

Scope

This Acceptable Use Policy (“Policy”) applies to customers’ use of all products and services offered by Esko (“Services”). By using the Services, customer and any users authorized by customer (“Users”) (collectively “You”) acknowledge and agree to abide by the terms of this Acceptable Use Policy (“AUP”).

The AUP is incorporated into any agreement between You and Esko that references this AUP (“Agreement”). Capitalized terms used, but not defined, herein have the meaning attributed them in the Agreement. Esko may modify or change this AUP at any time by posting a modified AUP to its website. Such modified AUP will become effective on the latter of: (i) its posting to the Esko site; or (ii) as otherwise set forth in the Agreement. If You violate this AUP, or assist or encourage others to violate this AUP, Esko may suspend or terminate Your access to the Services.

Compliance with laws

You agree to comply with applicable laws and regulations in connection Your use of the Services, including all data protection laws and regulations that may apply to You.

Compliance with Subprocessors

In addition, You agree to comply with the following:

- A. For hosted services performed by Esko through Accenture Cloud First (formerly known as Sentia Belgium), the following Acceptable Use Policy applies:

Please consult the most recent version of Acceptable Use Policy available at

<https://www.accenture.com/content/dam/accenture/final/a-com-migration/manual/r3/pdf/Accenture-Acceptable-Use-Policy.pdf> incorporated herein by reference.

- B. For hosted services performed by Esko through BT, the following Acceptable Use Policy applies:

Please consult the most recent version of Acceptable Use Policy available at

https://www.bt.com/assets/pdf/BTL_AcceptableUsePolicy.pdf, incorporated herein by reference.

- C. For hosted services performed by Esko through AWS, the following Acceptable Use Policy applies:

Please consult the most recent version of the Amazon Acceptable Use Policy available at

<https://aws.amazon.com/aup/>, incorporated herein by reference.

User Accounts

You are solely and fully responsible for:

- (1) Creating and managing User Accounts;
- (2) Ensuring that no false or misleading personal information is utilized in the creation or usage of a User Account;
- (3) Any usage by the User of a User Account;
- (4) Any performance of Users under a User Account;
- (5) The safe handling, storage, and confidentiality of User identifications, login credentials and/or passwords.

Each User shall have a designated User Account. No User is authorized to share its User Account information with any other person or entity.

Additionally, You are responsible for employing reasonable techniques, practices, technology and/or methodologies as are generally accepted in the industry to prevent unauthorized access to the Services. You are required to notify Esko promptly of any such unauthorized access and use best efforts to immediately stop any such unauthorized use.

Prohibited Actions

You may not:

- (1) Access any Service in a manner that violates the Service's terms for use;
- (2) Access any Service without permission, including attempting to probe, scan, or test the vulnerability of a Service or to breach any security or authentication measures;
- (3) Send, upload, store, distribute or disseminate, or offer to do the same, any 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;
- (4) Intentionally distribute viruses, worms, defects, Trojan horses, corrupted files, hoaxes, or any other items of a destructive or deceptive nature;
- (5) Use the Services in any manner that violates any applicable industry standards, third party policies or requirements that Esko may communicate to its users;
- (6) Remove any copyright, trademark or other proprietary rights notices contained in or on the Services or reformat or frame any portion of the web pages that are part of the Service's administration display;
- (7) Impersonate another person, entity or Esko (via the use of an email address or otherwise) or otherwise misrepresent themselves or the source of any email;
- (8) Violate the rights (such as rights of privacy or publicity) of others;
- (9) Generate or facilitate unsolicited commercial email (spam).
- (10) Conduct or forward multi-level marketing, such as pyramid schemes and the like;
- (11) Generate or facilitate SMS, MMS, or other text messages or push notifications in violation any applicable law including anti-spam, telemarketing or telephone consumer protection laws or regulations;
- (12) Promote, facilitate or encourage illegal activity;
- (13) "Mine" bitcoins and other cryptocurrencies;
- (14) 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;
- (15) Forge TCP-IP packet headers, e-mail headers, or any part of a message describing its origin or route. This prohibition does not include the use of aliases or anonymous remailers; or
- (16) Use a service in any manner that would disparage Esko.

Monitoring and Enforcement

You are solely responsible for exercising supervision and control over the Users, the User Accounts and Your data.

Esko reserves the right to:

- (1) Monitor or investigate any of Use access, or use of the Services (including the management of the User Accounts);
- (2) Notify You of any misuse of the Services or non-compliance under this AUP; or
- (3) Police or enforce the terms of the license(s) or permission(s) You have chosen to offer to the third parties in respect of Your data, or responsibilities related to the rights, access or license granted by You.
- (4) Investigate violations of this AUP or misuse of the Services;
- (5) Remove, disable access to, or modify any of Your data that violates this AUP or any other agreement Esko has with You for use of the Services; or
- (6) Report any activity that Esko suspects violates any law or regulation to appropriate law enforcement officials, regulators, or other appropriate third parties. Our reporting may include disclosing appropriate user information. Esko also may cooperate with appropriate law enforcement agencies, regulators, or other appropriate third parties to help with the investigation and prosecution of illegal conduct by providing network and systems information related to alleged violations of this AUP.



ACCEPTABLE USE POLICY

Violations

You agree to cooperate with us to remedy any violation. Your violation of this Policy will be considered a material breach of the Agreement governing Your use of the Services.

Questions

If you have any questions about this AUP, please contact your Esko Account Manager.

***** END OF DOCUMENT *****