An Roinn Dlí agus Cirt,
Gnóthaí Baile agus Imirce
Department of Justice,
Home Affairs and Migration

An Lárionad Náisiúnta
Cibearshlándála
National Cyber
Security Centre

Guidelines for Implementing a Coordinated Vulnerability Disclosure (CVD) Policy

This document provides guidelines to organisations on the process for implementing a Coordinated Vulnerability Disclosure Policy.

ncsc.gov.ie
1st May 2026

Contents

Executive Summary

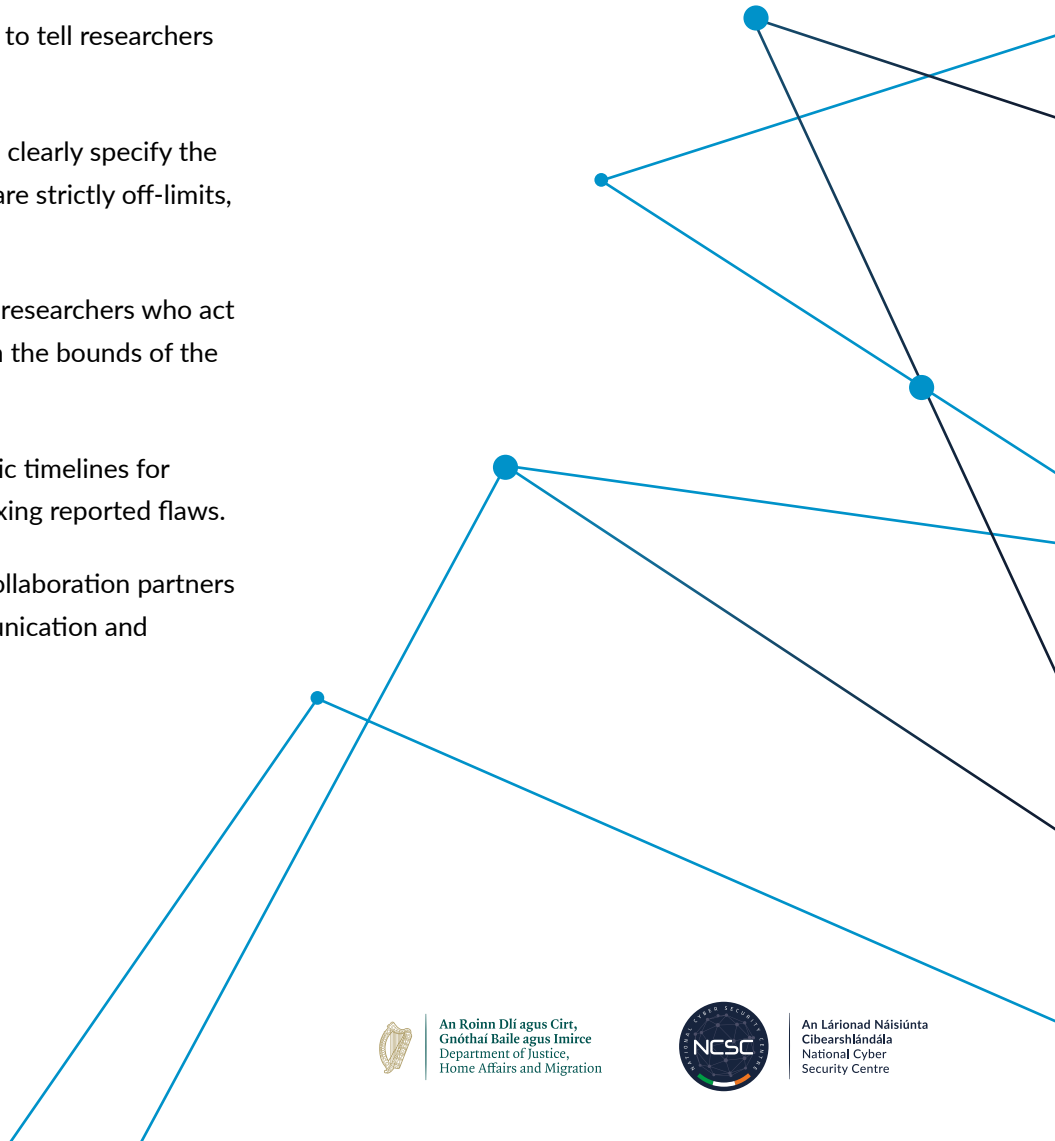
As Ireland's digital landscape continues to expand, security flaws in digital systems and software are inevitable. Without a formalised approach to receiving reports and addressing these flaws, organisations risk critical vulnerabilities going unreported, or being disclosed publicly before a fix is available. These guidelines establish a framework for a Coordinated Vulnerability Disclosure (CVD) process that recognises security researchers acting in good faith as early-warning partners.

By adopting these guidelines, organisations provide security researchers with a route to reporting security flaws, allowing fixes to be developed before they are exploited.

