AGREEMENT FOR SERVICES #273-S0811

THIS AGREEMENT made and entered by and between the County of El Dorado, a political subdivision of the State of California (hereinafter referred to as "County") and Daystar Computer Systems, Inc., an Illinois Corporation, duly qualified to conduct business in the State of California, whose principal place of business is 600 Jackson Boulevard, Chicago, IL 60661 and whose Agent for Service of Process is Corporate Creations Network, Inc., 131A Stony Circle, #500, Santa Rosa, CA; (hereinafter referred to as "Consultant");

WITNESSETH

WHEREAS, County has determined that it has a need for, and Consultant agrees to grant to County, a Legistar integrated agenda workflow system specifically capable of the generation and maintenance of agenda documentation for use by the Board of Supervisors, various County departments, commissions, committees, and the public within El Dorado County; and

WHEREAS, Consultant has represented to County that it is specially trained, experienced, expert and competent to perform the special services required hereunder and County has determined to rely upon such representations; and

WHEREAS, Consultant warrants and represents that the program identified herein will serve the intended and functional purpose for El Dorado County; and

WHEREAS, it is the intent of the parties hereto that such services be in conformity with all applicable federal, state and local laws; and

WHEREAS, County has determined that the provision of these services provided by Consultant is in the public's best interest, and that these services are more economically and feasibly performed by outside independent consultants as well as authorized by El Dorado County Charter, Section 210 (b) (6) and/or Government Code 31000;

NOW, THEREFORE, County and Consultant mutually agree as follows:

ARTICLE I
Scope of Services:

A. Software License

1. Consultant grants and County accepts a perpetual, nonexclusive and non-transferable license to use the Consultant's application (the "Software"), described as Legistar.

2. The Software referred to hereinabove is intended to be used for the general purposes of providing a customized, comprehensive, agenda workflow management and information retrieval system designed specifically to support the legislative process. The function of the Software includes, but is not limited to, the following purposes: information storage and indexing; scanned images and attachments; automatic agenda creation; automatic minutes; legislative tracking; information retrieval, public access web interface suite; and legislative reports.

3. The County is permitted one installation of the server data base portion of the Software and one secondary installation for testing. The License also permits an unlimited number of concurrent County workstation or internet connections to the Software, although County's use may be further governed by the performance or license limitations from third party providers of components of its network, data base, and hardware environment.

4. The Software or portions thereof, shall be used by County only on County's own computer equipment and only for the processing of County's own business.

   County shall not use the Software in the operation of a service bureau or in any other manner that would permit or allow the use of the Software, or any portion thereof, in connection with transactions in which County is not involved. County shall under no circumstances assign, sublicense, or otherwise transfer the License to any other entity.

   County shall at all times limit the use of the Software to its employees who have been appropriately trained.

   The Software is being provided to County in executable object code form only. County agrees not to modify, translate, decompile, nor create or attempt to create, by reverse engineering or otherwise, the source code from the object code of the Software, nor adapt the Software in any way to create a derivative work.

5. The County includes the right to make two security backup copies of the Software provided that (a) reasonable security precautions are taken to prevent the unauthorized copying or disclosure of the Software or any part hereof, and (b) that at all times Consultant's ownership of the Software is disclosed by prominent display of Consultant propriety and copyright notices.

6. Consultant represents that it is the owner of the Software and that it has the right to modify and to grant the right to use of the Software to County. All modifications, changes, enhancements, conversions, upgrades, or additions made to the Software and all related documentation, whether made by Consultant, County, or a third party, under this or any other Agreement, are and shall be the sole and exclusive property of Consultant, including all applicable rights to patents, copyrights, trademarks and trade secrets inherent therein, shall be considered a part of the Software, and shall be included in the license hereby granted to the County.

7. Both Consultant and County acknowledge and agree that successful operation of the Software in the County's environment shall require their full and mutual good faith cooperation, including, without limitation, the fulfillment of the obligations set forth in this Agreement.

8. In addition to providing Consultant with full, good faith cooperation and such information as may be required by Consultant in order to customize and execute the Software, County shall (a) appoint one or two employees of County who shall have sufficient computer systems experience and organizational authority to act as coordinator of all County activities in connection with the operation of the Software, and to supervise all tasks undertaken by County in connection with the modification, preparation, installation, use and support of the Software; (b) install and test all new revisions and updates of Software within thirty (30) days of receipt from Consultant, if circumstances warrant County may request a time extension that is mutually agreed upon by both parties; (c) provide written statements or descriptions of any Software problems at Consultant's request and perform any Software tests requested by Consultant support personnel who may be investigating any reported problems; (d) provide Consultant with suitable scratch media and supplies, which media will be returned upon request, to investigate reported problems; and (e) provide Consultant with the ability to remotely login to the Software using Internet Virtual Private Network (VPN), T1, DSL access or a phone modem at a communication rate of no less than 56 kbps.

9. County shall not sell, transfer, publish, disclose, display or otherwise make available to others any source code, or object code relating to the Software.

   County shall use its best efforts to assist Consultant in identifying and preventing any unauthorized use or disclosure of the source code or object code of the Software or of any portion of the Software, or any of the algorithms or logic contained therein. Without limitation of the foregoing, County shall advise Consultant immediately in the event that County learns or has reason to believe that any person who has had access to the Software, or any portion thereof, has violated or intends to violate the terms of this Agreement; and the County will cooperate with Consultant in seeking injunctive or other equitable relief in the name of the County or Consultant against any such person.

   County acknowledges that the Software contains proprietary trade secrets of Consultant and hereby agrees to maintain the confidentiality of the Software in a manner using at least the same degree of care and security as the manner used to maintain the confidentiality of County's own most confidential information.

Consultant acknowledges that in the course of implementing the Software for County it will necessarily be supplied with confidential or proprietary information of County concerning its business affairs, property, methods of operation, processing systems, or other information. Consultant hereby agrees to maintain the confidentiality of any such information which is clearly marked or labeled as confidential and to treat such information with the same degree of care and security as Consultant treats its own most confidential information.

All of the undertakings and obligations relating to confidentiality and non-disclosure, whether contained in this paragraph or elsewhere in this Agreement, and whether of Consultant or of the County, shall survive the termination of this Agreement for any reason.

Nothing in this paragraph shall prevent the operation of any law requiring that contracts with the County, and any other public records, be open to public inspection.

10. County shall, in addition to any license fee required hereunder, pay all applicable sales, use, transfer and other taxes and fees, whether federal, state or local, however designated, which are levied or imposed by reason of the transaction contemplated hereby; excluding, however Federal and Illinois State income taxes on profits which may be levied against Consultant. County agrees to reimburse Consultant for the amount of all such taxes and fees paid or accrued by Consultant as a result of this transaction.

11. Following Consultant's receipt of payment for services provided, County shall receive a Certificate of Escrow which entitles County to claim a copy of the Legistar Software Source Code per the terms and conditions set forth in Article IX E.

B. Software Maintenance

1. Consultant offers to County and County hereby accepts the following provisions for the maintenance and support of Software.

2. This Agreement includes the following support services provided at no additional cost to County:

   Classification (A) Unlimited Services:

   a. Investigation and correction of any software problems reported by County or discovered by Consultant;
   b. In house application maintenance including duplicate customized system upkeep;
   c. Interim version updates as they are made available;
   d. Technical assistance on the use and maintenance of the software.

The County may report any Classification (A) service requests to Consultant via email at support@daystarnet.com, fax transmittal to (312) 896-5052, voice at (312) 559-0900, or such other phone numbers or email addresses as Consultant might provide.

Unless special arrangements are made, Consultant shall provide software support by phone during its regular business hours (7 AM to 7 PM Central Time) Monday through Friday, except for holidays. When deemed necessary by Consultant or requested by County, Daystar will make arrangements to provide face-to-face support services either on County's site or at Consultant's offices. Consultant will respond to telephone inquiries within two (2) business hours.

