NORC at the University of Chicago

NORC Vulnerability Disclosure Policy

VERSION 1.0

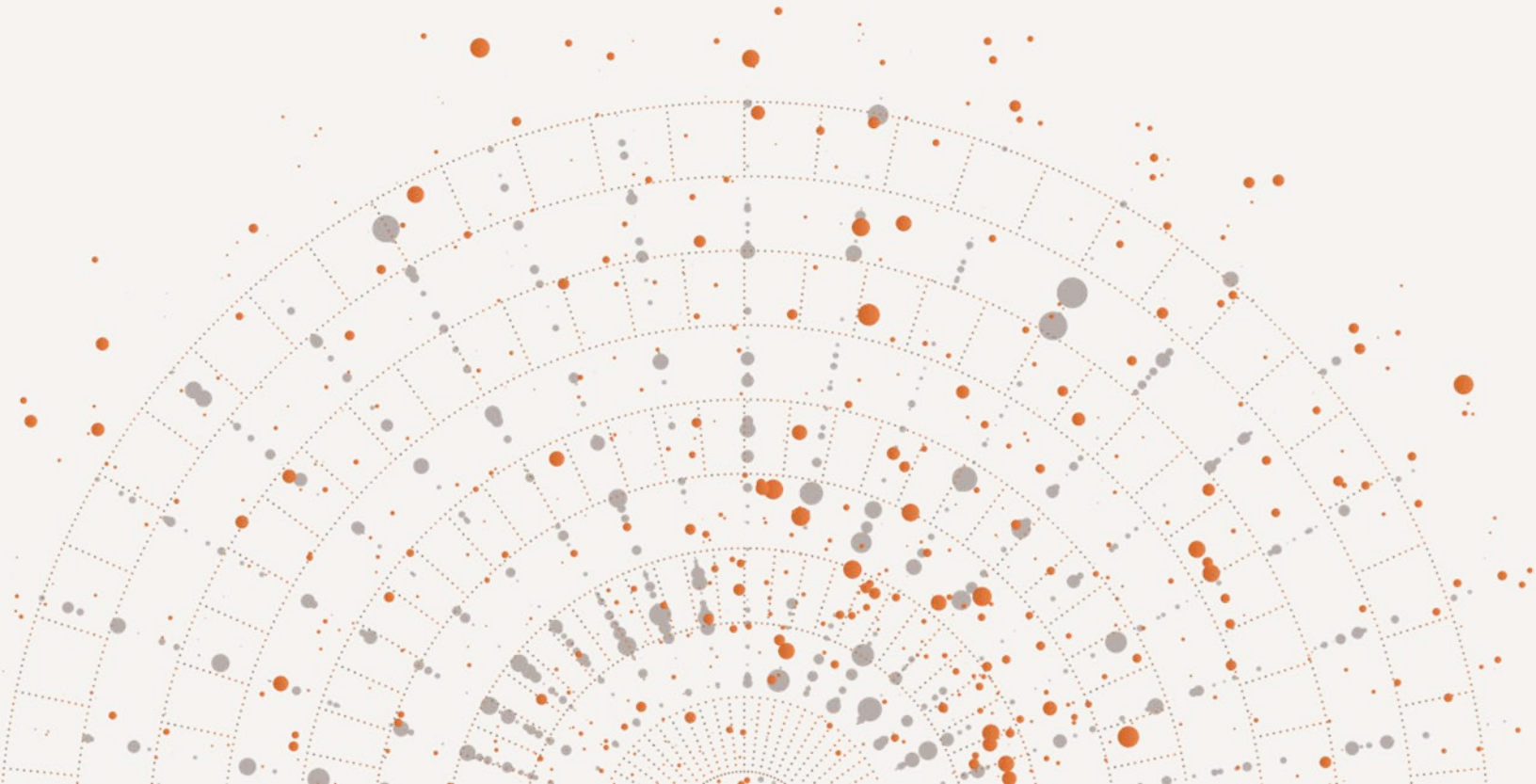

Table of Contents

1.0 Purpose

This Vulnerability Disclosure Policy (VDP) provides guidelines for how NORC:

1. Establishes formal channels for **internal and external** reporting of security vulnerabilities that may affect NORC's information systems, hosted applications, or networks.
2. Assesses, prioritizes, and remediates discovered vulnerabilities in a **timely**, **transparent**, and **secure** manner.
3. Ensures compliance with **NIST SP 800-171 Revision 3**, as well as NORC's existing policies governing:

    - **Incident Response**
    - **Configuration Management**
    - **System and Information Integrity**
    - **Risk Assessment**
    - **Vulnerability Scanning** (and patch management timelines)

By following this policy, NORC protects the confidentiality, integrity, and availability of systems and data, including **Controlled Unclassified Information (CUI)**.