Preparation is critical before any vulnerability reports come in. Having a plan and resources in place will make the handling process far more efficient and effective. Key preparation steps include:

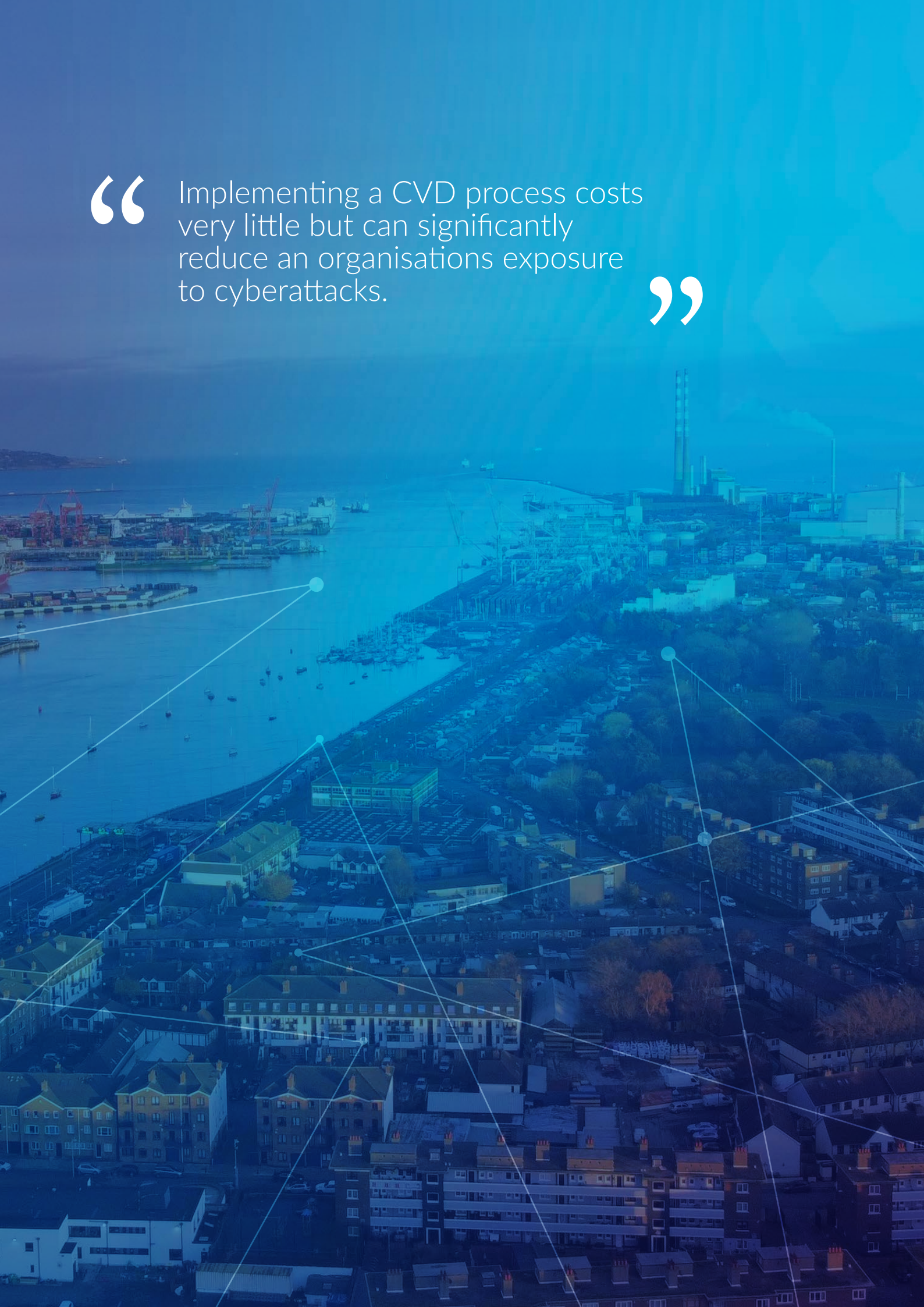
- Publish a '`security.txt`' file to tell researchers how to submit reports.
- A published CVD policy should clearly specify the systems "in scope", and which are strictly off-limits, for testing purposes.
- Commit to legal protection for researchers who act in good faith and remain within the bounds of the published CVD policy.
- Establish and commit to realistic timelines for acknowledging, triaging, and fixing reported flaws.
- Treat security researchers as collaboration partners by providing consistent communication and feedback on reports.

Implementing a CVD process costs very little but can significantly reduce an organisations exposure to cyberattacks. By publishing a CVD policy and engaging in the spirit of these guidelines, the organisation will move from a reactive to a proactive approach to product and service security, building public trust and safeguarding the nation's digital infrastructure.



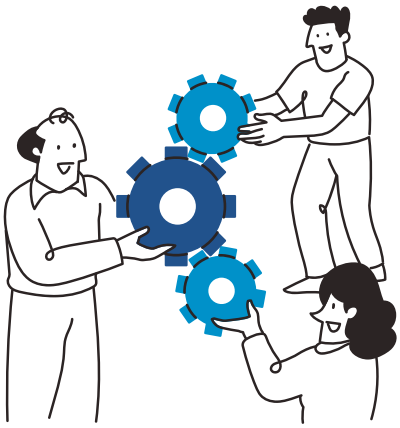
An Roinn Dlí agus Cirt, Gnóthaí Baile agus Imirce
Department of Justice, Home Affairs and Migration

NCSC
An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre



> Implementing a CVD process costs very little but can significantly reduce an organisations exposure to cyberattacks.

Coordinated Vulnerability Disclosure Guidelines



Introduction

In an increasingly digital and interconnected world, cybersecurity is a matter of national interest and public trust. These Coordinated Vulnerability Disclosure (CVD) Guidelines aim to promote a structured, transparent, and responsible process for the reporting and management of cybersecurity vulnerabilities that affect critical national systems, services, and digital infrastructure.

