INFORMATION TECHNOLOGY
Electronic Communications Policy IT 2

POLICY STATEMENT

The Los Angeles County Metropolitan Transportation Authority (Metro) encourages the use of electronic communications to share information and knowledge in support of Metro’s mission. To this end, Metro supports and provides interactive electronic communications systems and services for telecommunications including but not limited to Metro’s internal and external network connections, remote access, internet, intranet, and electronic mail message (e-mail) utilized in the course of conducting official Metro business. Recognizing the convergence of technologies based on voice, video and data networks, this policy establishes an overall framework for electronic communications.

PURPOSE

Metro electronic communications systems and services are used for purposes appropriate to accomplishing Metro’s goals and mission. The purpose of this policy is to ensure timely availability of services while minimizing or preventing security breaches and to instruct users of their responsibilities and boundaries for the use of Metro’s Electronic Communications systems and/or services as set forth within this policy.

APPLICATION

This policy applies to all persons engaged in business by Metro. It is the responsibility of all persons engaged with Metro, whether employee, consultant, temporary worker, contractor, vendor, affiliate or any other entity engaged in Metro business, who access or use Metro electronic communications systems and/or services (except resources made available for public access) to comply with the Electronic Communication Policy and to participate in the protection and control of these resources and capabilities.

CFO: Richard D. Brumbaugh
APPROVED: Legal Counsel or N/A
ADOPTED: CEO
Effective Date: 8/19/2005
1. STANDARDS

Metro shall implement electronic communications systems and services and conduct information processing operations in a manner that assures availability, integrity, confidentiality and recoverability, and the protection, safety and welfare of its employees.

1.1 Privacy and Ownership

1.1.1 Metro electronic communications systems and services, include and incorporate telecommunication services, desktop personal computers, mainframes, servers, portable devices and/or all related equipment, network and network devices, specifically including and relating to internet, intranet and electronic mail, are provided only for authorized Metro use.

1.1.2 Use of electronic communications systems and services are not for personal gain of any individual in accordance to Metro’s Employee Code of Conduct.

1.1.3 Unauthorized use of Metro electronic communications systems and/or services is prohibited.

1.1.4 Every authorized or unauthorized user shall have no explicit or implicit expectation of privacy when connected to Metro’s systems and services, regardless of whether they are working at a Metro facility, telecommuting from home or through a remote Internet connection to Metro’s system.

1.1.5 An employee’s work product is not personal property.

1.1.6 Any and all use of Metro’s systems, services and all files prepared, entered into, maintained or saved within Metro’s systems may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed by Metro authorized personnel.

1.1.7 Back-up copies of electronic files may be referenced for business, security and legal purposes.

1.1.8 Metro authorized personnel who monitor systems and services may not divulge any information observed to any person(s), except for legitimate business reasons.
1.2 Assignment of Accountability

1.2.1 Misrepresenting, obscuring, suppressing, or replacing a user's identity on the Internet or any Metro electronic communications system or services is prohibited.

1.2.2 User name, electronic mail address, organizational affiliation, and related information included messages or postings must reflect the actual originator of the messages or postings.

1.2.3 Each user is responsible for the content of all text, audio, programs or images that they place, retrieve or send over Metro electronic communication systems or services.

1.2.4 Users may not send e-mail or other electronic communications which hides the identity of the sender or represents the sender as someone else or someone from another company.

1.2.5 Users will not knowingly share their electronic identification (ID) and individual passwords with anyone else besides the authorized user. If an authorized user shares his/her password with an unauthorized user, the authorized user is responsible for the actions and use of Metro systems and services by the unauthorized user. For group password users, each individual group member is responsible for his/her actions and use of Metro systems and services.

1.2.6 Metro management/supervisory personnel may direct an employee to use the manager’s or supervisor’s identity to transact Metro business for which a manager or supervisor is responsible. In such cases, the manager or supervisor retains all responsibility and liability for the use of electronic identity at all times.

1.3 Compliance

Metro shall ensure compliance with all:

1.3.1 Contractual obligations or license agreements;
1.3.2 Regulatory requirements;
1.3.3 Applicable laws, with special regard for laws pertaining to computer related crime, protection of copyrighted or proprietary computer resources, and restricted technologies; and
1.3.4 Information Security policies and procedures.

1.4 Controls and Conduct

1.4.1 Access to Metro electronic communications systems and/or services is granted only for the purpose of conducting Metro business.

1.4.2 The Information Technology Services (ITS) Department procures, maintains and manages the electronic communications systems and services as required by Metro business units.

1.4.3 Access to Metro electronic communications systems and/or services shall be based on least privileged access, which requires written justification and approval from the requestor’s Department or Division Manager.

