
Universal Design Platform as a Service (UDPaaS) External-Facing Services Policy

1. Scope

This External-Facing Services Policy ("**Policy**") applies to the services offered by eTRANSERVICES Corp., ("eTRANSERVICES") to the extent Client uses such for advertising, sending electronic messages or for the creation and hosting of, or for posting material on, external-facing websites or the use of application programming interfaces (APIs) (the "**External-Facing Services**") as authorized by Federal Risk and Authorization Management Program (FedRAMP).

2. Changes to Policy

eTRANSERVICES may change this Policy by posting an updated version of the Policy at <https://UDPaaS.com/agreements> and such updates will be effective upon posting; provided, however, that any updates to the Policy that impose, on an existing Client, new material obligations or restrictions (applicable to functionality included in Client's External-Facing Services subscriptions as of the start date of the Client's then-current subscription term) will not apply to such Client until that Client's next Order for External-Facing Services. Once a Policy update takes effect for a Client, the Client's use of any External-Facing Services will be subject to the updated Policy.

3. Violations

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

4. Prohibited Material

Clients may not use External-Facing Services to display, store, process or transmit, or permit the use of External-Facing Services to display, store, process, or transmit:

- a. violates the FedRAMP authorization of UDPaaS authority to operate;
- b. material that infringes or misappropriates a third party's intellectual property or proprietary rights;
- c. obscene, excessively profane material or otherwise objectionable material;
- d. hate-related, bullying or violent material including material advocating discrimination or racial, religious or ethnic intolerance or material advocating or advancing computer hacking or cracking;
- e. material related to phishing or drug paraphernalia;
- f. malicious material;
- g. unlawful software;
- h. malicious code, such as viruses, worms, time bombs, Trojan horses and other harmful or malicious files, scripts, agents or programs; or
- i. material that violates or encourages conduct that would violate any applicable laws, including any criminal laws, or any third-party rights, including publicity or privacy rights.

5. Prohibited Actions

Clients may not and may not allow any third-party, including its users, to use an External-Facing Service to:

- a. Generate or facilitate unsolicited commercial email (spam). Such prohibited activity includes, but is not limited to:
 - i. imitating or impersonating UDPaaS, another person or his, her or its email address, or

-
- creating false accounts to send spam;
 - ii. data mining or harvesting any web property (including any External-Facing Service) to find email addresses or other user account information;
 - iii. sending unauthorized mail via open, third-party servers;
 - iv. sending email to users who have requested to be removed from a mailing list;
 - v. selling to, exchanging with, sharing with, or distributing to third-party personal information, including the email addresses of any person without such person's knowing and continued consent to such disclosure;
 - vi. sending unsolicited emails to significant numbers of email addresses belonging to individuals and/or entities with whom you have no pre-existing relationship;
 - vii. sending communications or email in violation of applicable anti-spam laws or regulations within your jurisdiction;
 - b. send, upload, distribute or disseminate, or offer to do the same with respect to, unlawful, defamatory, harassing, abusive, fraudulent, infringing, obscene, excessively profane, or otherwise objectionable material;
 - c. intentionally distribute viruses, worms, defects, Trojan horses, corrupted files, hoaxes, or any other items of a destructive or deceptive nature;
 - d. conduct or forward multi-level marketing, such as pyramid schemes and the like, or engage in any unauthorized commercial purpose;
 - e. engage in phishing;
 - f. generate or facilitate SMS, MMS, or other text messages or push notifications in violation of any applicable laws, including anti-spam, telemarketing, or telephone consumer protection laws or regulations within your jurisdiction;
 - g. use of the External-Facing Services in any manner that violates any applicable industry standards, third-party policies or requirements that UDPaaS may communicate to its users, including all of the applicable guidelines published by accepted industry associations, carrier guidelines, or other industry standards within your jurisdiction;
 - h. transmit material that may be harmful to minors;
 - i. illegally transmit another's intellectual property or other proprietary information without such owner's or licensor's permission;
 - j. impersonate another person, entity or UDPaaS (via the use of an email address or otherwise) or otherwise misrepresent themselves or the source of any email;
 - k. violate the rights (such as rights of privacy or publicity) of others;
 - l. promote or encourage illegal activity;
 - m. interfere with other users' enjoyment of an External-Facing Service;
 - n. engage in activity in connection with illegal peer-to-peer file sharing;
 - o. engage in or promote gambling, or run a gambling operation;
 - p. "mine" bitcoins and other cryptocurrencies;
 - q. sell, distribute or export prescription drugs or other controlled substances;
 - r. sell, distribute or promote drug paraphernalia;
 - s. access (including through any interfaces provided with an External-Facing Service), any UDPaaS