During the course of this Agreement, Consultant will provide copies of any updates or new feature releases of the Software at no cost to the County other than the costs of installation.

3. County's Obligations:

As conditions to receiving support under this Agreement, County agrees to:

a. Load and test all new revisions and updates of Consultant Software within thirty (30) days of receipt by County; if circumstances warrant County may request a time extension that is mutually agreed upon by both parties;
b. Perform any Software tests requested by Consultant support personnel who may be investigating any reported problems;
c. Provide written statements or descriptions of Software problems at Consultant's request;
d. Provide Consultant with suitable scratch media and supplies to investigate reported problems, these will be returned upon request;
e. Consult with Consultant prior to installing any Operating system patches, updates or service packets that may be applied to the Legistar server for assurance that they have passed out certification testing for compatibility;
f. Provide Consultant with the ability to remotely login to the system running the Daystar software using Internet Virtual Private Network (VPN), T1, DSL or dial-up modem accèss.

4. Remote Connectivity:

All installation, problem diagnosis, upgrades, and remote system administration support services specified in this Agreement will be delivered via remote electronic connection to the County's Legistar Server, in accordance with Exhibit "A", marked "El Dorado County Computer and Network Resource Usage Policies and Standards Guide", Section 3, Remote Access Policy, incorporated herein and made by reference a part hereof.

Internet or modem dial-up: County is responsible for purchase, installation and ongoing maintenance of any hardware or local communications services required. This includes internet access, ISP services, modem and phone line. All installation, troubleshooting, updates, remote system administration, and any other support services specified in this Agreement will be delivered via remote electronic connection to the County's Legistar Server.

Remote connection software will be the choice of the County's Information

Technologies Department. On-going acceptance or use of a particular communications software program or protocol is subject to change by either party.

In the event that the County specified any software or communications methodology that incurs any cost to Consultant, all work and costs will be provided on a time and materials basis and payable by the County.

In the event that Consultant and the County are unable to mutually agree on an acceptable remote communications protocol, Support Services under this Agreement will be restricted to those that can be provided via voice phone or email support.

ARTICLE II

Term: This Agreement is effective October 1, 2007 and shall renew annually unless terminated in accordance with **ARTICLE IX**.

ARTICLE III

Compensation for Services: For services and all deliverables provided herein, County agrees to pay Consultant annually in advance and within thirty (30) days following County's receipt and approval of itemized invoice(s). Payment for all included support shall be one annual payment of $10,420 due and payable thirty (30) days following the first day of the effective period as stated in **ARTICLE II** above. County and Consultant Agree that after the initial one (1) year period of this Agreement, the annual compensation for services to be provided upon renewal may increase by no more than five (5) percent annually. The total amount of this Agreement shall not exceed $10,420.00 for the first annual period and an amount less than or equal to the previous annual payment plus a five (5) percent increase for each subsequent year.

ARTICLE IV

Changes to Agreement: This Agreement may be amended by mutual consent of the parties hereto. Said amendments shall become effective only when in writing and fully executed by duly authorized officers of the parties hereto.

ARTICLE V

Consultant to County: It is understood that the services provided under this Agreement shall be prepared in and with cooperation from County and its staff. It is further agreed that in all matters pertaining to this Agreement, Consultant shall act as Consultant only to County and shall not act as Consultant to any other individual or entity affected by this Agreement nor provide information in any manner to any party outside of this Agreement that would conflict with Consultant's responsibilities to County during term hereof.

ARTICLE VI

Assignment and Delegation: Consultant is engaged by County for its unique qualifications and skills as well as those of its personnel. Consultant shall not subcontract, delegate or assign services to be provided, in whole or in part, to any other person or entity without prior written consent of County.

ARTICLE VII

Independent Consultant/Liability: Consultant is, and shall be at all times, deemed independent and shall be wholly responsible for the manner in which it performs services required by terms of this Agreement. Consultant exclusively assumes responsibility for acts of its employees, associates, and subcontractors, if any are authorized herein, as they relate to services to be provided under this Agreement during the course and scope of their employment.

Consultant shall be responsible for performing the work under this Agreement in a safe, professional, skillful and workmanlike manner and shall be liable for its own negligence and negligent acts of its employees. County shall have no right of control over the manner in which work is to be done and shall, therefore, not be charged with responsibility of preventing risk to Consultant or its employees.

ARTICLE VIII

Fiscal Considerations: The parties to this Agreement recognize and acknowledge that County is a political subdivision of the State of California. As such, El Dorado County is subject to the provisions of Article XVI, Section 18 of the California Constitution and other similar fiscal and procurement laws and regulations and may not expend funds for products, equipment or services not budgeted in a given fiscal year. It is further understood that in the normal course of County business, County will adopt a proposed budget prior to a given fiscal year, but that the final adoption of a budget does not occur until after the beginning of the fiscal year.

Notwithstanding any other provision of this Agreement to the contrary, County shall give notice of cancellation of this Agreement in the event of adoption of a proposed budget that does not provide for funds for the services, products or equipment subject herein. Such notice shall become effective upon the adoption of a final budget which does not provide funding for this Agreement. Upon the effective date of such notice, this Agreement shall be automatically terminated and County released from any further liability hereunder.

In addition to the above, should the Board of Supervisors during the course of a given year for financial reasons reduce, or order a reduction, in the budget for any County department for which services were contracted to be performed, pursuant to this paragraph in the sole discretion of the County, this Agreement may be deemed to be canceled in its entirety subject to payment for services performed prior to cancellation.

ARTICLE IX
Default, Termination, and Cancellation:

A. Default: Upon the occurrence of any default of the provisions of this Agreement, a party shall give written notice of said default to the party in default (notice). If the party in default does not cure the default within ten (10) days of the date of notice (time to cure), then such party shall be in default. The time to cure may be extended at the discretion of the party giving notice. Any extension of time to cure must be in writing, prepared by the party in default for signature by the party giving notice and must specify the reason(s) for the extension and the date on which the extension of time to cure expires.

Notice given under this section shall specify the alleged default and the applicable Agreement provision and shall demand that the party in default perform the provisions of this Agreement within the applicable period of time. No such notice shall be deemed a termination of this Agreement unless the party giving notice so elects in this notice, or the party giving notice so elects in a subsequent written notice after the time to cure has expired.

B. Bankruptcy: This Agreement, at the option of the County, shall be terminable in the case of bankruptcy, voluntary or involuntary, or insolvency of Consultant.

C. Ceasing Performance: County may terminate this Agreement in the event Consultant ceases to operate as a business, or otherwise becomes unable to substantially perform any term or condition of this Agreement.

D. Termination or Cancellation without Cause: County may terminate this Agreement in whole or in part seven (7) calendar days upon written notice by County for any reason. If such prior termination is effected, County will pay for satisfactory services rendered prior to the effective dates as set forth in the Notice of Termination provided to Consultant, and for such other services, which County may agree to in writing as necessary for contract resolution. In no event, however, shall County be obligated to pay more than the total amount of the contract. Upon receipt of a Notice of Termination, Consultant shall promptly discontinue all services affected, as of the effective date of termination set forth in such Notice of Termination, unless the notice directs otherwise. In the event of termination for default, County reserves the right to take over and complete the work by contract or by any other means.

E. In the event Consultant files bankruptcy, or ceases performance as described in items B. or C. above, County shall have the right to receive the contents of the source code escrow account as provided for in Article I herein, for the purpose of fulfilling Consultant's obligations under this Agreement.

ARTICLE X
Notice to Parties: All notices to be given by the parties hereto shall be in writing and served by depositing same in the United States Post Office, postage prepaid and return receipt requested.

