Guideline on Possible Cyber Security Vulnerability and Breach Reporting

True Group (hereinafter referred to as "the company", "we" or "our") welcomes any reports on the possibility of cyber security vulnerabilities or breaches.

For accurate and effective reporting, we ask that you follow the key points in this guideline. We would like to inform you that the company does not have any policies on providing reporting compensation and would like to express our deep appreciation for your goodwill.

If you found any possible cyber security vulnerabilities or breaches, you can send a report to Vulnerability@truecorp.co.th with the following details:

- your name and contact information;
- the affected system and a summary of the detected cyber security vulnerabilities or breaches;
- any supporting technical details, with an explanation or an example of detected system testing, e.g. exploit or attack code, packet captures, or screen captures, as well as your testing procedures.

After receiving the report, we will proceed to verify the information and work with you to investigate the root cause and find a solution as soon as possible. Your information will be kept confidential throughout the process.

In order to ensure that the reports are complied with our privacy policy and Cyber Security Policy, we ask that you report any possibilities of cyber security vulnerabilities and breaches with the following guidelines:

- avoid any actions that may violate, destroy, alter, or interrupt services, including employing vulnerability scanning tools;
- be mindful of the amount of data used during Proof of Concept (POC) and keep the amount to a minimum;
- do not store, distribute, control, or destroy any information of the company or its service users;
- in case of Personally Identifiable Information (PII) access, immediately cease the access and remove the data from your system;
- do not use Backdoor or any unauthorized methods in your system that may cause vulnerability or breach;
- keep all the related information about the cyber security vulnerability or breach confidential and do not disclose any information to the public or distribute them to external parties.

We do not condone or allow any illegal activities. Any actions that violate the legal principles are to be considered direct damage to the company, and legal actions will be taken against all involved in the activities.

The followings are the list of actions that are considered to be damaging to the company's Information Technology system but do not fall under the scope of cyber security vulnerability and breach reporting:

1. Physical Testing;
2. Social Engineering;
3. Phishing;
4. Denial of Service Attacks;
5. Any attacking methods that aim to deprive the system's resources;
6. Brute Force Attacks.

Once the cyber security vulnerability or breach is assessed, we will proceed to notify all the parties involved in order to promptly correct and improve the infrastructure. We would like to thank everyone for taking the time to report the incidents so as to achieve a safer and more secure system.