IT Policy

IT governance is an integral part of corporate governance of Sonu Marketing Private Limited (Company), and effective IT governance is the responsibility of the board of directors of Sonu Marketing Private Limited ("Board") and its executive management. This Policy ensures implementation of this IT Framework which, inter alia, includes (i) Security aspects; (ii) User Role; (iii) Information Security and Cyber Security; (iv) Business Continuity Planning Policy; (v) Back-up Data.

I. Objective

1. Purpose

This policy defines the control requirements surrounding the management of access to information on Company's computer and communications systems.

2. Scope

This policy applies to all Company's computer systems and facilities, with a target audience of Company's Information Technology employees and partners.

3. Policy applied to All the internal Parties

A. Access Control System

Access Control System – User ID Creation Date - Access control systems must be configured to capture and maintain the creation date for every user ID.

Access Control System – Last Logon Date - Access control systems must be configured to capture and maintain the date and time of the last logon for every user ID.

Access Control System – Last Logoff Date - Access control systems must be configured to capture and maintain the date and time of the last logoff for every user ID.

Access Control System – Password Change Date - Access control systems must be configured to capture and maintain the date and time of the last password change for every user ID.

Access Control System – User ID Expiration Date - Access control systems must be configured to capture and maintain an expiration date or every user ID that represents the last date that the user ID is active for use.

Malfunctioning Access Control - If a computer or network access control system is not functioning properly, it must default to denial of privileges to end-users.

Special Privileged Users - All multi-user computer and network systems must support a special type of user ID, which has broadly-defined system privileges that will enable authorized individuals to change the security state of systems.

Operating System User Authentication - Developers must not construct or install other mechanisms to identify or authenticate the identity of users without the advance permission of Company's management.

Access Control System Modification - The functionality of all access control systems must not be altered, overridden or bypassed via the introduction of additional code or instructions.

Password Generation Algorithms - All software and files containing formulas, algorithms, and other specifics used in the process of generating passwords or Personal Identification Numbers must be controlled with the most stringent security measures supported by the involved computer system.

Password Retrieval - Computer and communication systems must be designed, tested, and controlled so as to prevent both the retrieval of, and unauthorized use of stored passwords, whether the passwords appear in encrypted or unencrypted form.

Access Control Information in Cookies - Company's information systems must never store any access control information in cookies deposited on, or stored on, end-user computers.

System Capabilities and Commands - End users must be presented with only the system capabilities and commands that they have privileges to perform.

B. Authorization

Sensitive or Valuable Information Access - Access to Company's sensitive information must be provided only after express management authorization has been obtained.

Granting Access to Organization Information - Access to Company's information must always be authorized by a designated owner of such information, and must be limited on a need-to-know basis to a reasonably restricted number of people.

Information System Privilege Usage - Every information system privilege that has not been specifically permitted by the Company's management must not be employed for any Company's business purpose until approved in writing.

Granting System Privileges - Computer and communication system privileges must be granted only by a clear chain of authority delegation.

User ID and Privilege Approval - Whenever user IDs, business application system privileges, or system privileges involve capabilities that go beyond those routinely granted to general users, they must be approved in advance by the user's immediate supervisor and Company's management.

Owner Approval for Privileges - Prior to being granted to users, business application system privileges must be approved by the applicable information owner.

System Access Request Authorization - All requests for additional privileges on Company's multi-user systems or networks must be submitted on a completed system access request form that is authorized by the user's immediate manager.

Default User Privileges - Without specific written approval from management, administrators must not grant any privileges, beyond electronic mail and word processing, to any user.

Computer Access Training - All Company's users must complete an approved information security training class before they are granted access to any Company's computer systems.

C. Access and Privilege Assignment

Production Programs and Information Access - Access controls to production programs and information must be configured such that production programs and information systems software support personnel are not granted access privileges except for problem resolution.

Operations Personnel Information Access - Access controls to production programs and information must be such that computer operations personnel are restricted from modifying systems software, application software, and production information.

Privilege Restriction — Need to Know - The computer and communications system privileges of all users, systems, and programs must be restricted based on the need to know.

User IDs Employed in Abusive Activity - All access privileges for a user ID shown to be engaged in abusive or criminal activity must be immediately revoked.

Developer Access To Production Business Information - Where access to production business information is required so that new or modified business application systems may be developed or tested, only “read” and “copy” access must be granted on production machines. This access is permitted only for the duration of the testing and related development efforts, and must be promptly revoked upon the successful completion of these efforts.