product or Service, or other Service or website, in a manner that violates the terms for the use of, or access to, such Service or website;

- t. 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;
- u. perform significant load or security testing without first obtaining eTRANSERVICES' written consent;
- v. 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;
- w. access a third-party web property for 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; or
- x. use the External-Facing Service in any manner that would disparage UDPaaS.

6. U.S. Digital Millennium Copyright Act

Applicable only to those Clients who are physically located and hosted in the United States. Each Client 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) (the "DMCA") or the European Union Council Directive 2000/31, On certain legal aspects of information society services, in particular electronic commerce, in the Internal Market or other counterparts or their local counterparts, (ii) publicly display a description of its notice and takedown process under the DMCA on its instance of the External-Facing Services, and (iii) comply with that description.

If eTRANSERVICES receives a notice alleging that material on a Client's instance of an External-Facing Service infringes on another party's intellectual property, eTRANSERVICES may disable that Client instance of the External-Facing Service or remove allegedly infringing material. If eTRANSERVICES receives more than one such notice for the same Client, eTRANSERVICES Corp. reserves the right to immediately terminate such Client's subscriptions to the External-Facing Service as deemed necessary by eTRANSERVICES to ensure continued protection under the safe harbor provisions under the DMCA or to prevent violations of other applicable laws or third-parties' rights.

7. General Data Protection Regulation (GDPR)

It applies only to those United States Government Agencies under the material or territorial scope of the GDPR.

Each Client must comply with the Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and the free movement of such data. (GDPR)

Clients may not and may not allow any third-party, including its users, to use an External-Facing Service to:

Collect, distribute, disclose, solicit, or otherwise process, or attempt to process, personal data in a manner that is not per the GDPR.

- a. Collect or solicit personal data from minors below the age of 16 years without receiving adequate consent from the appropriate party;
- b. Collect or solicit special categories of personal data, defined in the GDPR as: 'personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data to uniquely identify a natural person, data concerning health or data concerning a natural person's sex life or sexual

orientation.’ You may only collect or solicit special categories of personal data if you meet one or more of the conditions set forth in Chapter 2, Article 9, Paragraph 2 of the regulation.

Clients must enforce the following requirements for their staff, their users, and any third-parties using the External-Facing Services:

- a. If you post or link your privacy policy to the External-Facing Services, you must comply with it;
- b. Where a data subject requests to execute their rights, you must facilitate the request per Article 12 of the GDPR if the request was made through the External-Facing Service, or if the External-Facing Service falls under the scope of the request.
- c. Client must comply with any requests by eTRANSERVICES Corp to rectify, enhance, or provide information on their data protection practices related to Client’s use of the External-Facing Service.

If eTRANSERVICES receives a notice alleging that the practices, contents, collection mechanisms, or policies on a Client’s instance of an External-Facing Service does not comply with GDPR, eTRANSERVICES may disable that Client instance of the External-Facing Service or remove the non-compliant aspects. If eTRANSERVICES receives more than one such notice for the same Client, eTRANSERVICES reserves the right to immediately terminate such Client’s subscriptions to the External-Facing Service as deemed necessary by eTRANSERVICES to ensure continued protection of data subject’s personal data, and their rights under the law, or to prevent violations of other applicable laws or third-parties’ rights.