lockrMail Security Vulnerability Policy

Effective Date: January 2023

lockr takes the security of our systems, products, and services very seriously.

If you discover a security vulnerability in any of our systems or products, we encourage you to contact us at privacy@loc.kr and disclose the vulnerability to us. Upon receiving security vulnerability reports, lockr commits to:

- Acknowledge receipt of your vulnerability report in a timely manner and respond accordingly;
- Confirm the validity of your report;
- Address and fix the vulnerability as soon as reasonably possible in line with our commitment to the privacy, safety and security of our customers; and
- Notify you when the vulnerability is fixed.

However, lockr is unable to render payment or any reward or bounty in exchange for such reports.

When reporting a vulnerability, please provide as much information and detail as possible including:

- The URL where the vulnerability occurs;
- If applicable, the parameter where the vulnerability occurs;
- The type of the vulnerability;
- A step-by-step instruction on how to reproduce the vulnerability;
- A demonstration of the vulnerability, by screenshots or video; and
- If applicable, an attack scenario (an example attack scenario may help demonstrate the risk and get the issue resolved faster).

By submitting a vulnerability report to lockr:

- You acknowledge that you have read and agreed to the terms and conditions set out in this Policy;
- You hereby grant lockr an irrevocable and transferable right, to use, reproduce, copy, modify and otherwise dispose of the report, the content therein and the information related to the security vulnerabilities, as lockr sees fit; and
- You hereby waive any claims of any nature, including implied or express contractual or quasi-contractual rights, arising out of any disclosure within the vulnerability report.

lockr appreciates proactive research and responsible disclosures in line with this Policy. Please note, however, that lockr does not permit you to do or attempt to do any of the following:

- Access, modify or destroy a lockr customer's account or data;
- Account enumeration using brute-force attacks;
- Interrupt or degrade our Service;
- Execute a "Denial of Service" attack;
- Post, transmit, upload, link to, send or store any malicious software;
- Send any unsolicited or unauthorized mail or messages;
- Violate any applicable law;
- Use social engineering techniques; or
- Perform any testing that would result in any of the above.

Further, you hereby agree to:

- Subject to any applicable legislation, to not disclose any security vulnerabilities or sensitive information / data to any third parties without the prior written consent of lockr; and
- That you shall not use any information or content of the vulnerability report for any marketing or financing purpose or as a reference in any personal or professional presentation, documentation or other material, or in any way utilize any lockr related name, logotype or trademark.

Contravening this Policy may result in (i) lockr suspending or terminating your access to lockr's website, applications, systems, products or services, (ii) contacting the relevant authorities and/or (iii) pursuing any other remedies available to lockr by law.

If you wish to report an issue that falls outside of the scope of this Policy, (such as suspected fraudulent activity or suspect that your account or login details may have been compromised), please contact our support team here (https://lockrmail.com/contact/). Your issue will be investigated immediately.