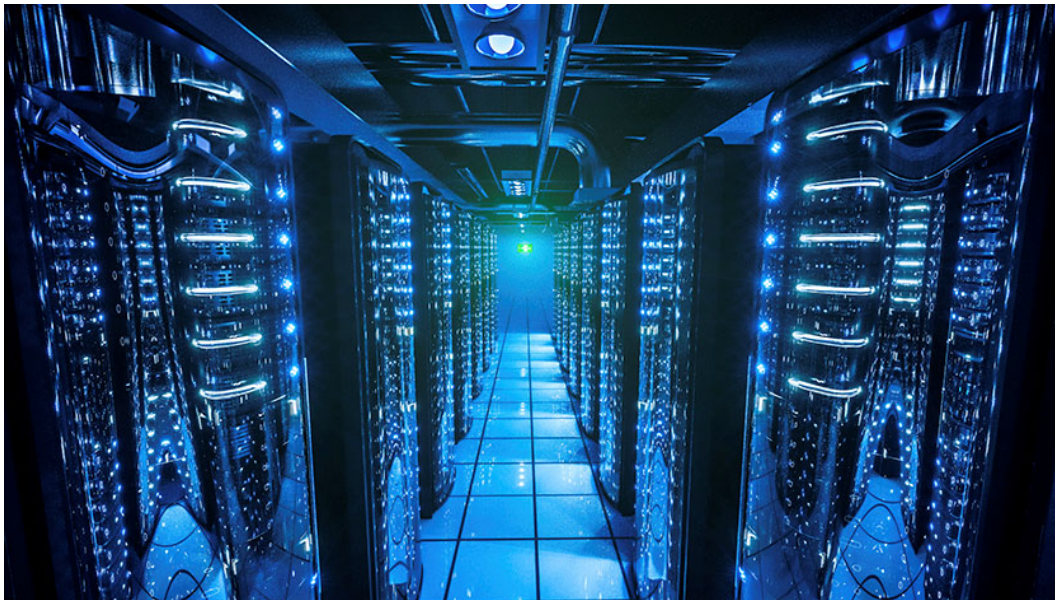


Los Alamos County
Information Technology Division

**STANDARDS AND SPECIFICATONS
FOR BUILDING AND CAMPUS
DISTRIBUTION SYSTEMS**



Los Alamos County
Administrative Services Department
Information Technology Division
September 15, 2016

Prepared by: Matthew T. Casados
Los Alamos County Program Manager
Version 3 Revision Date: 10/17/2016

CIO Approval Date:

Index

1.0	Introduction	
1.1	Background	1
1.2	Planning	1
1.3	Scope	2
1.4	Coordination	2
2.0	Building Specifications	2
2.1	Data Center (Server Room)	3
2.1.1	Electrical Systems	4
2.1.2	Grounding Systems	5
2.1.3	Fire Suppression\Detection System	6
2.1.4	HVAC	7
2.1.5	Water and Facility Location	7
2.1.6	Data Floor Design	7
2.1.7	Data Center Security and Access control	8
2.2	Telecommunication Spaces	8
2.2.1	General Telecommunication Space Design	8
2.2.1.1	Location	8
2.2.1.2	Accessibility	9
2.2.1.3	Cable Separation	9
2.2.1.4	Ceilings	9
2.2.1.5	Clearances	10
2.2.1.6	Doors	10
2.2.1.7	Dust and Static Electricity	10
2.2.1.8	Wall Requirements	10
2.2.1.9	Environmental Control	11
2.2.1.10	Lighting	11
2.2.1.11	Electrical	11
2.2.1.12	Grounding Systems	12
2.2.1.13	Fire Suppression\Detection Sys	13
2.2.2	Telecommunication Room	13
2.2.2.1	Floor Space Served	13
2.2.2.2	Size	13

2.2.3	Telecommunication Enclosure	14
2.2.3.1	Floor Space Served	14
2.2.3.2	Door\Enclosure Type	15
2.2.3.3	Electrical Power	15
2.2.3.4	Fire Protection	15
2.2.3.5	Grounding and Bonding	15
2.2.3.6	Environmental Control	16
2.2.3.7	Pathways	16
2.2.4	Equipment Room (ER)	16
2.2.4.1	Size	16
2.2.4.2	Equipment Room Requirements	17
2.2.4.3	Special Systems	17
2.2.5	Entrance Facility (EF)	17
2.2.5.1	Location	17
2.2.5.2	Underground Conduits	18
2.2.5.3	Handholds and Splice Vaults	19
2.2.5.4	Terminating conduit for EF	19
2.2.5.5	Aerial Cable	19
2.2.5.6	Telecommunications Backboard	19
	Figure 2.2E Handhold	21
	Figure 2.2F Splice Vault	22
	Figure 2.2G Vault/Handhold Installation Detail	23
3.0	Network Infrastructure Specifications	24
3.1	Conduits and Pathways	24
3.1.1	Conduits Specifications	24
3.1.2	Unacceptable Conduit Practice	24
3.1.3	Cable Tray	25
3.1.4	Other Pathway types	26
3.2	Horizontal Cabling Systems	26
3.2.1	Infrastructure Labeling	26
3.2.2	Fiber Optic Cabling	27
3.2.3	Unshielded Twisted Pair	28
3.3	Backbone Distribution (Outdoor Plant)	29

4.0	Field Testing	30
4.1	UTP Balanced Twisted-Pair Cabling Accept. Tests	30
4.2	Optical Fiber Cabling Acceptance Testing	31
4.3	Optical Fiber Cable Tagging	31

**Information Technology Usage and Security
Policy
Los Alamos County**

July 30, 2007

Approved

Los Alamos County Administrator

Max H. Baker

Date

7/30/07

1.	<i>Introduction</i>	3
2.	<i>Policy Direction and Maintenance</i>	3
3.	<i>Principles</i>	3
4.	<i>Security Program Components</i>	3
5.	<i>Risk Identification</i>	4
6.	<i>DOE Requirements</i>	4
7.	<i>Physical Security</i>	4
8.	<i>Access Management</i>	5
9.	<i>Requesting Account Access</i>	6
10.	<i>Naming Conventions</i>	6
11.	<i>Password Creation</i>	6
12.	<i>Account Control</i>	6
13.	<i>Account Suspension and Termination</i>	7
14.	<i>Security Training</i>	7
15.	<i>Data Security</i>	8
16.	<i>Usage Policy Overview</i>	9
17.	<i>Usage Policy: Prohibited Use</i>	10
18.	<i>Usage Policy: Personal Use of County IT Assets</i>	12
19.	<i>Remote Computing</i>	12
20.	<i>Enforcement and Sanctions</i>	13
21.	<i>Technology Components of Security</i>	14
22.	<i>Backup and Recovery</i>	15
23.	<i>Definitions</i>	15
	<i>Appendix A: Acknowledgement Form</i>	17
	<i>Appendix B: Master Computer Protection Plan</i>	18
	<i>Appendix C: ITD Supported Applications</i>	22

1. Introduction

This policy provides guidance to users of Los Alamos County (the County) information technology (IT) assets on proper use and protection of computing and communications resources, including: the Internet; email; the Integrated County Network (ICN); phones; data; desktop computers; personal devices (e.g. PDA's); servers; and applications.

These assets provide critical support for service delivery to County residents and visitors.

2. Policy Direction and Maintenance

The County must take prudent and reasonable measures to secure its systems and data to (1) meet legal and regulatory obligations and (2) for effective County operation. The Information Technology Division (ITD) prepares this policy based on direction from the IT Management Oversight Committee and approval by the County Administrator. It applies to all users of County IT assets.

ITD will update this policy at least yearly. Copies are available in every department and maintained on the County's web site. Questions about this policy should be referred to the Information Technology Division.

3. Principles

This policy and accompanying programs are based on several principles:

- 3.1. Compliance with DOE requirements (see below);
- 3.2. An optimum balance of security and productivity;
- 3.3. Providing defense in depth for known threats with flexibility to respond quickly to unknown or unexpected threats;
- 3.4. Being risk based - correlate security investments with risk;
- 3.5. Identifying roles and responsibilities for personnel, supervisors, and IT personnel;
- 3.6. Providing engineered solutions where possible to minimize the impact of risky human behaviors; and
- 3.7. Incorporating a process of incremental security improvement.

4. Security Program Components

The County's computing and communications security programs consist of administrative and technical components. Administrative components include the following:

- 4.1. Incident reporting and response;
- 4.2. Well-defined and documented usage policy;
- 4.3. Regular policy update and publication;
- 4.4. Training of personnel and supervisors; and
- 4.5. Account management and control.

The technology components include the following:

- 4.6. Physical security;
- 4.7. Infrastructure design;
- 4.8. Perimeter network defense; and
- 4.9. Inside network defense.

5. Risk Identification

Risks to County IT assets fall into three major categories. Major risks and their potential impact are defined below

- 5.1. **First, service interruption and/or destruction of data by untargeted attacks**, e.g. email viruses, worms, denial of service attacks, etc. This is the most common and well-publicized threat that affects County IT operations. This can take down networks, servers, and desktops, can damage data, and compromise County operations.
- 5.2. **Second, misuse of legitimate access to County assets**. While illegal, this problem usually represents a minimal actual loss to the County with respect to IT resources. Examples are County employees running their own businesses on County equipment and misuse of phones, computers, and/or Internet access. However, asset misuse also may represent systematic, planned use of IT assets to divert material resources to personal advantage, e.g. embezzlement. In such cases, losses may be substantial.
- 5.3. **Third, a targeted attack by an individual using illegitimate access**. This is the classic “hacking” portrayed in movies and fiction. While comparatively rare, it can be devastating if successfully pursued by a skilled and malicious individual.

6. DOE Requirements

Due to the contracts Los Alamos County has with the U.S. Department of Energy (DOE), there are certain requirements imposed on the County and its employees. By virtue of these contracts, the County will impose these same requirements on all IT users regardless of whether or not they are County employees. These requirements pertain to ensuring that information is not disclosed to unauthorized viewers. DOE requires that all account holders be diligent in determining if data is sensitive and seeing that it is protected from unauthorized viewers. Fire Chief's Directive 100.15A also addresses this requirement. It is the account holder's responsibility to bring to their supervisor's attention questions about whether information needs to be protected from unauthorized access so that inadvertent disclosure does not occur. The specific DOE requirements are detailed in the *Master Computer Protection Plan* included in Appendix B.

