chemelex

Coordinated Vulnerability Disclosure Policy

# 1. Purpose

This policy establishes requirements for the coordinated reporting, assessment, remediation, communication, and disclosure of cybersecurity vulnerabilities affecting products with digital elements.

The policy supports compliance with applicable product cybersecurity requirements, including the EU Cyber Resilience Act (CRA), and establishes a consistent approach for managing vulnerabilities reported by customers, security researchers, partners, suppliers, and other external parties.

# 2. Scope

This policy applies to products with digital elements and associated software, firmware, services, and third-party or open-source components for which the organization is responsible for vulnerability handling.

It applies throughout the applicable product support period and covers vulnerabilities identified through:

- External vulnerability reports.
- Internal security testing and reviews.
- Product testing and validation.
- Third-party and open-source vulnerability monitoring.
- Supplier notifications.
- Customer reports.
- Security research.
- Other vulnerability intelligence sources.

# 3. Policy Statement

The organization shall maintain and enforce a Coordinated Vulnerability Disclosure process that enables potential cybersecurity vulnerabilities to be reported, investigated, remediated, and disclosed in a controlled and timely manner.

The organization shall:

- Provide a designated point of contact for reporting suspected product vulnerabilities.
- Receive and track reported vulnerabilities through closure.

- Assess vulnerabilities for applicability, impact, severity, and exploitability, using Common Vulnerability Scoring System (CVSS) version 4.0.
- CVSS 4.0
- Address and remediate vulnerabilities without undue delay based on cybersecurity risk.
- Coordinate disclosure with vulnerability reporters where appropriate.
- Securely distribute security updates and mitigations.
- Communicate applicable product vulnerabilities and corrective actions to affected users.
- Assess vulnerabilities for applicable regulatory reporting obligations.
- Maintain records demonstrating execution of the vulnerability-handling process.

## 4. Vulnerability Reporting

A designated vulnerability reporting contact shall be maintained and made available to customers, security researchers, partners, and other interested parties.

Product information and documentation shall identify, as applicable:

- The vulnerability reporting contact or reporting mechanism.
- Where this Coordinated Vulnerability Disclosure Policy can be found.
- Information necessary to identify the affected product.

Vulnerability reporters should be encouraged to provide sufficient information to support investigation, including the affected product and version, a description of the vulnerability, reproduction information, potential impact, and relevant supporting evidence.

The organization supports good-faith cybersecurity research and encourages responsible reporting of security vulnerabilities. Individuals who identify and report vulnerabilities in accordance with this policy, act in good faith, avoid privacy violations, service disruption, data destruction, or unauthorized disclosure of information, and provide a reasonable opportunity for remediation prior to public disclosure, shall not be subject to legal action by the organization solely for such activities

## 5. Vulnerability Intake and Tracking

Reported vulnerabilities shall be recorded and tracked using the organization’s vulnerability management process.

Each reported vulnerability shall be reviewed to:

1. Acknowledge receipt where contact information is available.
2. Assign or associate an internal tracking identifier.
3. Identify the potentially affected product and versions.
4. Determine whether internally developed or third-party components are involved.

5. Assign responsibility for investigation and resolution.
6. Maintain the vulnerability record through assessment, remediation, disclosure, and closure.

Access to vulnerability information shall be appropriately controlled to reduce the risk of premature disclosure or misuse.

## 6. Triage and Risk Assessment

Reported or identified vulnerabilities shall be evaluated to determine, as applicable:

- Whether the vulnerability is valid and reproducible where applicable.
- Affected products, components, and versions.
- Potential security impact.
- Vulnerability severity.
- Exploitability and attack prerequisites.
- Availability of mitigations or workarounds.
- Whether exploitation is known or suspected to be occurring.
- Whether the vulnerability affects third-party or open-source components.
- Whether regulatory notification or escalation requirements apply.

Vulnerabilities shall be prioritized and managed according to cybersecurity risk.

