2017

Some Good Organization

[ACCEPTABLE USE POLICY]

[This policy outlines user behaviors that are acceptable for use and are consistent with protecting the information and assets of the *Some Good Organization*. Access to information resources is a privilege, not a right, and as such implies certain user responsibilities.]

Acceptable Use Policy

Policy Number:	0020002	Version:	01
Effective Date:	*to be completed on final approval*		
Last Revised Date:	May 1, 2017		
Responsible Office:	A. Jones		
Status:	Obsolete		

Executive Summary

This policy outlines user behaviors that are acceptable for use and are consistent with protecting the information and assets of *Some Good Organization*. Access to *Some Good Organization* information resources is a privilege, not a right, and as such implies certain user responsibilities. Such responsibilities may be defined by *Some Good Organization* policies, procedures, standards, federal, state or local laws or other regulations.

Purpose and Guiding Principles

The objective of this policy is to outline the appropriate employee and related third party behavior for the protection of *Some Good Organization* information and assets. Information Security is a team effort, and to be effective requires the involvement of every member of the organization.

Access to *Some Good Organization* information and resources are a privilege, not a right. This policy outlines the acceptable behaviors to protect the organization, its partners and its customers from damaging actions committed either knowing or unwittingly.

The Acceptable Use policy applies specifically to the information technology resources of *Some Good Organization* such as computers, applications, storage media and network accounts. Additionally it applies to such resources as email, the World Wide Web, FTP systems and others. These resources are intended to be used for *Some Good Organization* business purposes.

It is the responsibility of every user to familiarize themselves with this policy and its guidelines and to conduct their actions accordingly.

Scope

This policy applies to all divisions of *Some Good Organization*. It covers all *Some Good Organization* information technology resources, information that is or may be stored in digital form, as well as information and assets that may exist in physical form. All creation, processing, communication, storage, distribution and disposal of *Some Good Organization* information and assets are covered by this policy. Each employee of *Some Good Organization* contractor and other related third parties are bound by the guiding principles, statement of policy and related procedures outlined in this policy.

Statement of Policy

Privacy

In accordance with *Some Good Organization* policies regarding the use of company resources, users should have no expectation of privacy when using *Some Good Organization* information systems resources. This is notwithstanding the procedures implemented to protect the privacy of individual users.

Intellectual Works and Copyrights

Users are prohibited from unlawfully obtaining, installing, using, copying, storing or viewing copyright protected material on *Some Good Organization* owned information systems resources. In addition to potential legal issues, the use and dissemination of illegally obtained material increases the threat of malicious code (e.g. viruses, Trojans, etc) being introduced onto the organizations network systems.

Users creating intellectual works using *Some Good Organization* information systems resources should be aware that all rights, equities, royalties and other privileges are the sole property of *Some Good Organization* .

Data Confidentiality

Users are responsible for upholding the confidentiality of *Some Good Organization* data. Users should only access the data needed to perform their job function. Viewing, copying, or destroying any other users files without permission is prohibited.

Data Integrity

Users are responsible for protecting the integrity of *Some Good Organization* data. Modification or alteration of data without explicit permission is prohibited. Care should be exercised when working with applications that access stored data, that they do not unintentionally modify the stored data.

Responsible Use of Resources

Some Good Organization information systems resources are intended to be used for business purposes. This does not preclude the incidental use of company resources for personal use so long as such use meets the following standards

a) Use does not create a security risk

b) Use does not create any legal risk

c) Use does not consume significant computing resources

d) Use does not interfere with productivity

e) Use does not require the installation of any additional hardware or software

f) Use is appropriate for use or viewing within a workplace environment

Network Management

Some Good Organization IT management is responsible for the planning, installation and maintenance of network resources including, but not limited to network connections, dial-up modem connections and wireless connections. No hardware is to be added to the network without explicit written approval by IT management. This includes routers, switches, hubs, modems, wireless access points and other technologies.

Personally Owned Systems

Use of personally owned systems is prohibited on the *Some Good Organization* network. Users have a responsibility to protect the confidentiality and integrity of the organizations data, and as personally owned computing resources cannot be explicitly managed, use is prohibited. Any exception to this policy must be explicitly approved in writing by management.

Access Sharing

Users are individually responsible and personally accountable for the use and protection of their user credentials including their username and password. Passwords and other credentials should not be shared under any circumstances.

Unauthorized Access

Authorized users may not allow any unauthorized individual the use of *Some Good Organization* resources. This includes the installation or configuration of hardware or software to bypass or disable *Some Good Organization* network systems or security features.

Protection of Information

Users may, as a part of their regular job function, have access to sensitive or privileged information or assets that must be protected. Upon receiving access to such information, the user must ensure that the information or asset remains protected while in their possession.

Circumvention of Security Systems

Users are specifically prohibited from attempting to circumvent any application or systems security features. Examples of prohibited tools include following:

a) Password cracking tools

b) Port scanning tools

c) Vulnerability scanning tools (may exclude normal operating system features)

d) Keyboard logging

e) Packet capture tools

f) Network Sniffers

g) IP Spoofing

h) Use of any other users account credentials

The above listed tools are given as examples, and should not be considered to be all inclusive. Specific exceptions may be granted to IT or network staff for use in analysis or troubleshooting.

Outside Business

Some Good Organization computing facilities and network systems may not be used for any outside work, whether compensated or uncompensated, or for the benefit of any organization not related to *Some Good Organization* .

