Cyber Security Policy for Saral

Introduction

a. Purpose: The purpose of this policy is to establish guidelines for the secure use of company information technology (IT) resources and to ensure the confidentiality, integrity, and availability of company information.
b. The risk of data theft, scams, and security breaches can have a detrimental impact on a company's systems, technology infrastructure, and reputation. As a result, [company name] has created this policy to help outline the security measures put in place to ensure information remains secure and protected.
c. Scope: This policy applies to all employees, contractors, and other individuals who access company IT resources, including computer systems, networks, and data.
d. This policy applies to all of remote workers, permanent, and part-time employees, contractors, volunteers, suppliers, interns, and/or any individuals with access to the company's electronic systems, information, software, and/or hardware.

Information Security

a. Confidentiality: All employees and contractors must protect the confidentiality of company information and only access information that is necessary to perform their job responsibilities.

b. Integrity: Employees and contractors must take all necessary measures to ensure the accuracy and integrity of company information, and must report any suspected incidents of tampering or unauthorized changes.

c. Availability: Employees and contractors must take all necessary measures to ensure the availability of company information and IT resources, including backing up critical data and reporting any suspected incidents of disruption.

Access Controls

a. Passwords: Employees and contractors must use strong passwords and keep them confidential. Passwords must be changed regularly, and employees must immediately report any suspected incidents of password compromise.

b. Authorization: Access to company IT resources and information must be authorized and granted based on job responsibilities and the principle of least privilege.

c. Remote Access: Remote access to company IT resources must be secured using encrypted connections and multi-factor authentication.

Data Management

a. Data Backup: Critical data must be backed up regularly and stored in a secure location.

b. Data Retention: Data must be retained in accordance with company policy and legal requirements. Unnecessary data must be deleted in a secure manner.

c. Data Transfer: Company information must not be transferred to external devices or networks without proper authorization and encryption.

Incident Response

a. Reporting: Employees and contractors must report any suspected incidents of information security breaches to the IT department immediately.

b. Response: The IT department will respond to all suspected incidents of information security breaches in accordance with the company's incident response plan.

c. Investigation: The IT department will investigate all incidents of information security breaches and take appropriate action to contain and remediate the incident.

Training and Awareness

a. Awareness: All employees and contractors must be aware of this policy and their role in protecting company information and IT resources.

b. Training: Employees and contractors must receive regular training on information security, including the safe use of IT resources and the handling of confidential information.

Policy Compliance

a. Monitoring: The IT department will monitor compliance with this policy and take appropriate action to enforce it.

b. Sanctions: Employees and contractors who violate this policy may be subject to disciplinary action, up to and including termination of employment or contract.