

**December 5, 2012**

Agenda

**9:30 A.M. Business Meeting**  
Valencia County Commission Chambers  
444 Luna Avenue  
Los Lunas, NM 87031

Board of County Commissioners

Donald E Holliday, Chair District V  
Georgia Otero-Kirkham, Vice-Chair District II  
Mary Andersen District I  
Lawrence R. Romero District III  
Ron Gentry District IV

- 1) Call Meeting to Order
- 2) Pledge of Allegiance
- 3) Approval of Agenda
- 4) Approval of Minutes:

November 26, 2012..... Special Business Meeting

A handwritten signature in dark ink, appearing to read "Donald E. Holliday".

---

**PRESENTATION(S)**

- 5) Commission Presentation. *Commission Chair D. Holliday*
- 6) Planning/Zoning Update. *Jacobo Martinez*
- 7) Code Enforcement Update. *Jacobo Martinez*

**DISCUSSION (Non-Action) ITEM(S)**

None

**ACTION ITEM(S)**

- 8) Consideration to enter into a contract extension with Triadic Enterprises for an additional 6 months of support. *Lawrence Esquibel*
- 9) Consideration to accept the Information Technology Usage and Security Policy for Valencia County. *Lawrence Esquibel*
- 10) Consideration to approve the Findings of Fact and Conclusion of Law for a zone change from Rural Residential-2 (RR-2) to Community Commercial (C-2) (Simon and Catrina Montano) Application # ZC 12\_305. *Jacobo Martinez*
- 11) Consideration to approve the Findings of Facts and Conclusion of Law for a zone change Planned Development (P-D) to Heavy Industrial (I-3) (PNM) Application # ZC 12\_306. *Jacobo Martinez*

**FINANCIAL MATTERS:**

- 12) Approval of Financial/Payroll warrants. *Nick Telles*

**PUBLIC COMMENT:**

BOOK 074

PAGE 232

Please sign up on the sheet located just outside the Commission chambers. The Board will allow each member of the public wishing to address the Board a full and complete opportunity to address the Commission.

**EXECUTIVE SESSION:**

Pursuant to Section 10-15 1 (H) (2) (7) & (8), the following matters may be discussed in closed session: a. personnel: b. pending or threatened litigation: c. Competitive Sealed Proposals, d. other, specific limited topics that are allowed or authorized under the stated statute.

- ♦ Motion and roll call vote to go into Executive Session for the stated reasons
- ♦ Board meets in closed session
- ♦ Motion and vote to go back into regular session
- ♦ Summary of items discussed in closed session
- ♦ Motion and roll call vote that matters discussed in closed session were limited to those specified in motion for closure, and that no final action was taken, pursuant to the authority in §10-15-1 NMSA 1978.

**ACTION ITEMS:**

None

**NEXT COMMISSION MEETING:**

- ♦ **December 19, 2012 – Business Meeting @ 9:30 A.M.**  
**Valencia County Commission Board Room 444 Luna Ave. LL, NM**

**ADJOURN:**

*If you are an individual with a disability who is in need of a reader, amplifier, qualified sign language interpreter, or any other form of auxiliary aid or service to attend or participate in the hearing or meeting, please contact the Valencia County Manager's Office at the Valencia County Courthouse, Los Lunas, New Mexico, (505) 866-2014 at least one week prior to the meeting or as soon as possible. Public documents, including the agenda and minutes, can be provided in various accessible formats. Please contact the Valencia County Manager's Office at the old Valencia County Courthouse if a summary or other type of accessible format is needed.*

# VALENCIA COUNTY BOARD OF COMMISSIONERS

## BUSINESS MEETING

DECEMBER 5, 2012

<b>PRESENT</b>	
Donald E. Holliday, Chairman	
Georgia Otero-Kirkham, Vice-Chair	
Lawrence R. Romero, Member	
Ron Gentry, Member	
Mary J. Andersen Member	
Bruce Swingle, County Manager	
Adren Nance & Dave Pato, County Attorneys	
Sally Perea, County Clerk	
Press and Public	

1) The meeting was called to order by Chairman Holliday at 9:30 A.M.

2) Chairman Holliday led the Pledge of Allegiance.

3) Approval of Agenda

Commissioner Otero-Kirkham moved for approval of the agenda. Seconded by Commissioner Andersen. Motion carried unanimously.

