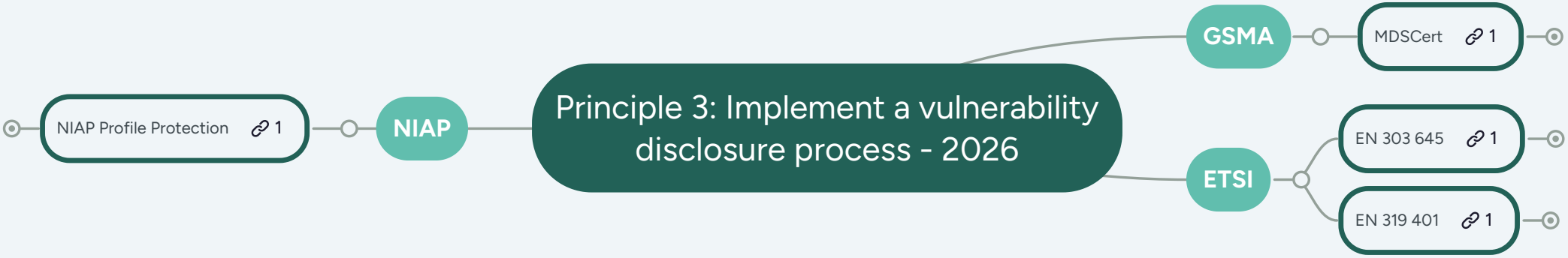
Principle 3: Implement a vulnerability disclosure process - 2026
NIAP
NIAP Profile Protection 1
GSMA
MDSCert 1
ETSI
EN 303 645 1
EN 319 401 1

Principle 3: Implement a vulnerability disclosure process - 2026

1. GSMA

1.1. MDSCert

Link: https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2025/02/FS.56-v1.0.pdf

Link: https://www.gsma.com/solutions-and-impact/technologies/security/wp-content/uploads/2025/02/FS.56-v1.0.pdf

1.1.1. ALC_CMS.2.2E

> The evaluator shall confirm that for external software components, the developer shall include the source and original maintainer of the component.

1.1.2. ALC_FLR.3.5D

> The developer shall provide a public vulnerability disclosure program to provide security bulletins about the flaws that have been remediated.

1.1.3. ALC_FLR.3.6D

> The developer shall establish procedures for ensuring that no known security vulnerabilities rated as High and Critical (e.g. as classified in public databases) are included in the TOE at public release.

1.1.4. ALC_FLR.3.14C

> The flaw remediation procedures documentation shall describe the process for publicly releasing security flaw remediation information, including the location(s) where this will be publicly available.

1.1.5. ALC_FLR.3.15C

> The flaw remediation procedures documentation shall describe the process for verifying known security flaws are not propagated into a new (not yet released) TOE.

2. ETSI

2.1. EN 303 645

Link: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf

Link: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf

2.1.1. Principle 5.2-1

The manufacturer shall make a vulnerability disclosure policy publicly available. This policy shall include, at a minimum:
• contact information for the reporting of issues; and
• timelines for initial acknowledgement of receipt of a vulnerability report; and
• timelines for when the person who reported the issue will receive status updates until the resolution of the reported issues.

NOTE 2: Different notations are possible to describe time values in the timetable (e.g. "7 days", "quickly", etc.). ETSI TR 103 838 [i.30] contains an example for a vulnerability disclosure policy including timelines for initial acknowledgement of receipt and a proposal for information on timelines for status updates until the resolution of the reported issues. The time needed to find a solution can vary depending e.g. on the criticality of the disclosed vulnerability.

A vulnerability disclosure policy clearly specifies the process through which security researchers and others are able to report issues. Such policy can be updated as necessary to further ensure transparency and clarity in the dealings of the manufacturer with security researchers, and vice versa.

Coordinated Vulnerability Disclosure (CVD) is a set of processes for dealing with disclosures about potential security vulnerabilities and to support the remediation of these vulnerabilities. CVD is standardized by the International Organization for Standardization (ISO) in the ISO/IEC 29147 [i.4] on vulnerability disclosure. Moreover, a guide to CVD is given in ETSI TR 103 838 [i.30]. CVD has been proven to be successful in some large software companies around the world. Multi-Party Coordinated Vulnerability Disclosure (MPCVD) refers to the application of CVD in a multi-stakeholder scenario, for example when products from multiple manufacturers are affected by the same vulnerability. Manufacturers can refer to the guidelines from ISO/IEC TR 5895 [i.33] and FIRST [i.32] to adapt their CVD processes accordingly.