Secret Information Access - Access to sensitive information must be granted only to specific individuals, not groups of individuals.

II. PASSWORDS

1. Introduction

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in a compromise of Company’s entire network. As such, all employees are responsible for taking the appropriate steps, as outlined below, to select and secure their password.

2. Purpose

The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change.

3. Policy

A. General

• All application-level passwords (e.g. Passwords used to logging into .net applications and web module) must be changed at least every 45 days and cannot be used the past 5 password.

• All user-level passwords (e.g., email, desktop computer, etc.) must be changed at least every 45 days and cannot be reused the past 10 passwords.

• Passwords must not be inserted into email messages or other forms of electronic communication.

• All user-level and application-level passwords must conform to the guidelines described below.

B. Guidelines

The Password Construction Requirements

i. Be a minimum length of eight (8) characters on all systems and maximum of twelve (12) characters.

ii. Not be a dictionary word or proper name.

iii. Not be the same as the User ID.

iv. Expire within a maximum of 45 calendar days.

v. Password must have at least one alphabet and one numeric character and one special character.

vi. Not be identical to the previous five (5) passwords.

vii. Not be displayed when entered.

viii. Ensure passwords are only reset for authorized user.

ix. Not be transmitted in the clear or plaintext outside the secure location.

a. Password Deletion

All passwords that are no longer needed must be deleted or disabled immediately. When a user quits (retires, resigned, suspended, dismissed, etc.), Default passwords shall be changed immediately on all equipment or the user id must be disabled immediately.

b. Password Protection Standards

Do not use your User ID as your password. Do not share passwords with anyone. All passwords are to be treated as sensitive and confidential information.

Here is a list of “do not’s”

• Don’t reveal a password over the phone to anyone
• Don’t reveal a password in an mail message
• Don’t reveal a password to the boss
• Don’ talk about a password in front of others
• Don’t hint at the format of a password (e.g., “my family name”)
• Don’t reveal a password on questionnaires or security forms
• Don’t share a password with family members
• Don’t reveal a password to a co-worker while on vacation
• Don’t use the "Remember Password" feature of applications
• Don’t write passwords down and store them anywhere in your office.
• Don’t store passwords in a file on ANY computer system unencrypted.

If someone demands a password, refer them to this document or have them call COMPANY help desk.

If an account or password is suspected to have been compromised, report the incident to COMPANY and change all passwords.

c. Application Development Standards

Application developers must ensure their programs contain the following security precautions:

• Should support authentication of individual users, not groups.
• Should not store passwords in clear text or in any easily reversible form.
• Copy paste of user id and password should be disabled in application.
• System should compel the user to change his password when he logs in for the first time.
• System should disable the user id, if wrong password is entered on three consecutive occasions.

d. Remote Access Users

Access to the COMPANY networks via remote access is to be controlled by using either a Virtual Private Network (in which a password and user id are required).

III. INFORMATION SECURITY

1. Policy Description

This is the collection of policies that implement the overall spirit of the management system. Policies are broad but topical in nature.

The Information Security Management System is

• Aligned to global standards for Information Security Management – ISO/IEC 27001:2013
• Adopt best practices for Information Security Management

There is adequate focus on ensuring adequate protection of information assets by

• Following efficient and effective processes • Protecting customers' and organization's information

a) An effective Management System is established for Information Security.
b) All policies are approved will be communicated to all Customers, vendors and other interested parties.
c) Periodic reviews of this policy will be carried out to ensure its continued suitability and applicability.
d) Periodic reviews of the policy implementation will be conducted by internal or external auditors.
e) Company adheres to their customer's policies, processes and other guidelines, if any, as required by and agreed with the customer.
f) There is an effective mechanism to ensure continual improvement of Processes practiced.
g) Senior management is fully committed to IT service management and information security.
h) Threats and risks to information system assets are properly identified using effectively managed and structured Risk Management framework on periodic basis i) All identified Security risks in information systems have been reduced to an acceptable level. j) Information is protected against unauthorized access and malicious activities with required security infrastructure in place k) Measures are taken to assure confidentiality, Integrity and availability of information l) Build, maintain and review a competent and professional security organization to manage the implementation of, and compliance with, Information Security Policy, Standards and Procedures m) Give top priority to security awareness and education in order to ensure that all personnel are fully aware of the security requirements and all relevant security measures n) Compliance with Government Regulations, legislative and contractual requirements are ensured o) All breaches of information security, actual or suspected, are reported to, and investigated by the Incident Management Process.