

## ACCEPTABLE USE POLICY

This ACCEPTABLE USE POLICY ("AUP") describes acceptable use of and access to the Services offered by Deloitte and its Subcontractors. BY ACCESSING OR USING THE SERVICES, CLIENT AGREES TO THE TERMS OF THIS AUP. If anyone using the Services, whether authorised by Client or not, violate this AUP or if Client authorizes or helps others to do so, Deloitte may suspend or terminate Client's use of the Services in accordance with the terms of the Agreement. This AUP forms part of the terms of the Agreement. Unless otherwise defined herein, all capitalized terms used within this AUP have the same meaning as ascribed to such terms in the Agreement.

### 1.Laws, regulations and codes

Client may not use Services to transmit, distribute, or store material in a manner that Deloitte believes:

- 1.1 Violates any local, state, national, foreign, or international statute, regulation, rule, order, treaty, or other law (each a "Law");
- 1.2 Violates the terms of this AUP, the terms of any applicable agreement with Deloitte, or any other Deloitte policy applicable through the Agreement;
- 1.3 Violates generally accepted standards of Internet usage;

### 2.Offensive Content

Client may not use Services to transmit, distribute, or store material in a manner that Deloitte believes:

- 2.1 Is abusive, deceptive, pornographic, obscene, defamatory, slanderous, offensive, or otherwise inappropriate;
- 2.2 Violates or otherwise encroaches on the rights of others, including, but not limited to, infringing or misappropriating any privacy, intellectual property, proprietary right of another;
- 2.3 Advocates or induces illegal activity;
- 2.4 Stalks, harasses, or harms anyone, including minors;
- 2.5 Impersonates any person or entity or otherwise misrepresents Client's affiliation with a person or entity;

### 3.Security and Protection

Client may not use Services to transmit, distribute, or store material in a manner that Deloitte believes:

- 3.1 Modifies, alters, tampers with, repairs, or otherwise creates derivative works of any software included in the Services;
- 3.2 Except as allowed by local law, reverse engineers, disassembles, or decompiles the Infrastructure or Services or software included in the Services;
- 3.3 Accesses or uses the Services in a way intended to avoid incurring fees or exceeding usage limits or quotas;
- 3.4 Interferes with or adversely affects the Services or use of the Services by other Deloitte customers;
- 3.5 Uses any high volume automated means (including robots, spiders, scripts or similar data gathering or extraction methods) to access the Services and any other accounts, computer systems, or networks connected to the Services (each a "System");
- 3.6 Connects to any users, hosts, or networks where Client does not have permission to communicate with such users, hosts, or networks, including, but not limited to:
- 3.7 Monitors or crawls a system so that such system is impaired or disrupted;
- 3.8 Conducts denial of service attacks;
- 3.9 Intentionally interferes with the proper functioning of any system, including any deliberate attempt to overload a system by any means;
- 3.10 Operates network services like open proxies, open mail relays, or open recursive domain name servers; or
- 3.11 Uses means (manual or electronic) to avoid any use limitations placed on a system, such as access and storage restrictions;
- 3.12 Distributes, publishes, sends, or facilitates unsolicited mass e-mailings, promotions, advertising, or solicitations, including commercial advertising and informational announcements;
- 3.13 Alters or obscures mail headers or assume a sender's identity without the sender's explicit permission; or
- 3.14 Collects or replies to messages if those messages violate this AUP.

### 4.Monitoring and Enforcement

Deloitte has no responsibility for any material or information created, stored, maintained, transmitted, or accessible on or through the Services and is not obligated to monitor or exercise any editorial control over such material.

While not obligated to perform investigations, in accordance with the terms of the Agreement, Deloitte may:

1. Investigate violations of this AUP or misuse of the Services;
2. Investigate and help prevent security threats, fraud, or other illegal, malicious, or inappropriate activity;
3. Remove, disable access to, or modify any material or resource that Deloitte believes violates this AUP or any other agreement Deloitte has with Client for use of the Services; or
4. Suspend or terminate provision of Services to Client for uses that violate this AUP or any other agreement Deloitte has with Client for use of the Services.

Deloitte may report any activity that it suspects violates any law or regulation to appropriate law enforcement officials, regulators, or other appropriate third parties. Deloitte's reporting may include disclosing appropriate Client information. Deloitte 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. Nothing in this AUP shall limit in any way Deloitte ' rights and remedies at law or in equity that may otherwise be available.

#### **5.Modifications to the AUP**

Deloitte may, in its sole and absolute discretion, modify this AUP from time to time. Deloitte will post notice of such changes on [www.deloitte.com/be/aup](http://www.deloitte.com/be/aup). If Client objects to any such changes, Client's sole recourse shall be to cease using the Services. Continued use of the Services following notice of any such changes shall indicate Client's acknowledgement of such changes and agreement to be bound by the terms and conditions of such changes.