5.0 INTERNET USE

5.1 PURPOSE

The purpose of this policy is to define the basic principles for both employee and Department business use of the County-owned Internet access infrastructure. The policies are intended to ensure that end users know their rights and responsibilities when using the Internet. It is also intended to ensure appropriate, cost-effective, and secure use of County-provided Internet access capabilities by County organizations.

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

5.2 DEFINITIONS

Discussion Group: An Internet service that allows users to "post" messages, opinions, or other information to a general "bulletin board," where the messages can then be viewed by other members of the group. Typically postings to a discussion group or bulletin board are archived for some period of time and can be retrieved at a later date.

Instant Messaging (IM): A popular type of application offered by many Internet service providers that allows "real-time" communication and file transfers between two or more individuals using the browser interface. The distinguishing feature of IM is that the architecture employs a centralized server managed by the Internet service provider, and this server controls communication between the participants.

Peer-to-Peer Connection (P2P): Also known as *file sharing*, P2P connections are a popular Internet application used for sharing and transferring messages and files. The distinction between IM and P2P services is that P2P does not employ a centralized server, and participants are directly connected to one another (thus "peer-to-peer"). Each "peer" in the relationship may have one or more simultaneous connections to other devices.

5.3 POLICIES

5.3.1 No Department shall implement its own connectivity to the Internet without prior written approval from the County CIO or designee.

5.3.2 Transmitting any electronic communication over the Internet that contains Confidential or Restricted information is prohibited, except under the conditions specified in the policy regarding Data Classification (Section 15.0).

5.3.3 No County employee, contractor, or consultant shall use the County's Internet infrastructure 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, including downloading licensed material without authorization or downloading copyrighted material without the publisher's permission.
- Accessing, creating, transmitting, printing, downloading or soliciting material that is or may be construed to be harassing or demeaning 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.
- Accessing, creating, transmitting, printing, downloading or soliciting sexually oriented messages or images.
- Propagating or downloading viruses or other contaminants.

5.3.4 All Department servers that are accessible from the Internet shall be protected by a security infrastructure that has been approved by the County CIO or designee.

5.3.5 County servers accessible from the Internet shall be configured and maintained so as to minimize security vulnerabilities. This includes proper patching and configuration, the installation and use of anti-virus software, and the installation and use of host-based intrusion detection systems (IDS).

5.3.6 County employees are prohibited from utilizing, participating in, or configuring Internet-based Instant Messaging (IM) services.

5.3.7 If needed to support legitimate business processes, a Department may participate in an internal, County-provided instant messaging service, if and when such a service is implemented, or a Department may implement such a service designed for use within its own local environment.

5.3.8 An IM service implemented by a Department shall not be used to communicate with IM services that are external to the County unless implemented via a security infrastructure that has been approved by the County CIO or designee.

5.3.9 County employees are prohibited from utilizing, participating in, or configuring Internet-based Peer-to-Peer or file sharing services.

5.3.10 Employees are prohibited from participating in Internet discussion groups unless there is a legitimate business need to do so, and explicit permission

to participate in such group(s) has been given, in writing, by Department management.

5.4 RESPONSIBILITIES

5.4.1 Each Department is responsible for addressing all relevant security concerns when evaluating use of the Internet to conduct Department business with other public entities, citizens, and businesses.

5.4.2 Each Department is responsible for ensuring that all employees, contractors, consultants, and vendors within its scope of authority utilize the County's Internet infrastructure appropriately.

5.5 LIMITATIONS

5.5.1 Access to the Internet is provided as a business tool. However, reasonable and incidental use of the Internet for personal purposes is acceptable, subject to specific exceptions by individual Departments, as long as this usage does not interfere with the performance of work duties or the operation of County information systems and/or networks.

5.5.2 Use of the Internet via the County's infrastructure must withstand public scrutiny. The California Public Records Act (CPRA), Government Code Section 6250, et seq., requires the County to make all disclosable 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. The CPRA stipulations apply to information processed, sent and stored on the Internet. Additionally, records of Internet use may be requested during litigation discovery.

5.5.3 Users should have no expectation of privacy in their usage of the Internet. Any messages, files, or other materials transmitted over the Internet can be monitored, stored, or disclosed to third parties.

5.5.4 Users should understand that the County monitors and logs all access to sites on the Internet that are made from County-owned IT resources. The information that is collected can be used to associate Internet activity to an individual workstation.

5.5.5 Either the County as a whole, or a Department head, may restrict access to certain Internet web sites that are deemed inappropriate and/or unnecessary for business purposes.

5.5.6 An audit authority designated by a Department head or other County authority may be given the responsibility to monitor usage of the Internet by the employees of one or more County organizations. If necessary and appropriate, an individual designated by the County Executive may audit Internet usage by an Agency or Department head.

5.5.7 This policy does not supplant legal protections intended 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.

5.6 RELATED IT SECURITY POLICIES

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

General Security Policies	-	Section 3.0
Email	-	Section 6.0
Encryption	-	Section 13.0
Data Classification	-	Section 15.0
Application Service Provider	-	Section 16.0