Use of Email

For purposes of this policy, email includes any electronic messaging involving *Some Good Organization* computers, assets and network systems. This includes messages sent from assigned email accounts, Instant Messenger messages, newsgroup or Usenet postings, text messages, messages sent using handheld devices such as smart phones or Blackberry devices. Email messages may be subject to retention standards or other regulatory guidelines, and as such, may be retained for a period of time even after a user has deleted them from their mailbox.

Users are responsible for all activity originating from their email accounts. The user should choose an appropriately strong password and should never share this password with others.

Users should be aware that their use of email may be monitored. Additionally, the unauthorized use or access of any mailbox other than ones own is strictly prohibited.

Users should use *Some Good Organization* email for business purposes only. Any vulgar or inappropriate language in email should be avoided. Users may be held liable for information that they disseminate inappropriately via email.

Users may not use *Some Good Organization* email systems for any of the following:

a) Chain mail

b) Hate mail or any abusive or harassing content

c) Virus Hoaxes

d) Sending or forwarding Spam or other Junk mail

e) Email that is not related to *Some Good Organization* business

f) Transmission of any sensitive information such as names, social security numbers, and account numbers, etc

The above items should be considered to be examples and are not exhaustive. The user should use good judgment in the use of email. In the event of a question, the user should contact their supervisor for clarification.

Litigation

In the event of litigation, users should be aware that all information resources are subject to discovery under federal and state rules of evidence. This includes, but is not limited to workstations, servers, laptops, cell phones, pagers, printers, home computers and any

other electronic equipment that is used as a part of *Some Good Organization* business. Use of information systems that contain subpoenaed information is subject to special procedures, and is to be done only under the guidance of counsel. Any attempt to alter or destroy evidence or subpoenaed information may subject the user to civil and criminal penalties and may result in immediate termination.

Procedures

Within this Section, the phrases must and recommended have specific meanings where highlighted in boldface. If a department correctly adheres to the guidelines given as must, then it can be considered as meeting the requirements for this policy. If they also adhere to the guidelines given as recommended, then they can be considered to be meeting the minimum requirements to be in accordance with generally accepted information security practices.

A. All use of *Some Good Organization* information resources must be in compliance with the Information Security Policy and Data Handling Policy

B. All users must be authenticated by a user ID and password or other reliable means.

C. Users must select strong passwords and change their passwords on a regular basis.

D. Users must not share their username and/or password with any other user under any circumstances

E. Creation of documents or other data must be in compliance with the Data Handling Policy.

F. Users must take appropriate means to protect *Some Good Organization* information and assets from physical or environmental harm. This includes storing sensitive files in locked cabinet or drawers, using cable locks or other means to protect laptops and other mobile assets and the use of controlled-access areas for file and application servers.

G. Users must ensure that anti-virus software on their systems is kept up-to-date and running appropriately. An IT administrator must be notified as soon as possible should a problem arise.

H. In the event that a virus outbreak is found or expected, users must cease use of the affected system and report the incident to an IT administrator or their supervisor as quickly as possible.

I. In the event of a security breach or suspected security breach, users must report the incident to their supervisor as quickly as possible. Users must not try to investigate or remediate the problem on their own.

J. Remote access to *Some Good Organization* network systems must be made via approved means. In no case may unapproved modems, wireless networks, or other non-approved network access devices be used to attempt to access the network.

Roles and Responsibilities

Each user of *Some Good Organization* s information and assets is responsible for familiarizing themselves with the contents of this policy and modeling their actions accordingly. Any user of the organizations information or assets is responsible for abiding by this policy, whether they are an employee, contractor, vendor or other related third party.

Additionally, users are responsible for exercising good judgment regarding the use of *Some Good Organization* information and assets. In cases where appropriate use is in question, users are responsible for immediately contacting their supervisor for resolution.

Users are responsible for immediately reporting any security breaches, incidents or perceived security weaknesses. In the event of a breach or suspected breach, every second is critical and as such, users should err on the side of caution and contact their supervisor immediately.

Compliance

Any person who uses *Some Good Organization* s information or assets consents to all provisions of this policy and agrees to comply with all of its terms and conditions, as well as with relevant state and federal laws and regulations. Users have a responsibility to use these resources in an effective, ethical and lawful manner. Any violation of this policy may result in disciplinary or administrative sanctions including loss of privileges, monitoring of use and up to and including termination depending on the severity and intent of offense. Additionally, non-compliance with this policy resulting in loss or disclosure of data may result in personal civil and/or criminal liability.

Policy Modifications

This policy may be changed by *Some Good Organization* Senior Management at any time, but typically will be modified in response to newly identified threats or risks. Changes to this policy will be communicated and distributed to all affected parties. Most major changes to the policy will be made during official policy review sessions on an annual basis, but if required a policy review session may be convened on a special basis.

Communication

Upon approval, this policy is to be distributed to all *Some Good Organization* employees, contractors, vendors and related third parties. Upon subsequent revisions, updates or amendments to this policy affected individuals will be notified of the change along with an office or individual to whom they can direct additional questions.

Acknowledgement of Understanding

I have been provided with a copy of the *Some Good Organization* Acceptable Use Policy and have read and reviewed the policy. I have been provided the opportunity to ask questions about the policy and am aware of resources to which I may look for more information. I understand that it is my responsibility to comply with the provisions of the policy and that failure to do so is subject to disciplinary action up to and including immediate termination. My signature below indicates that I have been provided with and have read the *Some Good Organization* Acceptable Use Policy and furthermore indicates my understanding and willingness to comply with the provisions of the policy.

_____

Employee

_____

Date