By fostering collaboration between security researchers, technology providers, and government agencies, these guidelines aim to enhance national cyber resilience, reduce risk, and protect citizens, businesses, and public institutions from potential harm arising from unaddressed security weaknesses.

These guidelines are grounded in EU law and offer a framework on meeting the requirements set out by the Network and Information Security (NIS)2 Directive[1] and Cyber Resilience Act (CRA)[2]. As the following come into effect through 2026, they will create a layered defence strategy addressing both organisational and product-level cybersecurity, thus enhancing overall resilience against cyber threats:

- NIS2 - Article 21 requires Essential and Important entities to implement robust risk management processes. This includes mechanisms for coordinating the disclosure and handling of vulnerabilities to ensure timely identification and response.
- CRA - Article 13 requires manufacturers of digital products to establish comprehensive CVD policies with clear reporting mechanisms, ensure prompt responses and mitigation, and promote transparency and collaboration to enhance the security and resilience of digital products.
- The forthcoming National Cyber Security Act - Will aim to further complement this by designating the Computer Security Incident Response Team – Ireland (CSIRT-IE), within An Lárionad Náisiúnta Cibearshlándála / the National Cyber Security Centre (NCSC), as the coordinator for the purposes of coordinated vulnerability disclosure.
- Cyber Fundamentals Framework also underscores this requirement in ID.RA-08.1:

> *The organisation shall establish and implement a vulnerability management plan to identify, analyse, assess, mitigate and communicate all types of vulnerabilities including in the form of a Coordinated Vulnerability Disclosure (CVD) according to applicable legal modalities*

[1] *EUR-Lex: Measures for a high common level of cybersecurity across the Union (NIS2)* https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng

[2] *EUR-Lex: Horizontal cybersecurity requirements for products with digital elements (CRA)* https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng

An Roinn Dlí agus Cirt, Gnóthaí Baile agus Imirce
Department of Justice, Home Affairs and Migration
NCSC
An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

The CVD Process

The purpose of a Coordinated Vulnerability Disclosure process is to bridge the gap between the discovery of a vulnerability and its remediation. By formalising a process for an organisation to respond to a researcher's report, a CVD process helps to address these vulnerabilities before they can be exploited by malicious actors. This process works best when both the organisation and the researcher follow the core principles of CVD.

Principles of CVD

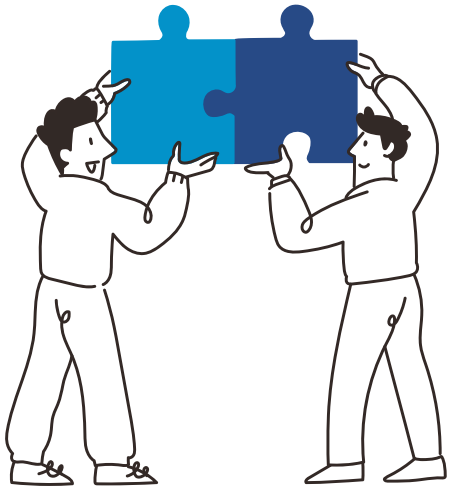
Ensuring the process is effective, all parties should adhere to these core principles:

- The organisation clearly defines what is "in scope" and "out of scope" for testing purposes thus providing strict boundaries that organisations authorise researchers to operate within.
- An organisation's "Safe Harbour" clause, described below under "Legal Context of CVD in Ireland", provides reassurance to researchers acting in good faith, and only within the CVD policy.
- An organisation must be given a reasonable timeframe to triage a report and remediate any issue.
- A good CVD process will emphasise speed in remediating without compromising quality.
- Commitment to timely updates by the organisation to the researcher signals a clear process for remediation.
- Researchers must not disclose information regarding a vulnerability, until a mitigation or patch is available.
- An organisation publicly disclosing a remediated vulnerability, will credit the researcher if they have consented.

Objectives of CVD

Implementing a formal CVD process aims to achieve:

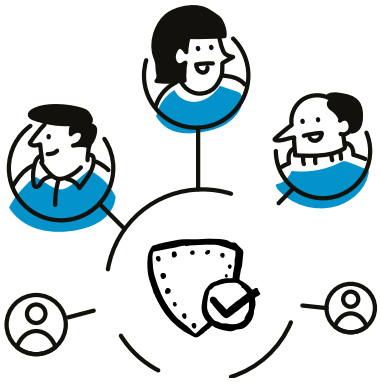
- Reduced risk by minimising the opportunity for attackers through a streamlined process from identification to remediation.
- Creation of formal and efficient communication channels between researchers and an organisations internal security team.
- Provides a reassurance to researchers by distinguishing ethical research activity from malicious cyber activity.
- Demonstrates an organisations maturity in the establishment of a robust, documented vulnerability handling process.



An Roinn Dlí agus Cirt, Gnóthaí Baile agus Imirce
Department of Justice, Home Affairs and Migration

NCSC
An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

Roles and Responsibilities



The CVD process is a shared responsibility model involving multiple roles that require collaboration across the identification, reporting, and resolution of security vulnerabilities. Success depends on clear communication across the lifecycle of the vulnerability remediation process.

Responsible Organisation

The responsible organisation is the overarching authority for the ICT system. This role encompasses governance, system ownership, engagement with vendors and manufacturers where applicable.