7. Physical Security

The occupier of County owned or leased physical space has responsibility for the physical security of IT resources in their areas. The level of physical security should be proportionate to the possible impact on the County of systems compromise or loss. For example, the level of physical security for a generic personal computer used by someone without access to County financial or material resources is not expected to have the same level of physical security as a

computer commonly used by someone with wide access to County financial data and transactions. In general, this means acceptance of the following responsibilities.

7.1. Responsibilities for all users:

- 7.1.1. Locking rooms except during business hours;
- 7.1.2. Not leaving computers unattended and logged in without password protection for extended periods of time;
- 7.1.3. Challenging visitors and unfamiliar people if found using County computer resources;
- 7.1.4. Not physically keeping passwords in the vicinity of a computer (e.g. in a desk drawer, pasted under the keyboard, etc.);
- 7.1.5. Maintaining physical control over mobile computing and communications units (laptops, PDA's, phones) and notifying ITD immediately if a unit is lost or stolen.
- 7.1.6. Not connecting a computing device to the network or reconfiguring a computing device connected to the network without contacting ITD;
- 7.1.7. Prompt reporting of any compromise of computing or communications devices or of passwords; and
- 7.1.8. Releasing unneeded resources, including access authorizations.

7.2. Supervisors have these additional responsibilities:

- 7.2.1. Limiting the number of computers used for critical transactions, e.g. financial adjustments;
- 7.2.2. Physical control over their computing and/or communication environments;
- 7.2.3. Coordinating with ITD installation, removal, and reconfiguring of equipment with network and computing capabilities (e.g. copiers);
- 7.2.4. Understanding and supporting the administrative components of the computer security policy; and
- 7.2.5. Reporting personnel changes in their organizations to ITD.

7.3. The ITD has the following additional responsibilities:

- 7.3.1. Physical security of servers and the Integrated Computer Network (ICN)
- 7.3.2. Training of users in computer security;
- 7.3.3. Assisting other County personnel in addressing security issues; and
- 7.3.4. Policy review and update.

8. Access Management

Access management is a key component of perimeter defense. Stopping the illegitimate user is a primary defense against illegitimate use (Risk 3). Good access management also enables monitoring of users' computing and communications activities, thereby greatly reducing the risk of misuse (Risk 2).

Any County employee or contractor may be authorized to use a specified set of County IT assets. An account is established for use by only one person for whom access has been requested and granted. This person becomes the account "owner" and is responsible for all activity taking place through that account. Supervisors are responsible for specifying the scope of the access.

9. Requesting Account Access

All access requests must come from a person having a County supervisory role (hereafter designated a County supervisor or, simply, a supervisor) and state the applications and specific functions required for an employee, elected or appointed official, volunteer, or contractor. (A list of available applications is included in Appendix C.) Requests should be received by the ITD at least one week prior to the user's need for access. Requests for contractor or volunteer access must be for a specified time period less than twelve (12) months, at which time the access may be renewed if so requested. Accounts will be requested by the supervisor via email (call the ITD help desk for instructions) or paper form and include a signed copy of the *Account Holder and Computer User Responsibilities* form (Appendix A) authorizing the account. This form must be used for any new account authorization including new hires, job changes, or any other change requiring different system access. Requests for direct dial-in access to the network must also be made on this form.

10. Naming Conventions

There are currently two naming conventions for accounts. For Windows-based systems, accounts are named using the employee's last name and first initial and, if necessary, a sequential number or middle initial. For AIX or Linux systems, accounts are named using the employee's first initial, last initial and a sequential number.

11. Password Creation

Each account requires a password. Since the password is the only thing keeping others from accessing your account, it is important that it be something that no one else can guess easily. Users should follow these standards when creating a password.

- 11.1. The password should be at least 8 characters long and must not be a word commonly found in the dictionary.
- 11.2. A password should not be a name of a family member, pet, or anything else that is commonly associated with the account-holder.
- 11.3. The password should contain at least two of the following categories: letters; numbers; and special characters.
- 11.4. The password should not contain repeating groups, e.g. abcabc or runs, e.g. mnopqrs

12. Account Control

Once set, your password is the primary defense used to prevent unauthorized access to IT resources. The County has set the following standards for password control:

- 12.1. Set up all computers with password protection that automatically activates after a short time period of inactivity (five minutes is recommended) to prevent unauthorized use of the computer (call the help desk if you need assistance);

- 12.2. Do not share your password with anyone (except as noted below);
- 12.3. Do not allow any other person to use your account (i.e. password);
- 12.4. Your password must not be written anywhere where it can be easily found. For example, don't write your password on your keyboard, on a post-it note on your monitor, or on a note in your desk; and
- 12.5. The system will require you to change your password every 90 days. The new password you choose must not be one that you have used previously. If you suspect that your password has been compromised, call the help desk immediately.
- 12.6. The County follows current industry best practice for passwords. Users are required to choose and maintain strong passwords for access to County computer resources.

Maintaining account security is a serious matter. In addition to safeguarding County information the County must enforce strict computer security to be in compliance with its contract with DOE. Sharing of passwords or other conduct that compromise the security of County IT assets or the ability of the County to perform its functions may subject the account holder to disciplinary action as defined in this policy. Account holders may share their passwords with ITD personnel in order to facilitate repair or recovery of systems or data. All such password sharing should be considered non-standard operating practice. Account holders will change their password immediately once the condition requiring the non-standard operating practice has been addressed. The account holder is still responsible for all activities in their account carried out under their password.

13. Account Suspension and Termination

If an account holder will be on leave from work for thirty (30) days or more, their supervisor must inform ITD so that the account may be temporarily suspended. Users or supervisors should immediately request account suspension and contact ITD if they have reason to believe that an account may have been compromised or is being misused.

Upon the termination of an account holder's employment or association with Los Alamos County, the supervisor should identify the access needed by coworkers or supervisors to the account holder's files and e-mail. This access will be provided for a period of two months, during which time it is the supervisor's responsibility to move items they wish to keep. At the end of two months, ITD will terminate the account and delete all remaining files. ITD will work with the department involved to transfer any important documents or data files to another designated person so that information is not lost. As part of the exit procedure, account holders must return to ITD or the supervisor all County-owned equipment.

14. Security Training

The County organization responsible for authorizing account access is responsible for training personnel in both desktop computer applications and organizational-specific applications. On request, ITD will work with County organizations on improving applications security and on finding courses to improve employee IT skills. The County recognizes the importance of computing skills for its employees and encourages County organizations to work with ITD on training needs.

ITD is responsible for network and desktop computer security training. Prior to receiving access and passwords a new account holder is required to successfully complete basic security training provided by ITD. This training covers password management, basic physical security, user responsibilities, and usage policies. The training includes an acknowledgment by the new account holders that they (1) have received computer training; (2) understand their rights and responsibilities as defined in this policy; and (3) recognize and understand the penalties for violating this policy. Updated IT security training will be provided by ITD and will be mandatory for account holders at least every five years. Account holders will sign an updated "Account Holder and Computer User Responsibilities" form whenever updated IT security training occurs.

Security questions should be directed to the help desk staff or, after hours, to the on-call IT staff member.

15. Data Security

15.1. The County is responsible for data that may be subject to laws and regulations regarding unauthorized disclosure, may be misused for personal gain, and/or may be of a proprietary nature. Therefore, all account holders must be aware of their responsibilities with respect to the access to, and use of, data in County IT systems. Non-ITD supervisors have the following responsibilities:

- 15.1.1. Knowing the potential risk of release or misuse of data and applications under their control or under the control of their subordinates;
- 15.1.2. Defining access policy with respect to applications, desktop hardware, and data and managing access rights consistent with such risk;
- 15.1.3. Allocating appropriate access authorizations to ITD personnel in writing or through normal application authorizations (at least one ITD staff will normally have the highest level of authorization);
- 15.1.4. Managing the access right allocation, modification, and termination within the capabilities of their applications package(s);
- 15.1.5. Training account holders with access rights on their responsibilities with respect to release and use of the data and use of the applications; and
- 15.1.6. Ensuring that any non-employee personnel with access to County data through their organization (whether such personnel have accounts or not) are fully aware of their responsibilities with respect to the data.

15.2. Personnel with access rights to County data have the following responsibilities:

- 15.2.1. Understanding the rights and duties with respect to the data and application system functions to which they have access;
- 15.2.2. Understanding the potential risk of release or misuse of data and applications under their control; and
- 15.2.3. Immediately communicating to supervisors and ITD any actual or suspected violation of County policies or practices with respect to misuse of data.

15.3. ITD personnel have the following responsibilities:

- 15.3.1. ITD personnel shall not modify data in any applications system without the consent of the supervisor responsible for the accuracy and reliability of that data;
- 15.3.2. ITD personnel may make immediate modifications with verbal authorization from an appropriate supervisor if a system is experiencing severe operational problems and ITD intervention is necessary to restore functionality to the system;
- 15.3.3. ITD personnel modifying applications data will normally inform the appropriate supervisor(s) in writing of their activities and results. If ITD activities bypass the audit/security controls in a system, ITD personnel are required to document their changes in writing to both the supervisor and ITD management;
- 15.3.4. ITD personnel should assist supervisors and personnel in understanding the potential risk of release or misuse of data and applications under their control; and
- 15.3.5. ITD personnel are responsible for hardware and software tool security (e.g. operating systems, data base systems). ITD personnel who become aware of actual or suspected breach of that security shall immediately report such breach to the appropriate applications supervisor and ITD management.

16. Usage Policy Overview

IT resources are critical assets for County operations. To encourage the effective and appropriate use of the County's IT resources, the following usage policies apply to all account holders.

