6411 Ivy Lane • Suite 606 • Greenbelt, MD 20770 • Phone: 301-345-1999 • Fax: 301-345-2874

**Vulnerability Disclosure Policy (VDP)**
**Organization:** Innovative Concepts Engineering, Inc.
**Policy Number:** POL-VDP
**Version:** 1.0
**Effective Date:** 11/4/2026
**Policy Owner:** Information System Security Manager (ISSM)
**Approval Authority:** Bob Bulk

**1. Purpose**

The purpose of this Vulnerability Disclosure Policy (VDP) is to establish a formal process for receiving, evaluating, tracking, and addressing reports of potential security vulnerabilities affecting information systems, system components, software, and technology products owned, operated, or utilized by Innovative Concepts Engineering. This policy supports the organization's implementation of NIST Special Publication 800-53, Revision 5, control RA-5(11), Public Disclosure Program.

The organization recognizes the value of responsible security research and encourages individuals, security researchers, software vendors, and other external parties to report suspected vulnerabilities through established reporting channels. The organization operates systems that may be isolated from external networks, including the Internet. This policy establishes a public reporting mechanism that allows external parties to submit vulnerability information without requiring direct access to, or connectivity with, organizational information systems.

**2. Scope**

This policy applies to vulnerability reports concerning:

- Information systems owned, operated, or maintained by Innovative Concepts Engineering.
- Hardware, software, firmware, and other system components incorporated into organizational information systems.
- Commercial off-the-shelf (COTS) products and third-party software utilized by the organization.
- Custom-developed software, applications, and system components developed or maintained by the organization.
- Vulnerabilities identified in technologies that may affect the confidentiality, integrity, or availability of organizational information systems.

This policy applies to reports submitted by members of the public, external security researchers, vendors, customers, business partners, and other interested parties.

**Offline and Isolated Systems**

The organization's offline and isolated information systems are included within the scope of this policy for purposes of receiving and evaluating vulnerability information. However, these systems are not publicly accessible and are not authorized targets for external security testing. External parties may report suspected vulnerabilities based on publicly available technical information, vendor security advisories, independent research, or other lawfully obtained information. Nothing in this policy authorizes external parties to access, scan, probe, test, or otherwise interact with isolated organizational systems or facilities.

**3. Public Vulnerability Reporting Channel**

The organization maintains a publicly accessible mechanism for receiving reports of suspected security vulnerabilities.

Reports may be submitted through one or more of the following channels:

- **Email:** security@company.com
- **Postal Address:** Innovative Concepts Engineering, 6411 Ivy Ln. Ste 606, Greenbelt, MD 20770
- **Telephone:** 301-345-1999

The public reporting channel is maintained separately from the organization's offline information systems. Submission of a vulnerability report does not provide, require, or establish connectivity to any isolated organizational system. Reports received through these channels are directed to designated security personnel for review and processing. The organization will make the reporting

instructions and contact information publicly available through its corporate website or another publicly accessible publication.

**4. Reporting Requirements**

Individuals submitting vulnerability reports are encouraged to provide sufficient information to enable the organization to understand, investigate, and evaluate the reported issue. Reports should include, when available:

- A description of the suspected vulnerability.
- The affected product, application, hardware, software, or system component.
- The version or configuration of the affected component, if known.
- The potential security impact.
- Technical details describing the vulnerability.
- Steps necessary to reproduce the issue, where applicable.
- Supporting documentation, publicly available references, or proof-of-concept information.
- Contact information for follow-up, if the reporter wishes to be contacted.

Anonymous submissions are permitted.

**Sensitive Information Restrictions**

Reporters must not submit classified information, Controlled Unclassified Information (CUI), export-controlled technical data, proprietary information belonging to third parties, credentials, or other protected organizational information through public reporting channels. Reporters must not attempt to obtain such information through unauthorized access or testing. If a suspected vulnerability involves classified information, CUI, or other protected information, the reporter should not transmit the information through the public reporting channel. The reporter should instead contact the organization's security office using the published telephone contact information to obtain appropriate reporting instructions.

**5. Authorized and Prohibited Activities**

The organization welcomes good-faith vulnerability research and the responsible disclosure of suspected vulnerabilities. This policy does not grant authorization to access or test organizational systems, networks, facilities, or information. In particular, external parties are not authorized to:

- Access or attempt to access organizational information systems without explicit written authorization.
- Conduct vulnerability scans, penetration tests, or other active security testing against organizational systems.
- Attempt to bypass access controls, authentication mechanisms, or other security protections.
- Introduce malicious software, execute destructive actions, or disrupt system operations.
- Attempt to access, obtain, modify, or disclose organizational information.
- Conduct denial-of-service testing or other activities that could affect system availability.
- Physically access organizational facilities or equipment without authorization.

Any security testing involving organizational systems must be separately authorized in writing by the appropriate organizational authority. Good-faith reporting of a suspected vulnerability through the designated reporting channels is encouraged.

**6. Vulnerability Report Handling and Evaluation**

The organization's designated security personnel are responsible for receiving and coordinating the evaluation of vulnerability reports.

Upon receipt of a report, the organization will perform the following activities:

1. **Receipt and Documentation:** Record the date of receipt, reporting method, affected product or component, and available technical details.
2. **Acknowledgment:** When contact information is provided, acknowledge receipt of the report within five (5) business days.
3. **Initial Review:** Evaluate the report to determine whether it represents a credible security concern and whether additional information is required.

