

	<h1 style="margin: 0;">Vulnerability Handling for EUCC</h1>	Document:	TB-VH-01-01
	Revision:	2.0	
	Date issued:	DD-MM-YYYY	
	Owner:	To be determined	
	Page:	1 of 17	

1. Purpose

This document defines how the ITSEF identifies, analyses, documents, and reports vulnerabilities relevant to EUCC-certified ICT products and how it supports the CB in vulnerability handling, reassessment, and coordinated vulnerability disclosure activities where requested.

This document implements the ENISA EUCC Guidelines on Vulnerability Management and Disclosure as they apply to the ITSEF's role within the broader EUCC vulnerability handling and certificate maintenance process.

2. Scope

This document applies to the ITSEF's role in:

- EUCC evaluations, including initial evaluations, re-evaluations, and delta evaluations
- Vulnerabilities identified during evaluation
- Post-certification vulnerabilities referred to the ITSEF by the CB for technical analysis or reassessment support
- Vulnerabilities identified through public or coordinated disclosure channels where technical evaluation input is requested

3. Roles and Responsibilities

Role	Responsibility
Certificate holder (product manufacturer, vendor, etc.)	<ul style="list-style-type: none"> • Maintain documented vulnerability handling and disclosure procedures • Provide and maintain a channel for receiving vulnerability reports • Verify, triage, and assess vulnerabilities affecting the certified product • Notify the CB of relevant vulnerabilities and proposed remediation where certification claims may be affected • Cooperate with monitoring, reassessment, and coordinated disclosure activities



	<h1 style="margin: 0;">Vulnerability Handling for EUCC</h1>	Document: TB-VH-01-01
	Revision: 2.0	
	Date issued: DD-MM-YYYY	
	Owner: To be determined	
	Page: 2 of 17	

Role	Responsibility
Certification body (CB)	<ul style="list-style-type: none"> • Monitor certified products for vulnerabilities relevant to certificate maintenance • Require and review vulnerability information, impact analysis, and remediation evidence from the certificate holder • Request technical support from the ITSEF where reassessment is needed • Assess certificate impact and decide on certificate status actions (maintain, restrict, suspend, withdraw) • Coordinate with the NCCA and other competent parties where required under applicable rules
Evaluation facility (ITSEF) where applicable	<ul style="list-style-type: none"> • Support the CB with technical analysis of vulnerability relevance and impact • Perform reassessment against the Security Target, Protection Profile, and evaluated TOE configuration where requested • Document technical findings and provide evidence to support CB decisions • Provide technical input to coordinated vulnerability disclosure activities where requested, without assuming responsibility for disclosure decisions
National Cybersecurity Certification Authority (NCCA)	<ul style="list-style-type: none"> • Acts as the national competent authority for cybersecurity certification oversight • May be involved in coordinated vulnerability disclosure and communication in accordance with national arrangements and applicable EUCC rules • Coordinates with the CB and other competent parties where escalation, oversight, or national coordination is required
CSIRT / designated vulnerability disclosure coordinator	<ul style="list-style-type: none"> • May support coordinated vulnerability disclosure by facilitating communication between relevant parties • May coordinate disclosure timelines, case handling, or communication where designated to do so • May work with the CB, NCCA, certificate holder, and other competent parties where escalation or coordinated handling is required

Where coordinated vulnerability disclosure is required, a CSIRT or other designated coordinator may facilitate communication and case coordination between the certificate

	<h1 style="margin: 0;">Vulnerability Handling for EUCC</h1>	Document:	TB-VH-01-01
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	3 of 17

holder, the CB, the ITSEF, the NCCA, and other competent parties in accordance with applicable arrangements.

4. Process Overview

- Vulnerability handling begins with the identification or notification of a vulnerability affecting a certified product.
- The certificate holder receives and assesses vulnerability reports and notifies the CB where certification claims may be affected.
- The CB monitors certificate impact determines whether certificate maintenance actions or reassessment are required and may request technical support from the ITSEF.
- Where requested, the ITSEF provides technical analysis, impact assessment, and reassessment evidence relevant to the certified product and evaluated TOE configuration.
- The NCCA and other competent parties, including CSIRTs where applicable, may be involved in oversight, escalation, or coordinated disclosure in accordance with applicable rules and national arrangements.
- For products at assurance level Substantial, certificate maintenance is normally handled by the CB. For products at assurance level High, the process may involve additional NCCA oversight, approval, or coordination in accordance with applicable national arrangements.