- 16.1. County account holders are expected to use IT assets to maintain their job performance, provide services to customers, and support County operations. The specific tasks to be performed are specified by supervisors, but normally include the following:
 - 16.1.1. Regular and timely usage of email;
 - 16.1.2. Knowledge of desktop computing basics;
 - 16.1.3. Familiarization with computer applications necessary to perform their job functions; and
 - 16.1.4. Usage of the Internet as an information resource for acquiring and using information relevant to their work.
- 16.2. Account holders shall utilize County IT resources solely for County business purposes except as otherwise specifically allowed by this policy and shall conduct themselves in a manner consistent with appropriate standards as established by existing County policies, rules, regulations and guidelines. All existing County policies, rules, regulations and guidelines relating to intellectual property protection, privacy, misuse of County equipment, sexual harassment, sexually hostile work environment, data security, and confidentiality apply to use of IT resources.
- 16.3. All data stored on networked data storage will be backed up nightly Monday through Friday by ITD. The account-holder is responsible for removing data files that are no longer needed in order to effectively manage limited storage space. The account holder

- is responsible for creating and maintaining backups of data on non-networked drives or data that needs to be backed up more frequently than nightly.
- 16.4. Should an account holder suspect their computer is infected with a virus or other unwanted software, or suspect their computer is not protected against viruses, they should immediately disconnect their computer from the network and contact ITD.
 - 16.5. Account holders should take appropriate protective measures to minimize the probability that their addresses will become targets for spam.
 - 16.6. Account holders shall have no expectations of privacy with respect to County IT resource usage. Data that is protected or otherwise confidential by operation of local, state or federal law, rule, regulation or policy must be protected by the account holder.
 - 16.7. Computer-based data available to the public under the New Mexico Inspection of Public Records Act, § 14-2-1 *et. seq.*, NMSA 1978 Comp. shall be released, if requested, consistent with and as required by the Act.

17. Usage Policy: Prohibited Use

IT resources are powerful tools purchased to increase productivity and improve the employee's work environment. Misuse of these powerful tools may subject an account holder to disciplinary action. Misuse that is intentional, ongoing, or extensive will be grounds for severe disciplinary action. Account holders should be thoroughly aware of the following prohibited uses, and, if any questions arise, contact Human Resources or ITD.

- 17.1. Account holders shall use County IT resources only for official County business unless otherwise specifically allowed in this policy.
- 17.2. Account holders shall not upload or otherwise transfer out of the County's direct control any software licensed to the County nor data owned or licensed by the County without explicit authorization from the supervisor responsible for the software or data.
- 17.3. Account holders shall not use IT resources to reveal confidential or sensitive information, client data, or any other information covered by existing county, state or federal privacy or confidentiality laws, regulations, rules, policies, procedures, or contract terms. Account holders who engage in the unauthorized or otherwise illegal release of confidential information via the County's IT resources, including but not limited to newsgroups or chat rooms, shall be subject to sanctions imposed by existing County policies and procedures associated with unauthorized release of such information or other relevant and appropriate policies, procedures, rules and regulations in addition to disciplinary action arising from misuse of IT resources.
- 17.4. IT assets may not be used to solicit or forward commercial ventures, religious or political causes, solicitation of Union membership or the conducting of official Union business, or solicitations for outside organizations, except as may be specifically authorized by the County Administrator. This does not limit an account holder's rights and responsibilities to distribute any document or information used in legitimate County operations, e.g. vendor proposals, zoning or permit requests, etc.

- 17.5. Account holders shall respect the copyrights, software, licensing rules, property rights, privacy, and prerogatives of others, as in any other business dealings. In particular, according to the US Copyright Law, illegal reproduction of software can be subject to civil damages of as much as \$100,000 per work copied, and criminal penalties, including fines and imprisonment. Los Alamos County prohibits the illegal duplication of software or acquiring or using illegal copies of software.
- 17.6. Account holders shall not load executable software, including freeware and shareware, on their personal computers unless directly applicable to performing their job responsibilities and approved by their supervisor and ITD. If a supervisor or County contract manager has determined that privately owned software or shareware or freeware is necessary for an account holder to perform his or her duties, and it cannot be purchased by the County, it must be approved in writing by ITD before installation on a Los Alamos County computer. Approval will require 1) proof of ownership 2) virus checking by ITD personnel; 3) that the software be compatible, in ITD's judgment, with existing County hardware and software.
- 17.7. Account holders shall not use County IT resources to download or distribute pirated software or data, including music or video files.
- 17.8. Account holders shall not use County IT resources to deliberately propagate any malicious code.
- 17.9. Account holders shall not use County IT resources to intentionally disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of the County's IT resources.
- 17.10. Unauthorized dial-up access to the Internet is prohibited from any device that is attached to any part of the County's network. Account holders shall not use the County's IT resources to establish connections to non-County Internet service providers unless they are authorized to do so in writing by ITD.
- 17.11. Account holders shall not access, store, display, distribute, edit, or record sexually explicit or extremist material using County IT resources. The incidental and unsolicited receipt of sexually explicit or extremist material, such as might be received through email, shall not constitute a violation of this section, provided that the material is promptly deleted and neither stored nor forwarded to other parties. The account holder shall report to ITD and the account holder's supervisor the repeated receipt of such material.
- 17.12. Account holders are prohibited from accessing or attempting to access IT resources for which they do not have explicit authorization by means of user accounts, valid passwords, file permissions or other legitimate access and authentication methods.
- 17.13. Account holders shall not use County IT resources to override or circumvent any security mechanism belonging to the County or any other government agency, organization or company.

- 17.14. Account holders shall not use County IT resources for illegal activity, gambling, or to violate the laws or regulations of the United States, any state or local jurisdiction, or any other nation.

18. Usage Policy: Personal Use of County IT Assets

Occasional and incidental personal use of the County's IT resources, including Internet, email, and phones is allowed subject to limitations. If account holders have any questions about allowable personal use, they should consult their supervisors. Departments may set departmental personal use policies differing from this policy with the approval of the County Administrator. After approval, those policies shall be forwarded to ITD for inclusion in this policy as an Appendix.

Personal use of County IT resources is not considered occasional and incidental if such use:

- 18.1. materially interferes with the use of IT resources by County staff, agents, representatives, officials or contractors;
- 18.2. burdens the County with additional costs;
- 18.3. interferes with the account holder's employment duties or other obligations to the County;
- 18.4. consumes a consequential amount of an account holder's time on the job;
- 18.5. includes any activity that is prohibited under this policy;
- 18.6. is a part of an ongoing for-profit business activity or unauthorized non-profit business activity; or
- 18.7. might reasonably be expected to cast the County, its employees, agents or representatives in a bad light or subject them to public ridicule

Note that allowing occasional and incidental use does not confer any expectation of privacy or ownership as a result of personal use. All email, phone records, systems and Internet access records, and data on County equipment may be public records subject to disclosure under the New Mexico Inspection of Public Records Act, whether used for County business or for incidental personal use. Employees should assume that any records, including personal records stored on County equipment, may be disclosed under that Act. The contents of such records may be disclosed within the County as allowed in Section 20 and approved in Appendix A without the knowledge of the employee.

19. Remote Computing

The County may allow or require selected account holders to access the County network and systems from home or while traveling. This access is granted for the convenience of the County and places specific obligations on the remote access account holder.

Systems security on County-owned laptops must meet the same requirements as systems security on any other County-owned machine. If account holders have any questions, they should call the ITD help desk.

Access to County email through the Internet does not require any special software or controls, although the County recommends all users have up-to-date anti-virus software on personal

machines. The County also recommends account-holders acquire anti-spyware software, install a firewall, and use caution when downloading software on their personal machine.

Account users who access the County network behind the firewall will need to have a County-owned laptop for this purpose. The County-owned laptop will conform to all provisions of this policy and, upon request, will be brought into ITD for review of machine setup, security, and operating practices. Such review shall be conducted upon reasonable notice to the account-holder. If County account-holders have any questions about remote access responsibilities, they should call the help desk.

Access of mobile devices including Personal Data Assistants (PDAs), Internet Enabled Cellular Phones, Wearable Computers, Flash Drives, Wireless Access Points, Switches, and Portable Computers to the County network will be allowed as follows:

The user of the mobile device will accept responsibility for taking reasonable precautions in protecting the data on the mobile device and agrees to adhere to this policy. The mobile device user will not be allowed to have administrative rights on the network unless granted by a special exception by the IT Systems Manager or designee. The user of the mobile device agrees to abide by the IT Technology Usage and Computer Security Policy. Any device that is connected at any time to the County network must adhere to the following:

- a. Devices connected to the County network must be determined to be a benefit to the County and to not impede the ability of the IT division to provide support to the County by the IT Manager or designee rather than a convenience.
- b. The Department Director or designee must submit the request to add the device.
- c. Any mobile device that can store County data must support encryption of the data; County data on mobile devices must be encrypted at all times.
- d. All mobile devices owned by the County or allowed on the County network must be identified by their MAC address to the IT division before being connected.
- e. The mobile device operator must be identified by name and contact information to the IT division.
- f. The mobile device operator must be familiar with the Information Technology Usage and Security Policy for Los Alamos County.

Devices not owned by the County on the County network are subject to software audit to ensure that no software that could threaten the network security is in operation. All computing devices are subject to a software audit at any time.

20. Enforcement and Sanctions

The County may install software and/or hardware to monitor and record IT resource usage, including email, Internet usage, telephone usage, and all files stored on County systems. All automated monitoring will be set up by ITD staff, must meet the authorizing criteria below, be authorized in writing, specify a time period, specify the assets to be monitored, and specify who will have access to the results.

The County Administrator may authorize ITD to perform temporary or permanent monitoring of individuals, organizational units, or all County account holders. Based on a complaint or a supervisor's request, a Department Head, with the concurrence of Human Resources, may authorize ITD to monitor an individual account holder. Records of such monitoring as well as the contents of monitored accounts are subject to standard County personnel records management and retention policies.

This policy on monitoring does not change supervisory responsibility for normal oversight of work activities. Supervisors with concerns about specific employees or activities should bring those concerns to Human Resources. This policy also does not change the responsibility for all account holders to report suspected misuse of County IT resources.