Notices to County shall be addressed as follows:

COUNTY OF EL DORADO
CHIEF ADMINISTRATIVE OFFICE
330 FAIR LANE
PLACERVILLE, CA 95667
ATTN: KELLY WEBB, PRINCIPAL ADMINISTRATIVE ANALYST

or to such other location as the County directs.

Notices to Consultant shall be addressed as follows:

DAYSTAR COMPUTER SYSTEMS, INC.
600 W. JACKSON BLVD., SUITE 580
CHICAGO, IL 60661
ATTN: JOHN CICHON, GENERAL MANAGER

or to such other location as the Consultant directs.

ARTICLE XI

Indemnity: The Consultant shall defend, indemnify, and hold the County harmless against and from any and all claims, suits, losses, damages and liability for damages of every name, kind and description, including attorneys fees and costs incurred, brought for, or on account of, injuries to or death of any person, including but not limited to workers, County employees, and the public, or damage to property, or any economic or consequential losses, which are claimed to or in any way arise out of or are connected with the Consultant's services, operations, or performance hereunder, regardless of the existence or degree of fault or negligence on the part of the County, the Consultant, subcontractor(s) and employee(s) of any of these, except for the sole, or active negligence of the County, its officers and employees, or as expressly prescribed by statute. This duty of Consultant to indemnify and save County harmless includes the duties to defend set forth in California Civil Code Section 2778.

ARTICLE XII

Insurance: Consultant shall provide proof of a policy of insurance satisfactory to the El Dorado County Risk Manager and documentation evidencing that Consultant maintains insurance that meets the following requirements:

A. Full Workers' Compensation and Employers' Liability Insurance covering all employees of Consultant as required by law in the State of California.

B. Commercial General Liability Insurance of not less than $1,000,000.00 combined single limit per occurrence for bodily injury and property damage.

C. Automobile Liability Insurance of not less than $500,000.00 is required in the event motor vehicles are used by the Consultant in the performance of the Agreement.

D. In the event Consultant is a licensed professional, and is performing professional services under this Agreement, professional liability (for example, malpractice insurance) is required with a limit of liability of not less than $1,000,000.00 per occurrence.

E. Consultant shall furnish a certificate of insurance satisfactory to the El Dorado County Risk Manager as evidence that the insurance required above is being maintained.

F. The insurance will be issued by an insurance company acceptable to the Risk Management Division, or be provided through partial or total self-insurance likewise acceptable to the Risk Management Division.

G. Consultant agrees that the insurance required above shall be in effect at all times during the term of this Agreement. In the event said insurance coverage expires at any time or times during the term of this Agreement, Consultant agrees to provide at least thirty (30) days prior to said expiration date, a new certificate of insurance evidencing insurance coverage as provided for herein for not less than the remainder of the term of the Agreement, or for a period of not less than one (1) year. New certificates of insurance are subject to the approval of the Risk Management Division and Consultant agrees that no work or services shall be performed prior to the giving of such approval. In the event the Consultant fails to keep in effect at all times insurance coverage as herein provided, County may, in addition to any other remedies it may have, terminate this Agreement upon the occurrence of such event.

H. The certificate of insurance must include the following provisions stating that:

1. The insurer will not cancel the insured's coverage without thirty (30) days prior written notice to County, and;

2. The County of El Dorado, its officers, officials, employees, and volunteers are included as additional insured, but only insofar as the operations under this Agreement are concerned. This provision shall apply to all liability policies except workers' compensation and professional liability insurance policies.

I. The Consultant's insurance coverage shall be primary insurance as respects the County, its officers, officials, employees and volunteers. Any insurance or self-insurance maintained by the County, its officers, officials, employees or volunteers shall be excess of the Consultant's insurance and shall not contribute with it.

J. Any deductibles or self-insured retentions must be declared to and approved by the County, either: the insurer shall reduce or eliminate such deductibles or self-insured retentions as respects the County, its officers, officials, employees, and volunteers; or the Consultant shall procure a bond guaranteeing payment of losses and related investigations, claim administration and defense expenses.

K. Any failure to comply with the reporting provisions of the policies shall not affect coverage provided to the County, its officers, officials, employees or volunteers.

L. The insurance companies shall have no recourse against the County of El Dorado, its officers and employees or any of them for payment of any premiums or assessments under any policy issued by any insurance company.

M. Consultant's obligations shall not be limited by the foregoing insurance requirements and shall survive expiration of this Agreement.

N. In the event Consultant cannot provide an occurrence policy, Consultant shall provide insurance covering claims made as a result of performance of this Agreement for not less than three (3) years following completion of performance of this Agreement.

O. Certificate of insurance shall meet such additional standards as may be determined by the contracting County Department either independently or in consultation with the Risk Management Division, as essential for the protection of the County.

ARTICLE XIII
Interest of Public Official: No official or employee of County who exercises any functions or responsibilities in review or approval of services to be provided by Consultant under this Agreement shall participate in or attempt to influence any decision relating to this Agreement which affects personal interest or interest of any corporation, partnership, or association in which he/she is directly or indirectly interested; nor shall any such official or employee of County have any interest, direct or indirect, in this Agreement or the proceeds thereof.

ARTICLE XIV
Interest of Consultant: Consultant covenants that Consultant presently has no personal interest or financial interest, and shall not acquire same in any manner or degree in either: 1) any other contract connected with or directly affected by the services to be performed by this Agreement; or, 2) any other entities connected with or directly affected by the services to be performed by this Agreement. Consultant further covenants that in the performance of this Agreement no person having any such interest shall be employed by Consultant.

/

/

/

/

/

/

ARTICLE XV

Nonresident Withholding (Form 588): All independent Consultants providing services to the County who are not California residents must file a State of California Form 588 certifying County's exemption from withholding where applicable; where not applicable, Consultant will indemnify and hold the County harmless for any action taken by the California Franchise Tax Board. The Consultant will be required to submit a Form 588 prior to execution of an Agreement or County shall withhold seven (7%) percent of each payment made to the Consultant during term of the Agreement where applicable. This requirement applies to any agreement/contract exceeding $1,500.00.

ARTICLE XVI

Taxpayer Identification Number (Form W-9): All independent Consultants or corporations providing services to the County must file a Department of the Treasury Internal Revenue Service Form W-9, certifying their Taxpayer Identification Number.

ARTICLE XVII

Administrator: The County Officer or employee with responsibility for administering this Agreement is Kelly Webb, Principal Administrative Analyst, Chief Administrative Office, or designee/successor.

ARTICLE XVIII

Authorized Signatures: The parties to this Agreement represent that the undersigned individuals executing this Agreement on their respective behalf are fully authorized to do so by law or other appropriate instrument and to bind upon said parties to the obligations set forth herein.

ARTICLE XIX

Partial Invalidity: If any provision of this Agreement is held by a court of competent jurisdiction to be invalid, void or unenforceable, the remaining provisions will continue in full force and effect without being impaired or invalidated in any way.

ARTICLE XX

Venue: Any dispute resolution action arising out of this Agreement, including, but not limited to, litigation, mediation, or arbitration, shall be brought in El Dorado County, California, and shall be resolved in accordance with the laws of the State of California. Consultant waives any removal rights it might have under Code of Civil Procedure Section 394.

ARTICLE XXI

Entire Agreement: This document and the documents referred to herein or exhibits hereto are the entire Agreement between the parties and they incorporate or supersede all prior written or oral Agreements or understandings.

