPORTING A SECURITY VULNERABILITY

If you believe you have identified a security vulnerability affecting an in-scope Blueshift system or service, please report it promptly by email to:

security@blueshiftcyber.com

When submitting a report, please include, to the extent available:

- A clear description of the vulnerability
- The affected product, service, or system
- Steps to reproduce the issue (if applicable)
- Any relevant logs, screenshots, or proofofconcept details sufficient to help us validate the issue
- Your contact information for followup

Please do not include sensitive personal data, regulated data, credentials, or other unnecessary confidential information in your report. If you believe access to that information is necessary to

describe the issue, please limit collection to the minimum necessary to demonstrate the vulnerability and notify Blueshift in your report.

2. AUTHORIZED TESTING AND RESEARCH BOUNDARIES

Blueshift supports **goodfaith security research** directed at identifying and reporting vulnerabilities in in-scope assets, provided that the activity is conducted in a manner that avoids harm to Blueshift, our customers, and other third parties, and strictly complies with this policy. Authorization under this policy is limited, conditional, non-exclusive, revocable at any time, and applies only to activity reasonably necessary to identify and document a suspected vulnerability for reporting to Blueshift. This policy does not grant any right to access, test, scan, copy, retain, use, or disclose any data except to the minimum extent unavoidably encountered in qualifying good-faith research, and it does not limit any restrictions set forth in applicable law, contract, website terms, platform terms, or other Blueshift policies, except solely to the extent Blueshift expressly states otherwise in this policy. For clarity, this authorization extends only to Blueshift-owned and expressly designated in-scope assets and does not extend to any customer, partner, channel partner, or other third-party environment, even where Blueshift provides managed services, monitoring, integrations, deployment assistance, or other support in relation to that environment.

The following activities are **not authorized** under this policy:

- Denialofservice attacks or traffic flooding
- Automated scanning, fuzzing, scraping, enumeration, or other testing that degrades system performance, bypasses access restrictions, triggers excessive requests, or materially increases operational, security, or availability risk
- Exploitation of vulnerabilities beyond what is reasonably necessary to confirm the existence of the issue and demonstrate impact in a minimal, non-destructive manner
- Accessing, modifying, deleting, copying, downloading, exfiltrating, or retaining customer data, personal data, confidential information, or other data not belonging to you, except to the minimum extent unavoidably encountered in good-faith testing and not further used, disclosed, or stored
- Social engineering, phishing, pretexting, or physical security testing
- Testing against customer environments, partner environments, or channel partner environments without explicit written authorization
- Penetration testing of Blueshift-hosted services without Blueshift's separate prior written approval, and no such approval under this policy authorizes testing of any customer, partner, or third-party tenant, instance, workspace, account, or environment

Establishing persistence, planting backdoors, deploying payloads, moving laterally within any environment, attempting privilege escalation, using stolen or third-party credentials, or accessing accounts, tenants, sessions, or resources beyond those strictly necessary for minimal validation of the reported issue

Any disruptive, destructive, or materially intrusive testing, including altering system configurations, modifying production data, interrupting service availability, or impairing monitoring, logging, or defensive controls
Testing any third-party asset, any customer or partner asset, or any Blueshift-related asset that has not been expressly designated by Blueshift as in scope under this policy

Blueshift does not permit customer-initiated penetration testing, vulnerability scanning, or similar assessment activity against Blueshift-hosted services unless Blueshift has expressly authorized such activity in a separate writing and in advance, and Blueshift may withhold, condition, or revoke any such authorization in its sole discretion. For avoidance of doubt, Blueshift's provision of managed SOC or XDR services does not make any customer, partner, or channel partner environment part of Blueshift's in-scope assets under this policy. For further avoidance of doubt, Customer integration environments — including Microsoft 365 tenants, cloud provider accounts, Salesforce orgs, and similar environments — remain outside the scope of this policy even where the IntelliThreat Autonomous offering is executing authorized actions within those environments under Customer-configured permissions. Authorized research under this policy does not extend to those environments under any circumstances.

3. COORDINATED DISCLOSURE TIMELINES

Blueshift asks researchers to provide a reasonable opportunity to investigate, validate, and address reported vulnerabilities before any public disclosure. We seek to follow a coordinated disclosure process that balances user protection, remediation complexity, and the public interest; however, any stated timelines are targets only, not commitments, and may be adjusted by Blueshift based on technical, operational, legal, customer-protection, or dependency-related considerations.