Serious disciplinary action, consistent with the County's Personnel Rules and Regulations, up to and including termination of employment may result from activity prohibited by this Policy. In the case of a contractor, the County may seek damages, penalties and any remedy available at law or in equity. Illegal activity involving County IT resource usage may be referred to appropriate authorities for prosecution.

In agencies or offices where exceptions to this policy are within legitimate job responsibilities, the County Administrator, or the Administrator's designee, may exempt one or more account holders from relevant portions of this policy. The exemption will be in writing with copies to the supervisor, Human Resources, and ITD.

ITD may immediately disable any account that is reasonably suspected of misuse or a security breach. ITD will immediately notify the relevant County supervisor(s) and Human Resources and retrieve pertinent account holder data and access records.

21. Technology Components of Security

ITD is responsible for putting in place technology-based perimeter defenses and insider defenses. The details of these defenses will not be released except on a need-to-know basis because of the potential guidance such details could give to individuals attempting unauthorized use. The sections containing the details are marked appropriately and are included in copies of this plan held by members of the Management Oversight Committee and ITD Staff.

Defenses include such tools as: network firewalls; virus detection and cleaning software and/or hardware; need-to-know separation; centralized account management and activity recording; and IT asset monitoring software and hardware.

Discussion of these security protection details outside of the Management Oversight Committee members and ITD staff and ITD's contactors without approval of the County Administrator or the Administrator's designee is a violation of this policy.

ITD is also responsible for establishing and enforcing all WLAN technology standards and will be the sole provider of design, specification, operation, maintenance and management services for all wireless access points. Employees may not independently install or operate WLAN access points in their departments. Only County employees and authorized visitors may use the County WLAN based upon the needs of the County; exceptions must be authorized by the IT Manager or designee. All WLANs must be configured according to County IT security standards. ITD is

responsible for managing the security of the County WLAN. All WLAN communications must be encrypted. All wireless devices using the County WLAN must be registered with ITD.

22. Backup and Recovery

All network data will be backed up regularly by ITD and stored offsite to minimize loss in the case of equipment or software failure. ITD will also maintain redundant hardware and automated failover for critical applications. Details are included in the ITD Disaster Recovery Plan.

Account holders should not store valuable County files or other County data on their personal computer. Central drives backed up as part of ITD's regular backup process are provided for storage of such files and data. Questions about this process or data backup/recovery should be referred to the help desk.

23. Definitions

As used in this policy:

- 23.1. **access** means the ability to read, change, or enter data using a computer or an information system.
- 23.2. **equipment** means computers, monitors, keyboards, mice, routers, switches, hubs, networks, or any other information technology assets.
- 23.3. **County-owned** includes equipment the county leases or controls under contract.
- 23.4. **freeware or shareware** means software that is available free of charge and available for download from the Internet. Freeware is protected by a copyright and is subject to applicable copyright laws.
- 23.5. **information technology resources (IT resources)** means computer hardware, software, databases, electronic message systems, communication equipment, computer networks, telecommunications circuits, or any information used by a County agency to support programs or operations that is generated by, transmitted within, or stored on any electronic media.
- 23.6. **malicious code** means any type of code intended to damage, destroy, or delete a computer system, network, file, or data.
- 23.7. **pirated software** means licensable software installed on a computer system for which a license has not been purchased or legally obtained.
- 23.8. **physical control** means knowing where your information technology resources are and knowing that they are not being misused.
- 23.9. **reconfigure** means any software, hardware, or parameter change that changes network address, computer name, operating system (e.g. Windows to Linux), computer security software, or function (e.g. creates a server from a workstation).
- 23.10. **security mechanism** means a firewall, proxy, Internet address-screening or filtering program, or other system installed to prevent the disruption or denial of services or the unauthorized use, damage, destruction, or modification of data and software.

- 23.11. **sexually explicit or extremist materials** means images, documents, or sounds that can reasonably be construed as:
- 23.11.1. Discriminatory or harassing;
 - 23.11.2. defamatory or libelous;
 - 23.11.3. obscene, of a primarily sexual nature, or pornographic;
 - 23.11.4. threatening to an individual's physical or mental well-being; or
 - 23.11.5. read or heard for any purpose that is illegal.
- 23.12. **strong password** means a password that is case sensitive; at least eight characters in length; and containing at least one capital letter, one lower case letter, one number, and one special character. This reduces the likelihood of guessing a password, but because the user can create their own password, it is not completely secure. An individual attempting to crack an eight character strong password using a single computer would take approximately 321 days compared to a six character mixed password which would take about 5.8 hours to crack. Most hackers use multiple computers to try and crack passwords.
- 23.13. **virtual private network (VPN)** means an encrypted communication link established between a remote device and the County network via the internet.
- 23.14. **WLAN** means a wireless local area network in which a mobile user can connect to a local area network through a wireless (radio) connection.
- 23.15. **Account holder** means an individual who has been authorized to access County IT resources and given an account, who is using County IT resources, and who meets one of the following criteria.
- 23.15.1. an employee of Los Alamos County;
 - 23.15.2. an elected official of Los Alamos County;
 - 23.15.3. an individual working under contract to the County; or
 - 23.15.4. a volunteer providing service to the County.

Appendix A: Acknowledgement Form

Los Alamos County

Information Technology Account Holder Acknowledgement Form

I understand that Los Alamos County information technology resources are for official business only, except where there is occasional and incidental personal use allowed by policy. There shall be no expectation of privacy in the use of Los Alamos County information technology resources. My information technology resources, including county-owned equipment used offsite, and all software programs and associated data are subject to waste, fraud, and abuse audits and monitoring by assigned County personnel at any time. I understand that audits and monitoring of County information technology resources that I use may be authorized and conducted without my knowledge and I hereby consent to any such audits and monitoring, except that audits of County equipment maintained offsite may be conducted only upon reasonable notice and at reasonable times.

I have read this form and the Los Alamos County Information Technology Usage and Security Policy. I acknowledge my responsibilities as an account holder, and agree to follow all the procedures and requirements set out in the Los Alamos County Information Technology Usage and Security Policy. I understand this document will be kept in my Personnel folder during my employment with Los Alamos County or, in the case of a contractor, the County contract file.

Account Name _____ Date _____

User Name _____ Number/Contract No. _____

User Signature _____

I validate that the above user has a need to access Los Alamos County computing resources in the performance of his/her duties and has a need-to-know for the information processed by the Los Alamos County computing resources related to his/her duties.

Supervisor/County contract supervisor/County Administrator Name _____ Date _____

Supervisor/County contract supervisor/County Administrator Signature _____

**Los Alamos County
Computer Security Policy
Appendix B**

Appendix B: Master Computer Protection Plan

MASTER COMPUTER PROTECTION PLAN

Incorporated County of Los Alamos

In fulfillment of the requirements of DOE Order 1360.2B, "Unclassified Computer Security Program."

M. Wayne Budwine
U.S. Department of Energy
Computer Security Operations
Manager Representative

Date

Los Alamos County Computer Security Policy Appendix B

Purpose

This Master Computer Protection Plan (MCP) addresses the requirements and responsibilities for establishing and maintaining a secure operating environment for computer systems that process unclassified and sensitive unclassified information. Unclassified information is that which is open for public use with no restrictions. Refer to the attachment for the definition of sensitive unclassified information.

Scope

This MCP applies to all Incorporated County of Los Alamos, hereinafter referred to as County, computer systems that are used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of unclassified data and information located on County-controlled property, as well as those used outside of County-controlled property by its employees.

Responsible Personnel

The following personnel are responsible for protecting information from unauthorized access, disclosure, modification, and destruction: (1) County Administrator, (2) County Information Technology (IT) Director, and (3) Computer Users. Computer users have primary protection responsibility for their systems, their primary and backup storage media, and the data on them. The IT Department has primary protection responsibility for centrally maintained systems, their associated media, and the data on them.

Administrative Safeguards

Computer users will be authorized, in writing, by their supervisors, County contract managers, or higher-level management, for access to information on a need-to-know basis. This information is to be utilized for official purposes only. Users will acknowledge their responsibilities by executing an *Account Holder and Computer Users Responsibilities* form included in the *Los Alamos County Computer Security Policy*.

County computer training provided to every computer user will address the requirements for maintaining a secure operating environment. Periodic security awareness training will be accomplished through initial briefings, completion of the *Account Holder and Computer Users Responsibilities* form, meetings, or by distribution of pamphlets, flyers, and memoranda.

Periodic reviews to detect and deter computer misuse and abuse will be conducted. The County will also conduct computer security self-assessment reviews, at

Los Alamos County Computer Security Policy Appendix B

least annually, to verify that information is being protected. As part of that annual review, this MCPP will be reviewed and updated as necessary. DOE will conduct periodic random program reviews to verify compliance with computer security requirements.

Disaster recovery/contingency planning should address information for backup and recovery as well as alternative processing measures to be activated should a computer system fail to operate. These plans will vary in detail based on the system and the need for its availability. Generally, a disaster recovery/contingency plan for a microcomputer is as simple as finding another compatible system to use. Extensive testing of these plans is not required.

Technical Safeguards

Anti-viral software is required on all systems. Media not originating on a County computer is to be checked for potential viruses prior to being placed into service. Computer users are encouraged to protect sensitive information by employing password screen savers, computer locks, desk or office locks, or other means of securing their workstations.

If available, user IDs, passwords, and audit trails will be utilized to control and monitor access to information on multi-user systems. Each user ID and password combination is intended for use by a single individual and should not be shared with or revealed to any other individual.

Prior to computers being released from the County, systems will be sanitized or memory overwritten so that no information is retained. This is to ensure that sensitive unclassified information is not revealed to unauthorized individuals.

DOE will be notified prior to any Internet connections and appropriate security measures will be implemented.

Physical Safeguards

The security environment is dependent upon the physical location of the computer system. Best business practices will be used to ensure that the level of physical security is appropriate to the value of the system hardware and software and the sensitivity of the data it processes.