In the IoT industry, CVD is currently not well-established [i.16] as some companies are reticent about dealing with security researchers. Here, CVD provides companies a framework to manage this process. This gives security researchers an avenue to inform companies of security issues, puts companies ahead of the threat of malicious exploitation and gives companies an opportunity to respond to and resolve vulnerabilities in advance of a public disclosure.

2.1.2. Principle 5.2-2

> Disclosed vulnerabilities should be acted on in a timely manner.
>
> A "timely manner" for acting on vulnerabilities varies considerably and is incident-specific; however, conventionally, the vulnerability management process is following a properly documented process including clear responsibilities and completed within 90 days for a software solution, including availability of patches and notification of the issue. A hardware fix can take considerably longer to address than a software fix. Additionally, a fix that has to be deployed to devices can take time to roll out compared with a server software fix.

2.1.3. Principle 5.2-3

> Manufacturers should continually monitor for, identify and rectify security vulnerabilities within consumer IoT products they sell, produce, have produced and associated services they operate during the defined support period.
>
> NOTE 3: Manufacturers are expected to exercise due care for all software and hardware components used in the product, this includes due care related to the selected third parties that provide associated services to support the functions of the product.
>
> Software solutions often contain open source and third party software components. Creating and maintaining list of all software components and their sub-components is a pre-requisite to be able to monitor for product vulnerabilities. Various tools exist to scan source code and binaries and build a so-called Software Bill Of Materials (SBOM), which identifies third party components and the versions used in the product. This information is then used to monitor for the associated security and licensing risks of each identified software component.
>
> Vulnerabilities are expected to be reported directly to the affected stakeholders in the first instance. If that is not possible, vulnerabilities can be reported to national authorities. Manufacturers are also encouraged to share information with competent industry bodies, such as the GSMA [i.21] and the IoT Security Foundation. Guidance on Coordinated Vulnerability Disclosure is available from the IoT Security Foundation [i.22] which references ISO/IEC 29147 [i.4].
>
> The management of vulnerabilities is expected to be performed for devices within their defined support period. However, manufacturers can continue this outside that period and release security updates to rectify vulnerabilities.

2.2. EN 319 401

Link: https://www.etsi.org/deliver/etsi_en/319400_319499/319401/03.02.00_20/en_319401v030200a.pdf

Link: https://www.etsi.org/deliver/etsi_en/319400_319499/319401/03.02.00_20/en_319401v030200a.pdf

2.2.1. REQ-7.9.2-10

For any vulnerability, given the potential impact, the TSP shall [CHOICE]:
- create and implement a plan to mitigate the vulnerability; or
- document the factual basis for the TSP's determination that the vulnerability does not require remediation.

EXAMPLE 2: The TSP can determine that the vulnerability does not require remediation when the cost of the potential impact does not warrant the cost of mitigation.

2.2.2. REQ-7.9.2-11

Incident reporting and response procedures shall be employed in such a way that damage from security incidents and malfunctions are minimized.

2.2.3. REQ-7.9.2-12

The TSP shall appoint trusted role personnel to follow up on alerts of potentially critical security events and ensure that relevant incidents are reported in line with the TSP's procedures.

2.2.4. REQ-7.9.2-15

The TSP shall respond to incidents in accordance with documented procedures and in a timely manner.

2.2.5. REQ-7.9.2-16

The incident response procedures shall include the following stages:
a) incident containment, to prevent the consequences of the incident from spreading;
b) eradication, to prevent the incident from continuing or reappearing;
c) recovery from the incident, where necessary.

2.2.6. REQ-7.9.2-17

The TSP shall establish communication plans and procedures:
a) with the Computer Security Incident Response Teams (CSIRTs) or, where applicable, the competent authorities, related to incident notification;
b) for communication among staff members of the TSP, and for communication with relevant stakeholders external to the TSP.

2.2.7. REQ-7.9.2-18

The TSP shall log incident response activities in accordance with the monitoring and logging procedures, and record evidence.

2.2.8. REQ-7.9.2-19

The TSP shall test at planned intervals their incident response procedures.

2.2.9. REQ-7.9.3-01

The TSP shall establish procedures to notify the appropriate parties in line with the applicable regulatory rules of any breach of security or loss of integrity that has a significant impact on the trust service provided and on the personal data maintained therein within 24 hours of the breach being identified.

2.2.10. REQ-7.9.3-05

The TSP shall put in place a simple mechanism allowing their employees, suppliers, and customers to report suspicious events.

2.2.11. REQ-7.9.4-01

The TSP shall analyse the reported events and assess their severity.

