2017

Some Good Organization

[INFORMATION SECURITY POLICY]

Information Security Policy

Policy Number:	0020002	Version:	01
Effective Date:	*to be completed on final approval*		
Last Updated:	May 4, 2017		
Responsible Office:	A. Jones		
Status:	Obsolete		

Contents

Executive Summary 4

Purpose and Guiding Principles 5

Scope 7

Statement of Policy 8

Procedures 9

Roles and Responsibilities 11

Senior Management 11

Employees 11

Compliance 13

Policy Modifications 13

Communication 13

Acknowledgement of Understanding 14

Executive Summary

The Information Security Policy exists in order to provide the organizations staff with a current set of clear and concise information security policies. These policies provide direction for the appropriate protection of the organizations information and assets.

The Information Security Policy has been created as a component of an overall Information Security Program (ISP) for the organization. The ISP outlines the organizations mission and objectives as they relate to information security, outlines details that are responsible for information security, documents policies relating to information security, indicates how the program is to be communicated and how people in the organization must be trained on their responsibilities, and includes a roadmap of how the program is to be carried out. In addition, the program includes strategies for its ongoing evaluation and adjustment, addressing of compliance issues, and management reporting.

Purpose and Guiding Principles

The purpose of this policy is to provide general guidance and specific recommendations for the protection of *Some Good Organization* information technology resources and the information stored on those resources. Additionally information and assets that exist in hard form are also protected by this policy. These information security measures are intended to protect the organizations information and assets and to preserve the privacy of *Some Good Organization* s employees, contractors, vendors, and other related third parties.

The broad goal of information security at *Some Good Organization* is to maintain Confidentiality, Integrity, and Availability of data. To achieve this goal, *Some Good Organization* has identified a set of core security principles to guide the creation of a policy based on the ISO 17799 framework. The policy will, in turn, be supported by detailed operational procedures. These simple principles make up the foundations of a strong security posture.

Universal Participation Every component of an organization could be a potential avenue of entry for unauthorized intruders. Thus a strong security infrastructure requires the cooperation of all parties in the organization. Everyone is responsible for security.

Risk-Based security An organizations security is defined by the unique risks it faces. These risks should be identified regularly and should remain the primary focus of any security policy or program.

Deny All That is Not Explicitly Permitted Anything not explicitly allowed is denied.

Least-Privilege Users and systems should only have minimum level of access necessary to perform their defined function. All unnecessary levels of access should be restricted unless explicitly needed.

Defense-in-Depth Overall security should not be reliant upon a single defense mechanism. If an outer security perimeter is penetrated, underlying layers should be available to resist the attack.

Compartmentalization If one compartment is compromised, it should be equally difficult for an intruder to obtain access to each subsequent compartment.

Secure Failure When a systems confidentiality, integrity, or availability is compromised, the system should fail to a secure state.

Defense through Simplicity A simple system is more easily secured than a complex system, as there is a reduced chance for error.

Dedicated Function Systems should be single-purposed to avoid potential conflicts or redundancies that could result in security exposures.

Need-to-Know Information will only be circulated to those parties that require it in order to perform their defined business function.

Effective Authentication and Authorization Firmly established identity and role-based authorization are essential to making informed access control decisions.

Audit Integrity Audit log events that are generated may not be altered by the entity that generated the event.

Scope

This policy applies to all divisions of *Some Good Organization*İt 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

The Information Security Policy exists in order to provide the organizations staff with a current set of clear and concise information security policies. These policies provide direction for the appropriate protection of the organizations information and assets.

The Information Security Policy has been created as a component of an overall Information Security Program (ISP) for the organization. The ISP outlines the organizations mission and objectives as they relate to information security, outlines details that are responsible for information security, documents policies relating to information security, indicates how the program is to be communicated and how people in the organization must be trained on their responsibilities, and includes a roadmap of how the program is to be carried out. In addition, the program includes strategies for its ongoing evaluation and adjustment, addressing of compliance issues, and management reporting.

The Information Security Policy has been reviewed, approved, and is endorsed by *Some Good Organization* management.

The Information Security Policy applies to all *Some Good Organization* employees, contractors, and any third-party providers that support any of the *Some Good Organization*ś services.

The Information Security Policy document contains rules and requirements that must be met in the delivery and operation of the *Some Good Organization*ś services. More detailed standards and specific procedures must be developed as adjuncts to this Information Security Policy to provide implementation level details for carrying out specific operational tasks. The procedures must be the instrument by which these *Some Good Organization* Security Policies are converted into action.

The Information Security Policy must be located in a central repository that is accessible to all *Some Good Organization* employees and related third parties.

The Information Security Policy must be distributed to all new and existing *Some Good Organization* employees for review. All *Some Good Organization* employees, contractors and third party providers are required to sign an agreement representing the fact that they have reviewed, and agree to adhere to, all policies within the Information Security Policy document.

Exceptions to the Information Security Policy must be authorized by both *Some Good Organization* management and the affected asset owner. Please refer to InformationSecurityResponsibleParty for exception process details.

