LINE Security Bug Bounty Program

LINE Corporation (“the Company”) will conduct the LINE Security Bug Bounty Program ("the Program") from June 2, 2016, whereby cash rewards will be paid for vulnerability reports, for the purpose of improving the security of the Company's online environment. Individuals desiring to participate in this program and receive a cash reward must agree to the provisions stipulated below ("these Terms of Service"). Individuals submitting a vulnerability report shall be deemed to have granted their agreement to these stipulations.

Article 1 (Purpose)

The purpose of the Program is to quickly discover any vulnerabilities that exist in the LINE messenger app (LINE for iOS, LINE for Android latest version in the time of reporting) (“the App”), and provide LINE users (“Users”) the most secure service possible.

Article 2 (Qualifications for Participation, How to Participate, etc.)

1. Those who wish to participate in the Program ("Participants") must:
   (i) be an adult
   (ii) not be an employee of the Company or an affiliated company
   (iii) not be an entity or part of an entity that had carried out or is carrying out a project that is being advanced with the Company
   (iv) be able communicate in Japanese or English
   (v) not reside in a country subject to Japanese or US economic sanctions at the time of reward payment for the Program
2. To take part in this Program, a Participant must create an account (“the Account”) in the website specified by the Company (URL: https://bugbounty.linecorp.com/apply/) to report vulnerabilities. In creating an Account, Participants are required to enter information requested by the Company.
3. Any expenses incurred by Participants as a result of participating in the Program shall be borne by the Participants.
4. If the Company must contact Participants for reasons related to the operation of the Program, they will be contacted via their Account.

Article 3 (Eligibility)

1. Cash rewards are limited to vulnerabilities found in LINE Corporation services that are displayed in the latest version of the App (LINE for iOS, LINE for Android latest version in the time of reporting) and have one of the following domains. However, LINE-related apps that are activated via another process after clicking a link within the App (LINE Family apps, LINE Game apps, etc.) are not eligible.
   (i) *.line-apps.com
   (ii) *.line.me
   (iii) *.line.naver.jp
2. Vulnerabilities not eligible for cash rewards include, but are not limited to, the following:
   (i) Reporting a vulnerability as-is after detection using an automated scanner
   (ii) Reporting hypothetical or theoretical vulnerabilities without actual verification code
   (iii) Reporting the susceptibility to a denial-of-service attack
   (iv) Reporting the susceptibility to brute force attacks aimed at retrieving passwords or tokens
   (v) Reporting the ability to spam LINE users arbitrarily with spam messages
   (vi) Reporting on the deficiencies of e-mail verification, expiration of password reset links, policy on password complexity, etc.
   (vii) Reporting on the absence of Cross-Site Request Forgery ("CSRF") token in non-critical processes
   (viii) Reporting login/logout CSRF
   (ix) Reporting the susceptibility to an attack via physical access to a user's device
   (x) Reports related to missing security header
   (xi) Reporting of script executions that do not affect Users
   (xii) Reporting of vulnerabilities found in services and devices beyond the scope of this program such as:
      (a) Domains other than *.line.me, *.line-apps.com, *.line.naver.jp
      (b) Platforms other than iOS and Android
      (c) LINE Family apps and/or LINE Games apps
   (xiii) Reporting vulnerabilities attributable to out-of-date browsers or platforms

(xiv) Reporting of content related to an auto fill web form
(xv) Reporting of absence of secure flag attribute for non-critical cookies
(xvi) Reports related to unsafe SSL/TLS ciphers
(xvii) Reporting of accessibility of user data via rooting device
(xviii) Reporting of accessibility of profile photos, Timeline photos, etc. by anyone via URL
(xix) Reporting of vulnerability attributable to virtual phone number
(xx) Reporting of vulnerability of which the Company has already received a report, or which the Company is already aware (including those attributable to specifications approved by the Company), or which has already been made public
(xxi) Reports related to the server banner information
(xxii) Reports related to information attributable to error messages (stack trace, server or application errors)
(xxiii) Reports related to a domain's SPF record, DMARC, or DKIM not being set
(xxiv) Reporting that an unauthorized HTTP method can be used
(xxv) Reports related to clickjacking

Article 4 (Program Dates)

1. In principal, the Program shall be conducted indefinitely from June 2, 2016. However, the Company may terminate provision of the Program without notice when circumstances so require.
2. Even in the case where the Company terminates provision of the Program per the preceding clause, the Company will continue to review the vulnerabilities reported by Participants, and the Participants will maintain their status as Participant until the results of their reported vulnerabilities are announced.

