Proemion Vulnerability Disclosure Policy

Aligned with ISO/IEC 29147:2018, ISO/IEC 27001:2022 (Annex A.5.24–A.5.27), and EU Cyber Resilience Act requirements

V1.0

Date 16/01/2026

Introduction

Proemion is committed to protecting the security of our products and services and the data of our customers. We recognize the valuable role that independent security researchers and our users play in identifying vulnerabilities in our software and hardware products. This Vulnerability Disclosure Policy (VDP) outlines a framework for responsible, coordinated disclosure of security flaws, enabling us to remediate issues while keeping customers safe. It is aligned with international best practices (ISO/IEC 29147:2018 for vulnerability disclosure and ISO/IEC 27001:2022 incident management controls) as well as the EU Cyber Resilience Act's requirements for coordinated vulnerability handling. The policy is intended for public consumption – providing transparent, professional guidance to researchers – and forms part of Proemion's Information Security Management System (ISMS). We view every reported vulnerability as an opportunity for continual improvement in our security processes.

Scope and Purpose: This policy applies to all Proemion products and services – including our telematics hardware devices and their firmware, software applications (web, mobile, cloud APIs), and other systems under Proemion's control. It defines how to report potential security vulnerabilities, what is in scope or out of scope for testing, what to expect in terms of Proemion's response and timelines, and the legal safe harbor assurances we offer to good-faith researchers. By publishing this policy, Proemion seeks to foster an environment of mutual trust and transparency between our organization and the security community, in line with the principles of coordinated vulnerability disclosure. We will publicly acknowledge researchers for valid reports and are dedicated to handling disclosures in a timely and responsible manner.

Reporting a Vulnerability

If you believe you have discovered a security vulnerability in a Proemion product or system, please report it to us as soon as possible. Our primary channel for vulnerability reports is email:

- **Email:** infosec@proemion.com

We kindly ask that you encrypt sensitive vulnerability reports if possible (PGP key available on request) or otherwise include "[VDP]" in the email subject for prompt handling. You may submit reports anonymously if you prefer. If you do share contact information, we will use it only for coordination and to provide you updates, and will not share your identity without permission.

Report Details: To help us triage and understand the issue quickly, please include as much of the following information as possible in your report:

- **Affected product or system:** The name of the product, hardware model, software application, website or IP address where the vulnerability was observed. Include version numbers or device firmware versions if applicable.
- **Vulnerability description:** A summary of the type of issue (e.g., buffer overflow, SQL injection, authentication bypass, etc.) and the potential impact. For example, *"Cross-site scripting (XSS) on the DataPortal user settings page allows theft of user session tokens."*
- **Reproduction steps:** A detailed, step-by-step description of how to reproduce the issue. If possible, provide a proof-of-concept (PoC) script, exploit, or screenshots that illustrate the vulnerability in action. This should be a benign proof-of-concept that does not harm data or systems (e.g., use non-destructive commands).
- **Suggested fix or mitigation (optional):** If you have suggestions for how to remediate the issue, we welcome them. Any insight into root cause or potential fixes can help accelerate our remediation efforts.
- **Your contact and preferences:** Let us know if you wish to be publicly acknowledged for the discovery or if you prefer to remain anonymous. Also indicate any urgency if you believe the issue is being actively exploited.

Please **do not** include sensitive personal data of others in your report. If user data was exposed, describe the nature of the data exposure without sending actual data. If needed, we can arrange a secure method to share such details.

When we receive your report, we will use the information for defensive purposes only: to verify the vulnerability, develop a fix or mitigation, and improve our security. If the reported issue affects a third-party component or another vendor's product as well as a Proemion product, we may share relevant details with that vendor or with the appropriate coordinator (such as a CERT) **as part of a coordinated disclosure process**, consistent with industry practice. We will not share your personal information with any third party without your explicit permission.

Scope of Vulnerability Testing

We encourage responsible security research on our products and systems covered by this policy. Below we outline what is in scope for testing and reporting, as well as activities and issues that are considered out of scope.

In Scope: Any vulnerability that **directly** affects the confidentiality, integrity, or availability of a Proemion product or customer data is within scope. This includes, but is not limited to:

- **Proemion hardware devices and firmware:** e.g. CANlink® telematics gateways, wireless modules, IoT devices, and their embedded software.
- **Proemion software and services:** e.g. the Proemion DataPlatform cloud services, DataPortal web application, Cloud CAN Connector, Remote Service Tool, Machine Companion mobile app, ProInsights platform, and any official APIs or web services under the *.proemion.com domain.
- **Corporate websites and infrastructure under proemion.com:** e.g. our main website, support portals, documentation sites, or other publicly accessible systems operated by Proemion.
- **Open source or third-party components** in the above products, *only insofar as* the vulnerability is manifest in Proemion's implementation. (We will coordinate with the component maintainers as needed.)