REQUESTING CONTRACT ADMINISTRATOR CONCURRENCE:

By:____________________________ Dated: ______________________
Kelly Webb
Principal Administrative Analyst
Chief Administrative Office

REQUESTING DEPARTMENT HEAD CONCURRENCE:

By:____________________________ Dated: ______________________
Laura S. Gill,
Chief Administrative Officer

/

/

/

/

/

/

/

/

/

/

/

/

/

/

/

IN WITNESS WHEREOF, the parties hereto have executed this Agreement on the dates indicated below, the latest of which shall be deemed to be the effective date of this Agreement.

--COUNTY OF EL DORADO--

Dated: ____________________

By: ______________________________
Chairman
Board of Supervisors
"County"

ATTEST:
Cindy Keck, Clerk
of the Board of Supervisors

By: ________________________ Date: ____________________
Deputy Clerk

--CONSULTANT--

Dated: ____________________

DAYSTAR COMPUTER SYSTEMS, INC.
A ILLINOIS CORPORATION

By: ______________________________
Ron Cichon, President
"Consultant"

By: ______________________________
Corporate Secretary

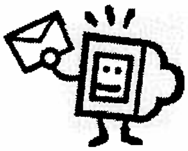
Dated: ____________________

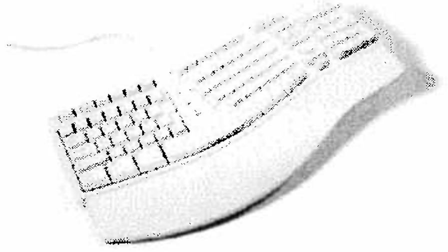
Exhibit "A"

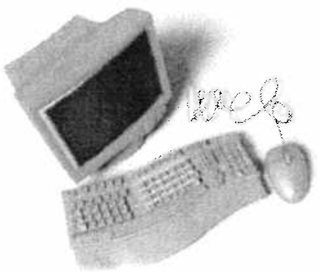
El Dorado County

Computer and Network Resource Usage Policies and Standards Guide

General Use







Revision Date: 12/4/06

Prepared by Information Technologies Department

Jackie Nilius, Director

Steve Featherston, Assistant Director

Renee Finelli, IT Manager, Programming

Tom Straling, Technology Officer

Reviewed and edited by the Information Technologies Steering Committee members.

INTRODUCTION

This Computer and Network Resource Usage Policies and Standards Guide has been created to assist El Dorado County employees in understanding their responsibilities when using County computer workstations, printers, peripherals, software, and network resources. The Guide is intended to comply with Board Policy A-19 and applies to all County Employees.

Page 13, "El Dorado County Computer and Network Resource Usage Policies Agreement" must be signed by all County employees indicating they have read and understood the General Usage Policies, "1.1 - Background" through "1.14 - Remote Access Policies".

SECTION 1
TABLE OF CONTENTS

GENERAL USAGE POLICIES

1.1 Background

El Dorado County has an extensive communication infrastructure with network and computing resources for use by County employees, contractors, vendors, quasi-governmental employees (fire departments, community services districts, etc) and temporary workers, hereafter referred to as "County User". In addition, the County provides a large and continuously growing number of computer workstations, printers, peripherals, software, training and supplies to all County sites. These items are provided by El Dorado County to allow County Users to perform tasks efficiently to meet the goals established by the El Dorado County Board of Supervisors.

While most are familiar with the term "computer", it is only one of the resources that are collectively known as network resources. Network resources consist of computers and their associated peripherals. These network resources, applications, and data provide the means to deliver services to El Dorado County residents.

While much of the data used by El Dorado County is "public" information, with legislative changes (HIPAA, Sarbanes-Oxley, etc.) there is a need to safeguard the data the County uses and to maintain the security and privacy of that data. Automatic and procedural security controls are in place to prevent or reduce unauthorized access to these resources. The primary responsibility for maintaining the integrity, security, and privacy of this information and its resources lies with the County User.

All computer systems furnished by the County, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic communication, file storage, Internet access ("www" browsing, use groups, etc.) and FTP (File Transfer Protocol), are the property of El Dorado County. These systems are to be used for business purposes in serving the interests of the County in the course of normal operations. Improper use of any of these resources can result in lost or degraded services to some or all County Users. Violation of local, State and Federal laws, rules and policies may call for prosecution under the law, including fines and imprisonment and disciplinary action.

County Users are responsible for reading, understanding, and following the appropriate use of County equipment and the release of County data. This document summarizes policies and offers standards and guidelines regarding the integrity, security, and privacy of County data, network resources and computers. County Users should contact their supervisors for any necessary clarification.

1.2 Purpose

The purpose of these policies is to define the acceptable use of computer equipment and networked resources throughout El Dorado County. These policies are in place to protect the County User and El Dorado County. Inappropriate use exposes El Dorado County to risks including but not limited to virus attacks, compromising network systems and services, and potential civil or criminal litigation. This policy applies to all computer equipment that is used by County Users or any device connected to the El Dorado County network.

Deviations from these policies may occur based on specific departmental technical needs. Deviations must be reviewed and approved by the IT Director or designee. IT decisions may be appealed to the IT Steering Committee.

1.3 General Use and Ownership

The County's business information, telephone, network, computer and software resources, peripherals and supplies are County property and are intended to be used to conduct County business. They do not belong to individuals and are used by County Users for the purposes required for their position while employed or contracted by the County.

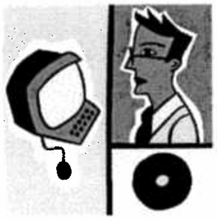
County Users should be aware that the data created or received on the County's computer systems remains the property of El Dorado County. There is no reasonable expectation of privacy regarding the confidentiality of information stored on any computer, terminal or network device belonging to El Dorado County, whether related to County business or to personal use.

It is the responsibility of the County User to safeguard confidential information from unauthorized disclosure or use. County Users shall not seek to use personal or confidential information for their own use or personal gain. County Users must take all reasonable precautions to ensure privacy is maintained under the law while handling information in any form, including but not limited to voice, electronic (disk file, diskette, CD ROM, DVD, magnetic tape, electronic communication, etc.), paper, photograph, and microfiche information.

Access to another County User's data will not be granted without written or electronic communication authorization from the appropriate department head or designee. All electronically stored data remains the property of El Dorado County; intentional destruction of this property is prohibited.

County Users are responsible for exercising good judgment regarding the reasonableness of personal use on personal time. County Users may engage in reasonable incidental personal use of the County's computer systems, to the extent permitted by the County User's department head, as long as such use does not degrade overall system performance (such as streaming media, i.e. music or video files), detract from a County User's productivity, duties, service to the public or to the County, violate any law, or any County policy, procedure, or regulation or tarnish the image of the County or contribute to the disrepute of the County.

For security and network maintenance purposes, Information Technologies staff members may monitor equipment, systems and network traffic at any time. This monitoring shall be done under the auspices of this policy, which is incorporated into Board Policy A-19.



1.4 Use of Personally Owned Software and Equipment

Personally owned software may not be installed on County computers, nor shall personally owned computer hardware or peripheral equipment be connected to County computers or attached to the County network.

1.5 Compliance with Software Copyright Laws

A copyright violation exposes the County to substantial risk of legal liability. County Users may not:

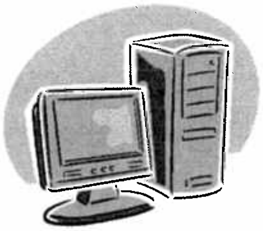
- Install any software without having proof of licensing;
- Install software licensed for one workstation on multiple machines; or
- Install or distribute "pirated" or other software products that are not appropriately licensed for use by El Dorado County.

County Users may not make unauthorized copies of copyrighted material including, but not limited to, photographs from magazines, books or other copyrighted sources, copyrighted music, or any copyrighted software for which the County or the County User does not have a valid license.