The organization shall maintain a documented methodology for vulnerability severity assessment using the Common Vulnerability Scoring System (CVSS) version 4.0. Vulnerability severity ratings shall be used to support prioritization, remediation timelines, escalation decisions, customer communications, and regulatory reporting assessments.

## 7. Vulnerability Remediation

Validated vulnerabilities shall be addressed without undue delay based on the risk posed to affected products and users.

Corrective actions may include:

- Software or firmware security updates.
- Configuration changes.
- Component updates or replacements.
- Compensating controls.
- Mitigation or workaround instructions.
- Other measures that reduce the associated cybersecurity risk.

Security fixes shall be appropriately reviewed and tested before release to confirm that the vulnerability has been addressed and that the corrective action does not introduce unacceptable security, safety, functionality, or reliability risks.

Where technically feasible, security updates should be separable from functionality updates.

## 8. Coordinated Vulnerability Disclosure

The organization shall support coordinated vulnerability disclosure to provide sufficient opportunity to investigate and remediate vulnerabilities before detailed vulnerability information is publicly disclosed.

Where appropriate, the organization shall maintain communication with the vulnerability reporter during the investigation and remediation process.

Communications may include:

- Acknowledgement of the report.
- Requests for additional technical information.
- Status updates.
- Coordination of anticipated disclosure timelines.
- Notification that remediation is available.
- Notification of public disclosure.

Disclosure timing shall consider the cybersecurity risk to affected users. Public disclosure may be delayed where premature disclosure would create a greater cybersecurity risk and users have not yet had a reasonable opportunity to apply available corrective measures.

## 9. Customer Vulnerability Disclosure

The organization’s standard customer-facing distribution mechanism for disclosed product vulnerabilities is the Tech Note.

Customer notification shall be considered where a vulnerability may significantly affect product security or safety, where customer action is required to implement a mitigation or security update, where exploitation is known or suspected, or where disclosure is necessary to enable the secure operation of affected products.

A vulnerability-related Tech Note shall be created when customer notification is required and should include, as applicable:

- Tech Note identifier and publication date.
- Affected product or products.
- Affected software or firmware versions.
- Description of the vulnerability.

- Security impact.
- Vulnerability severity.
- CVE identifier, where applicable.
- Corrected software or firmware version.
- Available security update.
- Mitigation or workaround instructions.
- Recommended customer actions.
- Relevant references or supporting information.

Vulnerability Tech Notes shall be reviewed and approved through the applicable product cybersecurity and technical publication processes before distribution.

Tech Notes shall be distributed through the established Tech Note publication and distribution mechanism.

## 10. Security Updates

Security updates shall be distributed through approved and secure product update mechanisms.

Where security updates are available to address identified security issues, they shall be made available without delay based on the associated cybersecurity risk and in accordance with applicable regulatory requirements.

Security updates shall be accompanied by sufficient advisory information to allow users to:

- Identify affected products and versions.
- Understand the security issue and potential impact.
- Obtain and apply the corrective update.
- Implement applicable mitigations or workarounds.
- Understand any additional actions required.

## 11. Third-Party and Open-Source Vulnerabilities

The vulnerability-handling process shall include vulnerabilities affecting third-party and open-source components incorporated into products.

Suppliers responsible for software, firmware, cloud services, or digital components incorporated into products shall, where applicable, be required through contractual, quality, or operational arrangements to notify Chemelex of relevant cybersecurity vulnerabilities, known exploits, security advisories, and available remediations that may affect products for which the organization is responsible.

When a third-party vulnerability is identified, the responsible team shall determine:

- Whether the affected component is present in a supported product.
- Which products and versions contain the component.
- Whether the vulnerable functionality is used or otherwise exploitable.
- The cybersecurity risk to the product.
- Whether an updated component, patch, mitigation, or other corrective action is available.
- Whether customer disclosure through a Tech Note is required.

Software Bill of Materials information shall be maintained and used, where appropriate, to support identification and assessment of affected components and products.

