



## **Acceptable Use and External-Facing Services Policy**

### **1. Scope**

- A. This Acceptable Use and External Facing Services Policy ("Policy") applies to customers' use of all services offered by salesforce.com, inc. or its affiliates ("SFDC").

### **2. Last Updated**

- A. November 5, 2020

### **3. Changes to Policy**

- A. SFDC may change this Policy by posting an updated version of the Policy at [www.salesforce.com](http://www.salesforce.com) and such updates will be effective upon posting.

### **4. Violations**

- A. A customer's violation of this Policy will be considered a material breach of the master subscription agreement and/or other agreement governing the customer's use of the services.

### **5. Prohibited Material**

- A. Customers may not, and may not allow any third party, including its users, to use services to display, store, process, or transmit, or permit use of services to display, store, process, or transmit:
  - I. Material that infringes or misappropriates a third party's intellectual property or proprietary rights;
  - II. Hate-related or violent material, and/or material advocating discrimination against individuals or groups;
  - III. Obscene, excessively profane material or otherwise objectionable material;
  - IV. Material advocating or advancing criminal hacking, cracking, or phishing;
  - V. Material related to illegal drugs or paraphernalia;
  - VI. Malicious material;
  - VII. Unlawful software;
  - VIII. Malicious code, such as viruses, worms, time bombs, Trojan horses, and other harmful or malicious files, scripts, agents, or programs; or
  - IX. Material that violates, encourages, or furthers conduct that would violate any applicable laws, including any criminal laws, or any third-party rights, including publicity or privacy rights.

### **6. Prohibited Actions**

- A. Customers may not use a service to, nor allow its users or any third party to use a service to:
  - I. Generate or facilitate unsolicited commercial email (spam). Such prohibited activity includes, but is not limited to:
    - a. Sending communications or email in violation of the CAN-SPAM Act or any other applicable anti-spam law or regulation;
    - b. Imitating or impersonating SFDC, another person or his, her, or its email address, or creating false accounts for the purpose of sending spam;
    - c. Data mining or harvesting any web property (including any External-Facing Service) to find email addresses or other user account information;

- d. Sending unauthorized mail via open, third-party servers;
  - e. Sending email to users who have requested to be removed from a mailing list;
  - f. Selling to, exchanging with, sharing with, or distributing to a third party personal information, including the email addresses of any person without such person's knowing and continued consent to such disclosure; or
  - g. Sending unsolicited emails to significant numbers of email addresses belonging to individuals and/or entities with whom you have no preexisting relationship;
- II. Send, upload, distribute, or disseminate, or offer to do the same, with respect to unlawful, defamatory, harassing, abusive, fraudulent, infringing, obscene, excessively profane, hateful, violent, or otherwise objectionable material, or promote, support, or facilitate unlawful, hateful, discriminatory, or violent causes;
- III. Intentionally distribute viruses, worms, defects, Trojan horses, corrupted files, hoaxes, or any other items of a destructive or deceptive nature;
- IV. Conduct or forward multi-level marketing, such as pyramid schemes and the like;
- V. Generate or facilitate SMS, MMS, or other text messages or push notifications in violation of the Telephone Consumer Protection Act, the Do-Not-Call Implementation Act, or any other applicable law including anti-spam, telemarketing, or telephone consumer protection laws or regulations;
- VI. Use the services in any manner that violates any applicable industry standards, third-party policies, or requirements that Salesforce may communicate to its users, including all of the applicable guidelines published by the CTIA, the Mobile Marketing Association, the Self-Regulatory Principles as directed by the Digital Advertising Alliance and the Network Advertising Initiative, or any other generally accepted industry associations, carrier guidelines, or other industry standards;
- VII. Transmit material that may be harmful to minors;
- VIII. Illegally transmit another's intellectual property or other proprietary information without such owner's or licensor's permission;
- IX. Impersonate another person, entity, or SFDC (via the use of an email address or otherwise) or otherwise misrepresent themselves or the source of any communication;
- X. Violate the rights (such as rights of privacy or publicity) of others;
- XI. Promote, facilitate, or encourage illegal activity;
- XII. Interfere with other users' enjoyment of a service;
- XIII. Mislead people about voting processes or census processes;
- XIV. Engage in activity in connection with illegal peer-to-peer file sharing;
- XV. Engage in or promote gambling, or run a gambling operation;
- XVI. "Mine" bitcoins and other cryptocurrencies;
- XVII. Sell, distribute, or export illegal or prescription drugs or other controlled substances or paraphernalia;
- XVIII. Access (including through any interfaces provided with a service) any SFDC product or service or other service or website, in a manner that violates the terms for use of or access to such service or website;
- XIX. Operate an "open proxy" or any other form of Internet proxy service that is capable of forwarding requests to any end user or third-party-supplied Internet host;
- XX. Perform significant load or security testing without first obtaining SFDC's written consent;
- XXI. Remove any copyright, trademark, or other proprietary rights notices contained in or on the service or reformat or frame any portion of the web pages that are part of the service's administration display;