1.6 Disposal of Copyrighted Software Material

All copyrighted material must be disposed of in such a way as to render it useless and to minimize the potential liability to the County. The media on which the copyrighted material was obtained must be physically destroyed (for example, CDs, DVDs or floppy disks, will be broken in half or shredded) and any license keys or any other information that is required in order to use the software legally must be destroyed.

1.7 Use of Computer Resources



County computer resources are used by hundreds of County Users. To ensure that these resources are available and working properly, personal use of these resources must not negatively impact others.

No County User may attempt to access computer systems, or their resources, unless proper authorization has been granted by the department head. Any attempt to maliciously alter, erase, damage, destroy or make otherwise unusable or inaccessible any data, software, computer, or network system may constitute a felony and may result in any combination of disciplinary action and/or prosecution and fines, including litigation costs and payment of damages under applicable Local, State, and Federal statutes.

No County User shall willfully or through negligence introduce a malicious program into the network, any server or computer, (e.g. virus, worm, Trojan horse, electronic communication bomb etc.), nor shall any County User use port scanners or other intrusive software intended to undermine the stability and integrity of the County network and attached resources.

No County User shall use a County computing resource to engage in procuring, viewing or transmitting material that is pornographic in nature or is in violation of sexual harassment or hostile workplace guidelines. In general, any material that may be considered objectionable or may tend to bring the County into disrepute should not be sent via the County's computer systems.

El Dorado County has a significant investment in network server hardware and associated data storage capacity. Please see General Usage Standards and Guidelines – 3.3 Server Storage Utilization for options and recommendations for the file storage options, directory structure and back-ups to maximize available server storage space.

1.8 Policy for the Use of Electronic Communication

The need to manage electronic communication systems properly can be viewed the same as other records keeping systems; namely, to ensure compliance with laws concerning the creation, retention, or access to such electronic communication documents and to manage resources storing such electronic communication documents.

El Dorado County government agencies that use electronic communications have an obligation to make County Users aware that electronic communication messages, like paper records, must be retained and destroyed according to established records management procedures. They should deploy, or modify, electronic communication systems to facilitate electronic records management. Specific procedures and processes will vary according to departmental needs and the particular requirements placed on them via specific governmental agency rules or applicable law.

Please see General Usage Standards and Guidelines, 3.1 Electronic Communication for detail standards in support of these policies.

1.8.1 Definitions

Electronic communication ***systems*** transport messages (store and deliver) from one computer user to another. Electronic communication systems range in scope and size:

- From a local area network electronic communication system that delivers messages within an agency or office.

- To a wide area network electronic communication system that carries messages to a variety of physical locations.

- To Internet electronic communication that allows users to send and receive messages from around the world.

Electronic communication ***messages*** are documents sent or received by a computer system. This definition includes: 1) the contents of the communication, 2) any transactional information, and 3) any attachments associated with such communication. Thus, electronic communication messages are similar to other forms of communicated messages, such as correspondence, memoranda, and circular letters.

1.8.2 Personal Use

Incidental personal use, if authorized by the appropriate department head, of the County's electronic communication system is permitted as long as it is not excessive and does not degrade the performance of services or interfere with the County's normal business practices and the performance of the County User's business tasks. County Users should exercise sound judgment and sensitivity to others when exchanging personal messages in the workplace.

Lotus Notes is the County standard E-mail system.

- All incoming E-mail must be addressed to the County User's County-supplied electronic communication address such as John.Smith@edcgov.us. Firstname.lastname is the Standard Naming Convention. Receipt of non-County addressed E-mail is not allowed (jsmith@hotmail or comcast.com) for example. Examples of permitted incoming E-mails include those ending with edcgov.us, co.el-dorado.ca.us, edso.org, or /PV/EDC or /SLT/EDC (Lotus Notes addresses).

- Accessing personal E-mail from a commercial Internet service provider (ISP) via HTML and an Internet browser over the County network is prohibited. Examples of this type of ISP are MSN, Yahoo, Comcast, and Hotmail.

- The use of internet based commercial instant messaging products such as AOL Instant Messaging, Windows Instant Messaging, MIRC, IRC, etc. is prohibited over the County's network.

- Some electronic communication clients allow the use of downloadable plug-ins, allowing the computer user to add "emoticons" and other animations to their electronic communication. The downloading, installation and use of any of these items is prohibited on County computer systems.

1.8.3 State and Federal Laws

Use of the County's electronic communication system is subject to all applicable Federal and State communications and privacy laws. In particular, County Users need to be aware that attaching programs, sound, video, and images to electronic communication messages may violate copyright laws, and data files containing County User or citizen information are subject to all privacy laws.

1.8.4 Restrictions

Electronic communication may not be used for:

- Unlawful activities.

- Advertising (unsolicited electronic communication commonly referred to as "Spam").

- Mail "bombs".

- Uses that violate Departmental, County, State or Federal policies, such as, but not limited to, obscenity, sexual harassment, hostile work place, etc .

- Any other use which interferes with computing facilities and services of the County.

The list of restrictions is indicative rather than inclusive of restrictions and electronic communication may not be used for reasons other than those specifically mentioned.

1.8.5 False Identity

County Users shall not employ a false identity in sending electronic communication or alter forwarded electronic communication out of the context of its original meaning.

1.8.6 Representation

County Users shall not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of the County unless they are appropriately authorized, explicitly or implicitly, to do so.

1.8.7 Network Capacity

The County's electronic communication system shall not be used for purposes that could reasonably be expected to cause, either directly or indirectly, excessive use of network service or capacity, or cause interference with other County Users use of electronic communication systems, or any computing facilities or services.

For example, attaching files larger than 5 MB to an E-mail message and sending the E-mail to multiple recipients. Files meant to be shared or accessed by multiple County Users should be stored on a shared drive and a file path (link) to the file should be sent to the intended recipients.

1.8.8 Possession

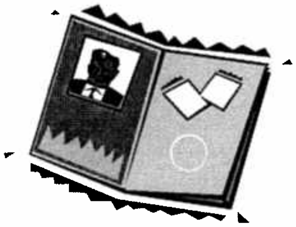
County Users are not responsible for "electronic communication in their possession" when they have no "reasonable" knowledge of its existence or contents.

Preservation of electronic communication (subject to litigation) is required when an individual knows or should reasonably know, by official notification or other communications, that probability of litigation exists or the process of discovery pursuant to litigation exists. Electronic communication and any associated attachments shall be preserved by all reasonable means until notified in writing by County Counsel that the litigation period has passed and that electronic communication pertaining to litigants no longer needs to be preserved. Preservation may include any and all electronic communication relating to possible litigation being copied onto readable media and delivered (with signed receipt) to County Counsel for later use. By not exercising reasonable and prudent precautions in preserving potential evidence, including electronic communication, you may subject yourself to criminal liability.

Every County User has a duty to preserve evidence in litigation! Destroying documents relevant to threatened or ongoing litigation may result in legal actions against that County User and against the County.

1.9 Use of the Internet

County User's incidental personal use of the Internet, if authorized by the appropriate department head, shall not encroach on or displace time spent performing their work duties. County Users shall not use the Internet in any way that may violate any other County rules, regulations, policies, procedures or practices, or bring civil or criminal liability or public reproach or any conduct tending to bring the County service into disrepute.



1.10 Computer User ID's and Password Policy

All County Users shall be assigned "user ID's" and passwords. Based on a County User's responsibilities and his or her supervisor's authorization, the County User may be provided with access levels which allow him or her to view, create, alter, delete, print, or transmit information.

County Users are responsible for maintaining the security of their personal account and may not release it for use by any other individual.

All user-level passwords (e.g., electronic communication, web, desktop computer, etc.) must be changed at least every six months. The recommended change interval is every four months. There are some systems, such as access for DMV records, that require passwords be changed more often. Please see Section 3.2, Passwords for the correct construction of passwords.