4) Approval of Minutes: November 26, 2012-Special Business Meeting

Commissioner Andersen moved for approval. Seconded by Commissioner Romero. Motion carried unanimously.

### PRESENTATION(S)

5) Commission Presentation- Commission Chairman Donald Holliday

Chairman Holliday thanked and presented a plaque to the outgoing Commissioners Georgia Otero-Kirkham and Ron Gentry for their hard work and dedication to Valencia County.

Commissioner Otero-Kirkham thanked the staff and said a lot was accomplished during their service to the county which included a new Judicial Complex, improvement of several of the fire stations and the paving of 44 miles of unpaved roads. Commissioner Gentry also thanked everyone.

6) Planning/Zoning Update-Jacobo Martinez

7) Code Enforcement Update- Jacobo Martinez

Valencia County Community Development Director Jacobo Martinez gave a brief update on Planning/Zoning and Code Enforcement Departments for 2012. For the year 2012 Code Enforcement has taken on 549 cases with 290 of those cases being resolved. Mr. Hoss Foster received the Flood Control Officer of the year presented to him by the New Mexico Flood Manager's Association. Mr. Foster helped 176 individuals get their homes that were placed in the flood zone back out of the flood zone which saved those individuals thousands of dollars in insurance. Mr. Martinez thanked the Community Development Division, the County Attorneys, Planning and Zoning Officers and the County Commission for their strength and courage in making their decisions in all of the cases as land use is not an easy thing to make decisions on. The Community Development Department was the first department to go live on the Tyler System and the Tyler System has really allowed them to be more accountable in their financing and reporting of collections. They found that there were about 1000 delinquent business licenses in Valencia County. They send out notices and received back 796 up to date business registrations for 2012 for a total of \$18,000.00 in revenues, there were 93 building permits totaling \$2,300 and 85 mobile home permits totaling \$6,500.00. These revenues from the Community Development Division total about \$36,000.00. They resolve to continue with community empowerment and quality of life in Valencia County.

### DISCUSSION (Non-Action) Item(s)

None

### ACTION ITEM(S)

8) Consideration to enter into a Contract Extension with Triadic Enterprises for an Additional (6) Months of Support – Lawrence Esquibel.

County Manager Bruce Swingle said Mr. Esquibel was not present at today's meeting due to family crisis and asked everyone keep him and his family in their prayers as this was a very difficult time for him.

Commissioner Gentry moved for approval. Seconded by Commissioner Andersen.

County Attorney Adren Nance asked that the motion be changed to delegate the authority to Mr. Esquibel and Mr. Swingle to enter into the contract in a timely manner at the prices that have been suggested so that they can work through a couple of additional problems, one which is concerning a request to pay in advance for services which may have some issues. Chairman Holliday suggested tabling this item until the next meeting.

Commissioner Andersen said she withdraws her second and agrees that this should be tabled.

Commissioner Gentry withdrew his motion and motioned to table this item. Seconded by Commissioner Andersen. Motion carried unanimously.

**9) Consideration to Accept the Information Technology Usage and Security Policy for Valencia County-Lawrence Esquibel / Bruce Swingle.**

Commissioner Andersen moved for approval. Seconded by Commissioner Otero-Kirkham. Motion carried unanimously. (SEE EXHIBIT A)

**10) Consideration to Approve the Findings of Fact and Conclusion of Law for a Zone Change from Rural Residential-2 (RR-2) to Community Commercial (C-2) (Simon and Catrina Montano) Application #ZC 12\_305 – Jacobo Martinez.**

Chairman Holliday moved for approval. Seconded by Commissioner Otero-Kirkham. Motion carried unanimously. (SEE EXHIBIT B)

**11) Consideration to Approve the Findings and Conclusion of Law for a Zone Change Planned Development (P-D) to Heavy Industrial (I-3) (PNM) Application #ZC 12\_306- Jacobo Martinez.**

Chairman Holliday moved for approval. Seconded by Commission Otero-Kirkham. Motion carried unanimously. (SEE EXHIBIT C)

**FINANCIAL MATTERS:**

**12) Approval of Financial Payroll/Warrants – Nick Telles.**

Commissioner Otero-Kirkham motioned for approval. Seconded by Commissioner Andersen. Motion carried unanimously. (SEE EXHIBITS D,E &F)

**PUBLIC COMMENT:**

Those individuals making comments at today's Business Meeting were Valencia County residents Charles Apodaca and Amavalise Jaramillo.