**Los Alamos County
Computer Security Policy
Appendix B**

**SENSITIVE UNCLASSIFIED INFORMATION
SUMMARY SHEET**

DEFINITION:

As defined in the National Telecommunications and Information Systems Security Policy, NTISSP #2, sensitive unclassified information is:

Information for which disclosure, loss, misuse, alteration, or destruction could adversely affect national security or Federal government interests. National security interests are those unclassified matters that relate to the national defense or foreign relations of the U. S. Government. Other government interests are those related, but not limited to the wide range of government or government-derived economic, human, financial, industrial, agriculture, technological, and law-enforcement information, as well as the privacy or confidentiality of personal or commercial proprietary information provided the U. S. Government by its citizens. Information found within the ADP system and its associated telecommunications system clearly falls into this category.

SENSITIVE unclassified information:

- That which requires discretionary protection due to statutory or regulatory restrictions
- Legal information
- Privacy Act information; personnel data, personal identifying information, payroll
- Caveat marked documents; Official Use Only or other headings/footings
- UCNI (Unclassified Controlled Nuclear Information)
- Proprietary Data; privileged information
- Technical Scientific data
- Limited Access information
- Other information denoted as needing protection

Appendix C: ITD Supported Applications

IT Support –

IT Support is available through the automated knowledge base or by submitting a request to IT in the Right Now Technology (RNT) tracking system.

Requests are entered into RNT by submitting a request through the link to RNT on the intranet, sending an email to IT Request, which creates a request in RNT, or by calling 662-8090 for emergency situations during work hours.

The knowledge base is available to employees 24x7. To get into the RNT system from the intranet, open Internet Explorer, click on IT Support and search the answers. There are over 20,000 answers in the IT knowledge base relating to the Applications used throughout Los Alamos County. If you are unable to find your answer in the automated help, you can submit a request from that site by clicking on the Ask IT or IT Requests button and submitting a request. By using your account and password, you can login and monitor your request as it progresses.

Emergency Support –

Call out support for emergency IT situations is available 24x7 by calling 662-8222 and asking them to page the IT person on call. This may result in a charge back to the Department. 24x7 automated support is always available by going to the intranet and clicking on IT Support and searching answers. There are over 20,000 answers in the IT knowledge base. End users can also submit a request by clicking on the Ask IT or IT Requests button and submitting a request. They can login and monitor their request as it progresses.

ITD Supported Hardware

1. **Approved hardware purchases.** Departments with budget approval can request a standard client PC from the Warehouse. If the department has special requirements or needs a notebook, they can place a written work request to IT explaining the requirements and asking for a special quote. IT will provide the quote to the department and the department will be able to order the computer through Procurement. Once the computer is ordered, either from the Warehouse or by Procurement, the manager of the person receiving the computer (or a person to whom that manager has delegated that authority in writing to IT) needs to fill out a computer request on the intranet.
2. **Approved portable device purchases.** IT will keep a list of currently supported Phone/PDA/Hand-held devices supported by IT on the intranet. If a department purchases a device that is not on that list, it will not be supported unless the following steps are taken:
 - Review by IT to ensure that device can be supported
 - Purchase by the Department of specific device for IT so that support can be provided

- Purchase by the Department of any software required to provide support for the portable device
3. **Client Hardware replacement policy.** Hardware will be purchased with a three year warranty for hardware support. Hardware will be supported by IT in conjunction with the vendor for up to four years after the hardware was purchased, as long as it is in good functioning order. If the computer fails between the three and four year time frame, the department will be asked to replace the hardware with a new unit. Replacement of hardware every four years is not an optional budget item and computers older than four years of age are subject to being removed from the network in order to maintain network security and operability.

ITD Supported Applications

Supported Applications-

Definitions from webopedia.com:

Application - A program or group of programs designed for end users. Software can be divided into two general classes: systems software and applications software. Systems software consists of low-level programs that interact with the computer at a very basic level. This includes operating systems, compilers, and utilities for managing computer resources.

In contrast, applications software (also called end-user programs) includes database programs, word processors, and spreadsheets. Figuratively speaking, applications software sits on top of systems software because it is unable to run without the operating system and system utilities.

End User - The final or ultimate user of a computer system. The end user is the individual who uses the product after it has been fully developed and marketed. The term is useful because it distinguishes two classes of users, users who require a bug-free and finished product (end users), and users who may use the same product for development purposes. The term end user usually implies an individual with a relatively low level of computer expertise. Unless you are a programmer or engineer, you are almost certainly an end user.

Client - The client part of a client-server architecture. Typically, a client is an application that runs on a personal computer or workstation and (usually) relies on a server to perform some operations. For example, an e-mail client is an application that enables you to send and receive e-mail.

On the client side, IT fulfills the following duties for supported applications:

- provides support for the installation of software, both systems and applications

- ensures the supported applications are compatible with supported operating systems and other supported programs
- works with the vendor to resolve problems
- retains installation media
- provides information on costs to allow departments to budget and purchase hardware and/or software to allow them to maintain compliant levels to meet supported vendor specifications for client machines and applications
- installs current levels on hardware, operating systems and application software in compliance with the Application vendors specifications

On the server side, IT fulfills the following duties for supported applications:

- provides support for the installation of applications,
- ensures the supported applications are compatible with supported operating systems and other supported programs
- works with the vendor to resolve problems.
- retains installation media,
- backs up application components on the server
- maintains current levels on hardware, operating systems and application software in compliance with the Application vendors specifications
- work with vendor and end users to get costs for departments to upgrade server side application components for budget purposes as needed
- budgets and pays for software maintenance for applications that are used centrally
- Understand and maintain interfaces to share data between applications
- Determine and maintain single data source for use throughout the County
- Outsource support to vendors based upon cost, staff and support requirements

End Users have the following responsibilities for supported applications:

- Backup data that is not stored on network drives
- Pay for licenses for individual productivity programs
- Pay for client access licenses as needed
- Pay for support for applications that are used in one department
- Work with vendor/IT staff as necessary to resolve problems within applications
- Notify IT when problems occur through approved mechanism
- Maintain inventory and control of department owned hardware and software most of which is available through reports that the department can run from the County inventory/stores order systems
- Keep machines and operating systems updated via replacement when the machine reaches four years from the date of purchase
- Ensure that the application licenses have been purchased and kept at supported levels for licenses purchased and/or maintained by the departments

- Submit interdepartmental requests and bring IT projects before management oversight committee for approval/resources
- Designate departmental project manager for projects
- Maintain appropriate departmental resources with expertise in the use of the application
- Keep up-to-date with enhancements to applications and coordinate the installation of these features with IT

ITD Permitted Applications and Hardware

Permitted Applications-

Permitted applications are applications for which IT does not provide direct support, but are on the County network with IT's knowledge and approval. These applications generally are supported by the vendor with Department/Division staff coordinating the support. Permitted applications are reviewed on a case by case basis. On occasion, a permitted application may cause conflicts with supported applications. In those cases, the permitted applications will be removed from the machine on which they are causing problems and the Department/Division may allocate a separate machine to run the permitted application.

Permitted Hardware Devices-

Permitted hardware devices are devices for which IT does not provide direct support, but are on the County network with IT's knowledge and approval. These devices generally are supported by the vendor with Department/Division staff coordinating the support. Permitted devices are reviewed on a case by case basis. On occasion, a permitted device may cause conflicts with supported devices or applications. In those cases, the permitted device will be removed.

A list of supported applications and devices will be provided by ITD.



INCORPORATED COUNTY OF LOS ALAMOS ADMINISTRATIVE PROCEDURE GUIDELINE

Index No. 1240

Effective Date: October 7, 2012

LOS ALAMOS COUNTY PERSONAL MOBILE DEVICE ACCEPTABLE USE POLICY

I. Purpose

The purpose of this policy is to define standards, procedures, and restrictions for end users who have legitimate business uses for connecting a personally owned mobile device to Los Alamos County's (LAC) corporate network and choose to do so. Foremost, the purpose is to protect the integrity of the confidential data that resides within LAC's technology infrastructure. This policy intends to prevent this data from being deliberately or inadvertently stored in an unsecured method on a mobile device or carried over an unsecure network where it could potentially be accessed by unauthorized entities.

II. Policy

It is the policy of LAC that any employee who uses a personal mobile device to access LAC resources ensures security protocols are used in the management of data. Employees that utilize personal mobile devices while conducting LAC business shall do so in a professional manner and shall provide all County records to the County in accordance with County policy 0310 – Records and Information Management Governance Policy.

The following shall be observed:

- A. Prior to consideration of mobile device usage on LAC network or applications, requests for mobile access must be approved and submitted to Information Management (IM) by employee's supervisor. Supervisor consideration shall be consistent with Personnel Rules and Regulations (which may be amended from time to time) as well as other LAC policies.
- B. Some devices, depending upon type and operating system, may or may not be able to integrate with the LAC network. IM will maintain a list of accepted mobile platforms known to integrate with LAC's network. This list will be updated periodically.
- C. End users who wish to connect mobile devices to non-LAC network infrastructure to gain access to enterprise data must employ LAC approved VPN for their

devices. Enterprise data is not to be accessed on any hardware that fails to meet LAC's established enterprise IM policies.