User accounts (e.g., root, enable, NT admin, application administration accounts, etc.) that have system-level privileges or administrative privileges must have strong unique passwords (6-8 character minimum) and will face regular mandatory password changes of no more than every four (4) months.

Passwords must not be inserted into electronic communication messages or other forms of electronic communication, including programming languages.

Any County User found to have violated this policy shall immediately have their access revoked.

Please see General Usage Standards and Guidelines - 3.2 Passwords in support of this policy. All user-level and system-level passwords must conform to the guidelines described in 3.2.1 Password Construction Guidelines.

1.11 Computer Viruses

The computer industry faces a continuing onslaught of malicious viruses, worms, malware and other damaging programs that attack computer and network resources. The County maintains equipment that reduces the potential impact of viruses, worms, spam, malware and phishing attacks in order to minimize impact of these invasions. It is the responsibility of the County User to take precautions to protect his/her computer and all network resources throughout the County.

Any computer or peripheral connecting to the El Dorado County network must use County approved anti-virus software. This software must be configured to receive regular software and virus signature file updates. All County computing equipment or peripherals, as applicable, shall run up to date versions of the County approved antivirus software.

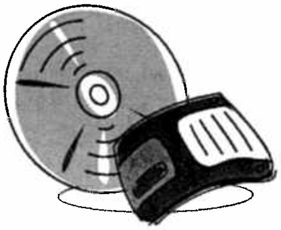
County Users should be cautious of opening electronic communication. Viruses can also be received from persons known to the recipient. If there is any doubt as to the validity of an attachment or the electronic communication, County Users shall delete the electronic communication and/or the attachment.

County Users may not download any software, including screensavers, from the Internet without prior authorization from the Director of Information Technologies, or designee.

Computers may not simultaneously connect to the County Wide Area Network (WAN) and other networks such as commercial, private, personal or direct Internet connections via dial-up, DSL or Broadband connections.

Critical data should be maintained on servers for security, anti-virus protection and to ensure data integrity through system tape back up.

All computers connecting to the County network are required to be current on all operating system, browser, Office Suite and application updates. These are the updates to the programs mentioned, not necessarily the most current release of the programs.



1.12 Removable Data Storage Devices

There are many forms of removable data storage devices in use today. These devices include, but are not limited to; floppy disk, CDs, DVDs, USB sticks, MP3 players and cameras being the most common. These devices can easily spread viruses to County computer equipment. To prevent the spread of worms, trojans or viruses note the following:

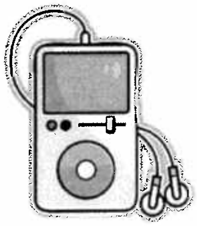
- Floppy drive use should be avoided at all costs. If floppy drive disks must be used to transport data, they should be scanned upon insertion into the floppy drive bay. Never insert floppy disks unless they are from a known source.

- CDs and DVDs must be scanned for viruses upon insertion.

  - USB memory sticks pose the same risks as floppy disks and should be handled in the same manner.

- County cameras connected to computers via docking stations pose little risk.

- MP3 players (IPOD's etc) may not be connected to County computing equipment. The downloading of music from the internet to County computers is prohibited. Downloading music at home to MP3 players and connecting to County computers is prohibited due to the very high risk of infection.



1.13 Portable Computing Devices (WPDA, PDA, Laptops, Tablets)

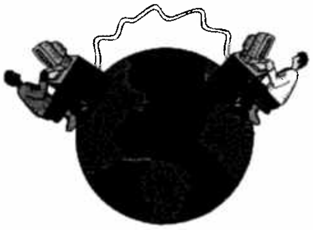
Portable computing devices such as wireless and/or standard personal digital assistants and laptop computers are subject to every element of the Computer and Network Resource Usage Policies.

Due to their portable nature they are much more prone to loss or theft. Users of these devices are required to practice due diligence in loss prevention of the physical device and data contained within.

The following practices must be observed when transporting or using these devices at work or in the field:

- Physical security is one of the most important aspects of protecting these devices. Never let them out of your sight or leave them any place unattended.
- If these devices must be left in a vehicle, store them in the trunk or other secure location, camouflaging them as necessary to keep them out of sight.
- These devices should be protected with their integral security systems:
    - Laptops with Biometric devices (finger print scanners, retinal scanners) or smart cards and should be used whenever possible, especially equipment containing sensitive or regulatory protected data.
    - Sensitive data should be stored on secured servers as much as possible. Data stored on local drives should be encrypted and password protected.
    - All portable computer devices should have appropriate County antivirus software installed and County approved firewall software for devices connecting to internet services to protect data from hackers.
    - Wireless Personal Digital Assistants may only communicate with the County E-mail system through the Intellisync gateway into the Lotus Notes/Domino E-mail system.
    - Data from unknown sources should not be beamed to your portable devices via infrared ports.
- Lost Devices must be immediately reported to your supervisor as soon after the incident as possible.

1.14 Remote Access Policy



This policy applies to County Users utilizing remote services to access the El Dorado County network. This policy applies to all implementations of remote access that are directed through a VPN Concentrator, firewall-to-firewall access, or dial-up service to access County network resources.

Approved County Users may utilize the benefits of remote access, which is a "user managed" service. This means that the County User will be responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees. When connecting to County hosted remote access services, the County User and his or her department are responsible for any and all toll charges associated with the use of remote access equipment.

The following policies apply to remote access users:

- It is the responsibility of County Users with remote privileges to ensure that unauthorized users are not allowed access to El Dorado County internal networks.
- When actively connected to the County network through dial-up services, all other connections to non-County networks will be disconnected.
- Remote access accounts will be created and managed by El Dorado County Information Technologies.
- All computers connected to El Dorado County internal networks via remote access must use up-to-date anti-virus software and properly updated operating systems, browsers and applications.
- Remote access users will be automatically disconnected from El Dorado County's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network.
- VPN connectivity will be through approved client software as defined by El Dorado County Information Technologies.
- By using remote access technology with personal equipment, County Users must understand that their machines are a de facto extension of El Dorado County's network, and as such are subject to the same rules and regulations that apply to El Dorado County-owned equipment, and their machines must be configured to comply with the security policies and standards of El Dorado County.
- At the current time, certain types of data cannot be transmitted through Virtual Private Network connections through commercial internet channels. Per Government code 6254.21, County Users are restricted from transmitting the following types of information, containing the name, address, phone number or personal information of the following protected classes:
    - Any Elected Official
    - Any Court Official
    - Any Law Enforcement Personnel
    - And Other Public Officials
- As a remote user of the County's information systems, you will have unique access to sensitive resources that are connected through the County network. To assure security throughout the entire County network, it is critical that all remote users actively support and fully comply with the measures described in these Policies. Failure to comply can place the entire County network at serious risk; and remote users who fail to comply will be subject to disciplinary action.

- Remote users are required to complete a questionnaire provided by Information Technologies. This questionnaire identifies security, antivirus and other computer protection methods used by the requesting party and needs to be signed by the department head After submission of this form and the completed questionnaire, Information Technologies will ensure remote systems meet County specifications prior to granting access.

COUNTY USER AGREEMENT

El Dorado County Computer and Network Resource Usage Policies Agreement

I have read and understand that:

1) As a user of the County's information technology resources, I may have access to sensitive resources that are connected through the County network. To assure security throughout the entire County network, it is critical that all users actively support and fully comply with the measures described in the Computer and Network Resource Usage Policies and Standards Guide. Failure to comply can place the entire County network at serious risk. Failure to comply may subject me to disciplinary action.

2) As a User of the County's information systems I shall at all times act in accordance with all applicable laws and County policies, rules or procedures. I shall not use County information technology resources in an improper or unauthorized manner.