## 12. Regulatory Reporting and Escalation

Identified vulnerabilities shall be evaluated against applicable cybersecurity regulatory reporting requirements.

Where a vulnerability is known or suspected to be actively exploited, or otherwise meets applicable regulatory reporting criteria, it shall be promptly escalated to the responsible product cybersecurity and compliance personnel and, where appropriate based on severity, to designated management stakeholders.

Required regulatory notifications shall be completed through the applicable regulatory reporting mechanism within required timelines.

Regulatory notification and customer disclosure are separate activities. Regulatory reporting shall not be delayed pending publication of a Tech Note, and customer disclosure shall be coordinated to avoid unnecessary or premature disclosure of sensitive vulnerability information.

## 13. Records and Evidence

Appropriate records shall be retained to demonstrate execution of this policy and the associated vulnerability-handling process.

Records may include:

- Original vulnerability reports.
- Reporter communications.
- Vulnerability tracking records.
- Triage and technical assessments.
- Severity and risk assessments.
- Affected product and version analysis.
- Third-party component assessments.

- Remediation decisions and implementation records.
- Security testing and verification results.
- Security update information.
- Tech Notes and associated approvals.
- Regulatory reporting assessments and submissions.
- Vulnerability closure records and rationale.

Records shall be retained and protected in accordance with applicable records-management and information-security requirements.

# 14. Roles and Responsibilities

### Product Cybersecurity

Product Cybersecurity is responsible for coordinating the vulnerability-handling process, supporting vulnerability assessment, determining cybersecurity risk, coordinating disclosure, evaluating regulatory reporting obligations, and maintaining appropriate vulnerability-management records.

### Product and Engineering Teams

Product and Engineering teams are responsible for supporting technical investigation, identifying affected products and versions, developing corrective actions, and supporting remediation and verification activities.

### Quality and Validation

Quality and Validation functions are responsible, as applicable, for supporting verification that vulnerability remediation has been appropriately tested before release.

### Product Management

Product Management is responsible, as applicable, for supporting assessment of affected products and customers and coordinating product-related customer communications.

### Technical Publications

Technical Publications is responsible, as applicable, for supporting preparation, approval, publication, and distribution of vulnerability-related Tech Notes.

### Compliance and Legal

Compliance and Legal functions shall be engaged where necessary to support regulatory reporting, disclosure decisions, contractual obligations, or other legal and regulatory considerations.

# 15. Exceptions

Exceptions to this policy shall be documented, justified based on cybersecurity risk, and approved by the responsible Product Cybersecurity authority and other applicable stakeholders.

An exception shall not override mandatory legal or regulatory obligations.

## 16. Compliance

Failure to follow this policy may result in unmanaged cybersecurity risk, delayed remediation, inappropriate disclosure, or non-compliance with applicable product cybersecurity requirements.

Compliance with this policy shall be periodically reviewed as part of applicable product cybersecurity governance, assessment, or audit activities.

This policy shall be reviewed periodically and updated as necessary to reflect changes in applicable regulatory requirements, cybersecurity standards, organizational responsibilities, product cybersecurity processes, or lessons learned from vulnerability management and disclosure activities.

## 17. Process Summary

The associated vulnerability-handling process follows the general workflow:

Report → Intake → Triage → Validate → Assess Risk and Severity → Remediate → Test → Release Security Update → Publish Tech Note → Close

Where regulatory reporting may be required:

Assess Vulnerability → Determine Active Exploitation / Reporting Applicability → Regulatory Escalation and Reporting → Continue Remediation and Coordinated Disclosure

## 18. References

- Regulation (EU) 2024/2847, Cyber Resilience Act.
- EU Cyber Resilience Act, Annex I, Part II, Vulnerability Handling Requirements.
- EU Cyber Resilience Act, Annex II, Information and Instructions to the User.
- EU Cyber Resilience Act, Article 14, Reporting Obligations of Manufacturers.
- Applicable internal product cybersecurity, secure development, vulnerability management, incident response, and records-management procedures.