- D. All mobile device connections to the LAC network through the Internet shall come through automated technology which will inspect the personal device including data and applications on that device. The automated technology will be centrally managed by IM. The automated technology is not configured to keep a log of applications and data on the device.
- E. In order to secure data management, the following shall be adhered to with regard to security:
 - 1. Employees using mobile devices and related software for network and data access shall use secure data management procedures and reasonable physical security measures as outlined in 1210-IT Security and Usage Policy (which may be amended from time to time).
 - 2. Any mobile device that is being used to store LAC data must adhere to the authentication requirements (e.g., login credentials, smart cards, fobs, certificates, etc.) of LAC and other applicable agreements, (i.e., end user license agreements, joint powers agreements, etc.) regulations and laws. In addition, all hardware security configurations must be pre-approved by taking to IM for inspection before any enterprise data-carrying device can be connected to the LAC network.
 - 3. IM will manage security policies, network, application and data access centrally using automated technology. Any attempt to bypass security implementations will be deemed an illegal or improper intrusion attempt and will be dealt with in accordance with 1210-IT Security and Usage Policy (which may be amended from time to time).
 - 4. Employees, contractors, and temporary staff will follow all enterprise-sanctioned data removal procedures to permanently erase County data from such devices once its use is no longer required. Before an employee discontinues use of a device for work purposes or disposes of the device, it is the employee's responsibility to either remove County data from the device and notify IM that they have done so or contact IM for help in removing the data which may include a request that the device be wiped remotely. In the event that the employee does not notify IM that they have permanently erased County data from their device, the device will be wiped remotely upon notification to IM that the staff member no longer works for the County.
 - 5. In the event of a lost or stolen mobile device, it is incumbent on the user to report the incident to IM prior to contacting the mobile device vendor so appropriate data wipe activities can occur. This should be done immediately when the device is noticed missing. The device will be remotely wiped of all data and locked to prevent access by anyone other than IM. If the device is recovered, it can be submitted to IM for re-provisioning. The LAC Remote

Wipe Waiver, which ensures that the user understands that their personal data shall be erased in the rare event of a security breach, shall be agreed to in writing before connecting the device to LAC resources.

III. Help and Support

- A. IM reserves the right, through policy enforcement and any other means it deems necessary, to limit the ability of end users to transfer data, including personal data, to and from specific resources on the enterprise network.
- B. Employees, contractors, and temporary staff will make no modifications to the hardware or software that change the nature of the device in a significant way (e.g. replacing or overriding the operating system) without the express written approval of IM.

IV. Organizational Protocol

- A. IM establishes audit trails, which will be accessed, produced and used as may be required by law. Such trails will be able to track the attachment of an external device to the LAC network, and the resulting reports may be used for investigation of possible breaches and/or misuse or for any other reason deemed appropriate by the County. This monitoring is necessary in order to identify accounts/computers that may have been compromised by external parties. As part of the written waiver, the end user agrees that his or her access and/or connection to LAC's networks may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity.
- B. The end user agrees to immediately report to his/her manager and IM any incident or suspected incidents of unauthorized data access, data loss, and/or disclosure of County resources, databases, networks, etc.

V. Responsibility

- A. Connectivity of all mobile devices will be centrally managed by LAC's IM Division and will use authentication and strong encryption measures. Although IM will not directly manage personal devices which connect to the LAC network, end users are expected to secure these devices when connected to non-LAC networks/resources (see Section 2.5.5 and 2.7 for additional information). Addition of new hardware, software, and/or related components to provide additional mobile device connectivity will be managed by IM. Non-sanctioned use of mobile devices to back up, store, and otherwise access any enterprise-related data is prohibited.
- B. This policy applies to all LAC employees, including full and part-time staff, contractors, and other agents who use a personally-owned mobile device to access, store or back up any LAC data. LAC does not automatically guarantee the initial or ongoing ability to use these devices to gain access to LAC networks and information.

- C. This mobile device policy applies to all LAC-supported devices.
- D. The policy applies to any hardware and related software that is not LAC owned or supplied, but could be used to access LAC resources. That is, devices that employees have purchased for personal use but also wish to use in the business environment.

VI. Violations

- A. Failure to comply with this policy may result in immediate suspension of that user's account. A breach could result in loss of information, damage to critical applications, loss of revenue, and damage to the LAC public image. Therefore, all users employing a mobile device connected to LAC's network, and/or capable of backing up, storing, or otherwise accessing LAC data of any type, must adhere to the LAC-defined processes for doing so.

The policy addresses a range of threats to, or related to the use of, enterprise data:

Threat	Description
Device Loss	Devices used to transfer or transport work files could be lost or stolen.
Data Theft	Sensitive LAC data is deliberately stolen and sold by an employee or unsanctioned third party.
Malware	Viruses, Trojans, worms, spyware and other threats could be introduced via a mobile device.
Compliance	Loss or theft of financial and/or personal and confidential data could expose LAC to the risk of non-compliance with various identity theft and privacy laws.

- B. Information Management (IM) reserves the right to refuse, by physical and non-physical means, the ability to connect personal mobile devices to LAC and LAC-connected infrastructure. IM will engage in such action if such equipment is being used in a way that puts the LAC's systems, data, users, and clients at risk.

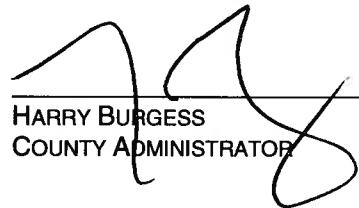
This policy is complementary to any previously implemented policies dealing specifically with data access, data storage, data movement, and connectivity of devices to any element of the enterprise network.

Failure to comply with the *Personal Mobile Device Acceptable Use Policy* may, at the full discretion of LAC, result in the suspension of any or all technology use

and connectivity privileges, disciplinary action, and possibly termination of employment.

VII. Definitions

Enterprise Data	Any information, whether a record or elements that can create a record, used in conjunction with LAC business, shared by many users throughout the organization.
Mobile Device	Any portable electronic device used to store information and communicate within/outside of LAC resources; SmartPhone, tablet PC, laptop
SSL	Secure Socket Layer are cryptographic protocols that provide communication security over the Internet.
VPN	Virtual Private Network is used to privately interconnect remote users through public communication infrastructure in a secure method.


HARRY BURGESS
COUNTY ADMINISTRATOR

10/4/13
DATE



LOS ALAMOS
where discoveries are made

INCORPORATED COUNTY OF LOS ALAMOS ADMINISTRATIVE PROCEDURE GUIDELINE

Index No. 0310

Revision Date: November 28, 2017

RECORDS AND INFORMATION MANAGEMENT GOVERNANCE POLICY

I. Purpose

The purpose of this policy is to establish consistent record and information management governance practices for all County employees, contractor employees, governing and advisory boards and commissions, appointed and elected officials who create records in connection with the transactions of County business. The Incorporated County of Los Alamos is committed to an effective Records and Information Management (RIM) program that includes all legal/regulatory requirements for protection, confidentiality and security and will show due diligence and best efforts in the governance of electronic information and hardcopy records. The Incorporated County of Los Alamos (ICLA) recognizes the need for the optimization of space and cost of retaining public records in any medium that have met their required retention within its custody. This policy applies to all record formats, created and stored on paper, electronic (in all its variations), e-mail, social media and web based platforms or any other mediums where County records may reside.

II. Definitions

- A. **Active Record:** Record needed to perform current operations, subject to frequent use, and usually located near the user, also known as a current record.
- B. **Appraisal:** Records analysis; the process of evaluating records based on their current operational, regulatory, legal, fiscal and historical significance, their informational value, and their arrangement and relationship to other records.
- C. **Confidential Information:** Information that can be found in records that may pertain to personal identifiable information (PII) or that should be protected and private under the Inspection of Public Records Act (§14-2-1 NMSA 1978) or as otherwise provided by law or County policy.
- D. **Disposition:** Destruction of records; prior notice to State Records Administrator

(§ 14-1-8, NMSA 1978). An official charged with the custody of any records and who intends to destroy those records, shall give notice by registered or certified mail to the State Records Administrator, State Records Center, Santa Fe, New Mexico, of the date of the proposed destruction and the type and date of the records intended to destroy. The notice shall be sent at least sixty days before the date of the proposed destruction. If the State Records Administrator wishes to preserve any of the records, the official shall allow the State Records Administrator to have the documents by calling for them at the place of storage.

- E. **Electronic Record:** Data or information that has been captured and fixed for storage and manipulation in an automated system and that requires the use of the system to render it intelligible by a person. Computer-generated information such as an e-mail message, document or image file created or received by the County in pursuance of law or in connection with the transactions of public business.
- F. **E-mail:** Information transmitted electronically over a communication network. A system that enables people to compose, send, receive and manage electronic messages and images across networks.
- G. **Essential Information:** Records designated by management as essential to the operational functions outside its normal parameters to provide business continuity during an emergency response.
- H. **File Plan:** A hierarchical structure of folders within a filing structure that provides a coherent location in which records can be stored, searched or retrieved.
- I. **Generally Accepted Recordkeeping Principles:** Through the use thereof allow an organization to create, organize, secure, maintain and use records in a way that effectively supports the activity of that organization. These principles are as follows:
 - (1) **Principle of Accountability:** The County shall create a recordkeeping program and delegate responsibility to appropriate individuals, adopt policies and procedures to guide personnel and ensure audit ability of the program.
 - (2) **Principle of Availability:** The County shall maintain records in a manner that ensures timely, efficient, and accurate retrieval of needed information.
 - (3) **Principle of Compliance:** The County shall construct a recordkeeping program that complies with applicable laws for maintaining records, as well as the organization's policies as they pertain to records and information management.
 - (4) **Principle of Disposition:** The County shall provide secure and appropriate disposition for records that are no longer required to be maintained under applicable laws.
 - (5) **Principle of Integrity:** The County shall construct a recordkeeping program where records and information generated or managed by or for the County has a reasonable and suitable guarantee of authenticity and reliability.

- (6) **Principle of Protection:** The County shall construct a recordkeeping program that ensures a reasonable level of protection to records and information that are private, confidential, privileged, or essential to business continuity.
 - (7) **Principle of Retention:** The County shall maintain its records and information for an appropriate time, taking into account legal, regulatory, fiscal, operational and historical requirements.
 - (8) **Principle of Transparency:** The processes and activities of the County's recordkeeping program shall be structured and documented in a manner that is open and verifiable and is available to all personnel and interested parties.
- J. **Inactive Record:** A record no longer needed to conduct current business but preserved until it meets the end of its retention period.
 - K. **Inspection of Public Records Act, §14-2-1 et seq., NMSA 1978:** The law that requires a representative government to provide access to its public records at the request from a person within a designated timeframe with few noted exceptions. It states that all persons are entitled to the greatest possible information regarding the affairs of government and the official acts of public officers and employees. This law can be found at <http://www.nmag.gov/office/Divisions/Civ/OMAIPRA/default.aspx>
 - L. **Inventory:** A detailed database created by the records staff that lists all inactive records stored in a centralized records location for ease in maintenance and retrieval.
 - M. **Lifecycle of Records:** Begins with the creation of the record, its use, storage in a format that is readable, its maintenance, retention and final disposition of all County records.
 - N. **Metadata:** Data describing context, content, and structure of records and their management through time. RIM has selected the following metadata string to capture information in a consistent manner, these include: ICLA File Plan Designation, Record Series or Citation, New Mexico Administrative Code Record Function, Incorporated County of Los Alamos Record Description, Creation and End Dates, Trigger Date, Disposition Date, Record Value and Record Classification.
 - O. **Migrated:** Method of preserving information to ensure continued access to information in any format. This includes the preservation of materials resulting from digital reformatting, but particularly information that is created digitally and has no analog counterpart.
 - P. **Naming Structure:** Specific metadata used to describe the contents of the record and to establish consistency within a records management program which also provides ease in searching, retrieval and retention.
 - Q. **NMAC:** New Mexico Administrative Code (1978) providing rules as well as referring to and interpreting statutes for governing public information.