**EXECUTIVE SESSION:**

Pursuant to Section 10-15-1 (H) (2) (7) & (8) the following matters may be discussed in closed session; a) Personnel b) Pending or threatened litigation c) real property d) other specific limited topics that are allowed or authorized under the stated statute.

None

**NEXT COMMISSION MEETING:**

The next Business Meeting of the Valencia County Board of County Commission will be held on December 19, 2012 at 9:30 A.M. in the County Commission Room at the Valencia County Courthouse.

**11) Adjournment**

Commissioner Andersen moved for adjournment. Seconded by Chairman Holliday. Motion carried unanimously. TIME: 10:10 A.M.

**NOTE:** All proposals, documents, items, etc., pertaining to items on the agenda of the December 5, 2012 Business Meeting (presented to the Board of County Commissioners) are attached in consecutive order as stated in these minutes.

**VALENCIA COUNTY BOARD OF COMMISSIONERS**




**DONALD E. HOLLIDAY, CHAIRMAN**



**GEORGIA OTERO-KIRKHAM, VICE-CHAIR**



**LAWRENCE R. ROMERO, MEMBER**

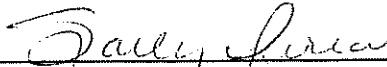


**RON GENTRY, MEMBER**



**MARY J. ANDERSEN, MEMBER**

**ATTEST:**



**SALLY PEREA, COUNTY CLERK**

12.19.2012

**DATE**

Information Technology Usage and Security  
Policy  
Valencia County

December 5<sup>th</sup>, 2012

Valencia County Manager:

---

Bruce Swingle

Date: 12/5/12

(EXHIBIT A)

## Table of Contents:

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

## **1. Introduction**

This policy provides guidance to users of Valencia 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. Smartphones, cell phones & tablet'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 Department (ITD) prepares this policy based on direction and approval of County Manager. It applies to all users of County IT assets.

ITD will update this policy at least annually. 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 Department.

## **3. Principles**

This policy and accompanying programs are based on several principles:

- 3.1. An optimum balance of security and productivity;
- 3.2. Providing defense in depth for known threats with flexibility to respond quickly to unknown or unexpected threats;
- 3.3. Being risk based - correlate security investments with risk;
- 3.4. Identifying roles and responsibilities for personnel, supervisors, and IT personnel;
- 3.5. Providing engineered solutions where possible to minimize the impact of risky human behaviors; and
- 3.6. 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, yet on the increase, these attacks can be devastating if successfully pursued by a skilled and malicious individual.

## 6. 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.

#### 6.1. Responsibilities for all users:

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

#### 6.2. Supervisors have these additional responsibilities:

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

#### 6.3. The ITD has the following additional responsibilities:

- 6.3.1. Physical security of servers and the Integrated Computer Network (ICN)
- 6.3.2. Training of users in computer security;
- 6.3.3. Assisting other County personnel in addressing security issues; and
- 6.3.4. Policy review and update.

## 7. Access Management

Access management is a key component of perimeter defense. Stopping the illegitimate user is a primary defense against illegitimate use (Risk 5.3). Good access management also enables monitoring of users' computing and communications activities, thereby greatly reducing the risk of misuse (Risk 5.2).

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.

## **8. 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.

## **9. Naming Conventions**

There are currently two naming conventions for accounts. For Windows-based systems, accounts are named using the employee's first name dot (.) last name and, if necessary, an X or middle initial. For the AS400 system, accounts are named using the employee's first name last initial.

## **10. 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.

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

## **11. 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:

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

- 11.2. Do not share your password with anyone (except as noted below);
- 11.3. Do not allow any other person to use your account (i.e. password);
- 11.4. 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
- 11.5. 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.
- 11.6. 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. Sharing of passwords or other conduct that compromises 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. The account holder is still responsible for all activities in their account carried out under their password.

## **12. Account Suspension and Termination**

If an account holder will be on leave from work due to an extended absence, leave, or suspension, 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 Valencia 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, director or department head all County-owned equipment.

