2019-10-16

Blue Safespring AB

Smidesvägen 12
171 41 Solna

SAFESPRING POLICY

Safespring Acceptable Use Policy

1. Introduction

Safespring offers its customers a variety of infrastructure cloud services. This policy sets forth the principles governing the use of any of Safespring's cloud services (the "Services") by its customers or partners ("Users"). Users are instructed to regularly visit Safespring's webpage to ensure compliance with the most recent version of this policy. On a general level, each User is responsible for setting up, as well as maintaining its own applications within the Services and to ensure that they are configurated in a safe way. Users are responsible for ensuring and maintaining the necessary systems to use the Services and to at all times ensure the adequate security of such systems. Users must adhere to any and all reasonable security instructions provided by Safespring.

Users are responsible for any information or content uploaded or otherwise inserted to the Services and Users must at all times adhere to all applicable legislation when using the Services.

2. Authorization

Users must be authorized as determined by Safespring. Users may not permit any person other than its authorized personnel or authorized users to access or use the Services. Each authorization is personal and may not be transferred to another person. The authorization is limited in time and expires when the User's agreement with Safespring governing the Services terminates or expires or when the basis upon which the authorization was granted expires or changes. The authorization also expires if an individual account has not been used for a period of 12 months.

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:

a) 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,

b) information in violation with applicable law, such as the General Data Protection Regulation

c) 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

i to publish, submit, receive, upload, download, post, use, copy or otherwise reproduce, transmit, distribute or store any information or content or

ii 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),

d) information considered to be political, ideological or religious propaganda,

e) information or data containing malicious codes (viruses, worms, trojan horses or other executables intended to inflict harm), or

f) 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

i will not use the Services in violation of any applicable export regulations (such as a country subject to U.S. Government embargo),

ii are not listed on any U.S. Government, EU, UN or any other relevant government list of prohibited or restricted parties, or

iii 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 continuously monitors the Services and may monitor Users' running applications' level of rudimentary protection against infringement and other types of attacks. Should Safespring detect that a User has not implemented rudimentary protection at a sufficient and adequate level, Safespring may inform the User that the relevant application is wrongly configurated which may cause access to the Services by unauthorized persons. While the User maintains the responsibility for its applications, Safespring may assist the User in order to facilitate the procedure towards an adequate security level.

If the User ignores or fails to reply to Safespring within a reasonable time based on the risk of the unsatisfactory security level, Safespring may and is entitled to equip the application with a filter to ensure that the application cannot be hacked and to protect the overall integrity of the Services. Once the application has been secured and public access has been suspended, the User will be informed thereof.

5. Information obligation

If the User becomes aware of a breach of this policy, the User must promptly notify Safespring and upon request provide Safespring with reasonable assistance for remedying the breach and mitigating any risks.