1.4.4 Access to any Metro electronic communications systems and/or services is based upon least privileged access, that is, an employee’s need to have access for performing business-related duties.

1.4.5 Access to and use of Metro electronic communications systems and/or services may be wholly or partially restricted or rescinded by Metro without prior notice and without the consent of the electronic communications user.

1.4.6 Proper use of Metro electronic communications systems and/or services include exchange of information that supports Metro’s mission, goals, objectives, job-related professional development for Metro management and staff, and communications intended to maintain job currency or gain additional knowledge that is directly or indirectly related to job functions.

1.4.7 Metro provides, through its connections, access to the Internet, access to other computer systems around the world. Users should understand that Metro does not have control of the content of information residing on these other systems. On a global network it is impossible to control the content of data and an industrious user may discover controversial material. Users are advised that some systems may contain defamatory, inaccurate, abusive, obscene, profane, sexually-oriented, threatening, racially offensive, or illegal material. Metro does not condone the use of such materials and does not permit usage of such materials.

1.4.8 Access to communications systems and/or services must be through Metro electronic communications systems and/or services; no other systems and/or service providers are permitted.
1.4.9 Users shall exercise caution when forwarding messages as some information is intended for specific individuals and may not be appropriate for general distribution and/or electronic communications.

1.4.10 Electronic communications records (as in e-mail messages) and Electronic communications tape backups will be retained in accordance with Metro's Records Retention Policy.

1.5 Prohibitions

Users of electronic communications systems and/or services shall not:

1.5.1 Participate in or contribute to any fraudulent, harassing, threatening, discriminatory, sexually explicit or obscene messages and/or materials;

1.5.2 "Spam," that is, exploit electronic communications systems and/or services for purposes beyond their intended scope to amplify the widespread distribution of unsolicited electronic communications;

1.5.3 "Letter-bomb," that is, send an extremely large message or send multiple electronic communications to one or more recipients to interfere with the recipients' use of electronic communications systems and/or services;

1.5.4 Intentionally engage in other practices such as "denial of service attacks" that impede the availability of electronic communications systems and/or services;

1.5.5 Breach, attempt to breach, tamper or disable any security mechanisms used by Metro to protect electronic communications systems and/or services, or any records or messages associated with these systems and/or services;

1.5.6 Publicly disclose internal Metro information via the electronic communications system or services that may adversely affect Metro's customer relations, or public image unless written approval of the Chief Communications Officer or Chief Executive Officer (CEO) has first been obtained;

1.5.7 Alter a message or attachment belonging to another user without the permission of the originator;

1.5.8 Download or install unlicensed and unauthorized software or applications onto Metro systems;
1.5.9 Utilize Metro resources to duplicate copyrighted materials without permission from the originator or creator;
1.5.10 Utilize Metro resources to store unauthorized copyrighted materials; and
1.5.11 Use Metro electronic communications systems and services for personal, illegal or unauthorized business.

1.6 Malicious Software (Malware) Protection

1.6.1 To reduce the impact of threats from malware such as viruses, “Trojan horses” or worms, the ITS Department shall install and maintain the consistent use of state-of-the-art anti-virus software to provide uniform protection throughout Metro’s networks, file servers, application servers, and workstations.

1.6.2 All systems internal and external to Metro including but are not limited to desktop personal computers, workstations, servers and portable devices that contain or support Metro’s information resources and/or information processing capabilities shall contain ITS approved state-of-the-art anti-virus software that is active, current and in good working order at all times.

1.6.3 To prevent destructive programs and codes that can destroy or modify Metro’s computer systems, servers, software, and data stored on them, all files (databases, software object code, spreadsheets, formatted word processing package files, etc.) will be screened with virus protection software prior to being used.

1.6.4 Users shall exercise caution when opening any electronically forwarded message or file. Users shall not open suspicious messages or files from familiar or unfamiliar senders or sites from which information is extracted and shall immediately delete such messages.

1.6.5 Users shall report any suspicions of virus infected e-mails, attachments, software, diskette, CD-ROM, operating systems or other technology, to the ITS Department.

1.7 Exceptions

Based on a written request stating technical necessities or a practical need to incorporate alternative measures, the Chief Information Officer (CIO) up to, and
including the CEO may authorize exceptions to this policy and any supplementary documents. All requests will be filed and retained with the CIO.

1.8 Violation of Policy & Discipline

1.8.1 Any deviation, subversion, non-compliance or violation by any individual or entity from the basic principles of the provisions of the specific elements of this policy or any supplementary policies, procedures and standards constitutes a violation of Metro’s Electronic Communications Policy.