2.0 Scope

This policy applies to:

- **All NORC-owned or -operated** information systems, including those processing CUI.
- **All third-party systems** operated on behalf of NORC or interfacing with NORC networks and services.
- **All NORC personnel,** which includes employees, contractors, and subcontractors.
- **External researchers, vendors, or other third parties** who discover and wish to report a vulnerability in NORC's environment.

3.0 Definitions

- **Vulnerability**: A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exploited to gain unauthorized access or compromise system/data confidentiality, integrity, or availability.
- **VDP**: The formal policy (this document) that outlines how vulnerabilities are reported, received, triaged, and resolved within NORC.

- **Incident**: Any occurrence that jeopardizes or has the potential to jeopardize the integrity, confidentiality, or availability of an information system. If a reported vulnerability is found to be exploited or in active use, the **Incident Response Policy** is triggered.
- **CUI (Controlled Unclassified Information)**: Information requiring safeguarding or dissemination controls consistent with federal law, regulations, and government-wide policies.

4.0 Policy Statement

4.1 Reporting Vulnerabilities

Disclosure Channels

- NORC provides the following channels to receive vulnerability reports:
  - A dedicated email address (**VDP@norc.org**)
- Internal personnel discovering a vulnerability must immediately report it to the internal service desk.
- Reporters may choose to submit vulnerabilities anonymously; however, if no contact information is provided, NORC may be unable to provide direct follow-up or status updates regarding remediation progress.

Information to Include

Reporters (internal or external) should provide:

- Detailed description of the vulnerability and its potential impact.
- Steps to replicate or proof-of-concept, if available.
- Any relevant logs, screenshots, or evidence supporting the discovery.

Good-Faith Testing

- NORC encourages good-faith security research and pledges not to pursue legal action against individuals who abide by this policy and do not intentionally cause harm or breach other legal constraints.

Pre-Disclosure Expectations

- Reporters must not publicly disclose details of the vulnerability until NORC has **validated and mitigated** it, unless otherwise agreed upon in writing.

4.2 In-Scope Systems, Testing Rules, and PII Non-Disclosure

4.2.1 In-Scope Systems

The following NORC systems and applications are **in scope** for vulnerability testing under this policy:

- **Public-facing NORC websites** (e.g., www.norc.org)
- **Externally accessible APIs and services** owned or operated by NORC
- **Any other NORC-owned systems that explicitly list themselves as "in scope"** in official NORC documentation or on the "Security/Contact" page

Any system **not** explicitly named in this list should be considered **out of scope** unless prior written permission is obtained from NORC's Information Security Team (IST).

4.2.2 Authorized Testing Methods

NORC **authorizes** the following testing activities on in-scope systems:

- Non-disruptive, **manual or automated scanning** for common web vulnerabilities (e.g., SQL injection, XSS)
- **Reconnaissance** on publicly available or open-source information about in-scope systems (e.g., DNS lookups, WHOIS, publicly accessible config files)
- **Proof-of-Concept** exploit attempts, provided they do not disrupt system availability or compromise actual data (e.g., local file or database extractions)

4.2.3 Prohibited Testing Activities

NORC **does not authorize**:

- **Denial-of-Service (DoS) or Distributed Denial-of-Service (DDoS)** attacks
- **Social engineering attacks** against NORC personnel (including phishing) without explicit prior approval
- **Physical attempts** to gain access to NORC facilities or equipment
- **Exfiltration of sensitive data** (including PII, PHI, or CUI) beyond what is minimally necessary to demonstrate the vulnerability
- Any action that would intentionally degrade, interrupt, or destroy NORC services, systems, or data

If you are unsure whether a specific testing activity is permitted, **contact the NORC Information Security Team (VDP@norc.org) before proceeding**.

4.2.4 Prohibition on PII Disclosure

To protect individuals' privacy and comply with regulatory requirements, **researchers and reporters must not publicly disclose any PII** discovered during security testing. Any PII that is unintentionally accessed must be:

1. **Immediately reported** to the IST via the official disclosure channels.
2. **Securely deleted or destroyed** after providing the minimal details needed to demonstrate the vulnerability (e.g., a sanitized sample or record count, not full records).

Under no circumstances should PII be published, shared on social media, or released to third parties not explicitly authorized by NORC and/or relevant regulations.

4.3 Triage & Validation

1. **Acknowledgment**

- The **Information Security Team (IST)** will acknowledge receipt of a vulnerability report within **2 business days** and provide a report-tracking identifier (e.g., ticket reference number).

2. **Initial Triage**

- The IST reviews the submission to confirm validity, duplicates, or out-of-scope issues.
- If warranted, the IST coordinates with the **Incident Response Team** if there is evidence of exploitation.

3. **Severity Rating**

- Verified vulnerabilities are assigned a severity level (Critical, High, Medium, Low, Informational) in line with NORC's **Vulnerability Scanning SOP** (using **CVSS v3** scoring or an equivalent method).