5. Detailed Process Description

5.1. Preparation and Readiness

Before vulnerabilities are identified during evaluation or received after certification, the certificate holder, the CB, and the ITSEF should maintain appropriate readiness arrangements to support timely and controlled handling. These arrangements should include documented roles and contact points, a maintained reporting channel, appropriate internal escalation paths, and readiness to record, assess, and communicate vulnerability information in accordance with this procedure. Where coordinated vulnerability disclosure arrangements are relevant, the parties should also be able to identify the appropriate CSIRT or other designated coordinator.

	<h1 style="margin: 0;">Vulnerability Handling for EUCC</h1>	Document:	TB-VH-01-01
	Revision:	2.0	
	Date issued:	DD-MM-YYYY	
	Owner:	To be determined	
	Page:	4 of 17	

- The certificate holder should maintain a documented reporting channel and relevant contact information for vulnerability handling.
- The CB and the ITSEF should maintain internal arrangements for receiving escalated cases, requesting technical support, and recording certificate maintenance actions.
- Where public sources or coordinated disclosure channels are relevant, the parties should be able to identify the appropriate route for escalation and coordination.
- For products at assurance level High, readiness arrangements should also take account of any national requirements for NCCA involvement or coordination.

5.2. Vulnerability Identification During Evaluation

Vulnerabilities may be identified through the following sources:

- Product documentation and design evidence review;
- Common Criteria vulnerability analysis activities (AVA_VAN);
- Penetration testing and attack potential assessment;
- Public vulnerability sources relevant to the TOE.

All identified vulnerabilities are:

- Documented in the evaluation working records;
- Traceable to the evaluated TOE configuration, the relevant evaluation activity, and the applicable SFRs/SARs.

5.3. Receipt and Verification of Reported Vulnerabilities

Where information about a potential vulnerability affecting a certified ICT product is received or identified after certification, the certificate holder is responsible for receiving and recording the case through its documented reporting channel. Consistently with EN ISO/IEC 30111, this includes cases where the holder of the EUCC certificate receives vulnerability information in accordance with Article 55(1)(c) of the CSA, receives information on a potential vulnerability from the CB that issued the certificate, becomes aware of a newly publicly disclosed vulnerability on the referenced online repositories in accordance with Article 55(1)(d) of the CSA that is also relevant to the EUCC-certified product, or identifies a potential related vulnerability through any other source.

The certificate holder should acknowledge receipt, perform an initial triage, determine whether the information is sufficiently complete, credible, and relevant to support verification, and record the case without waiting for final technical confirmation. Where the reported or identified issue may affect certified claims, the certificate holder must

	<h1 style="margin: 0;">Vulnerability Handling for EUCC</h1>	Document:	TB-VH-01-01
	Revision:	2.0	
	Date issued:	DD-MM-YYYY	
	Owner:	To be determined	
	Page:	5 of 17	

notify the CB and provide the available information needed for further review and vulnerability impact analysis. Where the certified ICT product forms part of a composite product and the potential vulnerability may affect dependent EUCC certificates, the certificate holder should also inform the holders of those dependent EUCC certificates without undue delay.

- The certificate holder should determine whether the reported or identified issue is complete, credible, and relevant to the certified product or evaluated TOE configuration.
- Where needed, the certificate holder may request clarification or additional information from the reporter or other relevant source before proceeding.
- A case shall be recorded and subjected to initial assessment and vulnerability impact analysis at the potential-vulnerability stage; it should be treated as a verified vulnerability only where sufficient evidence exists to confirm that the issue is reproducible or otherwise technically substantiated.
- Where certification relevance is unclear or the issue may affect certified claims, the CB may request technical support from the ITSEF to assist with verification, relevance assessment, or reassessment support.

5.4. Vulnerability Analysis and Classification

Following receipt, recording, and initial triage under Section 5.3, each reported, identified, or verified vulnerability that may affect a certified ICT product shall be subjected to vulnerability impact analysis and classification. During evaluation, this analysis is performed by the ITSEF as part of the evaluation activities. After certification, the certificate holder is responsible for carrying out the vulnerability impact analysis and for providing the results to the CB where certified claims may be affected; the CB may request technical support from the ITSEF where the relevance, scope, exploitability, or effect on the certified product requires further assessment.

