COUNTY OF SAN MATEO

Telephone and Voicemail Policy

Overview

The County's telephone and voicemail systems are customer service tools that enable the public to communicate with County agencies and receive timely assistance. These systems promote prompt and courteous customer service and are intended for official County use only.

Purpose

The purpose of this policy is to establish parameters for appropriate use of the County's telephone and voicemail systems. It is also to establish responsibility for and management of the telecommunications systems for the County.

Scope

The scope of this policy includes all users of the County of San Mateo's telephone system, including vendors, contractors, volunteers, temporary consultants, and any party who provides services to the County; collectively known as workforce members.

The policy applies to all telecommunications systems and services, including but not limited to traditional stationary telephones, mobile phones, software-based phones, conference services, and voicemail.

Policy

All communications devices are intended for calls related to the activities of the County. Telephones, telephony equipment, voicemail boxes, and messages contained within voicemail boxes are the property of the County of San Mateo. The Information Services Department (ISD) is responsible for negotiating, procuring, and installing all communication devices for the County as well as the administration of telephone and voicemail accounts.

The following uses of the County's telecommunications services are unacceptable and unauthorized under this policy:

1. The use of the County's communication systems to convey obscene, harassing, or offensive messages.
2. Unauthorized entry into a voice mailbox.
3. Broadcasting unsolicited personal views on social, political, or other non-business-related matters.
4. The use of County resources to solicit or conduct business for personal gain.
5. Making personal long-distance phone calls.

Telephones

Privacy of Data

All workforce members shall ensure that internal information not designated as public information shall be shared only within the County and only with authorized personnel as necessary to fulfill their job duties. Prior to releasing any information that is not designated as public over the telephone, the workforce member releasing the information must verify the requestor's identity by ensuring that the call is being made from an internal telephone number that has been assigned to the requester.

Voicemail

The County provides voicemail to its employees for business purposes. Policies governing the use of voicemail shall be consistent with other County policies. Voicemail is to be used as a backup in the event the workforce member is not available to answer a call and should not be used to screen calls. Each workforce member is expected to respond to voicemail messages in a timely manner.

As a result of unified messaging, which enables workforce members to access and retrieve voicemail messages from many different devices, this policy covers acceptable use to ensure protection of voicemail content.

Workforce members using voicemail shall be aware of the following in the protection of voicemail contents:

1. Protected Health Information (PHI) pursuant to the Health Insurance Portability and Accountability Act (HIPAA) and/or Personally Identifiable Information (PII) shall not be left on a voicemail message. This is to prevent such information from being forwarded to and/or stored on another device.

2. The content of voicemail messages is not private. All voicemail messages are discoverable for legal and investigative purposes.

Privacy of Data

As with telephone usage, it is up to the individual workforce member to ensure that he/she is abiding by HIPAA standards and all County security protocols. Prior to transferring any voicemail messages, the workforce member releasing the information must ensure that no confidential or sensitive information is being released. Internal information shall be shared only within the County and with authorized personnel as necessary for legitimate business purposes.

Confidential Data

Examples of confidential data include but are not limited to:

- Social Security Numbers
- Bank account or credit card numbers

- Personal Health Information or other data covered by the HIPAA. For a detailed list of identifiers as it relates to HIPAA, see this link.
- Data covered by the Criminal Justice Information Services (CJIS) security policy
- Login/password credentials

PIN Number

All voicemail boxes are protected with a PIN (personal identification number). Although the County makes every effort to protect the voicemail system, workforce members must comply with safeguarding their PIN to ensure the privacy of their messages. Workforce members must configure their PIN in a way that they cannot be easily guessed. PINs may not be shared or provided to others to facilitate access.

Voicemail Capacity

Workforce members are responsible for maintaining the capacity of their voicemail. Under no circumstances should voicemail be at capacity in that messages may no longer be recorded.

County's System Access

Workforce members shall be aware that all data on County systems is the property of the County. Workforce members shall have no right or expectation of privacy of information stored on the County's telephone and voicemail systems. The County maintains the right to access, audit, and delete any voicemail messages as well as monitor the telephone system on a periodic basis to ensure compliance with this policy. The County's telephone administrators may override workforce member's PIN to gain access to the voicemail without prior notification to the workforce member. Similarly, supervisors and managers shall have the right to review the voicemail messages of any workforce member supervised by them at any time and for any reason. The County reserves the right to monitor the telephone and voicemail systems and may report to the workforce member's department on usage and suspected misuse.

Responsibilities

The CIO or designee will review this policy annually and recommend any necessary changes to the County Manager. Department Heads shall be responsible for advising the CIO or designee of all situations that require deviation from or exception to this policy. It is also the responsibility of all County departments to ensure that their workforce members are familiar with this policy and for every workforce member to conduct their activities accordingly.

Other County Policies

The County has other policies that address specific areas of information security including policies on Internet use, email, mobile technology use, vendor/contractor access, and portable computing. Departments may have internal policies that also address these issues. These policies are cumulative and in the event of conflict, the policies providing the County with the greatest level of security shall apply.

Policy Enforcement

The CIO or designee is the policy administrator for information technology resources and will ensure this process is followed. Additionally, Division Directors, managers and Department Heads are responsible for compliance with county policy within their respective administrative areas.

Any violations of this policy shall be reported to the CIO. Violations will be investigated and may result in disciplinary action up to and including dismissal from County employment. For violations of patient confidentiality, the procedures of the Patient Confidentiality Sanctions Policy as regulated by HIPAA will apply.

Revision History

Effective Date	Changes Made
7/31/2018	Policy established
6/22/2020	Policy updated