[INSERT FIRM LEGAL NAME]

Voicemail Security Policy

[Insert Firm Logo]

Version 1.0

[Insert Date]

Contents

Instructions

Documents are in a template format and are to be customized to fit the appropriate business and operational requirements. Use the sample as a foundation to build a bespoke policy for your business.

If any element of the following Sample/Template is not operationally feasible or appropriate for a particular business, be sure to delete that element from the company-specific document. **Otherwise, it would be a liability exposure to establish a policy and not to comply with it.**

The following recommendations are designed to limit, but will not eliminate, the security risks associated with the use of the policy subject. Businesses should deploy a defense-in-depth security model of technical, operational, and physical security controls.

Delete the instructions after finalizing and adopting the policy.

Policy Overview

Information Security has the authority to review Personal Communication Devices (PCDs) and Voicemail accounts. All PCDs must comply with the security policy and any applicable federal regulations.

Policy Detail

The communication devices should not be used for private business or personal communications during working hours. An employee who is required to carry a PCD will be responsible for ensuring that all calls made on company time originate from that device. Any unauthorized calls made on company time by an employee will be considered for disciplinary action.

Handheld wireless devices (Bluetooth headsets, cell phones, smartphones, PDAs) are issued to individuals who need to conduct immediate, critical business. These devices should be used only when the user is away from their desk and/or out of the office. Voicemail messages should be left in accordance with the Corporate Policy as well as any other applicable guidelines or regulations.

Bluetooth
All authorized personnel who have received approval to access voicemail may use hands-free enabling devices, such as Bluetooth. Care must be taken to avoid being recorded when using a Bluetooth adapter. Bluetooth 2.0 Class 1 devices have a range of 330 feet that can be picked up by unauthorized personnel.

Voicemail
Voicemail boxes may be issued to personnel who require a method for others to leave messages when they are not available. Voicemail boxes must be protected by a PIN which must never be the same as the last four digits of the telephone number of the voicemail box. This PIN will only be known by the individual assigned to said box, and will not be released to anyone outside of IT.

Loss and Theft
All files containing confidential or sensitive data (including emails, documents, electronic spreadsheets, and any other type of sensitive information) may not be stored on a PCD unless protected by approved encryption. Never store confidential or sensitive data on your personal PCD. When leaving the organization, the employee is responsible for bringing all portable devices back to the IT department, along with an inventory list of equipment owned. Equipment must be returned in its original condition and can be replaced at cost to the employee if it is lost or stolen.

Personal Use
PCDs and voicemails are issued for business uses. In order to preserve the integrity of personal communication, personal use should be limited to minimal and incidental use.

Scope and Purpose

Scope

All use of Personal Communication Devices and Voicemail issued by or used for business is subject to this policy.

Purpose

This document describes Information Security requirements for Personal Communication Devices (PCDs), Voicemail, and Digital Voice Mail. These requirements include what IT staff can support and how the management of these systems will be conducted.

Compliance

The Information Security team will verify compliance with this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Exceptions

Any exception to the policy must be approved by the Information Security team in advance.

Revision Table

Revision History				
#	**Version #**	**Date**	**Updates/Changes**	**Owner**
1	1.0	2023	Initial Draft	Riskigy
2				