The vulnerability impact analysis shall refer to the target of evaluation and the assurance statements contained in the certificate and should determine whether the issue applies to the evaluated TOE configuration, falls within the scope of the Security Target or Protection Profile, affects the certified claims, and is exploitable within the assumed attacker model. The analysis should be carried out within a timeframe appropriate to the exploitability and criticality of the potential vulnerability, taking account of the potential effect on the certified product and certificate maintenance.

- Whether the issue applies to the target of evaluation, including the evaluated TOE configuration and affected certified versions or configurations



	<h1 style="margin: 0;">Vulnerability Handling for EUCC</h1>	Document:	TB-VH-01-01
	Revision:	2.0	
	Date issued:	DD-MM-YYYY	
	Owner:	To be determined	
	Page:	6 of 17	

- Whether the issue falls within the scope of the Security Target, Protection Profile, assurance statements contained in the certificate, and certified claims
- Whether the issue is exploitable within the assumed attacker model and, where applicable, the relevant attack potential assumptions and AVA_VAN level associated with the certificate

Where the issue is found to be relevant to the certified scope, the vulnerability impact analysis should assess the likely effect on the certified security claims, the severity and practical significance of the issue in the context of the evaluated product, and whether the residual risk remains acceptable within the assumptions of the certification. Where applicable, the analysis should include an attack potential calculation consistent with the relevant evaluation methodology and state-of-the-art guidance, taking account of the AVA_VAN level of the EUCC certificate. For products at assurance level Substantial, the analysis should focus on whether the vulnerability affects the certified claims and whether the residual risk remains acceptable within the evaluated attack potential assumptions. For products at assurance level High, the analysis must also take account of the greater evaluation depth, the higher attacker capability assumptions, and any additional national or scheme requirements applicable to certificate maintenance, reassessment, and possible NCCA involvement.

- Impact on certified security claims, affected scope, and certificate maintenance considerations
- Alignment with the claimed assurance level and the corresponding attacker model, evaluation depth, and maintenance requirements

5.5. Reporting to the Certification Body

During initial evaluation, the ITSEF reports relevant vulnerabilities and its technical assessment to the CB through the Evaluation Technical Report (ETR). The report should identify whether the vulnerability is within scope, whether it affects the certified claims, and whether the residual risk remains acceptable at the claimed assurance level.

- The ITSEF provides the technical evidence, rationale, and traceability needed to support the CB's certification decision.
- The CB reviews the reported vulnerability information and determines whether additional evaluation, conditions, or certification actions are required before certification is granted or maintained.

Where vulnerabilities are discovered after certification, the certificate holder remains responsible for notifying the CB where certification claims may be affected and for providing relevant vulnerability and remediation information. The CB reviews the

	<h1 style="margin: 0;">Vulnerability Handling for EUCC</h1>	Document:	TB-VH-01-01
	Revision:	2.0	
	Date issued:	DD-MM-YYYY	
	Owner:	To be determined	
	Page:	7 of 17	

information, determines whether certificate maintenance actions or reassessment are required, and may request technical support from the ITSEF. For products at assurance level Substantial, this review is normally handled by the CB within its certificate maintenance process. For products at assurance level High, the CB should also consider whether escalation to, approval by, or coordination with the NCCA is required under the applicable national implementation of the EUCC. In such cases, the ITSEF provides technical impact analysis, reassessment evidence, and other evaluation input requested by the CB.

5.6. CB Review and Decision

Where a reported or verified vulnerability may affect certified claims, the CB performs a certificate maintenance review based on the information provided by the certificate holder and any technical input from the ITSEF. The review should consider the relevance of the vulnerability to the certified product, the affected certified versions or configurations, the adequacy of the proposed remediation, the expected effect on the certified claims, and whether reassessment is required before the certificate can be maintained without restriction.

- The CB may open a formal review where a vulnerability is verified, where certification relevance is uncertain, or where the proposed remediation or disclosure approach may affect the certificate.
- The certificate holder should provide sufficient evidence to support the review, including the vulnerability description, affected versions or configurations, impact analysis, remediation status, and any proposed disclosure timeline.
- Where the available information is insufficient or where the technical impact on the certified claims is unclear, the CB may request reassessment or other technical support from the ITSEF.
- Following review, the CB determines whether the certificate may be maintained, maintained subject to conditions or restrictions, suspended, or withdrawn, in accordance with the applicable certification rules.
- For products at assurance level High, the CB should also consider whether escalation to, approval by, or coordination with the NCCA is required under the applicable national implementation of the EUCC.