- Establishes and publishes the organisations CVD policy that clearly defines the scope that researchers are permitted to operate within.
- Provides secure channels for reports to be made and prompt acknowledgment on receipt.
- Conducts the triage and verification to confirm if a report is valid and in-scope.
- Manages the full remediation process, including coordinating with any necessary third parties and conducting complete tests of the fix.
- Responsible for the decision-making process with regard to the vulnerability severity and disclosure.
- Acknowledges and credits researchers upon remediation.

Researcher

The individual or organisation that first identifies the vulnerability. They act as an early warning system for Irelands digital ecosystem and only operate within the scope of the organisations CVD policy.

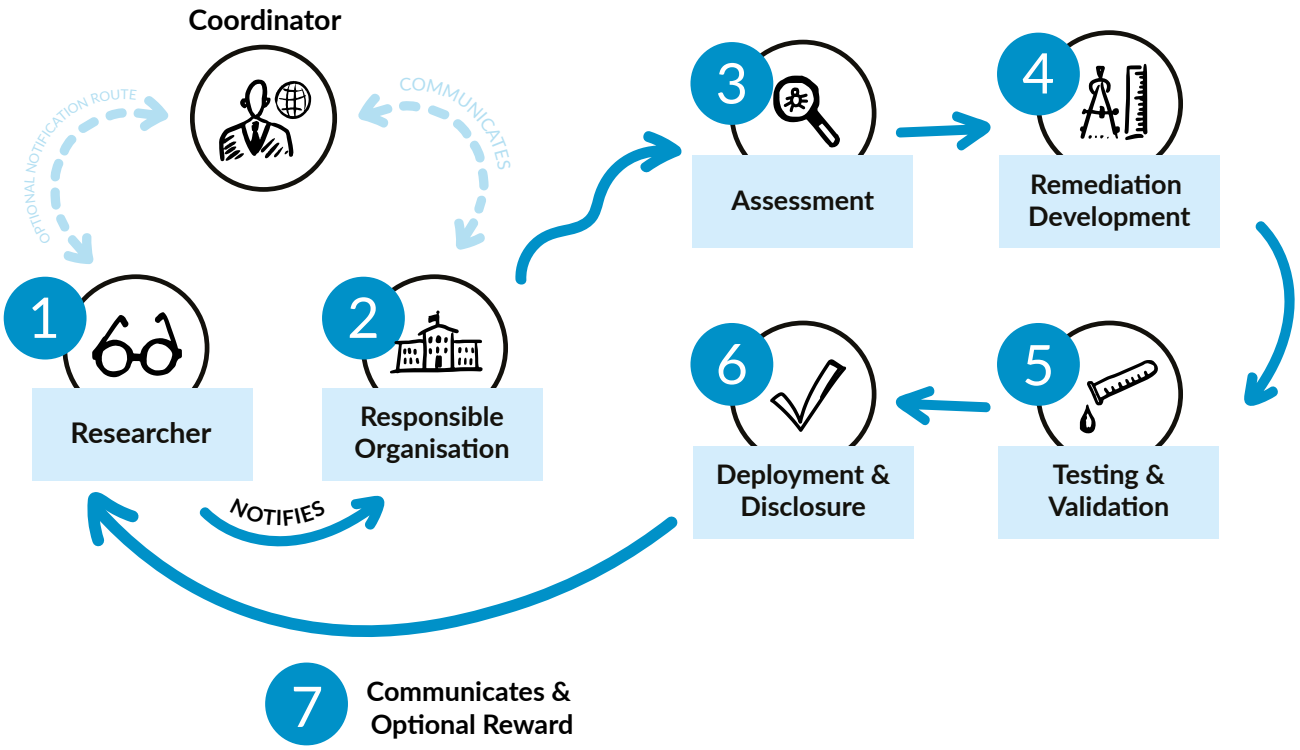
- Conducts research in “good faith” by strictly adhering to the relevant CVD policy, avoiding any activity that could result in service disruption, or a compromise of privacy.
- Provides clear, detailed, actionable information regarding the vulnerability to ensure that the organisation understands the nature of the issue and its potential impact.
- Maintains stict confidentiality regarding the vulnerability by not disclosing any details until a fix is deployed and the organisation has explicitly authorised.
- Operates strictly within the “in-scope” boundaries specified, accessing the minimum amount of data to prove the vulnerability, ceasing activity immediately on encountering a third-party system.
- Does not seek a reward outside of any specified in the organisations CVD policy.
- Does not conduct activities on systems without a published CVD policy.

An Roinn Dlí agus Cirt, Gnóthaí Baile agus Imirce
Department of Justice, Home Affairs and Migration
NCSC
An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

National Coordinator

The NCSC, through CSIRT-IE, will assume the role of the National Coordinator to facilitate the CVD process at a national level, and subject to its obligations at law:

- Act as an intermediary where the researcher is unable to contact an organisation or communication difficulties arise.
- Facilitate the anonymous reporting of a vulnerability if requested by the researcher. However, it should be noted that this anonymity is facilitated to encourage disclosure but does not provide legal protection against or limit an organisation's right to make a formal legal complaint against a researcher where the organisation deems same to be appropriate. For further information see the section on Legal Context of CVD in Ireland.
- Ensure follow-up action is carried out with regard to the reported vulnerability.
- Lead the coordination, in the event that a vulnerability is widespread impacting multiple organisations, is cross sectoral, or cross-border.
- In exceptional circumstances, may disclose a vulnerability publicly without the consent of the organisation if it is deemed necessary to protect the public interest.