1.8.2 Any violation of this policy, including but not limited to violations due to gross negligence or willful actions or omissions, shall be addressed with an appropriate response, and could lead to disciplinary action, up to and including termination of employment, contractual recourse with vendors, consultants, and any other entity under contractual agreement; and civil and/or criminal prosecution, as applicable to the violator.

1.9 Enforcement

1.9.1 Should any provision be ruled invalid or illegal, the remaining provisions shall stand on their own merit and shall be considered unaffected and fully enforceable.

1.9.2 The provisions of this policy shall not be affected by any delay, previous failure or previous ineffectiveness in enforcement of that provision or any other provision of this policy.

1.10 Amendments

Amendments to this policy and any supplementary policies, procedures, standards, and mandates require the approval of the CIO up to, and including the CEO.

2 DEFINITION OF TERMS

2.1 Electronic Communications: Any communication that is broadcast, created, sent, forwarded, replied to, transmitted, stored, held, copied, downloaded, displayed, viewed, 

Metro
read, or printed by one or several electronic communications systems or services. For purposes of this policy, an electronic file that has not been transmitted is not an electronic communication.

2.2 **Electronic Communications Records:** Electronic transmissions or messages created, sent, forwarded, replied to, transmitted, distributed, broadcast, stored, held, copied, downloaded, displayed, viewed, read, or printed by one or several electronic communication systems or services. This definition of electronic communications records applies equally to the contents of such records, attachments to such records, and transactional information associated with such records.

2.3 **Electronic Communications Resources:** Any combination of telecommunications equipment, transmission devices, electronic video and audio equipment, encoding or decoding equipment, computers and computer time, data processing or storage systems, computer systems, servers, networks, input/output and connecting devices, and related computer records, programs, software, and documentation that supports electronic communications services.

2.4 **Electronic Communications Systems and Services:** Any messaging, collaboration, publishing, broadcast, or distribution system that depends on electronic communications resources to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, or print electronic records for purposes of communication across electronic communications network systems between or among individuals or groups, that is either explicitly denoted as a system for electronic communications or is implicitly used for such purposes.

2.5 **Least privileged access:** Issuing only the level of security needed in performing a task. For example, if read access is required then only the level of security allowing read access is issued. If access to a resource is required then only access to this resource is allowed. If a person is requiring security clearance then only this person is issued clearance.

2.6 **Malware:** Malicious software designed specifically to damage, disrupt, corrupt or disclose systems, software or information, such as viruses, "Trojan horses," or worms.

2.7 **Metro Electronic Communications Systems and Services:** Electronic communications systems and services owned or operated by Metro or provided through contracts with Metro.

2.8 **Security Breach:** Activities or events resulting in the disclosure of information to unauthorized individuals or resulting in unauthorized modification or destruction of
system data, loss of computer system processing capability, or loss or theft of any computer system resource.

2.9 **Security Incident**: Any occurrence or circumstance presenting a potential threat or impact to security as a result of intentional or unintentional actions including but not limited to: unauthorized attempts to gain access to information or systems, introduction of malicious codes or viruses, loss or theft of computer media, or the failure of the security function to perform as designed.

2.10 **Software**: All or part of the program, procedures, rules, and associated documentation of a data processing system. System software is the operating system that controls the basic functioning capabilities of the computer and database management system, network software enables multiple computers to communicate with one another, language software is used to develop programs, and application software is any program that processes data for the user.

2.11 **Use of Electronic Communications Systems or Services**: To create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, or print electronic communications with the aid of electronic communications services. An electronic communications user is an individual who makes use of electronic communications services.

3 **RESPONSIBILITIES**

3.1 **ITS Department**

3.1.1 ITS maintains technology and services, including network systems, programs, Internet, electronic mail message system (e-mail) to allow Metro employees and persons authorized to use such services for Metro business at or outside Metro facilities within the network infrastructure.

3.1.2 ITS will provide system integrity, confidentiality and availability through security and sound professional practices.

3.1.3 ITS will provide reliable recoverability by performing regular backups and testing of electronic communications records, data, application programs, and systems under their jurisdiction.

3.1.4 ITS will implement and employ cost-effective audit technologies and practices to help identify security violators and speed up recovery from security violations.
3.1.5 To ensure policy compliance, ITS administrators on a regular basis will perform security, user activity and usage audits.

3.1.6 The ITS Department is responsible for trouble-shooting virus and technology situations as part of maintaining system integrity.

3.2 Chief Information Officer

The Chief Information Officer (CIO) is responsible for coordination and implementation of information security measures and ensuring that the organization is in compliance with policy, legislative and contractual requirements regarding Electronic Communications.