Article 5 (Reporting)

Participants are to report vulnerabilities using the Account that they create. Reports made by means other than the Account shall not be eligible for cash rewards.

Article 6 (Cash Rewards)

1. The Company will decide the cash reward at its own discretion, and based on the seriousness and novelty of the vulnerability reported. Refer to the table below regarding reward value guidelines.

Vulnerability	Description	Reward Ex.
SQL Injection	Ability to access private information through SQL injection attack	$3,000
Cross-Site Scripting (XSS)	Ability to hijack session or execute scripts through XSS attack	$500
Cross-Site Request Forgery (CSRF)	Ability to force the User to perform an undesired process through CSRF attack	$500
Remote Code Execution	Ability to execute arbitrary codes on a client or server	$10,000
Authentication Bypass	Ability to masquerade as another person by bypassing authentication procedures	$5,000
Purchase Bypass	Ability to obtain items while bypassing in-app payment procedures	$5,000
Encryption Break	Ability to obtain another person's authentication information by decrypting an encrypted communication	$10,000
Other	Other vulnerabilities	$500

Please note that the reward values are only a guide, and the monetary value stated for each vulnerability is not guaranteed.

2. In cases where the Company receives reports for similar vulnerabilities, it shall treat those that it determines to be the same vulnerability as one vulnerability. This includes but is not limited to:
   (i) the same vulnerability can be exploited under multiple parameters through a single method
   (ii) the same vulnerability exists for a method that runs across multiple domains
3. If the same vulnerability is reported by multiple participants, a cash reward will be paid only for the first report submission that the Company receives.
4. If the Company determines that a vulnerability reported by a Participant is

eligible for a cash reward, the Company will contact and inform the Participant.

5. Participants shall receive cash rewards via the following method. Participants shall promptly provide all valid and credible information ("the Information") needed for the remittance of cash rewards of which the value is determined by the Company if they receive a request to provide Information from the Company via their Account. Participants are deemed to have waived the right to receive their reward if they do not supply the relevant information within one month of the request from the Company. Bank transfer fees to deposit cash rewards shall be borne by the Company. (The same applies to all clauses in this paragraph hereafter.)
   (i) Participants with a Japanese bank account:
   Cash rewards are paid in Japanese yen via deposit to the Japanese bank account. For converting the cash reward into Japanese yen, the Company shall use the Company's designated exchange rate of the final date of the month in which the Participant reported a vulnerability that led to a cash reward. If said day is a Sunday or public holiday, the exchange rate of the previous business day will be applied (rounded down to the nearest yen).
   (ii) Participants with a foreign bank account:
   Cash rewards are paid in US dollars via deposit to the foreign bank account.
6. The only eligible bank account to receive a cash reward is one for which the name of the account holder is the same as the name provided in the Information stipulated in the preceding paragraph.
7. In cases where there is a legal requirement to pay withholding income tax for the cash reward given to a Participant, the Company shall pay to Participants the amount equivalent of the cash reward minus said tax.
8. In instances where the Company sends a message to a Participant's Account or email address and does not receive a reply within 30 days (including instances where there is a typo in the provided email address), or a Participant is unable to receive cash rewards, in whole or part, even after the Company completes the necessary remittance procedures based on the information received from a Participant per Paragraph 4 (including instances where there is a mistake in the Information, where there are banking system issues or the Participant is subject to economic sanctions) the Company's obligation to pay the cash reward

will be dissolved.

9. In cases where it is made clear that a Participant has violated these Terms of Service, the Company shall be able to refuse payment or request a refund for paid cash rewards to said Participant.

Article 7 (Prohibited Acts)

1. Participants shall not perform:
   (i) any act that violates the rights of others or the law
   (ii) a denial-of-service attack that interferes with the Company's service
   (iii) an attack using an automated vulnerability scanner
   (iv) spamming LINE users arbitrarily with spam messages
   (v) physical attacks against our Company assets or data centers
   (vi) viewing, deletion, modification or disclosure of other users' data using the discovered vulnerability
   (vii) viewing, deletion, modification or disclosure of source code, etc. using the discovered vulnerability
   (viii) any act in relation to vulnerability testing and reporting that violates others' rights
   (ix) any act other than those listed above that is contrary to the spirit and purpose of the Program
2. If a Participant is in violation of an item in the preceding paragraph, the Company shall be able to disqualify the Participant from participating in the Program.

