FORTIKECO

Vulnerability Disclosure Policy Standard for FORTIKECO AND ITS CLIENTS

1. Introduction

This **Vulnerability Disclosure Policy (VDP)** provides a structured process for the identification, reporting, and remediation of security vulnerabilities within our organization's systems, services, and products and the ones related to FORTIKECO as clients of our services and solutions and we represent. It establishes clear guidelines for both external reporters (researchers, users, and other stakeholders) and internal security teams to address vulnerabilities effectively, minimizing potential risks while maintaining trust and transparency.

The primary goal of this policy is to ensure that any identified vulnerabilities are responsibly disclosed, thereby reducing the likelihood of exploitation. This document outlines the VDP's scope, responsibilities, process, and legal considerations while adhering to best practices in cybersecurity.

2. Purpose

The purpose of this Vulnerability Disclosure Policy is to:

- Establish a structured and safe communication channel for individuals and organizations to report security vulnerabilities in our systems or the clients we represent.
- Ensure timely and responsible handling, investigation, and remediation of vulnerabilities reported on our channels or the clients we represent
- Promote collaboration with the cybersecurity research community to improve our security posture representing ourselves or clients we represent

- Mitigate security risks to our users, services, and infrastructure by providing clarity on how we manage vulnerability disclosures for us or the clients we represent.

3. Scope

This policy applies to all:

- Websites, web applications, APIs, services, networks, and infrastructure managed or owned by the organizations we represent.
- Internal and external systems, applications, and platforms, for ourselves or the clients we represent.
- Third-party components used in our technology stack, to the extent that we can reasonably mitigate vulnerabilities related to these components, for ourselves or the clients we represent.

It is important to note that this policy does not cover:

- Vulnerabilities in third-party systems that do not directly impact our infrastructure unless the third party in question we formally and explicitly represent as clients.
- Social engineering attacks against employees or service providers (e.g., phishing attempts).
- Physical security vulnerabilities, unless directly linked to digital infrastructure or the infrastructure of the clients we represent.

4. Roles and Responsibilities

This section defines the roles of all key stakeholders involved in vulnerability disclosure and management.

4.1. Security Researchers and External Reporters

Security researchers and other external reporters play a critical role in identifying and reporting vulnerabilities in a responsible manner. They are expected to:

- Follow this policy and applicable laws when identifying and reporting vulnerabilities.
- Avoid exploiting or causing harm to the systems, services, or data.

- Provide clear, concise, and actionable reports with detailed information regarding the vulnerability.
- Refrain from publicly disclosing vulnerabilities before they are resolved, unless explicitly authorized by the organization.

4.2. Internal Security Team

The internal security team is responsible for:

- Managing the vulnerability disclosure process and serving as the point of contact for external reporters.
- Investigating reported vulnerabilities in a timely manner.
- Prioritizing remediation efforts based on the severity and impact of the vulnerability.
- Communicating with external reporters to acknowledge reports, provide updates on the remediation process, and confirm resolution.
- Coordinating with relevant internal stakeholders, such as product teams, IT, and legal departments.

4.3. Product and Development Teams

The product and development teams must collaborate with the internal security team to:

- Assess and address vulnerabilities identified in their systems and applications.
- Prioritize fixes based on the potential risk and impact to users.
- Implement long-term solutions to prevent future occurrences of similar vulnerabilities.

4.4. Legal and Compliance

The legal and compliance teams are responsible for:

- Ensuring the organization's vulnerability disclosure practices comply with applicable laws and regulations.
- Providing legal guidance and support, particularly in situations involving complex legal issues (e.g., cross-border vulnerabilities or third-party involvement).

5. Reporting Process

A clear and structured process is vital for the efficient and safe reporting of vulnerabilities. The reporting process includes the following steps:

5.1. Submission of Vulnerability Reports

External reporters must submit vulnerability reports through the designated channels, such as a vulnerability disclosure web form or email. The following information should be included in the report:

- A detailed description of the vulnerability.
- The location of the vulnerability (e.g., specific URL, API endpoint, etc.).
- Steps to reproduce the vulnerability, including any relevant code snippets or screenshots.
- The potential impact of the vulnerability (e.g., data exposure, service disruption).
- Any suggestions for remediation or mitigation.

5.2. Acknowledgment of Receipt

Upon receiving the vulnerability report, the internal security team will acknowledge receipt of the report within 2-3 business days. The team will also provide an initial assessment of the report and may request additional information if needed.