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. Departments must limit access to information and assets to individuals that have been explicitly authorized by management.

B. Departments must protect all information resources (e.g. computers, communications, software, data) from theft, tampering, misuse, malicious software (e.g. viruses, worms, Trojan Horses), destruction, and loss.

C. Managers must ensure that individuals who use *Some Good Organization* information resources or assets have read both the *Some Good Organization* Information Security Policy as well as the *Some Good Organization* Acceptable Use Policy. Employees are bound by these policies as conditions of their employment. It is recommended that these policies be reviewed with individuals on at least an annual basis.

D. The IT manager must ensure individual and organizational accountability for the use and protection of information systems through the use of unique identifiers and authentication methods (e.g. user ID/password, digital certificates, or biometrics).

E. Departments and managers must prohibit the sharing or unauthorized disclosure of passwords or other confidential access information (e.g. access phone numbers, account names, codes, network information) except as explicitly authorized.

F. Each department must provide the IT manager prompt notification of changes in employee status (e.g. transfers, terminations, retirement) for all employees and other users of IT resources and systems.

G. Each department must control access to information based on the confidentiality of the data and the requirements established in the Data Access Policy. (NOTE: this requires that all significant collections of information have a defined data steward who is responsible for overseeing the appropriate use of the data collection).

H. The IT manager must ensure that appropriate controls exist to ensure only authorized use of software and hardware that is designed for bypassing or breaking through information security measures and procedures. Ensure appropriate audit procedures are established to monitor for inappropriate use of software and hardware that is capable of bypassing or breaking through information security measures and procedures.

I. As necessary the IT manager must be capable of producing, reviewing, and retaining audit trails of security related information for all systems that process or store *Some Good Organization* information.

J. It is recommended that each department or group regularly perform self-assessments and/or audits to detect security vulnerabilities and non-compliance to *Some Good Organization*'security policies and procedures. Upon discovery, each department must initiate corrective actions to ensure that compliance with these policies and procedures is restored.

K. Apply cryptographic controls as appropriate to protect critical information that is transmitted or stored on *Some Good Organization*'s network, workstations, laptops or servers. Passwords, keys, certificates or other means to decrypt data must be provided to management for escrow to facilitate the recovery of data. All laptop computers must use encryption to protect stored data in case of loss.

L. Each department as well as the IT manager must ensure that and procured IT resources are have sufficient capabilities to allow compliance with this policy, such as User ID/passwords, system integrity protection, and audit logging.

M. Each department must make sufficient plans to maintain continued availability of business-critical resources and information through appropriate business continuity and disaster recovery planning. It is recommended that departments review and test these plans on at least an annual basis.

N. Each department must apply information retention procedures that satisfy external and internal requirements, while ensuring the application of procedures to dispose of information that is no longer needed.

Roles and Responsibilities

Senior Management

Some Good Organization Senior management is responsible for:

A. Promulgating and enforcing the policies, standards, procedures, and guidelines for the protection of IT resources and information.

B. Furnishing necessary funding and other resources or limiting and eliminating services to ensure continued compliance with this policy.

C. Appointing an Information Security Coordinator and/or establishing departmental computer support and system administrators. Providing appropriate training and resources to the person(s) responsible for information security-related tasks.

D. Specifying and applying sanctions consistent with Human Resources policies to individuals and divisions that break provisions of this policy, either willfully, accidentally, or through ignorance.

E. Designating Data Stewards for each significant collection of business information, who in turn are responsible for determining the value of their information and implementing appropriate security measures as specified in the Data Access Policy.

F. Sponsoring internal awareness and training programs to familiarize employees, contractors and third-party providers with the security policy, procedures and recommended practices.

G. Defining guidelines and intervals for the review and update of this policy and to reassess existing risks and to identify potential new risks to *Some Good Organization* assets and information.

Employees

Each *Some Good Organization* employee is responsible for understanding and complying with the policies and procedures relating to information technology security and for fully cooperating with the information security staff at all levels to protect *Some Good Organization*ś information and assets.

Each employee must become familiar with *Some Good Organization*ś Computer and Network Usage Policy.

Some Good Organization computer and communications systems must be used for business purposes only. Incidental personal use is permissible if the use (a) does not consume more that a trivial amount of resources that could otherwise be used for business purposes, (b) does not interfere with worker productivity, and (c) does not preempt any business activity. Examples of permissible incidental use include the occasional use of electronic mail (email) or web access for other than official purposes.

Using *Some Good Organization* systems to download, use, or re-distribute unlicensed or inappropriate software, copyrighted movies, copyrighted music, or pornographic materials, place the Institute at risk and will not be tolerated. Conduct in violation of this policy may result in sanctions as provided in the Computer and Network Usage Policy. Report all actual or suspected instances of security or policy violations in accordance with the Incident Reporting section of this policy.

Compliance

Any person who uses *Some Good Organization*ś 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* Information Security 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 indicated that I have been provided with and have read the *Some Good Organization* Information Security Policy and furthermore indicates my understanding and willingness to comply with the provisions of the policy.

____

Employee

____

Date