5.7. Remediation Development and Planning

Where a verified vulnerability affects certified claims or could otherwise affect certificate maintenance, the certificate holder is responsible for developing and planning appropriate remediation. Remediation planning should identify the affected certified versions or configurations, the proposed corrective actions, any compensating

	<h1>Vulnerability Handling for EUCC</h1>	Document:	TB-VH-01-01
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	8 of 17

measures, the expected effect on the certified claims, and the proposed implementation and disclosure timeline. The CB reviews the adequacy of the proposed remediation as part of certificate maintenance, and may request technical support from the ITSEF where the effect of the remediation on the certified product or evaluated TOE configuration requires further assessment.

- The certificate holder should document the remediation approach, affected scope, implementation status, and any dependencies relevant to certificate maintenance.
- Where remediation changes the certified product, configuration, or security functionality, the CB may require reassessment or other technical analysis from the ITSEF.
- For products at assurance level High, the CB should also consider whether NCCA coordination, approval, or oversight is required in relation to the remediation plan.

5.8. Release and Post-Release Handling

Following implementation of remediation, the certificate holder is responsible for managing release of the corrective update or other mitigating measure and for maintaining appropriate post-release monitoring. The certificate holder should confirm which certified versions or configurations are affected, whether the remediation has been deployed, and whether any residual restrictions, conditions, or disclosure arrangements remain applicable. The CB reviews whether the release and supporting evidence are sufficient to support continued certificate maintenance, and may request additional technical evidence or reassessment from the ITSEF where needed.

- Post-release records should identify the released remediation, the affected certified versions or configurations, and any relevant deployment or customer communication information.
- Where the release materially affects the certified product, the CB may maintain conditions or restrictions until any required reassessment or review is completed.
- For products at assurance level High, the CB should also consider whether release-related coordination with the NCCA is required under applicable national arrangements.

5.9. Handling of Coordinated Vulnerability Disclosure (CVD)

Where a vulnerability is handled under coordinated vulnerability disclosure, the certificate holder remains responsible for receiving, verifying, and remediating the vulnerability and for proposing an appropriate disclosure timeline. The CB remains responsible for assessing any impact on the certificate and for determining whether

	<h1>Vulnerability Handling for EUCC</h1>	Document:	TB-VH-01-01
	Revision:	2.0	
	Date issued:	DD-MM-YYYY	
	Owner:	To be determined	
	Page:	9 of 17	

further reassessment is required. Where requested by the CB, the ITSEF provides technical analysis and reassessment support. Where a CSIRT or other designated coordinator is involved, it may facilitate communication between relevant parties and support coordinated case handling and disclosure timing. The NCCA and other competent parties may be involved in coordination, oversight, or communication in accordance with applicable rules and national arrangements.

For products at assurance level Substantial, coordinated vulnerability disclosure is normally managed through the certificate holder, the CB, and any relevant coordinated disclosure channels, which may include a CSIRT or other designated coordinator. For products at assurance level High, the CB should additionally consider whether NCCA involvement, approval, or coordination is required in accordance with applicable national arrangements and EUCC implementation requirements, alongside any designated coordinated disclosure arrangements.

- The ITSEF may support coordinated vulnerability disclosure by providing technical findings, impact analysis, and reassessment evidence to the CB and other authorised parties.
- The ITSEF does not assume responsibility for disclosure decisions or external communications unless specifically authorised to do so.

5.10. Confidentiality, Impartiality and Records

The ITSEF must maintain strict confidentiality regarding all vulnerability information it handles in line with confidentiality, impartiality, and records-keeping procedures. All details and findings related to vulnerabilities must be protected and not disclosed to unauthorised parties. Secure handling controls are to be applied and maintained until such time as a disclosure decision is executed by the CB or the certificate holder.

The ITSEF must retain comprehensive records to support the integrity and traceability of its activities. These records include:

- Vulnerability analysis records
- Impact assessment rationale
- Communications with the CB

Such documentation is essential for demonstrating due diligence and transparency in the evaluation process. The records maintained by the ITSEF serve to fulfil several critical requirements, including:

- Supporting the CB's monitoring obligations
- Facilitating accreditation and authorisation audits

	<h1>Vulnerability Handling for EUCC</h1>	Document:	TB-VH-01-01
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	10 of 17

The ITSEF must ensure that all vulnerability handling activities are conducted in a manner that does not compromise its independence or impartiality. In particular, the ITSEF does not provide advisory or remediation services to the certificate holder beyond the scope of the evaluation.