2.2.12. REQ-7.9.4-03

The TSP shall assess suspicious events to determine whether they constitute incidents and, if so, determine their nature and severity.

2.2.13. REQ-7.9.5-02

The TSP shall evaluate the TSP's exposure to such vulnerabilities and take appropriate measures.

2.2.14. REQ-7.9.5-03

The TSP shall identify the root cause of an incident and shall conduct a post-incident review possibly resulting in measures mitigating the risk of the recurrence of similar incidents.

2.2.15. REQ-7.9.5-04

The TSP shall ensure that each past incident led to a post-incident review.

2.2.16. REQ-7.9.5-05

Where appropriate, the TSP may carry out post-incident reviews after recovery from incidents.

2.2.17. REQ-7.9.5-06

The post-incident reviews shall, if carried out, identify, where possible, the root cause of the incident and result in documented lessons learned to reduce the occurrence and consequences of future incidents.

2.2.18. REQ-7.9.5-07

The TSP shall ensure that post-incident reviews contribute to improving their approach to network and information security, to risk treatment measures, and to incident handling, detection and response procedures.

2.2.19. REQ-7.9.5-08

The TSP shall review at planned intervals if incidents led to post-incident reviews.

2.2.20. REQ-7.10-01

The TSP shall record and keep accessible for an appropriate period of time, including after the activities of the TSP have ceased, all relevant information concerning data issued and received by the TSP, in particular, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service.

3. NIAP

3.1. NIAP Profile Protection

Link: https://www.niap-ccevs.org/static_html/protection-profile/516/PP_APP_V2.0.htm

Link: https://www.niap-ccevs.org/static_html/protection-profile/516/PP_APP_V2.0.htm

3.1.1. Basic Flaw Remediation ALC_FLR.1.1D

> The developer shall document and provide flaw remediation procedures addressed to TOE developers.

3.1.2. ALC_FLR.1.1C

> The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

3.1.3. ALC_FLR.1.2C

> The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

3.1.4. ALC_FLR.1.3C

> The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

3.1.5. ALC_FLR.1.4C

> The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

3.1.6. ALC_FLR.1.1E

> The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

3.1.7. ALC_FLR.2.1D

> The developer shall document and provide flaw remediation procedures addressed to TOE developers.

3.1.8. ALC_FLR.2.2D

The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.

3.1.9. ALC_FLR.2.3D

The developer shall provide flaw remediation guidance addressed to TOE users.

3.1.10. ALC_FLR.2.1C

The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

3.1.11. ALC_FLR.2.2C

The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

3.1.12. ALC_FLR.2.3C

The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

3.1.13. ALC_FLR.2.4C

The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

3.1.14. ALC_FLR.2.5C

The flaw remediation procedures shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.

3.1.15. ALC_FLR.2.6C

The procedures for processing reported security flaws shall ensure that any reported flaws are remediated and the remediation procedures issued to TOE users.

3.1.16. ALC_FLR.2.7C

The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.

3.1.17. ALC_FLR.2.8C

The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.

3.1.18. ALC_FLR.2.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

3.1.19. ALC_FLR.3.1D

The developer shall document and provide flaw remediation procedures addressed to TOE developers.

3.1.20. ALC_FLR.3.2D

The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.

3.1.21. ALC_FLR.3.3D

The developer shall provide flaw remediation guidance addressed to TOE users.

3.1.22. ALC_FLR.3.1C

The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.

3.1.23. ALC_FLR.3.2C

The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

3.1.24. ALC_FLR.3.3C

The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.

3.1.25. ALC_FLR.3.4C

The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

3.1.26. ALC_FLR.3.5C

The flaw remediation procedures shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.

3.1.27. ALC_FLR.3.6C

The flaw remediation procedures shall include a procedure requiring timely response and the automatic distribution of security flaw reports and the associated corrections to registered users who might be affected by the security flaw.

3.1.28. ALC_FLR.3.7C

The procedures for processing reported security flaws shall ensure that any reported flaws are remediated and the remediation procedures issued to TOE users.

3.1.29. ALC_FLR.3.8C

The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.

3.1.30. ALC_FLR.3.9C

The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.

3.1.31. ALC_FLR.3.10C

The flaw remediation guidance shall describe a means by which TOE users may register with the developer, to be eligible to receive security flaw reports and corrections.

3.1.32. ALC_FLR.3.11C

The flaw remediation guidance shall identify the specific points of contact for all reports and enquiries about security issues involving the TOE.

3.1.33. ALC_FLR.3.1E

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.