

Coordinated Vulnerability Disclosure Policy

Version	Date	Author	Description of Changes	Approved By
1.0	05/10/2026	Matteo Negroni	Initial release of Coordinated Vulnerability Disclosure Policy	

1. Purpose

At **Elemaster Group**, we are committed to maintaining the security, integrity, and availability of our information systems, services, and data. We recognize that security researchers, customers, suppliers, and other stakeholders play an important role in helping identify vulnerabilities that may otherwise remain undiscovered.

The purpose of this Coordinated Vulnerability Disclosure (CVD) Policy is to establish a clear and responsible process for reporting potential security vulnerabilities to **Elemaster Group**, enabling timely investigation, risk assessment, remediation, and communication.

This policy promotes collaboration between **Elemaster Group** and the security community by providing a structured framework for vulnerability reporting and coordinated disclosure. Our objective is to reduce cybersecurity risks, protect our customers and business operations, and continuously improve the security posture of our products, services, and supporting infrastructure.

Elemaster Group encourages responsible vulnerability reporting and is committed to working with reporters in good faith to validate and address legitimate security concerns in a timely and transparent manner.

2. Scope

This Policy applies to the reporting of security vulnerabilities affecting assets that are owned, operated, or managed by **Elemaster Group** including but not limited to:

- Public-facing websites and web applications;
- Customer, supplier, and partner portals;
- Cloud-hosted services and platforms;
- Public APIs;
- Internet-accessible infrastructure components;
- Corporate systems and services exposed to external users;
- Products, solutions, and services developed, maintained, or provided by **Elemaster Group**

This Policy is intended to facilitate the responsible disclosure of vulnerabilities that may impact the confidentiality, integrity, or availability of systems, services, or information managed by **Elemaster Group**.

The following activities are outside the scope of this Policy and are not authorized:

- Social engineering attacks against employees, contractors, customers, or partners;
- Physical security testing or unauthorized access to facilities;
- Denial-of-Service (DoS) or Distributed Denial-of-Service (DDoS) testing;
- Spam, phishing, or other forms of unsolicited communications;
- Destructive testing that may impact the availability, performance, or stability of production systems;
- Accessing, modifying, destroying, or exfiltrating data belonging to other users;
- Testing against systems, applications, or services owned by third parties and not controlled by **Elemaster Group**

Researchers are expected to conduct any testing in a manner that minimizes risk to systems, services, users, and business operations.

3. Reporting a Vulnerability

Elemaster Group encourages security researchers, customers, suppliers, partners, and other stakeholders to responsibly report any suspected security vulnerabilities affecting systems, services, applications, or infrastructure operated by the organization.

Vulnerability reports should be submitted to the Information Security team using the following contact information:

Email: cybersec@elemaster.com

To facilitate efficient assessment and remediation, reports should include, where possible:

- A clear description of the identified vulnerability;
- The affected system, application, service, or URL;
- Detailed steps required to reproduce the issue;
- Any relevant screenshots, logs, or supporting evidence;
- Proof of Concept (PoC) code, when appropriate;
- An assessment of the potential impact;
- The reporter's contact information for follow-up communications.

Upon receipt of a vulnerability report, **Elemaster Group** will:

- Acknowledge receipt of the report within **five (5) business days**;
- Perform an initial review and validation of the reported issue;
- Assess the potential impact and associated risk;
- Determine appropriate remediation or mitigation actions;
- Maintain communication with the reporter, where practical, throughout the investigation process.

Reporters are requested to provide sufficient time for investigation and remediation before publicly disclosing any vulnerability information. **Elemaster Group** will make reasonable efforts to coordinate disclosure activities with the reporter in a manner that minimizes risk to customers, partners, and business operations.

Reports submitted in good faith and in accordance with this Policy will be handled confidentially and treated as security-sensitive information.

4. Expectations for Researchers

Researchers should act in good faith, avoid privacy violations, stop testing if sensitive data is encountered, avoid data destruction or exfiltration and refrain from public disclosure before coordination.

5. Our Commitment

Elemaster Group values responsible vulnerability disclosure and is committed to working collaboratively with security researchers and other stakeholders who report potential security issues in good faith.

Upon receiving a vulnerability report, **Elemaster Group** will make reasonable efforts to:

- Acknowledge receipt of the report within **five (5) business days**;
- Conduct an initial assessment to determine the validity and potential impact of the reported vulnerability;
- Prioritize remediation activities based on the risk posed to the organization, its customers, partners, and stakeholders;
- Maintain appropriate communication with the reporter throughout the investigation and remediation process, where contact information has been provided;
- Implement corrective actions or mitigating controls for confirmed vulnerabilities within a timeframe proportionate to the associated risk;
- Treat vulnerability reports as confidential and handle any information provided in accordance with applicable legal, regulatory, and contractual requirements;
- Coordinate public disclosure, when appropriate, in a manner that minimizes risk and protects affected parties.

While **Elemaster Group** is committed to addressing legitimate security concerns, remediation timelines may vary depending on factors such as the complexity of the issue, potential business impact, technical constraints, and the availability of a suitable fix.

The submission of a vulnerability report does not guarantee specific remediation timelines, public disclosure, recognition, or compensation. However, all reports received in good faith will be reviewed and evaluated in accordance with this Policy.

Elemaster Group is committed to continuously improving its cybersecurity posture and views responsible vulnerability disclosure as an important component of its overall security and risk management program.

6. Disclosure Timeline

Confirmed vulnerabilities will be remediated according to risk and complexity. Public disclosure should be coordinated with the company.

7. Safe Harbor

The company will not pursue legal action against researchers acting in good faith and in accordance with this policy.

8. Prohibited Activities

To protect the confidentiality, integrity, and availability of systems, services, and information assets, **Elemaster Group** does not authorize any testing activities that may adversely affect its operations, customers, partners, or personnel.

The following activities are expressly prohibited under this Policy:

- Accessing, modifying, copying, disclosing, or deleting data that does not belong to the researcher;
- Accessing personal, confidential, proprietary, or sensitive information beyond what is strictly necessary to demonstrate the existence of a vulnerability;
- Conducting Denial-of-Service (DoS), Distributed Denial-of-Service (DDoS), resource exhaustion, or any other activity intended to disrupt or degrade service availability;
- Uploading, deploying, or executing malware, ransomware, backdoors, or other malicious software;
- Attempting privilege escalation or unauthorized access to accounts, systems, networks, or data belonging to other users;
- Performing destructive actions that could alter, corrupt, damage, or destroy systems, applications, configurations, or information;
- Conducting social engineering, phishing, impersonation, or other attempts to manipulate employees, contractors, customers, suppliers, or partners;
- Performing physical security testing, including unauthorized access to facilities, equipment, or restricted areas;

- Intercepting, monitoring, or tampering with communications, network traffic, or user sessions belonging to third parties;
- Using automated scanning or testing activities that may negatively impact system performance, stability, or availability;
- Publicly disclosing vulnerability details before coordination with **Elemaster Group** and sufficient time has been provided for investigation and remediation;
- Testing systems, applications, or services owned or operated by third parties, unless explicitly authorized by the respective owner.

Any activity that results in service disruption, data exposure, unauthorized access, or harm to **Elemaster Group**, its customers, partners, employees, or suppliers may be considered outside the protections offered by this Policy.

Researchers are expected to conduct all testing responsibly, in good faith, and in a manner that minimizes risk to people, systems, data, and business operations.

9. Recognition

The company may acknowledge researchers who submit valid reports. No bug bounty or monetary reward program is offered unless explicitly stated.

10. Contact

Security Team
cybersec@elemaster.com