6.0 EMAIL

6.1 PURPOSE

This policy addresses appropriate use of both Internet-provided email systems and the County's internal email systems. This policy is intended to ensure that County employees know their rights and responsibilities in using email systems, and to ensure that these systems are used in a secure, appropriate manner.

The County's official "Email Use" policy, approved by the Board of Supervisors, is provided as Attachment C of this document; in the event of conflict, this official policy takes precedence over any of the policies specified below.

6.2 DEFINITIONS

County (Internal) Email System: An email system that has been established for the sole use of County employees, and is maintained, controlled, and managed by County IT staff. Internal County email systems provide messaging services using end user email addresses linked to the County domain name structure.

Internet (External) Email System: Any email system or service that is external to the County and that is provided and supported by an Internet Service Provider or other Internet-based entity for use by the general public, such as *hotmail*. Internet email systems are not maintained, controlled or managed by County IT staff, and utilize email addressing that is not related to the County's domain name structure.

6.3 POLICIES

6.3.1 No employee, contractor or consultant shall use County-owned email systems for inappropriate purposes, such as, but not limited to the following:

- Personal profit, including commercial solicitation or conducting or pursuing their own business interests or those of another organization.
- Unlawful or illegal activities.
- Creating or disseminating harassing or demeaning statements toward any individual or group for any reason, including on the basis of sex, age, race, color, national origin, creed, disability, political beliefs, organizational affiliation, or sexual orientation as defined in Section A25-301 of the Merit System Rules, the County Policy on Sexual Harassment and any other relevant County Ordinances.
- Disseminating hoaxes, chain letters, or advertisements.
- Propagating or downloading viruses or other malicious software.

6.3.2 Each User of a County email system shall have an individual email account that is uniquely linked to that User. General-purpose email accounts, however, may be used for Departmental interaction between the

public and County employees; for example, the general email account TaxCollector@co.scl.ca.us can be used to communicate with the general public.

6.3.3 Users shall not use an internal County email account assigned to another individual to either send or receive messages.

6.3.4 Use of Internet (external) email systems from County networks and/or desktop devices is prohibited unless there is a compelling business reason for such use.

6.3.5 When used, the interface with an Internet (external) email system must be appropriately configured such that the email messages are inspected for malicious software and other potential sources of disruption or contamination. Chapter 6.0 of the IT *Security Procedures and Standards* document provides details on the approved configuration for utilizing Internet (external) email systems.

6.3.6 Users shall not configure or use automated forwarding of County email messages to Internet (external) email systems unless specifically authorized to do so, in writing, by a designated Department authority. Email messages that are forwarded manually must not contain information that has been classified as Confidential or Restricted.

6.3.7 Files or documents sent as attachments to email messages shall be governed by all procedures and standards specified by the County, based on the classification level of the data contained in the file and/or document. These same restrictions shall apply to information embedded within an email message as message text.

6.3.8 County-approved language, informing recipients how to handle the message and its contents/attachments, must be included in all email messages sent to recipients outside the County.

6.3.9 Special features designed to filter out malicious software contained in either email messages or email attachments shall be implemented on all County email systems.

6.3.10 Business-related messages on County email systems that are no longer necessary in the ordinary course of business shall be routinely deleted. Additional policies regarding the retention/deletion of email messages can be found in Section 18.0, Electronic Records Retention.

6.3.11 Users shall not delete email messages whose subject matter has been identified as relevant to pending or anticipated litigation or other legal processes. Users shall not delete any email message for the sole reason that its content is potentially embarrassing or harmful to the interests of the County or the author.

6.3.12 Departments shall formulate a policy on the use of encryption with email messages that is consistent with other County policies regarding data

privacy and confidentiality, and shall disseminate that policy to their User community.

6.3.13 Other than those mechanisms specifically authorized by a Department, the use of user-set passwords or other message locking/protection measures (such as encryption) are prohibited on County email systems.

6.3.14 Departments shall provide their Users with training on the appropriate use of both Internet and County email systems, and on handling email messages and attachments.

6.4 RESPONSIBILITIES

6.4.1 Each Department is responsible for ensuring that all employees, contractors, consultants, and vendors within its scope of authority utilize all email systems in an appropriate manner.

6.4.2 Departments are responsible for ensuring that all Users have received appropriate training in handling email messages and attachments in order to prevent the spread of email-related viruses and other forms of malicious software.

6.4.3 Individual Users are responsible for understanding and complying with all County policies, procedures, and standards related to the appropriate use of Internet and County email systems.

6.5 LIMITATIONS

6.5.1 County-provided email is intended as a business tool. However, reasonable, incidental use of County-owned email systems by employees for personal purposes is acceptable, as long as such use does not interfere with normal job functions or with the operation of the County's information systems.

6.5.2 Use of the County's email systems, as with other County systems, must withstand public scrutiny. The California Public Records Act (CPRA), Government Code Section 6250, et seq., requires the County to make all public records available for inspection and to provide copies upon request. A public record is any writing, including electronic documents, relating to the conduct of the people's business. Any information sent via email may be subject to disclosure under the CPRA or requested in the process of litigation discovery.

6.5.3 County email systems are not protected or encrypted by default, and employees should have no expectation of privacy for the content of email messages sent over County networks.

6.5.4 Users should be aware that even though an email message has been deleted from their in-box, it may still be possible to retrieve copies of the message.

6.5.5 County or Department authorization for an individual to use encryption or other measures to protect or "lock" email messages shall not constitute consent by the County or Department to maintain any such messages as private.

6.5.6 This policy does not supplant the legal protections available to shield confidential, internal County communications from third party requests, such as information exempt from disclosure under the CPRA, shielded by attorney-client privilege, or subject to state and federal law mandating confidentiality for specific subject matter.

6.6 RELATED IT SECURITY POLICIES

The following policies are related to the IT Security Policy regarding Email:

General Security Policies	-	Section 3.0
Internet Use	-	Section 5.0
Encryption	-	Section 13.0
Data Classification	-	Section 15.0
Electronic Records Retention	-	Section 18.0