	<h1 style="margin: 0;">Vulnerability Handling for EUCC</h1>	Document:	TB-VH-01-01
	Revision:	2.0	
	Date issued:	DD-MM-YYYY	
	Owner:	To be determined	
	Page:	11 of 17	

Annexes

Annex A – Vulnerability Handling Process Flow

Activity	Certificate holder	Certification body (CB)	ITSEF	NCCA	CSIRT / coordinator
1. Vulnerability identified during evaluation	Provides product, design, and evaluation evidence as required.	Receives relevant vulnerability information through the evaluation process.	Identifies, documents, and traces vulnerabilities found during evaluation.	Normally not involved unless national escalation is required.	Normally not involved at this stage.
2. Vulnerability report received after certification	Receives report, acknowledges receipt, records the case, and performs initial triage.	May be notified where certified claims could be affected.	Provides support only if requested by the CB.	Normally not involved at intake stage.	May receive or relay reports where acting as the designated disclosure coordinator.
3. Receipt and verification of reported vulnerability	Determines whether the report is complete, credible, relevant, and technically substantiated.	May request clarification or decide whether further review is needed.	May assist with verification or relevance assessment where requested.	Normally not involved unless escalation is required.	May support coordination and communication where the case is being handled through a coordinated disclosure channel.



	<h1 style="margin: 0;">Vulnerability Handling for EUCC</h1>	Document:	TB-VH-01-01
	Revision:	2.0	
	Date issued:	DD-MM-YYYY	
	Owner:	To be determined	
	Page:	12 of 17	

Activity	Certificate holder	Certification body (CB)	ITSEF	NCCA	CSIRT / coordinator
4. Vulnerability analysis and classification	Provides vulnerability details, affected versions, and remediation information where applicable.	Reviews whether the issue may affect certification and whether technical reassessment is needed.	Assesses scope, exploitability, effect on certified claims, and alignment with the claimed assurance level.	May be involved for High assurance or other nationally escalated cases.	Normally does not perform certification analysis, but may support coordinated handling context.
5. Reporting to the CB	Notifies the CB where certification claims may be affected and provides supporting evidence.	Receives the report and determines whether certificate maintenance review is needed.	Provides technical reporting through the ETR or other requested evidence.	May be informed where national arrangements require it.	May be informed where coordinated disclosure handling is already underway.
6. CB review and decision	Provides impact analysis, remediation status, and disclosure timing proposals.	Reviews the case, decides whether reassessment is required, and determines certificate outcome.	Provides reassessment support and technical evidence where requested.	May provide oversight, approval, or coordination, particularly for High assurance cases.	May be consulted on coordinated disclosure timing or handling where acting as coordinator.



	<h1 style="margin: 0;">Vulnerability Handling for EUCC</h1>	Document: TB-VH-01-01
	Revision: 2.0	
	Date issued: DD-MM-YYYY	
	Owner: To be determined	
	Page: 13 of 17	

Activity	Certificate holder	Certification body (CB)	ITSEF	NCCA	CSIRT / coordinator
7. Remediation development and planning	Develops the remediation approach, identifies affected scope, and proposes implementation and disclosure timing.	Reviews the adequacy of the remediation plan as part of certificate maintenance.	Provides technical assessment where remediation may affect the certified product or evaluated TOE configuration.	May be involved for High assurance or other nationally escalated remediation cases.	May support coordination where remediation planning interacts with coordinated disclosure timing.
8. Release and post-release handling	Manages release of the corrective update or other mitigating measure and maintains post-release monitoring.	Reviews release evidence and determines whether conditions, restrictions, or further review remain necessary.	Provides additional technical evidence or reassessment where the release affects the certified product.	May be involved where High assurance release handling requires national coordination.	May support communication and coordination where release timing is linked to coordinated disclosure handling.
9. Coordinated vulnerability disclosure	Receives, verifies, and remediates the vulnerability and proposes a disclosure timeline.	Assesses certificate impact and determines whether reassessment or restrictions are needed.	Provides technical findings and reassessment evidence to support authorised disclosure handling.	May be involved in oversight, coordination, or communication under national arrangements.	May coordinate communication between parties, support disclosure timing, and facilitate the coordinated disclosure process where designated to do so.