4. **Risk Assessment**

- If the vulnerability poses a major risk or affects **CUI** systems, the IST consults the **Risk Assessment Policy** to determine if a formal risk assessment is required.

4.4 Remediation & Mitigation

Remediation Timelines

- Per the **Vulnerability Scanning SOP** and **System and Information Integrity** controls, NORC adheres to the following baseline timelines:

  - **Critical**: Within 15 days
  - **High**: Within 30 days
  - **Medium**: Within 90 days
  - **Low**: Within 365 days
- Actual remediation dates may be accelerated based on business requirements, exposure, and risk level.

Configuration Management

  - All patches, upgrades, or system changes follow the **NORC Configuration Management Policy** and relevant SOPs.
  - **Change Requests** are documented in NORC's change management system, referencing the vulnerability identifier.

Verification

  - After remediation, the IST or appropriate team re-tests or re-scans to ensure the fix is effective.
  - If the fix is incomplete or introduces new issues, the process repeats until the vulnerability is fully addressed.

Accepted Risk & Exceptions

  - If patches are unavailable or cause significant operational disruption, the IST may recommend an **Accepted Risk** exception in accordance with NORC's **Policy/Procedure Exemption Process**.
  - The System Owner, NORC IT Director, and the **CISO** (or designated authority) must review and approve any risk acceptance.
  - All such exceptions must have an **expiration/review date** (e.g., 3, 6, or 12 months).

4.5 Incident Response Integration

If a reported vulnerability has already been exploited or indicates an active threat:

- **Incident Response** procedures (detection, analysis, containment, eradication, recovery) are initiated as detailed in the **NORC Incident Response Policy**.
- The IST coordinates with the **Incident Response Team** to document findings, notifications, and any required external reporting (e.g., for breaches involving CUI).

4.6 Communication & External Disclosure

Ongoing Communication

The IST communicates regularly (as appropriate) with the reporter, providing updates on progress and remediation timelines.

Disclosure to Third Parties

- If the vulnerability affects **federal or agency** systems, additional reporting requirements in the contract or law (e.g., 72-hour notice for certain agencies) may apply.
- The IST coordinates with the **CISO** and **legal counsel** to fulfill any mandatory regulatory disclosures.

Final Disclosure

Upon remediation or a mutually agreed-upon timeline, NORC and the reporter may choose to publish or otherwise share limited details of the vulnerability, emphasizing lessons learned or security improvements implemented.

5.0 Roles & Responsibilities

Chief Information Security Officer (CISO)

- Oversees the Vulnerability Disclosure Program, ensuring its integration with all relevant NORC policies and compliance requirements.
- Provides executive-level support and final approval for **risk acceptance** requests involving significant vulnerabilities or CUI.

Information Security Team (IST)

- Serves as the primary contact for vulnerability reports.
- Performs vulnerability validation, triage, and severity assignment.
- Coordinates with **System Owners**, **IT Engineers**, and **Incident Response** teams to ensure timely remediation.

System Owners / Project Owners

- Implement recommended patches or configuration changes in accordance with **Configuration Management** and **Change Control** policies.
- Communicate any business or technical constraints that could delay remediation.
- Confirm remediation efficacy through re-testing or scanning.

IT Engineering Teams (Server, Network, Application, etc.)

- Execute the actual patching or re-configuration.

- Document actions taken in the official change management system.

All NORC Personnel

- Report any suspected vulnerabilities immediately via the official channels.
- Abstain from unauthorized testing in production systems without IST approval.

6.0 Compliance & Enforcement

Mandatory Compliance

- All personnel and contractors must comply with this policy.
- Violations may result in disciplinary action, including potential termination and/or contract termination.

Periodic Audits & Reviews

- NORC or an external auditor may conduct periodic reviews to ensure the VDP aligns with **NIST SP 800-171 Rev. 3**, contract obligations, and best practices.
- The policy is reviewed at least **every 365 days** or upon significant changes to the threat environment or regulatory requirements.

Exceptions

Inability to meet or maintain compliance with this policy (e.g., technical limitations or financial constraints) requires documented justification, reviewed by the **CISO** and relevant stakeholders, and approved via NORC's **Policy/Procedure Exemption Process**.

7.0 References

- **NIST SP 800-171 Revision 3** – Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
- **NIST SP 800-53 Rev. 5** – Security and Privacy Controls for Information Systems and Organizations
- **NORC Incident Response Policy**
- **NORC Configuration Management Policy & SOP CM-3**
- **NORC System and Information Integrity Policy**
- **NORC Risk Assessment Policy**
- **NORC Vulnerability Scanning SOP**
- **NORC Policy/Procedure Exemption Process**

Version History

Version #	Date	Written / Revised By	Description
1.0	1/01/2025	Jorge Tardiff	Initial Release