Coordinated Vulnerability Disclosure

At AIS, the safety of information asset and system infrastructure are our priority. We support the good-faith security research community and welcome reports of vulnerabilities in our systems. To report potential vulnerabilities, please follow the report submission. instruction below

Please note, AIS does not offer a bug bounty program or compensation for this disclosure, however we will recognize your generosity.

Report Submission

Vulnerability information is extremely sensitive. Please submit the reports directly to vulnerability@ais.co.th and encrypt the report using our PGP public key.

It is critical to include the following information in the report:

- Your name, organization and contact information
- The affected system
- A detailed summary of the potential security vulnerability that you identified
- Supporting technical details, including descriptions or examples of exploit/attack code, packet captures, screen captures, and steps to reproduce the issue
- Your disclosure plans, if any

Coordinated Vulnerability Disclosure Guideline

- We will acknowledge your report as soon as we can.
- You shall avoid any privacy violations, destruction of data, and interruption or degradation of our services including the use of vulnerability scanning tools.
- You shall limit the amount of data you access to the minimum required for effectively demonstrating a Proof of Concept.
- You shall not store, share, compromise or destroy AIS or customer data. If Personally Identifiable Information (PII) is encountered, you immediately halt your activity and purge related data from your system.
- You shall not put a backdoor in the system, not even for the purpose of showing the vulnerability.
- We will keep all information confidential and work with you to make sure we understand the issue and address it as quickly as possible.
- After determine that a reported issue is a security vulnerability, we will collaborate to implement compensating controls, remediate the issue, and inform all parties as necessary based on the risk associated with the vulnerability.
- We request that you do not disclose any information publicly or share with any third-party until we have been able to understand the impact and mitigate the risk.

Any actions other than this guideline may be considered not using good faith to our company.

Out of scope vulnerability

These out of scope security vulnerabilities include, but are not limited to:

1. Physical testing
2. Social engineering
3. Phishing
4. Denial of service attacks
5. Resource Exhaustion Attacks
6. Utilize any brute-force techniques

AIS does not authorize or permit anyone to engage in any illegal activity. We are thankful to you for taking the time to report to us to help us improve and strengthen the safety of our systems.