## **13. 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.

## 14. Data Security

14.1. 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 directors, supervisors or department head; have the following responsibilities:

- 14.1.1. Knowing the potential risk of release or misuse of data and applications under their control or under the control of their subordinates;
- 14.1.2. Defining access policy with respect to applications, desktop hardware, and data and managing access rights consistent with such risk;
- 14.1.3. 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);
- 14.1.4. Managing the access right allocation, modification, and termination within the capabilities of their applications package(s);
- 14.1.5. Training account holders with access rights on their responsibilities with respect to release and use of the data and use of the applications; and
- 14.1.6. 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.

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

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

14.3. ITD personnel have the following responsibilities:

- 14.3.1. 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;
- 14.3.2. 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;
- 14.3.3. ITD personnel modifying applications data will normally inform the appropriate supervisors 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 department supervisor, department head and/or director and ITD director;

- 14.3.4. ITD personnel should assist supervisors and personnel in understanding the potential risk of release or misuse of data and applications under their control; and
- 14.3.5. 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.

## 15. 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.

- 15.1. 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:
  - 15.1.1. Regular and timely usage of email;
  - 15.1.2. Knowledge of desktop computing basics;
  - 15.1.3. Familiarization with computer applications necessary to perform their job functions; and
  - 15.1.4. Usage of the Internet as an information resource for acquiring and using information relevant to their work.
- 15.2. 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.
- 15.3. 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.
- 15.4. 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.
- 15.5. Account holders should take appropriate protective measures to minimize the probability that their addresses will become targets for spam, e.g. using their county email address as a return address for online personal purchases.
- 15.6. 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.

- 15.7. 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.
- 15.8. Access of personal email accounts should be limited to emergency access only and should not be accessed and left open while performing daily duties. Personal email accounts should not be used from county computers for the dissemination of chain email spam.

## 16. 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.

- 16.1. Account holders shall use County IT resources only for official County business unless otherwise specifically allowed in *this policy*.
- 16.2. 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.
- 16.3. 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.
- 16.4. 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 Manager. 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.
- 16.5. 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. Valencia County prohibits the illegal duplication of software or acquiring or using illegal copies of software.
- 16.6. 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 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 Valencia County computer. Approval will require 1) proof of ownership 2) virus checking by ITD personnel; 3) that the software is compatible, in ITD's judgment, with existing County hardware and software.

- 16.7. Account holders shall not use County IT resources to download or distribute pirated software or data, including music or video files.
- 16.8. Account holders shall not use County IT resources to deliberately propagate any malicious code.
- 16.9. 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.
- 16.10. Unauthorized remote 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.
- 16.11. 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.
- 16.12. 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.
- 16.13. 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.
- 16.14. 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.

## **17. 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.

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

- 15.1. Materially interferes with the use of IT resources by County staff, agents, representatives, officials or contractors;
- 15.2. Burdens the County with additional costs;
- 15.3. interferes with the account holder's employment duties or other obligations to the County;
- 15.4. consumes a consequential amount of an account holder's time on the job;
- 15.5. Includes any activity that is prohibited under this policy;



- 15.6. Is a part of an ongoing for-profit business activity or unauthorized non-profit business activity; or
- 15.7. 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.**

## **18. 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, Internet Enabled Cellular Phones (Smart Phones), Tablet PC's, 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 Director 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 Department to provide support to the County by the IT Director 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 ITD before being connected. A master list of all authorized devices will be maintained, by the ITD.
- e. The mobile device operator must be identified by name and contact information to the IT Department.
- f. The mobile device operator must be familiar with the Information Technology Usage and Security Policy for Valencia 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.

## 19. 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 Manager 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 Director, 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 Manager, or the Manager'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.

## 20. 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.

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 LTD's contactors without approval of the County Manager or the Manager'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 in writing 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.

## 21. Backup and Recovery

All network data will be backed up regularly, nightly, weekly and monthly by ITD with weekly and monthly backups 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, flash drives, or any other portable media. 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.

## 22. Definitions

As used in this policy:

- 22.1. **Access** means the ability to read, change, or enter data using a computer or an information system.
- 22.2. **Equipment** means computers, monitors, keyboards, mice, routers, switches, hubs, networks, or any other information technology assets.
- 22.3. **County-owned** includes equipment the county leases or controls under contract.
- 22.4. **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.

