Vulnerability Disclosure Policy

Overview of the Vulnerability Reporting Program / Policy

Kia India Private Limited ("**Kia India**" or "**We**") values the contributions of security researchers ("**Your**" or "**You**") and welcomes any information about potential cybersecurity vulnerabilities that can strengthen the security of our products and services in India, including our vehicles, websites, mobile applications, and digital services. As part of Kia's global commitment to cybersecurity, we are dedicated to investigating and responding to all legitimate vulnerability reports submitted in accordance with this Vulnerability Disclosure Policy (this "**Policy**").

If you discover any potential vulnerability in any Kia India product or service, we kindly request you to report it to us following the guidelines, as stated in this Policy. To ensure a coordinated response, please refrain from publicly disclosing any vulnerabilities until Kia India has had the opportunity to examine and analyse the issue and, if necessary, implement appropriate measures.

Please note that this program is designed solely to facilitate responsible vulnerability reporting and resolution. Kia India does not offer monetary compensation ("**bounties**") or non-monetary rewards for any submitted information or reports. Additionally, vulnerabilities or issues related to Kia India's or any of Kia's products, services, or IT environments outside of India and not specifically mentioned herein are out of scope for this program.

All information disclosed by you will be considered as confidential and will not be disclosed, except as required by any law, rule, regulation.

Scope of Vulnerability Disclosure

Please notify Kia India, as soon as possible, after you identify a potential vulnerability or security threat to **isms@kiaindia.net**. We currently accept reports about potential vulnerabilities related to the following Kia India products and services:

a. Kia Vehicles Manufactured or Sold in India.
b. Kia India Website (https://www.kia.com/in);
c. MyKia (India) Mobile Application;
d. Kia Connect Mobile Application;
e. Kia Smart Test Drive Mobile Application;
f. KDA Sales India Mobile Application; and
g. Related Digital Services under Kia India's Direct Control.

Vulnerabilities or issues found in Kia India products or services not listed above are considered out of scope for this Policy.

Vulnerability Disclosure Submission / Reporting Rules

For reasons of transparency between you and Kia India, we advise you seek prior written consent from Kia India, prior to conducting any test, research on any of Kia India's products, services, or its information technology environments.

By submitting, reporting a vulnerability / incident / potential security threat under this program, you acknowledge and agree to the following terms as listed below, which form an integral part of Kia India's Vulnerability Disclosure Policy:

a. You shall conduct all testing, research, and reporting activities in compliance with this Policy and any applicable laws, rules, regulations.

b. You shall not engage in testing or research of the vulnerability / security threat that may harm or put at risk the following, but not limited to Kia India, its affiliates, employees, customers, passengers in Kia vehicles, or any third-party individuals or entities, including Kia India dealerships and their employees.

c. You shall not disrupt, compromise, or harm any vehicle or data or any information technology environments owned or operated by Kia India, except those you own.

d. You shall not under any circumstances attempt to or gain access, exploit, modify, disclose, destroy, alter, delete, add or misuse any data, information, Kia India systems, website, code, application (including any personal data) belonging to Kia India customers, passengers, employees, third parties, which could impact their privacy.

e. You shall not compromise or disclose any data (be it confidential or proprietary information or non-confidential) belonging to Kia India, its affiliates, directors, officers, employees, customers, or third-party entities, including Kia India authorized dealerships and their employees.

f. You shall not test any security features / measures (including any protocols, procedures as applicable to information technology environments operated by or of Kia India) specific to Kia India's properties, facilities, or those of its affiliates or related third parties, including dealerships.

g. You shall not perform any denial-of-service (DoS) testing or actions that may contribute in over-exhausting the Kia India's information technology systems / environments or functions.

h. You shall not conduct social engineering, spam, phishing, or spear-phishing attacks.

i. You shall not by yourself or via any other individual, agency or entity, test the vulnerability / security threat (either directly or indirectly) after the intimation / reporting of the vulnerability / security threat to Kia India.

j. You shall not disclose any details of a submitted vulnerability to any individual, entity or any third parties (directly or indirectly or privately or publicly) before Kia India confirms complete remediation of the identified issue (if any) or mutually agrees otherwise. If any such details are to be disclosed then you shall seek prior written consent of Kia India, prior to any such disclosure.

k. If you are employed by Kia India, its affiliates, suppliers, or are acting on behalf of such an entity, please report the issue to your management for internal handling rather than submitting it through this program.

l. You shall have no expectation of any payment / monetary reward and you waive any future claims (whether made by you or any other person / party related to you) in relation to the vulnerability disclosure / report submission.

Items Not Considered as Vulnerabilities

The following are not considered as valid vulnerabilities under this Policy:

a. Reports from physical security testing of Kia India facilities or properties, or physical attacks (e.g., destruction of vehicle locks, relay/roll-jam attacks, gaining access via physical means).
b. Denial-of-service testing or actions causing IT function overload.
c. Vulnerabilities in systems not under Kia India's direct control (e.g., misconfigured third-party systems).
d. Issues unrelated to cybersecurity vulnerabilities (e.g., use of valid diagnostic functions).
e. Social engineering attacks (e.g., phishing) or speculative/self-exploitation reports (e.g., Self-XSS, cookie reuse) lacking evidence or exploitability details.

If a reported issue involves a third-party library, external project, or vendor, Kia India will forward the details to the appropriate party and communicate progress as needed, without any further obligation to the researcher.

Disclosure Submission Procedure

When submitting a vulnerability report, please include:

a. **Date and Time** – When the vulnerability was discovered.
b. **Detailed Steps to Reproduce** – A clear description of how the vulnerability was identified, along with reproducible steps.
c. **Proof-of-Concept Code (PoC)** – Where possible, provide a PoC to facilitate analysis and triage.
d. **General Conditions & Prerequisites** – Any conditions that must be met to exploit the vulnerability.
e. **Configuration Details** – The setup and modifications of Kia India products or services where the vulnerability was found.
f. **Impact** - Describe the potential impact, if the vulnerability is exploited / publicly disclosed.
g. **Potential Fixes or Recommendations** – Any known or possible remediation strategies.
h. **Contact Information** – Unless you wish to remain anonymous, provide your name, phone number, and email address for follow-up communication.
i. **Geographical Location and Miscellaneous** – Exact location (city, state, country) where the vulnerability was identified. Also share the relevant screenshots, attachments specifying the file size.

All the information under this, shall be communicated to Kia India, preferably in English language only.

Final Notes

Kia India sincerely appreciates the efforts of security researchers in helping us maintain the security of our products and services. By submitting a report, you contribute to our mission of ensuring a safe and secure experience for our customers. We will strive to maintain clear and timely communication throughout the process.

If you believe you have found a valid cybersecurity vulnerability, submit your findings via email to **isms@kiaindia.net**.

We aim to acknowledge your submission within **3 (three) business days**. Please refrain from disclosing vulnerability details to third parties until we have completed our analysis and remediation.

For any questions about this policy or the submission process, please contact us at **isms@kiaindia.net**

You are welcome to enquire about the status of the vulnerability resolution process, specific to your submission only, but we request you to limit the enquiry to only once in 30 (thirty) days.

We also invite you to share your suggestions towards improvement of this Policy. Please send in your suggestions at **isms@kiaindia.net**