5.9. Vulnerability Disclosure Policy (VDP)

Objective

5.9.1. Agencies implement a Vulnerability Disclosure Policy (VDP) to enable members of the public to report vulnerabilities in the agency's public-facing systems and applications and receive feedback on such reports.

Context

Scope

5.9.2. This section provides information on vulnerability disclosure for all externally-facing agency systems, including public-facing systems. Vulnerability disclosure relating to internal systems is covered in Chapter 12 – Product Security.

5.9.3. When selecting which systems, applications and data are within scope of a VDP, agencies may consider:

a. The sensitivity of information on the agency's systems, including financial data, medical information, proprietary information, customer data or other personal information.
b. Security safeguards that are already in place on the system, such as encryption of data at rest.
c. The agency's ability to segment its network or otherwise segregate sensitive information stored on its systems.
d. Regulatory, contractual, privacy or other restrictions placed on disclosure of protected classes of information (such as within the New Zealand Classification System).

5.9.4. Reference to other chapters and sections in this document is essential. In particular:

- Chapter 4 - System Certification and Accreditation;
- Chapter 5 – Information Security Documentation;
- Section 6.2 - Vulnerability Analysis;
- Section 6.3 - Change Management;
- Chapter 7 – Information Security Incidents;
- Section 12.4 – Product Patching and Updating;
- Chapter 14 - Software Security.

Agencies must expect vulnerabilities

5.9.5. Invariably all software, operating systems and applications have the potential to house exploitable vulnerabilities. Many vulnerabilities are identified by users and other third parties. Some vulnerabilities may be undiscovered or inherent in the application or software. Others may be introduced during upgrades, patches, configuration or other changes.

5.9.6. It is essential that agencies establish a policy and processes to identify and remediate such vulnerabilities.

Agencies must establish a vulnerability reporting mechanism

5.9.7. Published VDPs demonstrate that an agency has a mature and constructive approach when they receive a vulnerability report and also demonstrates openness and transparency in the management of agency systems.

5.9.8. Agencies should establish a process to allow any user (whether a member of the public, business partners, other agencies or agency staff), to report potential vulnerabilities. Any such reporting is on a "no blame" basis, without fear of repercussion or penalty, provided the agency's disclosure policy is followed and no illegal activity is undertaken.

5.9.9. The VDP must clearly state the conditions under which reports are received. In general terms this also includes a "no bug bounty" clause as well as limits on web site, system or application probing.

5.9.10. An agency's VDP will necessarily reflect that they may not control or own all of the software they use or the maintenance and development of underlying software (such as compilers, programming or scripting languages and so on). The VDP should clearly state that while the agency can receive reports about software, systems or services run on their behalf by third parties, providers or vendors, they may have to work with the reporting party to report the vulnerability to the relevant vendor.

5.9.11. Where specific legislation applies, for example a reported vulnerability may breach the Privacy Act, agencies must adhere to the legislation. This may change how reports are managed and action communicated to the finder or reporter. This does not change the requirement to maintain communication with the reporter/finder.

Agencies are expected to find and remediate vulnerabilities

5.9.12. The Protective Security Requirements places clear expectations on agencies to maintain awareness of vulnerabilities (see mandatory requirement INFOSEC4).

5.9.13. The NZISM section 12.4 - Patching & updating sets out expectations and controls to ensure security patches are applied in a timely manner.

5.9.14. The disclosure period commonly used by many vendors, manufacturers and government agencies is 90 days. Vulnerabilities will be either patched, mitigated or managed within this period. In some cases earlier notification is provided to allow users to take mitigating actions until a patch or other solution is available.

5.9.15. VDPs are expected to include a timeframe within which patches will be applied or remedial action taken when a vulnerability is reported to the agency.

Agencies to create a vulnerability reporting point

5.9.16. When security risks in agency services are discovered and reported to the agency, it is vital that a robust communication channel is available to receive the report.

5.9.17. This is commonly described as a "security.txt". A draft standard has been published (see References below) to help agencies (and other organisations) outline a process for security researchers to securely report security vulnerabilities.

Vulnerability disclosure policies are a normal part of learning about and patching vulnerabilities

5.9.18. Vulnerability disclosure (sometimes also referred to as responsible disclosure or coordinated vulnerability disclosure) is now an internationally accepted practice for technology organisations. The practice of vulnerability disclosure in modern computing dates to the late 1980s. There are related examples (non-computing) which appeared in the mid-1800s when locksmiths exchanged vulnerability information.

