Information Security Policy

UTILLI LLC

ISO 27001:2013

Document Version history

Version	Date	Change Description	Authored/Modified By	Reviewed By	Approved By
0.1	23-Jul-2021	Initial update	Ghanghor Singh	Raja Vemuri	Ali Saberi
1.0	26-Jul-2021	Feedback incorporated	Ghanghor Singh	Raja Vemuri	Ali Saberi

Version: 1.0
Classification: Public

Table of Contents

1. Purpose

The information security policy describes how information security has to be developed in an organization, for which purpose and with which resources and structures. A security policy describes information security objectives and strategies of an organization. The basic purpose of a security policy is to protect people and information, set the rules for expected behaviors by users, define, and authorize the consequences of violation

2. Policy Statement

This Information Security Policy is based on ISO 27001:2013 the recognized standards of Information Security. As a product, consulting, and service provider organization, Utilli is committed to ensuring the following security principles:

Confidentiality: all sensitive information will be protected from unauthorized access or disclosure;
Integrity: all information will be protected from accidental, malicious and fraudulent alteration or destruction; and,
Availability: Information services will be available throughout the times agreed with the users and be protected against accidental or malicious damage or denial of service.

Utilli will ensure the above three of it's information system using a Risk Management Methodology. Utilli strives to incorporate Information Security Principles, into organization's culture, by making it the responsibility of every stakeholder to build and maintain a robust information security environment and to continuously improve it thereafter by adopting latest trends and technology in the area of Information Security.

3. Responsibility

All employees and third parties - You are individually responsible for protecting the equipments, softwares and information in your hands. Security is everyone's responsibility.

4. Scope and Applicability

This Policy covers the security of information systems and data networks owned or used by Utilli as well as the information that is stored, transmitted or processed by those systems.

This Policy applies to all Utilli staff, assignees and contractors that provide services to Utilli, access and uses our information systems, is an integral part of the Utilli's Business Code of Conduct.

This Policy does not cover issues related to general physical and building security. It covers, however, physical security aspects of buildings or parts of buildings that directly affect the security of information owned by Utilli.

5. Information Security objectives

- To define the general security policy for Utilli Information Systems and the information stored, processed and transmitted by them, including outsourced services
- To ensure confidentiality of information
- To ensure integrity of the information
- To ensure availability of the information to authorized users whenever needed
- To ensure business continuity
- To ensure achievable level of compliance to regulatory, legislative and contractual requirements
- To train employees on information security so as to achieve awareness within organization
- To maintain/achieve stakeholder's confidence

6. Other Policies

At Utilli, considering the security requirements, Information Security policies have been framed based on a series of security principles. All the Information Security policies and their need have been addressed below:

- Asset Management Policy
- Information Risk Management Procedure
- Information Classification Policy
- Access control Policy
- Password Security policy
- Information Security Incident Management Policy
- Change Management Policy
- Network Security Policy
- Anti-Virus Policy
- Backup Policy
- Mobile Device Policy
- Business Continuity Policy
- Remote Access Policy

7. Periodic Review

The policy shall be reviewed every year or at the time of any major change in existing IT environment affecting policy and procedures, by CISO and placed to Board for approval.

This policy will remain in force until next review / revision.

8. Information Security Governance

Information security governance consists of leadership, organisational structures and processes that protect information and mitigation of growing information security threats.

Critical outcomes of information security governance include:

1. Alignment of information security with business strategy to support organisational objectives
2. Management and mitigation of risks and reduction of potential impacts on information resources to an acceptable level
3. Management of performance of information security by measuring, monitoring and reporting information security governance metrics to ensure that organisational objectives are achieved
4. Optimisation of information security investments in support of organisational Objectives

It is important to consider the organisational necessity and benefits of information security governance. They include increased predictability and the reduction of uncertainty in business operations, a level of assurance that critical decisions are not based on faulty information, enabling efficient and effective risk management, protection from the increasing potential for legal liability, process improvement, reduced losses from security-related events and prevention of catastrophic consequences and improved reputation in the market and among customers.

9. Management Responsibility

1. Approve policies related to information security function
2. Ownership for implementation of board approved information security policy
3. Ownership for establishing necessary organisational processes for information security
4. Ownership for providing necessary resources for successful information security
5. Ownership for establishing a structure for implementation of an information security program(framework)

10. Compliance

Compliance with Regulatory requirements

- Compliance to statutory, regulatory and contractual requirements as applicable in the country of business, directives and recommendations issued by the Government.
- Compliance with terms/conditions and license requirements for the usage of copyrighted software or any other proprietary information/material shall be maintained
- Cross border movement of data shall be in accordance with legal and regulatory requirements
- Records shall be retained and managed based on legal and regulatory requirements

Compliance with Information Security policy and procedures

- Information processing facilities shall be used as per information security policy and acceptable usage policy
- While Utilli respects the privacy of its employees it reserves the right to audit and/or monitor the activities of its employees and information stored, processed, transmitted or handled on any assets/devices/services used by employee
- Exception to security policy and procedure shall be approved through the exception management process
- Policy exceptions shall be reviewed at least annually and as deemed necessary based on security risks envisaged, emerging threats etc.
- Violations or any attempted violations of security policies and procedures shall result in disciplinary actions

Information Systems Audit

- Audits shall be conducted to ensure compliance with the information security policies, procedures and guidelines
- The use of information systems audit tools shall be controlled and authorised to prevent any possible misuse of tools.