XXII. Access a third-party web property for the purposes of web scraping, web crawling, web monitoring, or other similar activity through a web client that does not take commercially reasonable efforts to identify itself via a unique User Agent string describing the purpose of the web client and obey the robots exclusion standard (also known as the robots.txt standard), including the crawl-delay directive;

XXIII. Use a service in any manner that would disparage Salesforce;

XXIV. Use the Einstein Bot feature to communicate with any third party without clearly communicating that the individual is speaking with a bot;

XXV. Use Einstein Vision, Einstein Language, Einstein Discovery, or Einstein Prediction Builder for the purposes of predicting an individual's racial or ethnic origin, and past, current, or future political opinions, religious or philosophical beliefs, trade union membership, age, gender, sex life, sexual orientation, disability, health status, medical condition, financial status, criminal convictions, or likelihood to engage in criminal acts. The previous sentence does not limit or prohibit use cases or tools designed specifically to identify security breaches, unauthorized access, fraud, and other security vulnerabilities. Additionally, for Einstein Vision, customer may not submit images of individuals for the purposes of creating or analyzing biometric identifiers, such as face prints or fingerprints or scans of eyes, hands, or facial geometry;

XXVI. Use Sales Cloud Einstein, Pardot Einstein, Salesforce Inbox, Einstein Engagement Scoring, Einstein Vision, Einstein Language, Einstein Bots, Service Cloud Einstein, Einstein Discovery, or Einstein Prediction Builder as part of a decision-making process with legal or similarly significant effects, unless customer ensures that the final decision is made by a human being. In this case, customer must take account of other factors beyond the Einstein Services' recommendations in making the final decision; or

XXVII. Directly manage, as the primary operator, private, for-profit prison facilities or detention centers in the United States. For-profit prisons and detention centers refer to privately owned facilities in which persons are incarcerated or otherwise involuntarily confined for purposes of execution of a punitive sentence imposed by a court or detention pending a trial, hearing, or other judicial or administrative proceeding.

- B. Worldwide, customers may not use a service to transact online sales of any of the following firearms and/or related accessories to private citizens. Firearms: automatic firearms; semi-automatic firearms that have the capacity to accept a detachable magazine and any of the following: thumbhole stock, folding or telescoping stock, grenade launcher or flare launcher, flash or sound suppressor, forward pistol grip, pistol grip (in the case of a rifle) or second pistol grip (in the case of a pistol), barrel shroud; semi-automatic firearms with a fixed magazine that can accept more than 10 rounds; ghost guns; 3D printed guns; firearms without serial numbers; .50 BMG rifles; firearms that use .50 BMG ammunition. Firearm Parts: magazines capable of accepting more than 10 rounds; flash or sound suppressors; multi-burst trigger devices; grenade or rocket launchers; 80% or unfinished lower receivers; blueprints for ghost guns; blueprints for 3D printed guns; barrel shrouds; thumbhole stocks; threaded barrels capable of accepting a flash suppressor or sound suppressor.

## **7. U.S. Digital Millennium Copyright Act or Similar Statutory Obligations**

- A. To the extent a customer uses the services for hosting, advertising, sending electronic messages, or for the creation and hosting of, or for posting material on, websites, each customer must:
- I. Comply with any notices received under Title II of the Digital Millennium Copyright Act of 1998 (Section 512 of the U.S. Copyright Act) or similar statute in other countries (the "DMCA");
  - II. Set up a process to expeditiously respond to notices of alleged infringement that comply with the DMCA and to implement a DMCA-compliant repeat infringers policy;
  - III. Publicly display a description of its notice and takedown process under the DMCA on its instance of the services; and
  - IV. Comply with such processes, policy(ies), and description.

- B. It is SFDC's policy to respond expeditiously to valid notices of claimed copyright infringement compliant with the DMCA. In appropriate circumstances, SFDC will terminate the accounts of customers who SFDC suspects to be repeatedly or blatantly infringing copyrights.
- C. If SFDC receives a notice alleging that material on a customer's instance of a service infringes another party's intellectual property, SFDC may disable that customer's instance of the service or remove the allegedly infringing material. If SFDC receives more than one such notice for the same customer, SFDC reserves the right to immediately terminate such customer's subscriptions to the services as deemed necessary by SFDC to ensure continued protection under the safe harbor provisions under the DMCA or to prevent violations of other applicable laws or third parties' rights.