5.3. Initial Triage and Validation

The security team will conduct an initial triage to assess the validity of the report and determine the severity and potential impact of the vulnerability. The triage process includes:

- Verifying that the vulnerability exists and is exploitable.
- Determining the potential risk level (e.g., critical, high, medium, or low).
- Assigning internal resources for further investigation and remediation.

5.4. Remediation Process

After validation, the relevant teams (e.g., product, IT, or development) will work on remediating the vulnerability. This process includes:

- Developing a fix or mitigation strategy based on the vulnerability's severity and potential impact.
- Conducting thorough testing to ensure the fix is effective and does not introduce new vulnerabilities.
- Deploying the fix in a controlled and timely manner, prioritizing critical and high-severity vulnerabilities.

5.5. Communication with External Reporters

The internal security team will maintain communication with the external reporter throughout the remediation process, providing updates on the following:

- Status of the investigation.
- Planned remediation timeline.
- Confirmation once the vulnerability has been resolved.

5.6. Public Disclosure

Once the vulnerability is resolved, the organization may choose to publicly disclose the details of the vulnerability, including how it was remediated. Public disclosure will only occur with the explicit consent of the external reporter and after ensuring that users are no longer at risk.

6. Severity Rating

To ensure vulnerabilities are handled based on risk, the organization uses a standardized severity rating system, typically aligned with the Common Vulnerability Scoring System (CVSS) framework.

- **Critical**: Vulnerabilities that pose an immediate threat to the confidentiality, integrity, or availability of sensitive data or critical systems.
- **High**: Vulnerabilities that could lead to significant risk if exploited but may require specific conditions or access to be viable.
- **Medium**: Vulnerabilities that present moderate risk but are less likely to be widely exploited or have minimal impact.
- **Low**: Vulnerabilities that pose minimal risk and may only impact non-critical systems or features.

Each severity rating dictates the response time for remediation. For example:

- **Critical vulnerabilities** must be addressed immediately, with fixes deployed as soon as possible.
- **High and Medium vulnerabilities** should be addressed within a defined period (e.g., within 30 days for high and 90 days for medium).
- **Low vulnerabilities** can be fixed during regular maintenance cycles.

7. Rewards and Recognition

To encourage responsible disclosure, the organization may choose to implement a **Bug Bounty Program case by case**, depending on the mandate of the clients we represent offering rewards to external researchers for identifying valid vulnerabilities. Not automatic reward is offered please ask formally on the report itself

The reward amount typically depends on the severity and complexity of the vulnerability.

In addition to financial rewards, researchers may also be publicly recognized for their contributions on a **Hall of Fame** or similar recognition platform, subject to their consent.

8. Safe Harbor Provisions

The organization supports ethical hacking and responsible disclosure by providing **safe harbor** for security researchers who act in good faith under this policy. Researchers will not face legal action or sanctions for their security research as long as they:

- Act within the bounds of this policy and applicable laws.
- Avoid causing harm or disruption to the organization's systems and services.
- Refrain from exploiting the vulnerability for personal gain or malicious purposes.

Any actions taken outside of this policy or malicious exploitation of vulnerabilities will void safe harbor protection and may result in legal consequences.

9. Legal Considerations

This policy is designed to align with legal frameworks governing cybersecurity and vulnerability disclosure. Key considerations include:

- **Data Protection**: Vulnerabilities involving personal data must be handled in compliance with relevant data protection regulations, such as the **UK GDPR** or **EU GDPR**.
- **International Disclosure**: In cases where vulnerabilities are discovered across jurisdictions, the organization will comply with applicable laws and work with local authorities, or third parties as required.
- **Third-Party Vulnerabilities**: When vulnerabilities are identified in third-party components, the organization will follow established processes for reporting the issue to the vendor and work collaboratively to address the issue.

10. Policy Updates

The organization commits to regularly reviewing and updating this policy to reflect evolving best practices in vulnerability management and changes in the cybersecurity landscape. Any updates to this policy will be communicated publicly, and the policy will be made available on the organization's website.

11. Conclusion

this document implies a well-defined and comprehensive Vulnerability Disclosure Policy fosters trust between the organization and external stakeholders, including security researchers and users. It establishes a clear process for responsibly managing vulnerabilities while mitigating potential risks. By adhering to this standard, the organization demonstrates its commitment to safeguarding the security and privacy of its systems, users, and data.