4. **Technical Assessment:** Coordinate with appropriate technical personnel to determine whether the reported vulnerability affects organizational systems or system components.
5. **Risk Evaluation:** Evaluate the potential impact to the confidentiality, integrity, and availability of organizational information systems and information.
6. **Disposition:** Document the results of the evaluation and determine whether corrective action, additional investigation, or no further action is warranted.
7. **Tracking and Closure:** Maintain a record of the report, investigation results, remediation activities, and final disposition.

Vulnerability reports that cannot be independently reproduced because of the organization's offline operating environment may be evaluated using available technical documentation, vendor advisories, software version information, configuration information, and other appropriate evidence.

**7. Handling of Vulnerabilities Affecting Offline Systems**

Because certain organizational information systems operate in an offline or isolated environment, additional procedures are established to ensure vulnerability information is appropriately reviewed without compromising system isolation.

When a report potentially affects an offline system:

- Designated security personnel will identify the potentially affected system or component.
- The ISSM or designated security representative will coordinate with system owners and technical personnel to determine applicability.
- Vulnerability information will be transferred into the offline environment only through approved information transfer procedures.
- Any required transfer of files, software updates, patches, or technical documentation will comply with applicable media protection, malware scanning, configuration management, and information security procedures.
- No direct network connection between the public reporting infrastructure and the offline information system will be established for the purpose of processing vulnerability reports.

The organization will preserve applicable system isolation requirements throughout the vulnerability evaluation and remediation process.

**8. Vulnerability Remediation and Coordination**

Confirmed vulnerabilities affecting organizational information systems will be addressed in accordance with the organization's vulnerability management and risk assessment processes.

The organization will:

- Determine whether the vulnerability affects deployed systems or components.
- Evaluate the severity and potential operational impact.
- Identify appropriate mitigation or remediation actions.
- Coordinate with software and hardware vendors when necessary.
- Implement corrective actions in accordance with applicable configuration management and change control procedures.
- Document remediation activities and verify corrective actions when technically feasible.

When a vulnerability affects a third-party product, the organization may coordinate with the applicable vendor or supplier to obtain additional technical information, mitigation guidance, or corrective updates. Vulnerabilities affecting DoD information systems or potentially exposing DoD information will be handled in accordance with applicable contractual, regulatory, incident reporting, and customer notification requirements.

**9. Communication and Responsible Disclosure**

The organization encourages reporters to coordinate disclosure of identified vulnerabilities with the organization before publicly releasing technical details that could increase the risk of exploitation. When contact information is provided, the organization will make reasonable efforts to maintain communication with the reporter regarding the status and disposition of the report. The organization requests that reporters allow a reasonable period for investigation and remediation before publicly disclosing vulnerability details. A period of ninety (90) calendar days following the initial report is

requested as a general guideline. The period may be adjusted based on vulnerability severity, remediation complexity, operational considerations, and potential impacts to national security or DoD missions. The organization does not require indefinite non-disclosure as a condition of submitting a vulnerability report. The organization will not publicly disclose classified information, CUI, export-controlled technical data, proprietary information, or other protected information in connection with vulnerability disclosures.

**10. Roles and Responsibilities**

**Information System Security Manager (ISSM)**

- Owns and maintains this policy.
- Ensures vulnerability reports are appropriately evaluated.
- Coordinates with system owners and security personnel.
- Ensures applicable vulnerabilities are addressed through established risk management processes.
- Maintains oversight of the vulnerability reporting program.

**System Owners**

- Assist in determining whether reported vulnerabilities affect assigned systems.
- Coordinate technical evaluation and remediation activities.
- Ensure corrective actions comply with applicable system security requirements.

**Information Technology and Security Personnel**

- Receive and document vulnerability reports as assigned.
- Perform technical evaluations and risk assessments.
- Coordinate approved transfer of vulnerability information to offline systems.
- Maintain records of investigation and remediation activities.

**Management**

- Provides resources necessary to support the vulnerability disclosure program.
- Reviews and approves this policy.
- Ensures identified risks are addressed in accordance with organizational risk management requirements.

**11. Records Retention**

The organization will maintain records associated with vulnerability reports, including:

- Original vulnerability submissions.
- Acknowledgment and follow-up communications.
- Technical evaluation and risk assessment results.
- Remediation and mitigation activities.
- Final disposition and closure documentation.

Records will be protected and retained in accordance with organizational records retention requirements and applicable contractual and regulatory obligations.

**12. Policy Review and Maintenance**

This policy will be reviewed at least annually and updated as necessary to reflect changes in organizational systems, vulnerability management processes, reporting mechanisms, and applicable security requirements.

The ISSM is responsible for ensuring that the public vulnerability reporting channel remains operational and that the reporting instructions remain publicly accessible.

**13. References**

- NIST SP 800-53, Revision 5, RA-5(11), Public Disclosure Program.
- NIST SP 800-53, Revision 5, RA-5, Vulnerability Monitoring and Scanning.
- NIST SP 800-216, Recommendations for Federal Vulnerability Disclosure Guidelines.
- Applicable DoD cybersecurity requirements and contractual security obligations.
- Organizational Vulnerability Management Policy.
- Organizational Incident Response Policy.
- Organizational Configuration Management Policy.

**14. Approval**

This policy is approved by the undersigned and is effective upon approval.

**Approved By:** ___Bob Bulk_____

**Title:** ___President, FSO_____

**Date:** ___11/04/2026_____