An Roinn Dlí agus Cirt, Gnóthaí Baile agus Imirce
Department of Justice, Home Affairs and Migration
NCSC
An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

Obligations of Responsible Organisations

This section outlines the obligations of the responsible organisation when receiving and processing vulnerability reports in accordance with a coordinated vulnerability disclosure process. Organisations should follow these recommendations regarding communication, transparency and remediation to support the security of the Irish digital ecosystem. The NCSC strongly recommends that organisations create and publish a CVD policy, a sample template is provided in the Appendices.

Communication and Accessibility

A CVD policy can only be effective if discoverable by researchers and it is essential that organisations provide clear access to all available CVD information. A defined process that is adhered to will strengthen the relationship with the researcher.

- A CVD policy should be a clear, publicly accessible document and contain a number of core components, such as:
  - A brief statement welcoming reports and outlining a commitment to security.
  - Explicitly define which domains, products, or IP addresses are in-scope for testing, and which are not in scope.
  - An undertaking that the organisation will not pursue legal action against researchers acting in good faith and strictly within the scope of the CVD policy.
  - Clear instructions on how to submit a report (e.g. through a secure web form or a dedicated email address).
  - What the researcher can expect in terms of acknowledgment timelines, updates and rewards (if considered).
  - What is expected of the researcher such as not to disrupt services or publicise vulnerabilities until the organisation has had reasonable time to investigate/remediate.

- Organisations should publish their CVD contact details in a globally standardised (as per RFC 9116[3]) `security.txt` file. This file should be hosted in the `/.well-known/` directory of the organisation's primary domain.

- Define methods of reporting:
  - Provide a secure web form for a standardised and user-friendly reporting process.
  - or, provide a dedicated email address with an associated PGP Public Key for the encryption of submissions.
  - Respond to reports in accordance with the organisations defined timelines.

- Maintain transparent communications throughout the disclosure process, updating the researcher when appropriate.

[3] *RFC 9116: A File Format to Aid in Security Vulnerability Disclosure*
https://www.rfc-editor.org/info/rfc9116/

Scope and Exclusions

To maintain focus on high severity security flaws and control over the testing of their ICT systems, responsible organisations must explicitly define what is in-scope and out-of-scope for researcher activity and reporting. The following, non-exhaustive list, are the types of activities and reports that could be considered for exclusion, and an example of in-scope assets:

- Prohibited testing methods
  - Any testing that risks a degradation of services or system crashes e.g. DoS/DDoS.
  - Actions that risk the confidentiality or integrity of the organisations data.
  - Social engineering of employees, customers or any third parties.
  - Unauthorised physical access to all organisation related facilities, such as offices, data centres, etc.
  - Accessing data beyond what is necessary to prove the vulnerability.

- Assets in-scope for testing
  - Specify URL's or IP ranges owned by the organisation.
  - List public facing API's including those hosted on separate infrastructure.
  - Optional: Include a catch-all for any public facing assets owned or operated by the organisation to ensure forgotten/legacy systems are encompassed.

- Third-party systems and services
  - Explicitly exclude services used by the organisation but not owned by them.
  - Direct researchers to the CVD policies of the relevant third parties.

- Reporting exclusions
  - User interface (UI) and user experience (UX) bugs and spelling mistakes.
  - Version information of software without demonstrable exploit.
  - Reports from automated tools or scans.
  - Vulnerabilities related to out of date or unsupported browsers and plugins.

Remediation Lifecycle

The responsible organisation should establish a formal remediation workflow to ensure processing of vulnerability reports from receipt through to remediation. Which may include the following activities:

- Gather the data provided by the researcher, including technical details, logs, evidence etc. required to support the System Owner in recreating the vulnerability.
- Analysis of the report to identify the technical root cause of the reported vulnerability, to determine the impact to the ICT system, respective users and owners, and identify any other affected systems.
- Cross reference with previously submitted reports to assess the risk and severity of the vulnerability.
- Once the vulnerability is assessed, the organisation coordinates with the system owner and/or vendor/manufacturer to develop the required fix. The focus is on producing a patch, making a configuration change or establishing a temporary workaround to negate the threat until a fix is implemented.
- This may also include steps for retesting to ensure that the issue has been resolved. The organisation, system owner and vendor/manufacturer should commit to carrying out positive tests to verify that the solution works properly and negative tests to ensure that the solution does not disrupt the proper functioning of other existing functionalities.
- Manage the notification to all necessary third parties and the public disclosure of information regarding the vulnerability, ensuring a security notice or advisory is distributed with the fix, if required.
- Conduct a formal review of the internal CVD process to evaluate how the report was handled. Identify any issues and update the CVD policy or internal procedures to improve future responses.

Response Timelines

Establishing clear response timelines will provide transparency to the researcher by managing expectations for feedback and maintain a collaborative relationship, as appropriate. While a timely resolution is encouraged, varying remediation complexities means that organisations should define their own estimated timelines for all stages in their process.

- Acknowledgment on receipt of the report.
- Confirmation that the report is in-scope and a valid vulnerability.
- Vulnerability risk assessed and prioritised.
- Remediation planning and development of a fix.
- Testing and validation.
- Deployment and disclosure.

Disclosure

The purpose of disclosure is to inform system users, and the public, about a security risk only after a fix has been made available, with a view to preventing exploitation through 'zero-day' exploitation. The information provided in the disclosure should be informative and actionable.