If you are unsure whether an asset or product is in scope, please contact us at infosec@proemion.com for clarification *before* proceeding with testing. We may

expand the scope of this policy over time, and we welcome discussions about including additional systems.

Out of Scope: The following types of testing or issues are **excluded** from this policy and are not authorized:

- **Physical attacks or social engineering:** Any attempt to gain access to Proemion offices, hardware labs, or to trick our employees, partners, or customers (phishing, vishing, etc.) is not permitted. For example, do not attempt to obtain sensitive information by impersonating personnel or through coercive means.
- **Denial of Service (DoS/DDoS) and brute-force attacks:** Do not perform any testing that degrades the performance or availability of our systems. This includes overwhelming network services, flooding interfaces with high-volume requests, or other disruptive automated scanning. Even if a vulnerability might theoretically permit a DoS, such testing should be coordinated with us separately.
- **Exploiting or accessing other users' data:** You must not intentionally access, copy, or modify data that isn't yours. If during your testing you inadvertently access confidential data (including personal data), you should stop immediately, report the issue, and not further interact with the data. Any such data should not be saved, shared, or retained after reporting.
- **Excessive or destructive exploits:** Do not use exploits beyond what is necessary to confirm a vulnerability's existence. For instance, once you have proven that you can execute code or extract one record, do not proceed to extract additional data or pivot to other systems. Avoid techniques that might crash systems or corrupt data.
- **Non-technical issues and best-practice critiques:** Findings that do not pose a real security vulnerability, such as reports solely about missing security headers, outdated software versions without a known exploit, use of deprecated protocols (e.g. TLS 1.0) without evidence of impact, or other "best practice" configuration gaps, are generally out of scope. We focus on issues that demonstrably affect security. (If you have such suggestions for improvement, you can still share them with us, but they may not qualify for acknowledgment under this VDP.)

- **Third-party products and services:** Vulnerabilities in systems not owned or operated by Proemion are out of scope and should be reported to the appropriate vendor. For example, if the issue lies in a library or platform we use, and not in how Proemion implements it, consider reporting to that vendor directly. (If unsure, report to us and we will route it appropriately.)
- **Compliance or policy issues:** This VDP is not a channel for reporting non-security bugs, content issues, license/compliance issues, or complaints about our services that are unrelated to security. Those should be directed to our customer support.

Any activities falling outside the scope of this policy will be considered unauthorized. Additionally, **do not perform testing on any system without explicit permission** if it's not covered here. Testing other companies' systems or our customers' data through our platform is strictly prohibited.

Guidelines for Good-Faith Security Research

When conducting security testing on in-scope Proemion products, we ask that you adhere to the following guidelines to ensure your actions remain in good faith and authorized:

- **Do no harm:** Your testing should never intentionally cause degradation of our services or harm to other users. Use non-destructive methods of proof-of-concept and avoid any actions that could disrupt service or endanger data.
- **Respect privacy:** Make every effort to avoid accessing or exposing personal information, confidential business data, or sensitive intellectual property. If a vulnerability potentially exposes such data, demonstrate the issue with a minimal example and **cease further exploration** of sensitive data. Immediately report the situation to us so we can contain any privacy risks.
- **Limit scope of exploitation:** Only use exploits or techniques **to the extent necessary** to confirm the presence of a vulnerability. Do not exploit a vulnerability to pivot to other systems, establish persistent access, or exfiltrate data. For example, if testing reveals you can drop into a system shell, do not proceed to elevate privileges or explore the internal network.
- **Maintain confidentiality:** Do not publicly disclose or share any details of the vulnerability with anyone else until we have had a reasonable time to resolve it.

Coordinated disclosure means **you report to us first**, we work together on a fix, and then public disclosure happens in an agreed manner. Premature public disclosure can put users at risk, so please refrain from posting information in public forums, social media, etc. while remediation is in progress. (We generally expect researchers to avoid public disclosure for at least 90 days, or longer if mutually agreed, as discussed in the next section on timelines.)

- **No extortion or blackmail:** Report vulnerabilities to us with the goal of improving security, not for personal financial gain. We **do not permit any form of extortion** – for example, asking for money in exchange for withholding disclosure or threatening to release data. We will not negotiate pay-offs, and any such behavior will be considered malicious, not in good faith.
- **Follow applicable laws:** You must abide by all relevant laws during your research. For example, do not engage in unauthorized access beyond what this policy permits, and do not violate privacy laws or abuse data. This policy is meant to offer you safe harbor (as described below) for lawful, good-faith research – it is not an immunity from legal consequences if laws are egregiously broken. In short, **do not do anything that would be illegal outside the scope of this policy.**

By following these guidelines, you help ensure that any security testing remains non-intrusive, lawful, and beneficial. Proemion will consider your activities to be "authorized" and in good faith as long as you **play by these rules** and the ones outlined in the Scope section above. Our goal is to work **with** you, not against you, to resolve vulnerabilities and protect users.