I have read, understand and am fully aware of the El Dorado County Computer and Network Resource Usage Policies and Standards Guide. I agree to comply with the terms of this policy.

User Name: ______________________________

Signature: ______________________________

Date: ______________________________

This form shall be signed on an annual basis and be retained in the department, district or agency file.

GENERAL USAGE STANDARDS AND GUIDELINES

3.1 Electronic Communication

The County encourages the use of electronic communication to enhance communication and business activities. Standards are necessary to ensure the appropriate use of electronic communication and to prevent or limit disruptions to work activity and computer services.
The nature of electronic communication at the present time makes it susceptible to misuse. County Users need to be aware that sensitive or private information can be easily forwarded to other individuals the originator never intended, both internal and external to the County.

Users of the County's electronic communication services need to be aware that use of these services is a privilege granted with the expectation that it will be used for business purposes and in a professional and courteous manner similar to other forms of communication. All electronic communication sent or received by individuals through County User's accounts is the property of the County and may be examined by other staff at the request of a County User's department head with concurrence from the Director of Human Resources.

It is important to understand and use electronic communication appropriately within the County use policy and your specific departmental electronic communication use policy. Additionally, for a guide to safe electronic communication use please refer to the EDC Web Site: http://edcnet/is/safe_computing.html.

3.1.1 Security and Confidentiality

The confidentiality of electronic communication cannot be assured. County Users should exercise extreme caution in using electronic communication to communicate confidential or sensitive material. Any electronic communication that contains confidential information, such as HIPAA-protected data, must be encrypted before it is electronically communicated.

3.1.2 Anti-Spam Measures

Never respond to a spam electronic communication. Many spam electronic communications may contain instructions on how to remove your address from their address list. More often than not, your response only confirms they have a valid address. They will continue to send you spam and will sell or share the now confirmed active address to other spammers.

Never use your County electronic communication account for Internet purchasing, auction sites (EBay etc.) or supply your County internet E-mail account address to suspicious or un-trusted sites.

El Dorado County has made a significant investment in technologies designed to minimize our exposure to spam and viruses. This equipment will quarantine suspicious electronic communication. The equipment uses a serious of counter-spam /antivirus measures to assign a point value to incoming mail. When an electronic communication hits these thresholds it is normally quarantined. Often times, incoming electronic communication may be quarantined due to poor maintenance and/or security measures at the senders end, causing their electronic communication services to be "blacklisted" and resulting in quarantine at our servers. These actions are by design and meant to protect our systems and your County computers.

We realize this can delay the delivery of electronic communication. IT's Staff check quarantine areas regularly to minimize the impact on County staff members. Although this quarantine process may at times be inconvenient, it is necessary to prevent the entry of unwanted and potentially dangerous electronic communication into the County system.

3.1.3 HIPPA and Compliance with Electronic Communication Privacy Act

Standards are under development to comply with above regulations and acts. In general, electronic communication under the umbrella of these regulations requires data and electronic communication encryption. The County is currently analyzing solutions to meet these acts and regulations,

3.1.4 E-mail Retention Policy

Formal E-mail retention policies are under review and will be complete in the near future; after the appropriate review and approval processes. E-mail retention policies differ from E-mail archiving. Archiving manages the size of E-mail files. Retention manages the age of E-mail and deletes E-mail that age past a certain date.

Exceptions to retention periods would be E-mail subject to statutes or regulations requiring a longer retention period. There is much work yet to be completed in the area of E-mail retention. All opinions will be addressed as IT works through committees and County Counsel to establish the proper retention policy for County Users.

3.1.4.1 Account File Size Restrictions and E-mail Retention Standard

E-mail attachments can consume large amounts of storage space on County electronic communication servers. It is recommended that attachments be detached and stored on a local computer or stored on a server and deleted from electronic communication to preserve electronic communication server storage.

County User practices should include proper management of their E-mail records. Departments must develop guidelines pertinent to their business requirements that dictate how long specific electronic communication should be kept and what should be deleted. Departments may have differing needs for retention based on Local, State, and Federal law as well as accepted best practices within their industries.

A departmental E-mail retention standard is designed to reflect the need for each County User to manage his or her E-mails effectively and efficiently. This standard will help minimize the impact on County resources in storing and managing the County's enterprise E-mail system.

3.1.5 Production E-mail File Standard

You may receive and manage your 'production' E-mail file and create folders as you wish and according to your department's electronic communication policy. You may have E-mail file size usage up to 250 MB. Once you have reached this limit, you will be notified via the E-mail system that you are approaching your file size quota. You will need to clean up and/or archive old E-mail at this time. You will have an additional 50 MB beyond your base 250 MB of storage as a 'buffer'. The buffer, once used, will allow up to 300 MB of storage. The E-mail system will prevent you from sending any additional E-mail messages until the file size has been reduced.

3.1.6 Managing Your E-mail

You can manage your E-mail by:

- Delete E-mail you no longer need.
- Save only E-mail that you are required to save; by department policy or based on legal requirements, to a designated archive folder(s). (This process will move your 'Archived' E-mail from your 'limited' production area to your Archive storage location.)
- Remove attachments from E-mail and store on local computer and/or server storage.
- Print out your E-mail and save the printed copy (or 'PDF') and then delete the E-mail.

These processes will bring your E-mail file size below the limits as designated.

3.1.6.1 Archiving E-mail

You can move an E-mail to a permanent (but easily accessible) storage area called archived mail storage. This archived area can contain manageable folders for you to place E-mail you wish to keep on a more permanent basis. Using Lotus Notes for archiving normally preserves data folder structures. You will personally manage these folders and it will be up to you to periodically delete any E-mail that you are not required to save.

You should not keep old E-mail that unnecessarily takes up space on County storage devices. (For example: if your departmental policy is to save all E-mail pertaining to 'public complaints about potholes in the road' for two years from its receipt, you should periodically delete those E-mails if they are older than two years.) Your archived E-mail file limitation is 500 MB, which should be large enough for any departmental policy directing the saving of pertinent E-mail (you will be notified by the system if you exceed your limitation). Exemptions may be granted for those that need larger space based on Local, State, or Federal requirements for retaining E-mail data. You will need to explain the process for exemptions and all requests will be reviewed on a "case by case" basis.

Note: In both your 'production' E-mail and your 'archived' E-mail area, files or E-mail records that have been deleted (and not restored by IT) will be un-recoverable from all backup media after 90 days following deletion.

These standards will be in effect after a period of three months from adoption by the County's Board of Supervisors. This initial 3-month 'wait' period will allow for time to get your 'production' E-mail file size below the 250 MB limitation. A short 'users manual' explaining "Production and Archived E-mail" will be available on the EDCNET Information Technologies home page site. You may contact the Information Technologies Department for additional information and help.

3.1.6.2 Backup Process for Production E-mail and Archived E-mail

- Production E-mail will be backed up daily (normal business day).
- Production E-mail will be backed up to tape on a weekly basis for 'off-site' disaster recovery purposes.

- Archived E-mail will be backed up during every archived cycle (the cycle period will be based on storage movement needs as well as backup processes, to be determined).
- Archived E-mail will be backed up to tape at this same interval cycle for off-site disaster recovery purposes.

3.1.6.3 E-mail Account Deletions

All Internet electronic communication is forwarded to the Intranet E-mail system. When a County User is confirmed to have permanently left County service, the Internet account is deleted. Their Intranet E-mail files are moved to "obsolete" and the County User's name is removed from the Intranet E-mail list. Files placed in "obsolete" are retained for 60 days and then deleted. Departments requiring any deviation from this standard should contact the Information Technologies department immediately!