- R. **Non-record Materials:** The following specific types of materials are defined as non-record and may be disposed of at the convenience of the County when they have no more value/use to the County: extra copies of correspondence and other documents preserved only for convenience of reference; blank forms, books, etc., which are outdated; materials neither made nor received in pursuance of statutory requirement nor in connection with the functional responsibility of the office/county; preliminary drafts of letters, reports, and memoranda which do not represent significant basic steps in preparation of record documents; shorthand notes, steno tapes, mechanical recordings which have been transcribed, except where noted on the County's retention schedule; routing and other interdepartmental forms which do not add any significant material to the activity concerned; stocks of publication already sent to archives and processed documents preserved for supply purposes only; form and guide letters, sample letters, form paragraphs. All other materials either related or received in pursuance of statutory requirements or in connection with the transaction of public business which belongs to the office concerned are government property and not personal property of the officer or employees concerned. Therefore, any material not included in the above definition cannot be destroyed, given or taken away, or sold without complying with all the statutory requirements specifically relating to said records.
- S. **Personal devices:** To include personally owned computers, flash drives, external hard drives, smartphones, other mobile/cellular phones, tablet computers, e-readers, portable media devices, PDAs, portable gaming devices, ultra-mobile personal computers (UMPCs), laptops/notebook computers and any other mobile device capable of storing data and connecting to a network.
- T. **Physical records:** To include calendars, appointment books, memos, correspondence, reports, studies, projects in a paper format as well as all other physical media, including optical media (magnetic media), microfilm, microfiche, which stores public information created in the course of conducting or related to County business.
- U. **Public Records:** Means all books, papers, maps, photographs or other documentary materials, regardless of physical form or characteristics, made or received by any agency in pursuance of law or in connection with the transaction of public business and preserved, or appropriate for preservation, by the agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations or other activities of the government or because of the informational and historical value of data contained therein. Library or museum material of the state library, state institutions and state museums, extra copies of documents preserved only for convenience of reference and stocks of publications and processed documents are not included (§14-3-2 NMSA 1978).
- V. **Records and Information Management (RIM) Program Manager:** The Incorporated County of Los Alamos employee, who will serve as the person responsible for this information governance policy and implementation. This employee is also authorized to transfer, withdraw or destroy County records with the approval from the New Mexico State Records Administrator.

- W. **Record Center:** A County storage facility where inactive records are managed, organized, appraised, inventoried, protected and tracked for retrieval, audit, retention and final disposition. A temperature and humidity controlled facility is preferred to secure, protect and maintain the County's legacy of information for as long as required.
- X. **Records and Information Management (RIM):** Field of management responsible for the efficient and systematic control of the creation, receipt, use, maintenance, and disposition of records, including the processes for capturing and maintaining evidence of and information about business activities and transactions in all record formats and mediums.
- Y. **Records Personnel:** Staff, trained and authorized by the County RIM Program Manager to handle County records under this established recordkeeping policy, procedures and principles including copies of those public records maintained by the County Clerk, not otherwise stored or managed pursuant to New Mexico State Statute or the County Charter/Code.
- Z. **Retention Schedule:** A comprehensive list of records series titles/functions, indicating for each series the minimum length of time it is to be maintained. Records may be kept longer with justification and nominal risk to the County.
- AA. **Social Media and Web Based Services and Platforms:** External and internal Web sites or services most of which integrate web technology, social interaction and user-generated content to collaborate, combine and share information. These provide a variety of ways for users to interact. These platforms may be operated by nongovernmental third part entities. Examples of social network services include but not limited to Facebook, Twitter and Linked In.
- BB. **Third-party repository:** The storage of data online in the cloud or on other social media sites wherein an organization's data is stored in and accessible from multiple distributed and connected resources. The ICLA is fully responsible for any and all records and information transferred and stored in an offsite repository.

III. Policy

It is the policy of the Incorporated County of Los Alamos that all Public Records will be responsibly managed in accordance with the Public Records Act (NMSA 1978, §14-3-1 et seq.), the Inspection of Public Records Act (IPRA) NMSA 1978, §14-2-1 et seq., the Incorporated County of Los Alamos Retention Schedule and recordkeeping standards and procedures, 1.21.2 New Mexico Administrative Code (NMAC) Retention and Disposition of Public Records, 1.21.3 NMAC Local Government Records Management Guidance and other applicable rules, statutes and regulations issued by the New Mexico Commission of Public Records, except as expressly referenced and modified herein. This includes 1.13.3 NMAC (Management of Electronic Records), 1.13.4 NMAC (Management of Electronic Messaging), 1.12.7

Information Technology (Electronic Authentication) as well as other Federal retention rules and schedules that pertain to specified record series created by specific divisions.

It is the policy of the Incorporated County of Los Alamos to provide employees, appointed and elected officials the applicable records management training to assist in the performance of their work. All resources and services shall be managed in a lawful manner by all County employees, appointed and elected offices, or contractors. County employees shall classify information (using the specified naming structure format) and retention schedule to ensure electronic repositories are in compliance with this policy and applicable law.

County employees shall have no expectation of privacy in anything they send or receive including electronic messaging in the course of conducting County business. All records created while employed, appointed or elected with the Incorporated County of Los Alamos are the property of the County and cannot be destroyed, distributed, sold or stored without complying with this policy.

IV. Responsibility

All affiliated County personnel are required to follow the approved Incorporated County of Los Alamos Retention Schedule by reference for all recordkeeping purposes and ensure the Generally Accepted Recordkeeping Principles, which include accountability, integrity, protection, compliance, availability and transparency apply to all County records while in their custody. The principles of retention and disposition shall be the responsibility of the County's RIM personnel to ensure haphazard or indiscriminate dumping is avoided.

All inactive physical records are required to be centrally located and managed by the RIM personnel to ensure records can be easily located and securely managed. All physical records transferred to the County's Record Center shall include on the outside of each file the title and description of the record, the creation and end dates, and indication whether the record contains confidential or essential information. Active records will remain within Division offices for operational use for as long as needed. Once inactive, records shall be transferred by the Departmental Records Data Liaison to the County's Record Center for evaluation, appraisal, inventory, storage, maintenance and final disposition.

Electronic records will be managed in place by the record creator on user controlled storage, under this established record management criteria. To create consistency and uniformity, records shall use the following Naming Structure format: *yyyymmdd_Title of Record_creator's first initial and complete last name. Example: 20160923_Information Governance Policy_BRicci*. This will allow the creator to file the e-record within the County's centralized File Plan by year thus improving the ease for retrieval and final disposition. Electronic records include those records on network drives, cloud repositories, external hard drives, USB flash drives, digital assistants to

include mobile devices, and digital cameras. Active electronic records will remain the responsibility of the creator who shall maintain the official record under these established recordkeeping practices. The naming structure format does not pertain to input of content in an established database. When entering content in a database, end-user is not required to name the record but must comply with the standards established within the designated system. Only one copy needs to be maintained as the official record to satisfy the retention requirements of the Public Records Act. All duplicated files are considered reference material and shall be deleted as non-record including drafts in any form, which do not add significant material or value to the activity concerned.

The maintenance and accessibility of inactive electronic records shall be safeguarded by the Information Management (IM) Division against deliberate tampering, alteration or in any way change the content of the record for fraudulent purposes. The Incorporated County of Los Alamos RIM Program Manager shall work with IM to ensure electronic records are migrated when records have not met retention and where there is hardware or software obsolescence or when records are stored within a third party repository. Records shall be migrated to a new hardware or software or be converted to a human readable form. RIM and IM will determine appropriate time periods to insure that they are protected from accidental or deliberate loss. Permanent archival or long-term records in physical and on electronic media shall be maintained by RIM and stored in an appropriate environmental setting.

V. Procedures

- A. **Record/Data Liaison (RDL).** Each Department or affiliated body or group shall designate a County Record/Data Liaison (RDL) who understands the records created by the Department or group and who will be the point of contact for the County's RIM Program Manager and the County's Records Center. This responsibility shall become part of the Records/Data Liaison's job duties. All RDL's are required to attend County RIM Training Sessions given or sponsored by the County RIM Program Manager to include and implement all recordkeeping principles. The Records/Data Liaison shall actively support the Records and Information Management policies and procedures and will be the person(s) who reports on all record training and communication at department, affiliated body or group meetings. Any record concerns or issues shall be directed to the County's RIM Program Manager, RIM personnel, designee or subsequent chain of command.

- B. **Record Retention Rules, Schedules, File Plans and Data Entry Portal.** Each department's RDL will determine which records are inactive and shall prepare physical records to be transferred to the County Records Center by boxing the records in designated boxes and by entering each file's metadata into the Data Entry Portal inventory forms. The Data Entry Portal is accessible to all RDL's via the Incorporated County of Los Alamos Intranet. RIM personnel will evaluate, verify and quality check the data entered into the Data Entry Portal against the

actual records and will either accept or reject the box. At the end of each fiscal and calendar year, a Disposition Report will be generated by the RIM personnel on all inventoried records by division and distributed to each RDL. A 30-day review period will be allowed for notice and comment by Department management or affiliated body or group. If no issues, audits or holds pertain to the records listed, the County's RIM Program Manager will proceed with approval from State Records Administrator for final disposition. Once granted, all record formats will be destroyed and disposed of accordingly. Destruction of all records is performed on location in a confidential manner supervised by the RIM personnel with final Certificate of Destruction maintained on file.