- Avoid Non-Disclosure Agreements (NDAs) as this will actively discourage reporting and open collaboration. Both parties abiding by the published CVD Policy will build trust.
- All communication should be conducted through secure channels, ensuring that all information is encrypted and stored securely, to prevent unauthorised access.
- Once a report is submitted, the researcher should cooperate with the organisation, as required, allowing sufficient time for the remediation fix.
- Public disclosure should take place at the earliest possible time, together with the deployment of a solution and the distribution of a security notice to users.
- Researchers should only publish findings after a fix has been implemented, and only if the organisation explicitly gives authorisation.
- The organisation should commit to monitoring feedback from users on the deployment of the solution and to take the necessary corrective measures to address any issues with the solution, including compatibility with other products or services.

In complex cases and in the interests of national security, the NCSC may take additional actions in response to a reported vulnerability.

- If a vulnerability impacts multiple organisations or sectors, the NCSC may issue warnings and share information with key entities and authorities.
- In exceptional cases the NCSC may disclose vulnerabilities publicly without the organisation's consent if it serves the public interest and only if permitted by law.
- Prior to any public disclosure involving a third-party ICT system, the NCSC will make every effort to notify the affected party.

Confidentiality and Anonymous Reporting

The confidentiality of researchers should be protected by the responsible organisation, and their identity should not be disclosed to any third parties unless explicit consent is provided by the researcher. Trust is foundational to a successful CVD process, and it is encouraged that a CVD policy clearly states how this data is handled.

- All personal data of the researcher should be subject to strict data protection controls and in compliance with relevant data protection laws and regulations.
- If an organisation wants to credit a researcher, this should only be done if they have consented to this.
- A commitment that anonymous reports will be treated with the same priority as identified reports.
- Researchers wishing to report anonymously can do so through the NCSC, who will coordinate with the organisation on the researcher's behalf.

Rewards

A reward may be offered by the responsible organisation to the researcher upon discovering and reporting a vulnerability. This is at the discretion of the organisation and should be specified in the CVD policy.

An Roinn Dlí agus Cirt, Gnóthaí Baile agus Imirce
Department of Justice, Home Affairs and Migration

NCSC
An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

Reporting Requirements

To ensure an efficient process in handling a reported vulnerability, the responsible organisation should define the specific information it requires from a researcher. A high quality, detailed report can significantly assist the organisation in identifying/ reproducing the flaw, to quickly establish its impact and severity.

The organisation should request that a report contains at least the following information, where relevant:

Researcher Identity

- Researcher name or pseudonym.
- Contact information for follow-up and communicating updates.
- Confirmation that the research was conducted within the parameters of the CVD policy.

Technical Evidence

- A clear description of the vulnerability type.
- The technical context including details of affected IP addresses, URL's, API endpoints, software versions etc.
- A detailed explanation of the steps required to reproduce the vulnerability.
- Supporting evidence including screen shots/ recordings, scripts that demonstrate the issue.
- Assessment on potential impact of the vulnerability.

Research Methodology & Environment

- A summary of operations performed, to include any specific tools used.
- Dates and times of the testing, to assist the organisation in cross referencing internal logs.
- Details of the researcher's environment, such as operating system, browser version etc.
- Common Vulnerabilities and Exposures (CVE) number if applicable.

Impact Assessment & Mitigation

- Brief, non-technical, summary of findings and - potential risk to the organisation.
- Disclosure of any data accessed before research was terminated.
- If possible, the researcher should provide recommendations for a fix or temporary workaround.

An Roinn Dlí agus Cirt, Gnóthaí Baile agus Imirce
Department of Justice, Home Affairs and Migration
NCSC
An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

Legal Context of CVD in Ireland

The primary legislation in Ireland governing cybercrime activities is the Criminal Justice (Offences Relating to Information Systems) Act 2017 (the Act)[4]. Under this Act, several activities are classified as criminal offences if committed "without lawful authority,":

- Accessing information system (Section 2);
- Interference with information system or data (Sections 3 & 4);
- Intercepting transmission of data (Section 5); and
- Use of computer programme, password, code or data for purposes of section 2, 3, 4 or 5 (Section 6).

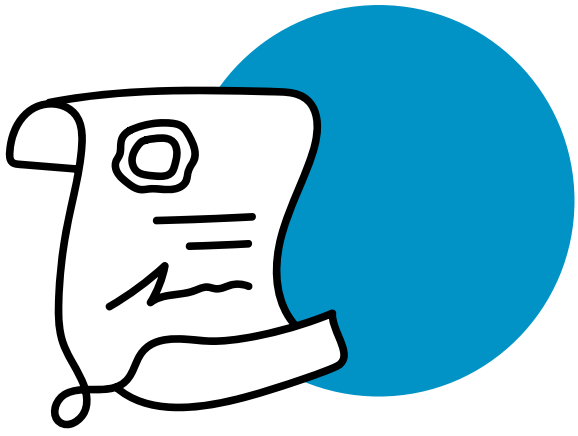
The Act provides that authorisation from the owner or a system or a right holder of a system can constitute "lawful authority" so an organisation can define what it considers to be "authorised activity" within its published CVD policy That provides a level of protection or a "Safe Harbour" for the activities of researchers carried out with "authority" of the organisation as set out in the CVD policy.

The concept of "Safe Harbour" is that an organisation publishing a CVD policy can provide a certain level of reassurance to researchers acting in good faith but only if their activities are limited to the confines of the authorisation specified in their CVD policy.

