COMPLIANCE

# Acceptable Use Policy

Rules for use. Explains customer responsibilities, restricted behavior, and how access, systems, and content must be handled safely and lawfully.

| | |
|---|---|
| Version | 1.1 |
| ID | 65d031118b1a-dirty |
| Prepared by | Safespring |
| Approver | Safespring |
| Date | 2026-04-23 |
| Classification | Public |

Safespring AB
Rattarvagen 3, 169 68 Solna
www.safespring.com

Tel: +46 (0)8-551 073 70
hello@safespring.com

*Users are responsible for any information or content uploaded or otherwise inserted to the Services.*

# 1. Introduction

Safespring provides infrastructure cloud services (the “Services”) to its customers and partners (the “Users”). This Acceptable Use Policy (“Policy”) sets out the rules governing the use of the Services. Users are responsible for configuring, operating, and maintaining their applications and systems in a secure manner. Users must ensure that their use of the Services complies with applicable laws and with any reasonable security instructions provided by Safespring. Users are responsible for all content and data processed, stored, or transmitted through the Services.

Users shall ensure that all employees, consultants and other personnel who access or use the Services on the User’s behalf do so in accordance with this Acceptable Use Policy. Users are responsible for all content and data processed, stored, or transmitted through the Services.

# 2. Authorization

Users must ensure that access to the Services is limited to authorized personnel. Access credentials are personal and may not be shared or transferred. Users are responsible for maintaining the confidentiality and security of authentication credentials and must implement appropriate measures to detect and respond to unauthorized access. Authorizations are valid only for the duration of the User’s agreement with Safespring and may be revoked if no longer required or if inactive for an extended period.

Users are responsible for, and must inform its authorized personnel or authorized users to, keeping any and all passwords secure. Passwords or any other method of accessing the Services are personal and may not be shared. All Users must have effective routines to identify unauthorized access to the Services and/or compromised passwords or security and to minimize the impact of such incidents.

# 3. Using the Services

The Services are owned by Safespring with the intention of being used only by the Users for the Services’ intended and agreed purposes. Users may inter alia not use the Services for the distribution, storage or transmission of information for illegal or immoral purposes, including but not limited to distributing, storing or transmitting:

1. threatening, obscene or offensive material, or information in violation with criminal law, such as but not limited to legislation on incitement to racial hatred or child pornography,

2. information in violation with applicable law, such as the General Data Protection Regulation
3. information in violation with the rights of any person, including rights protected by copyright, trade secret legislation, patent or other intellectual property (including, for the avoidance of doubt, that the Services may not be used
    3.1. to publish, submit, receive, upload, download, post, use, copy or otherwise reproduce, transmit, distribute or store any information or content or
    3.2. to engage in any activity that violates the intellectual property rights, including but not limited to copyright, patent, trademark or trade secret, or privacy or publicity rights of Safespring or any third party),
4. information considered to be political, ideological or religious propaganda,
5. information or data containing malicious codes (viruses, worms, trojan horses or other executables intended to inflict harm), or
6. information to be used as or for the purposes of unsolicited bulk e-mail (spam).

Users may furthermore not use the Services for any illegal purposes (including using illegal materials or violating applicable laws or decisions and/or guidelines from public authorities in connection with the use of the Services) or for engaging in any network security violations, including but not limited to attempts to circumvent user authentication or security of any host, network or account, by accessing data not intended for such User, logging into or making use of a server or account which the relevant User is not authorized to access, or by probing, scanning or testing the vulnerability of the Services. This includes that the Services may not be used to interfere or attempt to interfere with, gain unauthorized access to or otherwise violate the security of Safespring's or any other party's server, network, network access, computer or device, software or data such as through phishing, flooding or by uploading or distributing time bombs, spyware or harmful bots. Users may furthermore not use any program script, command or equivalent measure designed to interfere with, disable, deny or disrupt any other party's service or terminal session.

Users may not use the Services in moral or ethical gray zones, such as the fields of gambling, pornography, guns, alcohol and microloans. Users may not reverse engineer, decompile, modify, adapt, make any copy, or create a derivative work of the whole or any part of the Services for any purpose or remove or alter any copyright or other proprietary notice on any part of the Services. Users may not use or otherwise export or re-export the Services except as authorized by applicable law. All Users represent and warrant, that they

1. will not use the Services in violation of any applicable export regulations (such as a country subject to U.S. Government embargo),
2. are not listed on any U.S. Government, EU, UN or any other relevant government list of prohibited or restricted parties, or
3. will not export or resell the Services to any such targeted person, or export or resell the Services without the required export licenses and approvals.

## 4. Safespring's monitoring

Safespring may monitor the Services to maintain their security, integrity, and performance. Such monitoring does not transfer responsibility for security to Safespring. Users remain solely responsible for the configuration and security of their applications and systems.If Safespring identifies a material security risk, it may notify the User and recommend corrective actions. If the User fails to address a significant security risk within a reasonable timeframe, Safespring reserves the right to take proportionate measures, including restricting access to affected services, to protect the overall integrity of the Services.

## 5. Information obligation

Users must promptly notify Safespring of any actual or suspected breach of this Policy or security incident related to the Services. Users shall provide reasonable cooperation and assistance to investigate, mitigate, and remediate such incidents.

## 6. Enforcement / Suspension

Safespring reserves the right to suspend or terminate access to the Services without prior notice if it reasonably determines that a User is in breach of this Policy or poses a risk to the security, integrity, or availability of the Services.