Bug Bounties

5.9.19. "Bug bounties" are a monetary reward to security researchers for the discovery and reporting of software and other information system vulnerabilities to the agency. Bug Bounties are separate to VDPs and should only be covered if the agency has a bug bounty programme in place.

Vulnerability disclosure policy (VDP) Content

5.9.20. A VDP will typically include:

- A scoping statement setting out which systems the policy applies to (e.g. the agency's website and other public-facing systems);
- Details of how finders can contact the agency's security team (including any public keys for encrypting reports);
- Permitted activities;
- Acknowledgement of reports and a response time (typically 60 or 90 days) for corrections, adjustments, or other "fixes";
- Reporters/finders agreeing to not share information about the vulnerability until the end of the disclosure period, to let the organisation fix the issues before it becomes public;
- Illegal activities are not permitted (specifying any relevant legislation, such as the Crimes Act, the Privacy Act etc.); and
- Either a statement that bug bounties will not be paid for any discoveries, or information about the agency's bug bounty programme.

References

5.9.21. Additional information relating to system auditing is contained in:

Reference	Title	Publisher	Source
ISO 29147	Information technology — Security techniques — Vulnerability disclosure	ISO	https://www.iso.org/standard/72311.html
ISO 30111	Information technology — Security techniques — Vulnerability handling processes	ISO	https://www.iso.org/standard/69725.html
IEFT draft protocol for Security.txt	A File Format to Aid in Security Vulnerability Disclosure	ITEF	https://datatracker.ietf.org/doc/draft-foudil-securitytxt
	A proposed standard which allows websites to define security policies	security.txt	https://securitytxt.org/
	CERT NZ coordinated vulnerability disclosure policy	CERT NZ	https://www.cert.govt.nz/it-specialists/guides/reporting-a-vulnerability/cert-nz-coordinated-vulnerability-disclosure-policy/
	NZITF Coordinated Disclosure guidelines	NZITF	https://nzitf.org.nz/coordinated-disclosure
BOD 20-01	Binding Operational Directive 20-01: Develop and Publish a Vulnerability Disclosure Policy	US Department of Homeland Security	https://cyber.dhs.gov/bod/20-01/
	Vulnerability Disclosure Policy Template	US Department of Homeland Security	https://cyber.dhs.gov/bod/20-01/vdp-template/
	CISA announces new vulnerability disclosure policy (VDP) platform, July 2021	US Cybersecurity & Infrastructure Security Agency	https://www.cisa.gov/blog/2021/07/29/cisa-announces-new-vulnerability-disclosure-policy-vdp-platform
	CISA Coordinated Vulnerability Disclosure (CVD) Process	US Cybersecurity & Infrastructure Security Agency	https://www.cisa.gov/coordinated-vulnerability-disclosure-process
List of US Federal agencies VDPs	VDPs in the US Government's executive branch	CISA	https://github.com/cisagov/vdp-in-fceb
	A Framework for a Vulnerability Disclosure Program for Online Systems1 Version 1.0 (July 2017)	Cybersecurity Unit Computer Crime & Intellectual Property Section Criminal Division U.S. Department of Justice	https://www.justice.gov/criminal-ccips/page/file/983996/download
	Vulnerability Disclosure Toolkit	NCSC UK	https://www.ncsc.gov.uk/information/vulnerability-disclosure-toolkit
	See Something, Say Something - Coordinating the Disclosure of Security Vulnerabilities in Canada	Canada – Cybersecure policy exchange	https://www.cybersecurepolicy.ca/vulnerability-disclosure
	Vulnerability Disclosure Cheat Sheet	OWASP	https://cheatsheetseries.owasp.org/cheatsheets/Vulnerability_Disclosure_Cheat_Sheet.html