	<h1 style="margin: 0;">Vulnerability Handling for EUCC</h1>	Document:	TB-VH-01-01
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	14 of 17

Activity	Certificate holder	Certification body (CB)	ITSEF	NCCA	CSIRT / coordinator
10. Confidentiality, records, and closure	Maintains records of handling, remediation, release, and disclosure decisions.	Retains certificate review records and outcome documentation.	Maintains technical records, traceability, and confidentiality controls.	May retain oversight records where involved.	May retain coordination records where involved in the case.



	<h1 style="margin: 0;">Vulnerability Handling for EUCC</h1>	Document:	TB-VH-01-01
	Revision:	2.0	
	Date issued:	DD-MM-YYYY	
	Owner:	To be determined	
	Page:	15 of 17	

Annex B – Coverage of This Procedure Against EUCC Vulnerability Handling Expectations

EUCC / ENISA topic	Relevant source expectation	Covered in this SOP
Role separation between certificate holder, CB, ITSEF, NCCA, and CSIRT coordinator	ENISA EUCC guidance describes distinct responsibilities for the certificate holder, CB, ITSEF, NCCA, and designated CSIRT coordinator in vulnerability handling and disclosure.	Sections 3, 4, 5.4, 5.5, 5.8, Annex A
Preparation / readiness	ENISA guidance expects a documented vulnerability handling process and reporting channel to be maintained before reports are received.	Sections 3, 5.1
Receipt of vulnerability reports	ENISA guidance includes receipt, acknowledgement, recording, and initial triage of reports.	Section 5.3, Annex A
Verification of reported vulnerabilities	ENISA guidance distinguishes report triage from technical verification and relevance assessment.	Section 5.3, Annex A
Impact analysis and classification	EUCC vulnerability handling expects assessment of scope, exploitability, impact on certified claims, and assurance-level relevance.	Section 5.4, Annex A
Certificate holder notification to the CB	EUCC requires notification to the CB where vulnerabilities may affect certification claims or certificate validity.	Sections 3, 4, 5.3, 5.5, Annex A
CB review and certificate maintenance decision	The CB is expected to review certificate impact, request reassessment where needed, and determine certificate outcomes under EUCC rules.	Sections 3, 4, 5.5, 5.6, Annex A
Remediation development	ENISA guidance includes development and planning of remediation, including scope, timing, and effect on certified claims.	Section 5.7, Annex A
Release and post-release	ENISA guidance includes release of remediation, post-release monitoring, and confirmation of the effect on the certified product.	Section 5.8, Annex A
ITSEF technical support role	ENISA guidance positions the ITSEF as a technical support actor for analysis, reassessment, and evidence rather than a disclosure decision-maker.	Sections 3, 4, 5.4, 5.5, 5.6, 5.9, Annex A



	<h1>Vulnerability Handling for EUCC</h1>	Document:	TB-VH-01-01
	Revision:	2.0	
	Date issued:	DD-MM-YYYY	
	Owner:	To be determined	
	Page:	16 of 17	

EUCC / ENISA topic	Relevant source expectation	Covered in this SOP
Coordinated vulnerability disclosure (CVD)	ENISA guidance includes structured coordinated disclosure involving the certificate holder, CB, designated CSIRT coordinator, and other competent parties as applicable.	Sections 3, 5.9, Annex A
Substantial and High assurance-level distinction	EUCC distinguishes Substantial and High assurance levels, with High potentially involving additional NCCA oversight or approval depending on national implementation.	Sections 4, 5.4, 5.5, 5.6, 5.7, 5.8, 5.9, Annex A
Confidentiality, impartiality, and records	EUCC and ENISA guidance require secure handling, traceability, and retention of vulnerability-related records, while preserving impartiality.	Section 5.10, Annex A



	<h1>Vulnerability Handling for EUCC</h1>	Document:	TB-VH-01-01
		Revision:	2.0
		Date issued:	DD-MM-YYYY
		Owner:	To be determined
		Page:	17 of 17

Version History

Version	Date	Author	Summary of changes	Status
1	28-04-2026	Khalimatou Samirah (NSAI)	Initial draft created.	Draft
2	02-06-2026	Khalimatou Samirah (NSAI)	Updated sections as per review comments,	Approved