If you are ever in doubt about whether an action might be going out of bounds, **stop and contact us**. We are happy to clarify any uncertainty about scope or acceptable techniques. Open communication will always be valued and will help protect both you and Proemion.

Our Commitment to Researchers

When you report a vulnerability to Proemion, you can expect us to handle it with professionalism and gratitude. We commit to the following actions and timelines, aligned with industry best practices for coordinated disclosure:

- **Prompt Acknowledgment:** We will acknowledge receipt of your vulnerability report **within 7 calendar days**. In practice, our goal is to respond as soon as

possible (many organizations target acknowledgment within 48 hours). If you haven't heard from us within a week, please feel free to reach out again – it's possible we may not have received your report.

- **Assessment and Triage:** Our security team will investigate and validate the reported issue. We will make every effort to triage the report and determine its validity and impact within **10 working days** of acknowledgment (often sooner for critical issues). During this phase, we might contact you for clarification or additional information. Please be responsive to any follow-up questions – your insights can help us reproduce and understand the problem.
- **Remediation Plan:** Once the issue is validated, we will work on fixing it. We prioritize remediation based on the severity of the vulnerability and the complexity of the fix, taking into account potential impact on users. For complex or high-impact products (especially hardware or firmware), some fixes might require thorough testing. However, we **aim to remediate vulnerabilities within 90 days** of the report whenever feasible, in line with common 45–90 day disclosure timelines in the industry. If a fix cannot be developed within 90 days, we will communicate with you about the delay and may ask for an extension of the disclosure timeline.
- **Status Updates:** We will keep an open line of communication and strive to be as transparent as possible about our progress. At minimum, we will notify you when the vulnerability has been confirmed and when a fix has been implemented. We may also provide interim updates (for example, if a patch is in testing or if a rollout is planned). Our goal is to ensure you are not left in the dark. You are welcome to inquire about the status at reasonable intervals (we kindly ask that you avoid overly frequent check-ins, such as more than once every two weeks, to allow our team to focus on the fix).
- **Validation of the Fix:** After we deploy a fix or mitigation, we will inform you of the closure of the vulnerability. If feasible, we may invite you to test or validate that the solution adequately resolves the issue. Your re-testing can help confirm that the vulnerability is fully addressed. If the fix does not fully resolve the issue, we ask that you let us know immediately so we can continue to work on it.
- **Coordinated Disclosure & Public Notification:** In alignment with the EU Cyber Resilience Act and ENISA guidelines, once a security fix is available, Proemion will **publicly disclose information about the vulnerability and its resolution** in a

security advisory or bulletin. This disclosure will include a description of the issue, affected products, severity, and mitigation steps for users, but will not expose exploit details that could harm users who haven't updated. We will time this public disclosure to ensure users have had a chance to patch (generally, we publish advisories when releasing the fix or shortly after). We will **credit you, the researcher, for the discovery** in the advisory or on our website Hall of Fame, **if you desire public acknowledgment**. (If you prefer to remain anonymous or to use an alias, we will honor that.) Our acknowledgment is our way of thanking you for helping improve security.

- We ask that you **delay any public disclosure** (e.g. blog posts, conference talks) until we have jointly agreed it is appropriate. In most cases, this means waiting until the fix is released or the 90-day window has passed. We are open to discussing the timing of public release with you to accommodate things like conference deadlines while ensuring users are protected.
- **No Compensation (Currently):** Proemion does not offer a paid bug bounty program at this time, and we do not provide monetary rewards for vulnerability reports. Our commitment is to address the issue promptly and give you credit for the discovery. By submitting a report, you acknowledge that you are not entitled to financial compensation. We hope that our acknowledgement and the improvement of product security serve as thanks. (If our policy changes in the future to include rewards, we will update this document accordingly.)

Throughout this process, we promise to treat you with respect and consideration. We understand that reporting a vulnerability can be an act of trust, and we appreciate your effort to help us. Our security team is committed to working **with** you in a constructive manner – our questions or comments will remain professional, and we will avoid any unnecessary secrecy or delay. If at any point you feel we are not meeting these commitments, please let us know and we will do our best to address the concern.