Our target for coordinated disclosure is generally:

- **Critical and High severity vulnerabilities (CVSS Base Score ≥ 7.0): approximately 90 days from Blueshift's receipt of a sufficiently detailed initial report. Medium and Low severity vulnerabilities (CVSS Base Score < 7.0): approximately 120 days from Blueshift's receipt of a sufficiently detailed initial report. These periods are non-binding targets only.**

In some circumstances, additional time may be reasonably necessary, including where a vulnerability is unusually complex, affects shared or thirdparty dependencies, presents heightened risk to customers or users, or requires staged remediation. Blueshift will endeavor to communicate in good faith regarding status and timing, and coordinated public disclosure timing may be discussed on a casebycase basis.

4. CONDITIONAL SAFE HARBOR

Subject to your full compliance with this policy, Blueshift will not, based solely on your qualifying security research under this policy, initiate legal action against you or refer the matter to law enforcement for specific testing activity that Blueshift determines in its reasonable discretion was conducted in good faith and within the scope of this policy. This statement applies only to Blueshift's own decisions and actions and does not bind any third party, including law

enforcement, regulators, customers, partners, service providers, or other affected persons or entities.

- Act in good faith
- Comply fully with this policy
- Avoid privacy violations, unnecessary access to data, data destruction, service disruption, and other harm
- Do not exploit the vulnerability for personal gain, competitive advantage, extortion, or any purpose other than goodfaith testing and reporting

This safe harbor is limited and conditional. It applies only to qualifying activity that Blueshift determines was conducted in accordance with this policy, and it does not apply to conduct that exceeds authorized boundaries, violates applicable law, affects customer, partner, or thirdparty systems or environments, involves data exfiltration or misuse, or otherwise creates material risk or harm. This policy does not constitute permission for any activity not expressly authorized herein, and Blueshift disclaims any representation or warranty that conduct consistent with this policy will be lawful in any jurisdiction or will avoid claims by any third party. Blueshift reserves all rights and remedies with respect to any non-compliant, unlawful, or harmful activity.

5. NO BUG BOUNTY, NO CONTRACT, AND NO COMPENSATION

Blueshift does not currently operate a bug bounty or other monetary reward program. Submission of a vulnerability report does not entitle the reporter to compensation, reimbursement of expenses, or any other payment. Submission of a report also does not create any contractual relationship, partnership, agency, employment, joint venture, fiduciary duty, or other legal obligation on the part of Blueshift, including any obligation to review, validate, remediate, respond to, or publicly disclose any reported issue within any particular timeframe. Blueshift may, in its sole discretion, acknowledge a reporter’s contribution, but is under no obligation to do so.

6. COMMUNICATION, CONFIDENTIALITY, AND COORDINATION

Blueshift will endeavor to acknowledge qualifying reports within five (5) business days and may contact the reporter for clarification, validation details, or additional information. Any acknowledgment, follow-up, investigation, or other communication is provided as a courtesy only and does not create any obligation to continue communications, provide status updates, share remediation details, or take any particular action. We ask reporters to maintain the confidentiality of non-public vulnerability information during our investigation and remediation efforts and to cooperate in good faith with reasonable requests needed to assess and address the reported issue.

Unless Blueshift expressly agrees otherwise in writing, reporters must not publicly disclose specific vulnerability details before Blueshift has had a reasonable opportunity to investigate and remediate the issue under the coordinated disclosure framework described in this policy. After that period, Blueshift expects any public disclosure to be coordinated in good faith, and where legally permitted Blueshift may request reasonable delay or redaction to reduce avoidable risk to

customers, users, and other affected parties. Public disclosure that is premature, uncoordinated, or inconsistent with this policy may result in loss of safe harbor protections and any other accommodation Blueshift might otherwise extend.

7. POLICY UPDATES

This policy may be updated, suspended, or withdrawn from time to time to reflect changes in our security practices, operational requirements, legal obligations, or business needs. The most current version will be posted in the TRUST CENTER DOCUMENT SUITE and will supersede prior versions as of its stated effective or updated date, or immediately upon posting if no later date is stated. Any activity conducted after an update is subject to the then-current version of this policy.

8. CONTACT

For questions regarding this policy or to report a vulnerability, contact:

Blueshift Cybersecurity, Inc. Email: **security@blueshiftcyber.com;** 2022 Hendry Street, Fort Myers, Florida 33901