Article 8 (Rights)

1. A Participant holds the right to modify the App including altering, processing, and replicating to the extent necessary for participation in this Program.
2. In instances where a Participant creates an invention, methodology or design for verifying or studying repair methods for a vulnerability ("Inventions, Etc."), industrial property rights and other patent filing/application rights related to Inventions, Etc. (including rights prescribed in Copyright Act, Article 27 and 28) and all other rights shall be transferred to the Company with the submission of the vulnerability details via the Participant's Account, and the Company shall be able to freely exercise and dispose of those rights.
3. In instances where Inventions, Etc. are copyrighted material, Participants shall not claim or exercise author's moral rights associated with relevant

copyrighted materials against the Company or other entities the Company has granted authority.

Article 9 (Handling of Confidential Information)

1. Participants shall treat vulnerability information as confidential information, and even after the conclusion of the Program, cannot disclose, leak, or make public said vulnerability information to a third party until the Company finishes fixing the vulnerability and makes such information publicly available. In the event that there is information which the Company determines as being confidential (such as details on how to attack) including cases in which Users may be subject to damage due to related vulnerabilities (vulnerabilities related to those reported by Participants or similar vulnerabilities that the Company has not yet fixed), Participants cannot disclose, leak, or make public said confidential information.
2. The statement in the preceding clause does not apply if one year has passed since the vulnerability report was received by the Company.

Article 10 (Handling of Personal Information)

1. The Company respects the privacy of Participants.
2. The Company will use the personal information provided by Participants for identification, contacting, report reviewing, payments, prevention of unauthorized use, smooth operation of the Program and any other necessary clerical processes. The handling of other privacy matters shall be in accordance with the LINE Privacy Policy.
3. The Company gives the utmost care to safely managing the information collected from Participants.
4. The Company shall store the Information received from Participants for one year since the last date on which Participants log into their Account.

Article 11 (Withdrawal)

1. If Participants wish to withdraw from the Program, they are to make a request for withdrawal to the Company from their Account.
2. Once the Company receives a withdrawal request from a Participant in accordance with the instructions in the preceding paragraph, the Company shall withdraw the Participant from the Program as well as destroy all Information received from the Participant.

3. The Company shall also withdraw Participants who do not log into their Account for one year or longer.
4. In the event that a Participant violates, or is likely to violate, any of the prohibited acts stipulated in Article 7 of these Terms of Service, the Company shall have the right to withdraw the Participant from the Program.

Article 12 (Hall of Fame)

1. Participants submitting vulnerability reports eligible for cash rewards can have their names and personal photos ("Participant Information") posted on the Company's Hall of Fame. Participants shall declare and ensure that the Participant Information they provide to the Company does not infringe on any rights of third parties, including copyrights, trademarks, or any other intellectual property rights. Furthermore, the decision to post said Participant Information on the Hall of Fame shall be made by the Company.
2. In instances where a complaint, assertion, request, demand or protest ("Complaint, Etc.") is received from a third party due to the posting of Participant Information on the Hall of Fame, the Participant shall be obligated to resolve said Complaint, Etc. at their own expense, and in instances where the Company has suffered damages, shall also bear responsibility for paying compensation immediately for the loss. In cases where the company has resolved a Complaint, Etc., Participants shall bear all expenses for that resolution.

Article 13 (Liability Exemption)

1. Participants shall participate in the Program at their own responsibility, and the Company shall bear no responsibility for any damages incurred in relation to participation in the Program.
2. The Company shall not involve itself in any disputes arising between Participants or Participants and third parties in relation to the Program, and Participants shall resolve such disputes at their own responsibility and expense.

Article 14 (Changes to These Terms of Service)

1. The Company may amend the content of these Terms of Service without notice.
2. In the event where the Company amends the content of these Terms of Service per the preceding paragraph, Participants are deemed to have accepted the

amendments by their continued participation in the Program, and the updated Terms of Service shall apply.

Article 15 (Language and Standard Time)

1. The Japanese Terms of Service shall be the official text, and the Japanese version shall prevail in case of any inconsistencies exist between the Japanese version and the English translation.
2. Unless specified otherwise, all dates and times used in relation to this Program are of Japan.

Article 16 (Governing Laws and Court of Jurisdiction)

Disputes between Participants and the Company arising from or in relation to participating in this Program shall be the exclusive jurisdiction of the Tokyo District Court or the Tokyo Summary Court as the court of first instance.

Article 17 (Inquiries Regarding the Program)

The Program is operated by the Company.
All inquiries regarding the Program are to be submitted using the form below. Inquiries sent by any other method will not receive a response.

https://contact.line.me/en/
(Example: Select "LINE" under Service, "Other" under Category, and "Promotions" under Details)