Coordinated Vulnerability Disclosure (CVD) Policy

1 Purpose

Our organization is committed to maintaining a high level of cybersecurity. This Coordinated Vulnerability Disclosure (CVD) Policy describes how external parties can report potential security vulnerabilities and how we handle such reports responsibly.

2 Scope

This policy applies to all digital products, services, and systems operated by **ApplicGate Network Security e.U.**, unless explicitly excluded.

3 Reporting a Vulnerability

Researchers can report suspected vulnerabilities through the following channel:

- **Email:** security@applicgate.com

Please include:

- A detailed description of the vulnerability
- Steps to reproduce
- Potential impact
- Any supporting evidence (screenshots, logs, proof-of-concept)

4 Expectations for Researchers

We ask that researchers:

- Act in good faith and avoid privacy violations, service disruptions, or data destruction
- Do not access more data than necessary to demonstrate the vulnerability
- Do not publicly disclose the vulnerability before we complete remediation
- Follow applicable laws and avoid exploiting the vulnerability beyond what is required for reporting

5 Our Commitments

Upon receiving a report, we will:

- Acknowledge receipt within **5 business days**
- Provide regular updates on the remediation progress
- Work to resolve the issue within **90 days**, depending on complexity
- Credit the researcher publicly (if desired) after the issue is fixed
- Not pursue legal action against good-faith research conducted under this policy

6 Recognition

We may offer:

- Public acknowledgment on our “Security Hall of Fame” page
- Optional certificates of appreciation
- Additional recognition depending on the severity and impact of the vulnerability

7 Legal Considerations

This policy is designed to align with applicable laws, including EU cybersecurity and data protection regulations. Researchers acting in good faith within the boundaries of this policy will not be penalized.

8 Policy Updates

We may update this policy periodically to reflect legal, technical, or organizational changes.

9 Table of Contents