It is important to note that while the NCSC is publishing these Guidelines, the granting by the relevant organisation of "lawful authority" to access its information system for research activity is at the sole discretion of the relevant organisation concerned through its own published CVD policy. It is the published CVD policy of the organisation which must provide clear and unambiguous authorisation for such activities in order for a "Safe Harbour" to exist.

The National Coordinator will perform an initial non-technical assessment of a report to determine its admissibility and how it should be routed for coordination. They do not investigate researcher activity or conduct. The role is to assist organisations in receiving and thus addressing vulnerability reports. We encourage all parties to engage in the spirit of these Guidelines. However, researchers should note that while the National Coordinator acts as a neutral intermediary, it may be legally obliged to make a report to the appropriate authorities if in the course of facilitating a report it becomes aware of information that gives rise to a requirement under Section 19 of the Criminal Justice Act 2011 (as amended). This is particularly relevant where an organisation has no published CVD policy.

IMPORTANT: Appropriate legal advice should be sought by researchers in respect of the activities described under the Act so that they can be advised whether or not their proposed activities are lawful in light of the provisions of that Act and the details of a relevant organisation's CVD policy and the granting of this "lawful authority".



[4] *Criminal Justice (Offences Relating to Information Systems) Act 2017*
https://www.irishstatutebook.ie/eli/2017/act/11/enacted/en/html

Conclusion

Implementing a Coordinated Vulnerability Disclosure Policy represents a significant commitment to the security and integrity of Ireland's digital infrastructure. CVD can transform potential threats into opportunities for hardening ICT system security.

By providing a clear scope, maintaining transparent communication, and establishing "Safe Harbour" protections, organisations take ownership of the vulnerability lifecycle and empower researchers.

A mature CVD process fosters a culture of transparency and continuous improvement. Through the collaboration of researchers, organisations, and the NCSC, we can promote a more secure and resilient digital environment in Ireland.

NCSC Disclaimer

These Guidelines are intended to support awareness for organisations and researchers and to assist organisations in moving from a reactive to a proactive posture by embracing a suggested procedural framework for CVD, encouraging transparency, and cultivating a culture of vulnerability management. The Guidelines do not represent legal advice, regulatory direction, operational approval or risk acceptance. No part of these Guidelines should be interpreted as validation, endorsement, or confirmation that a particular approach, control set, or decision meets legal, regulatory, or supervisory requirements. Any examples, opinions, or suggested approaches shared here are illustrative in nature and are not a substitute for your own governance, assurance processes, or independent professional advice. Organisations and researchers remain solely responsible for their own security decisions, compliance obligations, and risk management outcomes.

These Guidelines may not be relied upon as evidence of compliance, organisational approval, or due diligence, and may not be cited as a defence, justification, or mitigating factor in any regulatory, audit, investigative, or enforcement context (including statements such as "this was approved" or "confirmed acceptable").

An Roinn Dlí agus Cirt, Gnóthaí Baile agus Imirce
Department of Justice, Home Affairs and Migration

NCSC
An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

Appendices

Appendix 1
Sample CVD Policy Template

This sample CVD policy template is intended to assist organisations in creating a Coordinated Vulnerability Disclosure Policy (CVDP). It should be published and branded, as appropriate, as the organisation's own document whether on the organisation's headed PDF or within a dedicated security page on the organisation's website. As a sample template it is strongly recommended that organisations intending to use this template should amend it to address their own specific circumstances and processes. Organisations are also advised that they should seek their own legal advice when preparing their CVD policy.

Last updated: **[Date of latest revision]**

1. Introduction

At **[Organisation Name],** the security of our systems and the privacy of our users are of paramount importance. We value the work of the security research community and believe that a collaborative relationship with researchers is vital to maintaining a resilient digital environment.

This policy outlines our commitment to investigating reported vulnerabilities and provides a framework for researchers to report their findings to us in a responsible and coordinated manner.

2. Safe Harbour

[Organisation Name] will not initiate legal action against any individual or entity that conducts security research and discloses vulnerabilities to us in accordance with this policy. We consider any activity conducted in good faith and within the defined scope of this policy to be activity carried out with our authority and therefore to be "lawful authority" under the Criminal Justice (Offences Relating to Information Systems) Act 2017. That said, ultimately it is a matter for any individual or entity to obtain its own independent legal advice to satisfy itself as to the lawfulness of its intended activities to ensure that no criminal offence under the Criminal Justice (Offences Relating to Information Systems) Act 2017 would be committed.

We waive any claims against researchers for accidental, good-faith violations of this policy, provided that the researcher ceases activity immediately upon discovering the violation and contacts us.

3. Scope

This policy applies to the following systems and services:

- In-Scope:
  - *.example.com (All subdomains)
  - **[Specify internet facing IP ranges]**
  - **[Specify mobile applications/hardware models]**
- Out-of-Scope:
  - Any third-party services used by us (e.g., Microsoft 365, AWS, Zendesk).
  - **[Specify any sensitive production systems to be excluded]**

4. Prohibited Activities & Exclusions

To ensure system stability and user privacy, any testing that impacts system Confidentiality, Integrity, and/or Availability is strictly prohibited. This includes, but is not limited to:

- Denial of Service (DoS/DDoS).
- Social Engineering: Phishing or physical security attacks against staff, vendors, or customers.
- Data Destruction: Deleting, altering, or corrupting data not owned by the researcher.
- Privacy Violations: Accessing or retaining Personal Identifiable Information (PII) beyond what is strictly necessary to prove a flaw.

