UltrArmor
Vulnerability Disclosure Policy

1. Purpose and Importance of the Policy

UltrArmor places great importance on information security and is committed to continually enhancing the security of all its products and services. This Vulnerability Disclosure Policy is intended to encourage and guide security researchers, users, and partners to report potential information security vulnerabilities in a responsible manner. By doing so, the company can detect and address risks at an early stage, thereby protecting customer data, system operations, and corporate reputation.

This policy adheres to international standards for vulnerability handling, including ISO/IEC 29147:2018 and ISO/IEC 30111:2019, and is informed by industry best practices and the principles of Coordinated Vulnerability Disclosure (CVD).

2. Vulnerability Reporting Procedure

If you discover a potential vulnerability in UltrArmor's products, services, or systems, please report it by following the steps below:

2.1 Report Contents Should Include:

- Vulnerability Description: A clear explanation of the issue, the affected resources, and the conditions under which it occurs
- Attack Process (if applicable): Proof of Concept (PoC), attack path, and potential impact
- Vulnerability Reproduction Method: Detailed instructions or supporting evidence such as screenshots or videos
- Contact Information: A reply-to email address is recommended for follow-up communication

2.2 Reporting Method:

Please send the complete vulnerability details via email to service@ultrarmor.com
Include "[Security Vulnerability Report]" in the subject line to facilitate prompt handling.

2.3 Response Mechanism:

Upon receipt and validation of the reported vulnerability, UltrArmor will provide progress updates based on the severity of the issue. If appropriate, we will coordinate with the reporter regarding the timing and content of any public disclosure.

3. Vulnerability Remediation Procedure

Once a reported vulnerability is verified, UltrArmor will follow the steps below to address the issue:

- Risk Assessment and Prioritization: Classify the vulnerability based on factors such as severity, exploitability, and potential impact.
- Remediation Planning and Testing: Determine and internally evaluate appropriate remediation methods.
- Patch Deployment: Release updated firmware or software patches to resolve the issue.
- Public Disclosure (if applicable): In coordination with the reporter or security community, publish a security advisory or assign a CVE identifier at an appropriate time.

4. Additional Notes

4.1 What Is a Vulnerability?

A vulnerability refers to a security weakness that could lead to information leakage, system compromise, unauthorized code execution, or improper access. Examples include:

- Failure of authentication or access control mechanisms
- Unauthorized data access or code execution
- Security flaws in data encryption or transmission processes
- Web-based vulnerabilities such as XSS, SQL Injection, and CSRF

4.2 The Following Types of Reports Will Not Be Accepted:

Reports based solely on automated scanning tools without further validation

- Vulnerabilities affecting outdated or unsupported versions
- Low-risk UI issues such as clickjacking or stack traces on error pages
- Recommendations related to SPF, DMARC, or DKIM configuration
- Missing Secure/HTTPOnly attributes in cookie settings
- Access to public directories or the presence of robots.txt files

5. Legal Liability and Disclaimer

UltrArmor states that as long as your research and disclosure are conducted in good faith and in accordance with this policy, we will not pursue legal action. In the event of legal claims from third parties, the company will support your legitimate research activities. However, violations of any of the following may result in legal consequences:

- Unauthorized access to or destruction of systems or data
- Denial-of-Service (DoS) attacks, social engineering, or phishing activities
- Public disclosure of vulnerabilities or sensitive information without consent

6. Confidentiality Obligation

Before a vulnerability has been fully remediated, you must not disclose or publish any related information—including the report content, proof of concept (PoC), or system details—to prevent the risk of unpatched vulnerabilities being exploited.