	Responsible Disclosure Policy Example	Dutch National Cyber Security Centre (NCSC)	https://responsibledisclosure.nl/en/
	Vulnerability disclosure policy	Incibe Cert (Spain)	https://www.incibe-cert.es/en/what-is-incibe-cert/vulnerability-disclosure-policy
	Vulnerability disclosure policy	Office of the Privacy Commissioner New Zealand	https://www.privacy.org.nz/assets/New-order/About-us/Transparency-and-accountability-/Vulnerability-Disclosure-Policy-December-2015.pdf
	Responsible disclosure guidelines	NZ – The Ministry of Social Development	https://www.msd.govt.nz/about-msd-and-our-work/tools/responsible-disclosure-guidelines.html
	Ministry of Health Responsible disclosure guidelines	NZ – Ministry of Health	https://www.health.govt.nz/our-work/digital-health/digital-health-sector-architecture-standards-and-governance/responsible-disclosure-guidelines
	Vulnerability disclosure policy	Bank of England	https://www.bankofengland.co.uk/vulnerability-disclosure-policy
	Vulnerability disclosure policy	Crown Commercial Service (UK)	https://www.crowncommercial.gov.uk/about-ccs/vulnerability-disclosure-policy/
	Vulnerability Disclosure Policy	Met Office (UK)	https://www.metoffice.gov.uk/about-us/legal/vulnerability-disclosure-policy
	History of Vulnerability Disclosure, 3 August 2015	Duo	https://duo.com/labs/research/history-of-vulnerability-disclosure

PSR References

5.9.22. Relevant PSR requirements can be found at:

Reference	Title	Source
PSR Mandatory Requirements	GOV3, INFOSEC1, INFOSEC2, INFOSEC3 and INFOSEC4	Home | Protective Security Requirements Security governance (GOV) | Protective Security Requirements Information security (INFOSEC) | Protective Security Requirements

Rationale & Controls

Vulnerability disclosure policy (VDP) Risk Assessment

5.9.23.R.01. **Rationale**

Selection of public-facing systems and services included in any VDP will be based on a risk assessment undertaken by the agency. Considerations for such selection are discussed in the Context section above.

5.9.23.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:7130]

An agency MUST undertake a risk assessment to determine which systems and services to include in the agency's VDP.

Vulnerability disclosure policy (VDP) Essential Content

5.9.24.R.01. **Rationale**

In order to demonstrate a mature and constructive approach to vulnerability discovery, management and remediation, an agency requires a VDP to inform the public about:

- the scope of public-facing systems covered by its VDP; and
- the nature of vulnerabilities which can be reported under its VDP.

5.9.24.R.02. **Rationale**

To aid consistency, it is important that government agencies have a core set of content in their VDP.

5.9.24.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:7133]

An agency MUST develop and publish a VDP.

5.9.24.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:7134]

An agency's VDP MUST contain at least the following core content:

- A scoping statement listing the systems the policy applies to;
- Contact details;
- Secure communication options (including any public keys);
- Information the finder should include in the report;
- Acknowledgement of reports and a response time;
- Guidance on what forms of vulnerability testing are out of scope for reporters/finders (permitted activities);
- Reporters/finders agreeing to not share information about the vulnerability until the end of the disclosure period, in order to allow the agency to address any issues before they become public;
- Illegal activities are not permitted (specifying the relevant legislation, such as the Crimes Act); and
- Either that "Bug bounties" will not be paid for any discoveries, or it should provide information about the agency's bug bounty programme.

Vulnerability disclosure policy (VDP) Additional Content

5.9.25.R.01. **Rationale**

As well as mandatory content listed above, additional information that agencies may consider providing includes guidance for reporters/finders to locate the agency's policy and how to confidentially communicate technical details to the agency's security experts.

5.9.25.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:7136]

An agency SHOULD publish a security.txt to permit secure communications and direct any reports to a specific agency resource, in accordance with the agency's VDP.

Vulnerability disclosure policy (VDP) Setting Expectations

5.9.26.R.01. **Rationale**

Agencies must set clear expectations for reporters/finders on the timeframe within which agencies intend to address and remediate vulnerabilities that have been reported to them. The industry standard for a vulnerability disclosure policy is 90 days.

5.9.26.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:7138]

An agency MUST commit to addressing disclosed vulnerabilities within the timeframe it sets in its policy.

5.9.26.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:7139]

An agency's vulnerability disclosure timeframe SHOULD be set to no more than 90 days.

Vulnerability disclosure policy (VDP) Integration

5.9.27.R.01. **Rationale**

It is essential that a VDP is integrated and consistent with an agency's information security documentation and its policies, processes and procedures for Incident Management, Product Security and Software Security (Chapters 5, 7, 12, 14).

5.9.27.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:7141]

Agencies MUST ensure they integrate their VDP with other elements of their information security policies.