Finally, once the vulnerability is fully resolved, we would like to publicly thank you for your contribution to our security (subject to your consent as noted). We maintain a **"Security Researchers Acknowledgement"** page on our website to recognize those who have helped improve our products. This public acknowledgment is optional – if you prefer to stay unnamed, that's absolutely fine. The important thing is we greatly appreciate your help in keeping Proemion and our users safe.

Safe Harbor Policy

This policy is intended to provide you with **safe harbor** for your security research activities, as long as those activities are conducted in good faith and in accordance with this policy. “Safe harbor” means that Proemion **authorizes** your research on our in-scope systems and will not pursue or support any legal action against you for security testing **that aligns with the guidelines and scope of this policy**. In fact, we consider such activities to be **exempt** from any restrictions in our terms of service that might otherwise be interpreted to prohibit security testing. We will not penalize or suspend your access to our services if you are acting in line with this policy.

Specifically, we commit that **no action will be taken** (be it civil, criminal, or via law enforcement) against researchers who:

- Act in good faith to discover and report vulnerabilities.
- Respect the rules of engagement defined in this policy (scope limitations, guidelines on methods, no harm done, etc).
- Avoid compromising privacy or causing damage.
- Report the issue to us privately and give us a reasonable opportunity to fix it before any public disclosure.
- Do not engage in malicious activities or extortion.

If a third party initiates legal action against you for activities conducted under this policy, Proemion will make it known that your actions were **authorized** and **encouraged** as part of our vulnerability disclosure program. For example, if someone accuses you of violating the law (such as anti-hacking statutes) for your good-faith research, we will confirm that we invited such research and that it was beneficial to our security.

However, it is important to understand that this safe harbor is **null and void** for any activities that are **not** in good faith or not in compliance with this policy. If you engage in prohibited actions (for instance, exploiting data beyond what’s necessary, causing intentional harm, or targeting out-of-scope systems), or if you break any applicable laws, this safe harbor protection may not apply. This policy does **not** provide you a free pass to perform acts that would otherwise be illegal or unethical.

We believe that a strong safe harbor commitment is fundamental to encouraging researchers to come forward with security findings. We want you to feel safe and protected when helping us. To that end, we have designed this policy in alignment with EU best practices on coordinated vulnerability disclosure and safe harbor provisions. Our intent is to **minimize uncertainty** for researchers: if you follow the rules in this policy, then you are conducting authorized activity. This policy and our authorization herein will serve as your defense against any claim that your accessing of our systems was unauthorized or unlawful.

Note: This safe harbor provision is provided in good faith, but it does not supersede or contradict applicable law. It is meant to ensure Proemion's stance on your research is non-adversarial. We cannot bind external parties, but we will do our utmost to protect well-intentioned researchers. If you have any questions or concerns about whether your activities will be protected by this policy, please discuss them with us before proceeding.

Continuous Improvement and Feedback

Proemion is dedicated to continuously improving our security posture and incident response processes. All vulnerability reports are logged and reviewed not just for immediate fixing, but also for lessons learned. Our internal security team conducts post-incident analyses to determine how we can prevent similar issues in the future and strengthen our development practices. This aligns with ISO/IEC 27001:2022 control A.5.27 on learning from information security incidents – every valid report contributes to making our products and processes more robust over time. We truly consider the security research community an extension of our team, helping us safeguard our technology ecosystem.

If you have any **questions** about this policy or suggestions to improve it, please contact us at infosec@proemion.com. We welcome feedback. In fact, this policy itself will be reviewed and updated periodically (especially as laws, regulations, or best practices evolve – for example, to remain compliant with the latest EU cybersecurity directives and the Cyber Resilience Act). Any changes will be published on our website along with a change log.

Thank you for reading Proemion's Vulnerability Disclosure Policy. Your efforts to responsibly disclose security issues help us ensure the safety and reliability of our

products and protect our customers. We appreciate your contributions to our security and will strive to reciprocate your trust with a prompt, professional response. Together, through coordinated disclosure, we can build more secure products and a safer connected world.

Proemion Information Security Council

Last updated: January 23, 2026

Appendix A

Security.txt file structure example

Path:

`/.well-known/security.txt` (recommended)

and optionally also `/security.txt`

```
Contact: mailto:infosec@proemion.com

Preferred-Languages: en, de

Policy:  https://www.proemion.com/security/vulnerability-disclosure-policy

Acknowledgments: https://www.proemion.com/security/acknowledgments

Disclosure: https://www.proemion.com/security/vulnerability-disclosure-policy#coordinated-disclosure

Encryption:  https://www.proemion.com/.well-known/pgp-key.txt

Hiring: https://www.proemion.com/careers

Canonical:  https://www.proemion.com/.well-known/security.txt

Expires: 2027-01-31T00:00:00Z
```