Policy

Company Acceptable Use Policy

1.0 Purpose

The purpose of this policy is to outline the acceptable use of Company's computing and network resources (IT resources) as well as other organizational and supporting assets. These rules are in place to protect the employee and Company, as inappropriate use exposes Company to risks including virus attacks, compromise of systems and services, and legal issues.

2.0 Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at Company, including all personnel affiliated with third parties. This policy also applies to all IT resources owned or leased by Company.

3.0 Policy

3.1 General Use and Ownership

Users of Company's IT resources are expected to abide by the following guidelines that are built around the underlying principles of acceptable use of organizational assets:

- Comply with all local and applicable international laws.
- Comply with the customer's contractual security obligations and requirements.
- Comply with all information security policies, regulations, procedures, and rules.
- Respect and protect the intellectual property rights of Company, its customers and other users within Company.
- Refrain from sharing passwords or accounts with anyone, including trusted friends or family members. Users will be held responsible for any actions performed using their accounts.
- Apply the same level of etiquette in all communication using Company's IT resources to all non-electronic communication.
- Respect others when using Company's IT resources.
- Only access files or data belonging to you or that are publicly available or where the owner of the data has permitted you to access them.
- Use corporate email accounts, internet IDs and web pages for corporate communications.
- Use the internet/intranet and electronic communication judiciously. The distribution of any information through the internet, computer-based services, email, and messaging systems is subject to the scrutiny of the IT team and Security team. Company reserves the right to determine the suitability of this information.
- While Company's IT department desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of Company.
- Employees must use extreme caution when opening email attachments received from unknown senders, as such email attachments may contain viruses or other malware.

***

Policy Conditions for PCI DSS:

- Employees must only utilize technologies, including end-user, from the list of approved technologies when operating or working in Stova's environment.
- Use Stova implemented technologies on only approved and defined network locations within the organization's environment.

***

3.2 Prohibited Usage of Company's IT Resources

The following usages of Company's IT resources are prohibited. Under no circumstances is an employee of Company authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Company-owned resources.

The lists below are by no means exhaustive but attempt to provide guidelines for activities that fall into the category of unacceptable use:

- Circumvention of any security measure of Company, its customers or other entities.
- Intentionally interfering with the network's regular operation, including the propagation of computer viruses and sustained high volume network traffic that substantially hinders the network performance.
- Violations of the rights of any person or organization protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, which includes but is not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Company.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of copyrighted sources and the installation of any copyrighted software for which Company or the end-user does not have an active license is strictly prohibited.
- Revealing or publicizing Company's confidential or proprietary information, which includes, but is not limited to: financial information, new business and product ideas, marketing strategies and plans, databases and the information contained therein, customer lists, technical product information, computer software source codes, computer/network access codes, and business relationships.
- Visiting internet sites that contain obscene, hateful or any objectionable material.
- Making or posting indecent remarks, proposals or materials on the internet.
- Downloading any software or electronic files without implementing anti-virus protection measures approved by Company.
- Intentionally using, distributing or creating viruses, worms or other malicious software.
- Operating a business, usurping business opportunities, organizing political activity or conducting activity for personal gain.
- Implying that the user is representing, giving opinions or otherwise making statements on behalf of Company without prior authorization or using. Company trade names, logos, or trademarks without prior written authorization.

- For business needs and based on approval, if BYOD (Bring Your Own Devices) arrangements are in place, i.e., Personally-owned workstations or mobile devices are used for business purposes, users shall not create or store confidential or sensitive information on personally-owned workstations.
- To prevent the introduction of malware and information leakage or data loss in Company, the use of USB (Universal Serial Bus) flash drives and any other portable storage media is prohibited unless specifically authorized by the IT department.

***

Policy Conditions for PCI DSS:

- For solutions to business needs, critical technologies shall not be implemented or installed without explicit approval by the authorized parties to prevent opening gaps that put critical systems and cardholder data at risk.

***

3.3 Email and Communications Activities

Users of Company's email and communication resources shall abide by the responsibilities and expected behavior and refrain from:

- Sending unsolicited email or other types of electronic messages, including sending "junk mail" or other advertising material to individuals who did not specifically request such material (spam).
- Using unsolicited emails originating from within Company's networks or from other internet/intranet/extranet service providers on behalf of, or to advertise, any service hosted by Company or connected via Company's network.
- Soliciting emails that are unrelated to business activities or for personal gains.
- Sending confidential emails without suitable encryption.

3.4 Blogging and Social Media

Blogging and using social media by employees, whether using Company's property and systems or personal computer systems, are also subject to the terms and restrictions outlined in this policy. Employees must abide by the responsibilities and expected behavior for use of social media, social networking sites, and external sites/applications.

Limited and occasional use of Company's systems to engage in blogging or other social media is acceptable, provided that it is done professionally and responsibly and does not otherwise violate Company's security policies. Blogging or using social media from Company's systems is also subject to monitoring.

As such, employees are prohibited from revealing any Company confidential or proprietary information, trade secrets or any other confidential information when engaged in blogging. Employees shall not engage in any blogging or social media use that may harm or tarnish the image, reputation or goodwill of Company and any of its employees.

Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or using social media.

Employees may also not attribute personal statements, opinions or beliefs to Company when engaged in blogging or using social media. If an employee is expressing their beliefs or opinions in blogs, the employee should not, expressly or implicitly, represent themselves as an employee or representative of Company.

Employees assume any risks associated with blogging or using social media.