- C. **Public Records Requests.** All public record requests shall be the responsibility of the Records Custodian designated by the County Manager. Together with the Records Center, all Record/Data Liaisons shall provide requested records within the designated timeframe under their custody as required by the Inspection of Public Records Act.
- D. **Storage.** All County inactive records shall be stored in the County's Records Center. Electronic records including email shall be responsibly managed on County computing platforms and County managed storage appliances in compliance with current policies. Individuals who choose to use their personal devices to conduct County business must follow the County's records and information management policies and procedures. The designated IM personnel must be informed by the individual using any personal device and will maintain a current listing of those individuals who use personal devices to conduct County business. County information stored may be subject to inspection and discovery under applicable public records laws, county policy and discovery mechanisms, respectively.

When an employee's employment ends with the County, all records created by the employee that are inactive shall be gathered by the designated Records/Data Liaison and transferred to County's Record Center for evaluation, inventory, storage and/or final disposition. Active records shall be distributed by the RDL to the new designee. RIM and IM policies and procedures pertain to all issued equipment that store the County's public records.

- E. **Social Media and Web-Based Platforms.** County employees utilizing social media in the course of County business shall follow the County's Social Media policy. Such employees shall be responsible for all public records created on third-party sites and shall maintain an archive of all information posted with all supporting documents attached in a readable format and in compliance with existing policies. Official records posted under this category must follow this policy and the accepted Incorporated County of Los Alamos Retention Schedule for the entire lifecycle of these public records.


F. Reporting. The Records personnel will provide the County Manager and County Council with reports on the Records and Information Management program as requested.

G. Elected and Appointed Officials. The Records personnel will support all elected or appointed offices of the County Council, Boards and Commissions, County Assessor, Clerk, Sheriff, Municipal and Probate Judges and Municipal Court to utilize the accepted Retention Schedule or a specific schedule that pertains solely to their office.

VI. Additional Regulatory Requirements

This policy shall not be construed in a manner that is inconsistent with statutory regulations and requirements within the Incorporated County of Los Alamos Charter.

Prepared by: RIM Program Manager



Harry Burgess
County Manager

11/30/17
Date



INCORPORATED COUNTY OF LOS ALAMOS ADMINISTRATIVE PROCEDURE GUIDELINE

Index No. 1220

Effective: October 1, 2013

E-SIGNATURE POLICY

I. Purpose

This policy is to allow for e-signature use at LAC by means of methods that are practical, secure, and balance risk and cost. It is not the intent of this policy to eliminate all risk but rather to provide a process that gives parties assurance that appropriate analysis was completed prior to implementation of e-signature, and that the level of user authentication used is reasonable for the type of transaction conducted.

A. Electronic Signatures Acts

Both federal and state law address electronic signatures and give electronic contracts the same weight as those executed on paper. The federal act is known as the "Electronic Signatures in Global and National Commerce Act," (Act) and is found at 15 U.S.C. Sections 7001-7006, 7021 & 7031. The New Mexico act is known as the "Uniform Electronic Transactions Act," and is found at Sections 14-16-1 through 14-16-19, N.M.S.A. (1978). Links to these statutes are provided below. All references herein are to the New Mexico act unless otherwise specified. The act has some specific exemptions or preemptions. *Although the act enables documents to be signed electronically, the ability to do so arises only when both parties agree to conduct transactions by electronic means. Any LAC department using E-signatures shall also provide methods for conducting transactions with its customers that do not require E-signatures in the event the customer declines to agree to such to conduct transactions by electronic means.* The act specifically avoids stipulating any 'approved' form of electronic signature, instead leaving the method open to interpretation by the marketplace. Any number of methods is acceptable under the act. Methods include simply pressing an *I Accept* button, digital certificates, smart cards and biometrics.

E-signatures may be implemented using various methodologies depending on the risks associated with the transaction. Examples of transaction risks include: fraud, repudiation, authentication, hacking, security and financial loss. The quality and security of the e-signature method shall be commensurate *with the risk and needed assurance of the authenticity of the signer. Authentication is a*

way to ensure that the user who attempts to perform the function of an electronic signature is in fact who they say they are and is authorized to "sign".

II. Policy

- A. It is the policy of LAC that every user shall have unique identifying credentials. Authentication entails verifying the user's unique credentials, such as username and password, or a digital certificate.
- B. Under this policy LAC departments may implement use of e-signatures, but shall also maintain alternative processes available for any consumer who declines to conduct transactions by electronic means. The LAC department is the organization conducting business by means of an e-signature. Implemented e-signatures will be reviewed periodically for appropriateness, and continued applicability.
- C. An e-signature may be accepted in all situations if requirement of a signature/approval is stated or implied. This policy does not supersede situations where laws specifically require a written signature or where a party declines to conduct transactions by electronic means.

III. Responsibility

- A. Security and access to LAC specific information is determined by the Access Control Authority (ACA) for the electronic system. ACA's shall have the ability to develop enabling procedures and are responsible for compliance with all legal obligations related to information, as well as determining the utilization, access, and release of data under their jurisdiction. ACA's are a representative from the requesting department or other designated representative (i.e., IT liaison, TAG representative). In some instances there are multiple ACA's for various systems. The ACA will ensure that appropriate controls and monitoring of required software/hardware required for implementation are in place.
- B. LAC departments shall complete LAC risk assessment tool (E-Signature Authentication Request Process) and shall describe the reason for risk, identify the steps that will be taken to mitigate the risk and obtain the signed approval of the County Administrator. LAC departments shall conduct periodical reviews of every implementation, no less than every three years, which will include an evaluation of the e-signature use to determine whether any applicable legal, business, or data requirements have increased the risk of the e-signature implementation.
- C. The Information Management Division (IMD) shall assist LAC department ACA's in preparation of their application and provide technological expertise (i.e., IT liaison).
- D. III.4. The ACA may, after consultation with the County Attorney, reject any E-Signature application deemed in violation of or failing to meet statutory or regulatory requirements. The ACA, after consultation with the County Attorney, shall establish specifications for recording, documenting, and/or auditing the e-signature as required for non-repudiation and other legal requirements.
- E. The County Administrator shall review and have final approval of each e-signature application.

- F. Records Information Management (RIM) shall retain a formal record of the risk assessment evaluation, e-signature method selection, and justification.

IV. Procedure

The E-Signature Authentication Request Process tool outlines the process required by a department to apply for an e-signature implementation and shall address known identified risks.

- A. An evaluation will be performed by the ACA to identify risks associated with using an e-signature and to determine the quality and security of the e-signature method required. An evaluation will be made using the E-Signature Authorization Request Process tool. The reports resulting from the assessment shall be included as part of the official record for this e-signature implementation and submitted with the proposal.
- B. Requests for LAC e-signature transactions shall be evaluated by the ACA in conjunction with IMD, who will determine whether to recommend an e-signature method for approval, by understanding the systems and procedures associated with using that electronic signature, and whether the use of the electronic signature is at least as reliable as the existing method being used. The IMD review will include process, security and records review with a recommendation to the department on whether or not to proceed.
- C. The ACA will request a review of the application from the County Attorney. Once that review has been completed and recommendation to proceed has been granted, the ACA will seek authorization to implement e-Signature from the County Administrator.
- D. The signed document shall be included as part of the official record for this e-signature implementation.
- E. Once approved, the implementation process will likely differ for each transaction and for each LAC department or affiliated body, as it is dependent on many factors such as records management requirements, technical environment, appropriate assurance level, and the nature of the transaction.
- F. Software and/or hardware required for e-signatures, such as Public Key Infrastructure (PKI) certificates, “fobs”, or “dongles”, or other credential devices shall be purchased by the department or affiliated body.
- G.

V. Resources and Links

- A. Electronic Signatures in Global and National Commerce Act (ESIGN):

<http://frwebgate.access.gpo.gov/cgi->

[bin/getdoc.cgi?dbname=106_cong_public_laws&docid=f:publ229.106.pdf](http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws&docid=f:publ229.106.pdf)

- B. NIST Electronic Authentication Guidelines: 800-63;

http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

C. Electronic Signatures in Global and National Commerce Act, 15 U.S.C. Sections 7001-7006, 7021 & 7031; <http://uscode.house.gov/download/pls/15C96.txt>

D. Uniform Electronic Transactions Act, Sections 14-16-1 through 14-16-19, N.M.S.A. (1978);

<http://www.conwaygreene.com/nmsu/lpext.dll?f=templates&fn=main-h.htm&2.0>

VI. Definitions

Access Control Authority (ACA)	Department representative, or designee, who understands the data and manages the request for e-signature application process and implementation.
Affiliated Body	Board or Commission who act on behalf of a LAC Department.
Authentication	A method to ensure that the user who attempts to perform functions in a system is in fact the user who is authorized to do so in order to ascertain the identity of the originator, verify the integrity of the electronic data and establish the link between the data and the originator.
Electronic Record	Computer-generated information such as an e-mail message, document or image file created or received by the County in pursuance of law or in connection with the transactions of public business.
Electronic Signature (E-Signature)	The electronic signing of a document consisting of establishing a verifiable link between the originator and the document using an electronic sound, symbol, or process attached to or logically associated with a record and execute or adopted by a person with the intent to sign the record.
Non-repudiation	Specific identification of a user plus the need to specifically link the user to a transaction; i.e., to prove that the user intended to be bound by the transaction.
Record	Information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in a perceivable form.
TAG (Technology Advisory Group)	This group provides technological oversight to LAC and any member thereof may act as an ACA.
Transaction	Specific actions that users can perform to achieve a desirable result. A transaction is an actor, plus an action, resulting in a desired outcome.


 HARRY BURGESS
 COUNTY ADMINISTRATOR

12/1/15
 DATE