- 22.5. **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.
- 22.6. **Malicious code** means any type of code intended to damage, destroy, or delete a computer system, network, file, or data.
- 22.7. **Pirated software** means licensable software installed on a computer system for which a license has not been purchased or legally obtained.
- 22.8. **Physical control** means knowing where your information technology resources are and knowing that they are not being misused.
- 22.9. **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).
- 22.10. **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.
- 22.11. **Sexually explicit or extremist materials** means images, documents, or sounds that can reasonably be construed as:
- 22.11.1. Discriminatory or harassing;
  - 22.11.2. Defamatory or libelous;
  - 22.11.3. Obscene, of a primarily sexual nature, or pornographic;
  - 22.11.4. threatening to an individual's physical or mental well-being; or
  - 22.11.5. read or heard for any purpose that is illegal
- 22.12. **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
- 22.13. **Virtual private network (VPN)** means an encrypted communication link established between a remote device and the County network via the internet.
- 22.14. **WLAN** means a wireless local area network in which a mobile user can connect to a local area network through a wireless (radio) connection.

22.12. **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.

22.12.1. An employee of Valencia County;

22.12.2. An elected official of Valencia County;

22.1.5.3. An individual working under contract to the County; or

22.12.4. A volunteer providing service to the County.

Appendix A: Acknowledgement Form

Valencia County

Information Technology Account Holder Acknowledgement Form

I understand that Valencia 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 Valencia 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 Valencia 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 Valencia County Information Technology Usage and Security Policy. I understand this document will be kept in my Personnel folder during my employment with Valencia 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 Valencia County computing resources in the performance of his/her duties and has a need-to-know for the information processed by the Valencia County computing resources related to his/her duties.*

Supervisor/County contract supervisor/County Manager Name Date \_\_\_\_\_  
\_\_\_\_\_

Supervisor/County contract supervisor/County Manager Signature \_\_\_\_\_

**Valencia County  
Computer Security Policy  
Appendix B**

**Appendix B: Master Computer Protection Plan**

**MASTER COMPUTER PROTECTION PLAN**

**County of Valencia**

---

Lawrence. Esquibel

Date 12/5/12

Information Technology Director

BOOK 074

PAGE 254

## Valencia 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 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 County of Valencia, 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 Manager, (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 *Valencia 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 least annually, to verify that information is being protected. As part of that annual review, this MCP will be reviewed and updated as necessary.



## Valencia County Computer Security Policy Appendix B

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.

### 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.

## 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 SpiceWorks helpdesk tracking system.

Requests are entered into SpiceWorks by submitting a request through the link to SpiceWorks on the intranet, sending an email to the IT group address within Outlook, which creates a request in SpiceWorks, or by calling 288-9117 for emergency situations during work hours.

By using your account and password, you can login and monitor your request as it progresses. End users can also submit a request by accessing the intranet and clicking on Services> and IT Support Request and submitting a request. They can login and monitor their request as it progresses.

### Emergency Support -

Call out support for emergency IT situations is available 24x7 by calling 288-9117.

## ITD Supported Hardware

1. **Approved hardware purchases.** Departments with budget approval can request a standard VDI unit from the ITD. If the department has special requirements or needs a notebook, they can place a written work request to ITD explaining the requirements and asking for a special quote. ITD will provide the quote to the department and the department will be able to order the computer through Procurement.
2. **Approved portable device purchases.** IT will keep a list of currently supported Smart Phone/Tablet/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. The end use is financially responsible for the replacement of any device provided to them by the county should it be lost, damaged or stolen.

## 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 job-ready 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
- ITD will be advised in writing of any software maintenance agreements entered into with a vendor and the duration and contact information for the vendor.
- 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
- Replace hardware as dictated by this policy
- 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/Department 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 director 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/Department 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.**

BEFORE THE BOARD OF COUNTY COMMISSIONERS  
OF VALENCIA COUNTY

In the matter of Amending the Zone Map  
from RR-2 to C-2, Valencia County, New  
Mexico, application by Simon and Catrina  
Montano

**FINDINGS OF FACT, CONCLUSIONS OF LAW AND DECISION**

**THIS MATTER** came before the Board of County Commissioners of Valencia County ("the Board") on November 14, 2012, and was held pursuant to the applicants Simon and Catrina Montanos's application to Amend the Zoning Map from a Rural Residential-2 (RR-2) zoning designation to a Community Commercial (C-2) zoning designation on the property commonly described as: T6N, R2E, Section 3, Map 79; NMPM; Lands of Gabaldon Kids, LLC; Tracts 27-1, 27-C & Lot 17; Zoned RR-2; Filed in book 361, page 7151; of the office of the Valencia County Clerk; Also known as 3165 Highway 47, Los Lunas, NM.