3.1.6.4 Anti-Virus Measures and E-mail Attachments

Never open any file attached to an electronic communication from an unknown, suspicious or untrustworthy source. Delete these electronic communications immediately, then "double delete" them by emptying your Trash. One of our best lines of defense against malicious attacks is the computer user. Regularly check electronic communication for notifications sent to you by Information Technologies regarding viruses and electronic communication "scams". An informed computer user is an aware user and can better identify suspicious content in electronic communication.

Delete spam, chain, and other junk electronic communication without forwarding.

Never download files from unknown or suspicious sources or web sites. Never visit "underground" sites, hacking sites, or any site that is not required in the execution of your duties as a County User. These sites can put the integrity of the County network at risk through malicious code, either intentionally or un-intentionally.

Avoid direct disk sharing (peer to peer) with read/write access unless there is a business requirement to do so.

3.1.7 Electronic Communications – Instant Messaging

The County is using Lotus Instant Messaging as an additional form of electronic communication between County Users. All Policies applicable to electronic mail apply to electronic messaging. Special precautions must be observed with the use of instant messaging due to the nature in which transcripts of instant messaging are logged.

Should any County User receive objectionable, offensive or threatening content during an instant message session, it is important to follow these procedures:

- Do not close the instant message session or turn off your computer
- Contact your supervisor to report the behavior in question

As applicable, your supervisor will take the appropriate action, up to and including contacting the Human Resources department who will direct the collection of the data in question, following strict confidentiality guidelines.

3.2 Passwords

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of El Dorado County's entire corporate network. As such, all El Dorado County Users are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

The purpose of this standard is to establish criteria for creation of strong passwords, the protection of those passwords, and the frequency of change. This includes all County Users who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any El Dorado County facility, has access to the County network, or stores any non-public County information.

3.2.1 Password Construction Guidelines

Passwords are used for various purposes in El Dorado County. Some of the more common uses include: personal computer accounts, network server accounts, web accounts, electronic communication accounts, screen saver protection, voice electronic communication password, and mainframe accounts.

Poor or weak passwords have the following characteristics:

- The password contains less than eight characters.
- The password is a word found in a dictionary (English or foreign).
- The password is a common usage word such as:
  - Names of family, pets, friends, co-workers, fantasy characters, etc.
  - Computer terms and names, commands, sites, companies, hardware, software.
  - The words "El Dorado County, "County", "EDC", or any derivation.
  - Birthdays and other personal information such as addresses and phone numbers.
  - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
  - Any of the above spelled backwards.
  - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong or effective passwords have the following characteristics:

- The password contains at LEAST 8 characters.
- The password contains both upper and lower case characters (e.g., a-z, A-Z)
- The password has digits and punctuation characters as well as letters (e.g., 0-9, ! @ # $ % ^ & * ( ) _ + | ~ - = \ ` { } [ ] : " ; ' < > ? , . /)

- The password is not a word in any language, slang, dialect, jargon, etc.
- The password is not based on personal information, names of family, etc.

Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way to Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do **NOT** use either of the above examples as passwords!

3.2.2 Password Protection Standards

Do not use the same password for El Dorado County accounts as for other non-County access (e.g., personal ISP account, EBay, personal electronic communication accounts, etc.). Do not share El Dorado County passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential County information.

Here is a list of password "don'ts":

- Don't reveal a password over the phone to un-authorized personnel.
- Don't reveal a password in an electronic communication message.
- Don't reveal a password to the manager without a written request for such information from your manager.
- Don't talk about a password in front of others.
- Don't hint at the format of a password (e.g., "my family name").
- Don't reveal a password on questionnaires or security forms.
- Don't share a password with family members.
- Don't reveal a password to co-workers while on vacation.
- Don't use the "Remember Password" feature of applications (e.g., Internet Explorer, Outlook, Outlook Express, and Entourage).
- Don't write passwords down and store them anywhere in your office.
- Don't store passwords in a file on ANY computer system (including PDA's) without encryption.

All computing equipment deployed in El Dorado County shall have screen savers with password protection enabled and set to lock the computer after ten (10) minutes of inactivity. County Users should hit "Ctrl/Alt/Delete keys and lock their computers to protect against un-authorized access whenever leaving their work station.

If someone demands a password, refer them to this document or have them call the Director of Information Technologies. Departments needing authorized access should contact the Information Technology department to securely address this need.

If an account or password is suspected to have been compromised, report the incident to Information Technologies immediately and change all passwords.

3.2.3 Application Development Password Standards

Application developers must ensure their programs contain the following security precautions:

- Support authentication of individual users, not groups.
- Do not store passwords in clear text or in any easily reversible form.
- Provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
- Support TACACS+, RADIUS and/or X.509 with LDAP security retrieval, wherever possible. Contact the Information Technologies department for more information on these security measures.

3.2.4 Pass Phrases

Pass phrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the pass phrase to "unlock" the private key, the user cannot gain access.

Pass phrases are not the same as passwords. A pass phrase is a longer version of a password and is, therefore, more secure. A pass phrase is typically composed of multiple words. Because of this, a pass phrase is more secure against "dictionary attacks."

A good pass phrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good pass phrase:

"TheTrafficOn50WasTerribleThisMorning"

All of the rules above that apply to passwords apply to pass phrases.

3.2.5 Use of Passwords and Pass Phrases for Remote Access Users

Access to the El Dorado County networks via Virtual Private Networking (VPN) access and some networked resources are controlled using the username/password (challenge/response) mode of authentication. Access to the County network via VPN is tightly controlled.

3.3 Server Storage Utilization

To maximize server storage, County Users should properly manage their data and directory structures. There are several methods of file storage and associated back-up. The recommendations in the next section provide options and recommendations for file storage, directory structure and back-ups to ensure the availability of server storage space.

3.3.1 File Storage Options

- Operating system and applications are loaded on the desktop computer and all data files are stored on the local machine hard drive. *This option provides local access to the computer data files, but offers no backup of those files. Hard drive failure will result in complete loss of data files. This option is* ***not recommended.***

- Operating system and applications are loaded locally and all data files are stored on a network server. *This option safeguards data in two ways: 1) data files reside on servers, 2) data files on servers are backed up to tape nightly. A possible drawback to this option is the inability to access data on the server in the event of server or network problems.*

- Operating system and applications are loaded locally. All data files are stored on the local hard drive and its directory structure configured to allow for scheduled copying of local data files to the server. *This option safeguards data in three ways: 1) data files reside on local drives, 2) data files reside on server hard drives, 3) data files are backed up to tape nightly. In the event of network or server problems, data files stored locally will be available. While this method requires the largest amount of user intervention due to regularly scheduled backups of local data files to server drives, it does provide maximum availability and protection of data files.* **Systems will soon be in place Countywide to automate the synchronization of files between your computer and servers, maintaining copies of your important data on both the local drive of your computer and your server.**

- "Thin Client" computer; all files reside on a server. The operating system and applications run at the server level, data files are stored on server drives. Proper file management at the server level preserves hard drive space.

3.3.2 Server File Storage

- The majority of County computers are connected to Novell or Windows based servers. These servers store data files and send print jobs to networked printers. Storage must be managed to maximize storage capacity.

- Server hard drive arrays have finite capacity. NEVER copy the entire contents of local drives to server drives. This wastes server-based storage.

- County User-specific data files should be copied only to the County User's server home directory which is normally designated as the "H:" drive.

- Data files common to a group should only be copied to the "shared" server directory's appropriate sub-directory. Always store data files in the appropriate sub-directory as defined within your department and/or group. NEVER store data files at the root of shared directories.

- Do not store multiple copies of data files on a server. There is no need to have a copy of the same file in your home directory and a group directory. Do not decompress operating system or application service packs or updates to server hard drives.

- Clean up your directories at least monthly. Delete old data files or files no longer needed and remove unnecessary iterations or versions of data files. Server storage is not to be used for storing non-work-related music, video, or picture files.