***Acceptable Use Policy of***

***Our Company, Inc.***

**9 October 2015**

James Levan

Anthony Lucas

Alaa Abuali

Vinh Nguyen

**1. Overview**

“Our Company” is committed to establish and maintain a level of trust, respect, integrity and openness within the company. “Our Company’s” purpose for establishing the Acceptable Use Policy is to protect the organization's employees, the company, and its affiliates from offensive, malicious or possible brand damaging actions or scenarios resulting from intentional or unintentional actions or misuse of assets by an individual.

**2. Purpose**

The purpose of this policy is to set forth the guidelines and standards for the acceptable use of computer workstations, Internet Access and all Network related application, system software and services.

**3. Scope**

The Acceptable Use Policy or “AUP” applies to all users, employees, and all personnel who have authorized access to “Our Company’s” technology resources. This policy covers the use of “Our Company’s” computer hardware, security policy, Internet and Network access and applications and software, information and data exchanged within the Intranet and Internet including all email, and memorandum.

**4. Policy**

**4.1 General Use**

1. All employees, affiliates, and authorized users of “Our Company’s” technology resources are responsible for exercising good judgment while using the company’s technology.
2. “Our Company” employs the use of proprietary software; this software is to be considered to be the property of “Our Company” and its licensor if applicable and is not available or authorized for copy, distribution, and use on personal computing devices.
3. Computer activity will be monitored, without notice, for violations of the company IT policies.
4. All data shared and stored within or system is subject to compliance auditing.
5. The uses of portable storage media (e.g. flash drives and SD cards) is prohibited.
6. All data stored within the company’s system is considered to be confidential unless otherwise classified as public.
7. Employees must comply with all laws governing the use and access of consumer information
8. Employees will use reasonable precautions to safeguard company assets and data.
9. Internet use is limited/restricted to functions related to the business. Accessing sites deemed to be inappropriate or offensive is prohibited.

**4.2 Security**

1. Employees shall have access to systems relevant to their job functions.
2. Employees will protect access to the computer system by use of passwords. Passwords are to contain a minimum of eight (8) characters consisting of alphabetical, numerical and symbol characters.
3. Passwords are to be changed every ninety (90) calendar days and must be different from the previous four (4) passwords used. Employees are not permitted to reveal passwords to any individual.
4. Employees are prohibited to reveal or disclose any information deemed to be proprietary, trade secret, confidential, copyrighted, and financial data that is not available to the general public, or records of any kind including business and legal documentation.
5. The use of unauthorized and/or unlicensed software is prohibited on computers or other devices owned by “Our Company.”
6. Emails containing attachments from unknown sources are not to be opened due to the potential exposure to virus or malware; all such emails should be reported to the IT department immediately.
7. Any portable, mobile or communication device that has been issued by the company for use by an employee is to be password protected, make use of data encryption applications, and be physically secured by locking or preventative use device if applicable.
8. Copying, transferring, removing of data through use of portable storage devices is prohibited.
9. Encryption is required for all emails containing sensitive, confidential or other information the company classifies as private.

**4.3 Unacceptable Use**

1. The use of the network or email for illegal, criminal or suggestive behaviors
2. The download, upload, display, printing or storing of any material deemed to be offensive, obscene, or threatening in nature.
3. Use of company logos, name, copyrighted material to solicit funds, gifts or favors for personal gain.
4. Intentionally creating and/or sending material that contains profanity, racially, or sexually explicit messages and/or pictures or inappropriate content.
5. Disclosure of personal information of clients and employees.
6. Disclosure or misuse of security identifiers such as ID badges, revealing passwords or allowing unauthorized access to an individual not having privilege to such information, without the consent of executive management.
7. Hacking or attempting to access or otherwise breach the computer systems or network devices.
8. Deny, interfere with, or otherwise impede the audit or review of systems within the company.
9. Social media shall not be used to defame, criticize, and reveal private company information.
10. When using social media, the individual must disclose his/her position with the company if content is related to “Our Company.”
11. If you are to state an opinion, post blog or uploads comments in reference to “Our Company,” it must be disclosed that the comments are of your own opinion and not that of “Our Company.”
12. Disclosure of legal matters, lawsuits, internal complaints and disciplinary matters not available to the general public. All matter should be referred to HR.

**5. Policy Compliance**

1. All information sent or received over the internet or through email applications is subject to monitoring and review. No reasonable expectation of privacy in regards to this subject is to be expected.
2. “Our Company” will not be responsible for damages to employee personal property or loss of data resulting from improper use of company technology or negligence on the part of the employee.
3. “Our Company” has the right to monitor, deny or revoke access, audit employee data logs or take other appropriate actions should there be a reasonable detection of a violation of the company policies.
4. Violations of the company policies can result in disciplinary actions up to and including loss of privileges, termination, and legal action.
5. “Our Company” reserves the right modify this Acceptable Use Policy at any time.
6. If you have any questions or are aware of any violations of the AUP, you are encouraged to contact the system administrator at policy@ourcompany.com.

**6. Policy Reference**

1. Email Policy
2. Password/Security Policy
3. Social Media Policy
4. Data Access Policy

**7. Definitions**

1. User-any individual with network access
2. Company- “Our Company” and affiliates
3. Social Media-online forums such as Facebook, Instagram, Vine, Etc...
4. “Our Company” – registered name of the business entity, referred to as the company.

**8. Revision History**

Version 10.09.2015.1. This is the most up to date version.

**References**

[**https://www.sans.org/security-resources/policies/general/pdf/acceptable-use-policy**](https://www.sans.org/security-resources/policies/general/pdf/acceptable-use-policy)

**“Policy and Policy Making”** Edmund R. Gray,

<http://www.referenceforbusiness.com/encyclopedia/Per-Pro/Policies-and-Policy-Making.html>

**“How to Write an Information Security Policy”,** Jennifer Bayuk,

http://www.csoonline.com/article/2124114/strategic-planning-erm/how-to-write-an-informationsecurity-

policy.html

[**http://www.nicholasfinancial.com/AccpUse.pdf**](http://www.nicholasfinancial.com/AccpUse.pdf)

[**http://searchmidmarketsecurity.techtarget.com/tip/Acceptable-use-policy-for-Internet-usage-helps-data-protection-efforts**](http://searchmidmarketsecurity.techtarget.com/tip/Acceptable-use-policy-for-Internet-usage-helps-data-protection-efforts)

[**http://searchmidmarketsecurity.techtarget.com/tip/Acceptable-use-policy-for-Internet-usage-helps-data-protection-efforts**](http://searchmidmarketsecurity.techtarget.com/tip/Acceptable-use-policy-for-Internet-usage-helps-data-protection-efforts)