Standard Technical Exclusions (Reports not eligible for credit):

- Reports of missing security headers (e.g. CSP, HSTS, X-Frame-Options) without a working exploit.
- SSL/TLS best practices (e.g. weak ciphers, expired certificates).
- Reports from automated scanners that have not been manually verified.
- “Banner grabbing” or version disclosure without a functional Proof of Concept (PoC).

5. Researcher Obligations

We ask that researchers:

- Report Promptly: Notify us as soon as a potential vulnerability is discovered.
- Provide Detail: Use our Vulnerability Report Template to provide clear, technical reproduction steps.
- Maintain Confidentiality: Do not disclose any information regarding the vulnerability to third parties or the public until a fix has been deployed and we have provided explicit written authorisation.
- The “Stop Rule”: If you encounter sensitive data (PII, financial data), you must stop testing immediately, report the find, and securely delete any local copies.

6. Our Commitment (Remediation Lifecycle)

When you report a vulnerability to **[Organisation Name]**, we commit to:

- Acknowledgment: Confirming receipt of your report within **[2-3]** business days.
- Verification: Updating you once the flaw has been verified and triaged.
- Remediation: Working to resolve the issue based on a risk-based priority (Critical, High, Medium, Low).
- Recognition: Crediting you in our **[Security Hall of Fame / Release Notes]** upon successful remediation, should you wish to be named.

7. How to Report

Please submit your findings via one of the following secure channels:

- Secure Web Form: **[Link to form]**
- Encrypted Email: **[security@example.com]**
- PGP Key ID: **[Insert Key ID]**
- PGP Fingerprint: **[Insert Fingerprint]**

Appendix 2
CVD Readiness Checklist

In advance of publishing a CVD policy, the following checklist may assist in implementing the necessary operational and governance processes necessary for a successfully CVD program.

Governance

- ☐ Are the “in-scope” and “out-of-scope” assets (domains, IPs, products, etc.) clearly listed?
- ☐ Have you identified the system owners for each asset, and who manages relevant vendor interactions?
- ☐ Does your CVD policy include a clear “Safe Harbour” statement?
- ☐ Has the CVD policy been reviewed by your legal/compliance team?

Communication Channels

- ☐ Is your CVD policy discoverable through a security.txt file?
- ☐ Have you provided a secure webform or a PGP encrypted email address for reports?
- ☐ Is there a process to acknowledge receipt of a report within a reasonable timeframe (2 business days suggested)?
- ☐ Does the team know how to process anonymous reports, or those made using the NCSC as an intermediary?

Remediation Workflow

- ☐ Is there a technical team ready to triage, verify and assign a severity to reports?
- ☐ Are there adequate testing protocols to validate fixes and verify regression?
- ☐ Is the team aware of providing appropriate updates to the researcher at key milestones?

Compliance & Disclosure

- ☐ Are there appropriate templates and channels established, for issuing security advisories?
- ☐ Have you considered NIS2 risk management and CRA vulnerability handling requirements?

An Roinn Dlí agus Cirt, Gnóthaí Baile agus Imirce
Department of Justice, Home Affairs and Migration
NCSC
An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

Appendix 3
security.txt

A `security.txt` file is a plain-text file placed in the `/.well-known/` directory of a website to allow security researchers to easily find contact information for reporting vulnerabilities.

e.g. https://example.com/.well-known/security.txt

It is recommended that the `security.txt` file is digitally signed using an OpenPGP cleartext signature and that organisations use the "Canonical" field, thus allowing the digital signature to authenticate the location of the file.

For further detailed information on `security.txt` (and the RFC9116 standard) see: https://www.rfc-editor.org/rfc/rfc9116.

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256
# --- Security Disclosure Information ---

# REQUIRED Contact: Where to report - email or web form
Contact: mailto:security@example.com
Contact: https://www.example.com/security/report

# REQUIRED Expires: When data contained in this file is considered stale and should not be used.
Expires: 2027-01-28T12:00:00.000Z

# OPTIONAL Canonical: Location of security.txt for digital signature authentication - RECOMMENDED when using digital signature
Canonical: https://example.com/.well-known/security.txt

# OPTIONAL Policy: Link to the CVD Policy
Policy: https://www.example.com/security/policy

# OPTIONAL Encryption: Link to a PGP key so reports can be sent securely
Encryption: https://www.example.com/pgp-key.asc
```

Appendix 3
security.txt (continued)

```
# OPTIONAL Acknowledgments: Link to a page where security researchers are recognised for their reports and collaboration.

Acknowledgements: https://www.example.com/security/hall-of-fame


# OPTIONAL Preferred-Languages: Preferred reporting languages - comma separated

Preferred-Languages: en, ga


-----BEGIN PGP SIGNATURE-----

...signature...


-----END PGP SIGNATURE-----
```

Contact Details

National Cyber Security Centre, Tom Johnson House,
Haddington Road, Dublin 4, Ireland, D04 K7X4

contact@ncsc.gov.ie

+353 1 6782333

www.ncsc.gov.ie

An Roinn Dlí agus Cirt,
Gnóthaí Baile agus Imirce
Department of Justice,
Home Affairs and Migration

An Lárionad Náisiúnta
Cibearshlándála
National Cyber
Security Centre