3.3 Metro Department Heads

3.3.1 Department heads are responsible for implementing measures and maintaining practices/procedures in compliance with all provisions of Metro’s Electronic Communications Policy.

3.3.2 Department heads are responsible for safeguarding and protecting classified data and/or information, copyrighted and/or licensed resources and restricted technologies from unauthorized or accidental disclosure.

3.4 Metro Supervisory and Management Personnel

3.4.1 Supervisors and managers shall ensure that all personnel within their business unit either are provided or made aware of the Metro Electronic Communications Policy.

3.4.2 Management is responsible for protecting resources and personnel falling within the scope of this policy from all reasonably avoidable and unauthorized access, use, disclosure, transfer, alteration, modification, contamination, disruption, restriction, sabotage, damage, injury, loss or destruction.

3.4.3 If management personnel becomes aware of a security risk, they are responsible to report it to the ITS Help Desk and take appropriate measures to halt the risk until it can be mitigated or eliminated.
3.5 Employees, Consultants, Temporary Workers, Contractors, Vendors, Affiliates, Etc.

3.5.1 Employees, consultants, temporary workers, contractors, vendors, affiliates or any other entity engaged in Metro business (referenced as employees and authorized Metro users), who access or use Metro information processing resources (except resources made available for public access), shall be responsible for complying with Metro’s Electronic Communications Policy and participating in the protection and control of resources and capabilities.

3.5.2 Employees and authorized Metro users must report any security breach, either internal or external, to the CIO.

3.5.3 Employees and authorized Metro users shall be responsible for reading, understanding and complying with the provisions of Metro’s Electronic Communications Policy, procedures, standards, measures or mandates.

3.5.4 Employees and authorized Metro users shall understand that Metro’s information resources and information processing capabilities are critical to its operations and service to its customers, and that protection and control of these resources and capabilities is the responsibility of all Metro employees, consultants, temporary workers, contractors, vendors, affiliates or any other entity engaged in Metro business (as reasonable and appropriate within the scope of their duties and expertise).

3.5.5 Employees and authorized Metro users shall understand that access to and usage of Metro’s computers and associated resources is restricted to users specifically authorized by Metro and to Metro business only.

3.5.6 Employees and authorized Metro users shall understand that the contents of all Metro computers and associated resources as well as activities associated with any such resources are subject to (as applicable) audit, inspection, examination, or seizure by authorized Metro security at any time and without notice.

3.5.7 Employees and authorized Metro users shall not be entitled to any expectation of privacy with regard to these computers, resources or associated activities and workspaces, including, but not limited to the contents of desks, cabinets, files, electronic mail, voice mail or messages, electronic notepads or information storage devices, facsimile (FAX) machines and FAX transmissions, data photographic film, microfilm, optical storage devices, photocopy machines and
output, printers and communications equipment and data transmissions, video conferencing transmissions, telephone utilization logs, documentation in any form and the following computer-related items; data media storage containers, data media, data, programs, utilities, applications, software, firmware, operating systems, processes, commands, messages, queues, logs and output (no information or processing activities in Metro's environment is beyond Metro's purview).

3.5.8 Employees and authorized Metro users shall be personally accountable for all activities conducted through the use of any computer or associated resource access, user identification, password, access code, access device or access media that is personally used or is assigned.

3.5.9 Employees and authorized Metro users shall understand it is not permitted to disclose any Metro information that is accessed as a consequence of employment capacity or from access to or usage of Metro computers or associated resources, except as necessary within the scope and course of assigned duties or unless specifically authorized to do so by Metro.

3.5.10 Employees and authorized Metro users shall understand that they are expected to handle all Metro data, information resources and documents in a manner consistent with their position, responsibilities and duties, and shall handle data according to its intended purpose; and while public documents are available in accordance with the Records Management Program, any Metro information resources marked "INTERNAL USE ONLY" are for use only within the Metro organization, and those marked "CONFIDENTIAL" are for use only as specifically authorized.

3.5.11 This restriction includes information that is not secured and/or is generally available to the public, with the understanding that all information disclosures are to be made only through channels and procedures authorized by Metro.

3.6 User

A "user" is identified as an employee, consultant, temporary worker, contractor, vendor, affiliate or any other entity engaged in Metro business, who accesses or uses Metro information processing resources.
4.0  FLOWCHART

Not Applicable

5.0  REFERENCES

GEN 8     Records Management Policy
EO 1-3    Harassment Policy
          Employee Code of Conduct
          Information Security Procedures

6.0  ATTACHMENTS

Not Applicable

7.0  PROCEDURE HISTORY

8/19/05    New Policy