The Board, having considered the documents in the record before it, testimony of staff, applicants and members of the public, and argument by the parties and/or their legal representatives, **FINDS:**

**Findings of Fact**

1. Notice of the regularly scheduled meeting of the Board of Commissioners of Valencia County, New Mexico (the "Board") on November 14, 2012, at which the final hearing of the Application to Amend Zoning Maps was published according to New Mexico Statutes and the Valencia County Interim Comprehensive Zoning Ordinance, Ordinance 2004-05, as amended ("Zoning Ordinance").
2. The applicant's request is for an amendment to the Zoning Map from a Rural Residential-2 (RR-2) zoning designation to a Community Commercial (C-2) zoning designation on the property commonly described as: T6N, R2E, Section 3, Map 79; NMPM; Lands of Gabaldon Kids, LLC; Tracts 27-1, 27-C & Lot 17; Zoned RR-2; Filed in book 361, page 7151; of the office of the Valencia County Clerk; Also known as 3165 Highway 47, Los Lunas, NM.
3. Approval of the application will result in allowing a residential and commercial security system shop on the subject property.
4. The property for which the zone change is requested has a Rural Residential-2 (RR-2) zoning designation.
5. The purpose of the Rural Residential Districts is to provide for varying densities of rural residential development on selected lands identified in the comprehensive plan for preservation of low density rural living.
6. The proposed use is not permitted in the Rural Residential-2 (RR-2) zoning district.
7. The purpose of the Community Commercial (C-2) District is to provide for more intensive commercial services than in the C-1 District for numerous neighborhoods in the geographic area.
8. The proposed use is for a residential and commercial security system shop
9. The proposed use is a Permitted Use in the Community Commercial (C-2) zoning district.
10. The Planning and Zoning Commission heard this request at the monthly P&Z hearing on October 24, 2012. After hearing testimony from the applicant and taking public comments on the matter, the P&Z Commission voted 5-0 to recommend approval of the zone change.
11. The Planning and Zoning Commission found that the zone change was appropriate considering the surrounding land uses and changes in the area.
12. The Board adopts the findings of the Planning and Zoning Commission having found them to be well taken.
13. The Board of County Commissioners held a Public Hearing on this request on November 14, 2012. After hearing testimony from the applicant and taking public comments on the

(EXHIBIT B)

matter, the Board of County Commissioners voted 5-0 to approve this request on November 26, 2012.

14. There is a pattern of C-2 commercial zoning designations in the area.
15. The pattern of development in the area is predominately commercial.
16. The findings made by the Board are each independent reasons for the decision of the Board in conditionally approving the zone change.

### Conclusions of Law

The following conclusions of law are cumulative, but are severable and independent of each other.

A. The County is a zoning authority with the power to regulate and restrict use of land. NMSA 1978, § 3-21-1 (1995).

B. The Board of County Commissioners is the body that exercises the powers of a county as a body politic and corporate. NMSA 1978, § 4-38-1 (1876).

C. The Board takes notice that the Zoning Ordinance was adopted according to New Mexico statutory authority and duly recorded in the records of the Clerk of Valencia County.

D. The Board has discretion in making zoning decisions. *See Singleterry v. City of Albuquerque*, 96 N.M. 468, 471, 632 P2d 345, 348 (1981).

E. The Board has authority and jurisdiction over the Petition for Zone Change filed by Simon and Catrina Montano.

F. All parties entitled to notice were afforded notice in accordance with the applicable Valencia County Ordinances, New Mexico State Statutes, and common law.

G. The applicant and the public were afforded due process pursuant to the United States Constitution, the New Mexico Constitution, and in accordance with the applicable Valencia County Ordinances.

H. The Board takes notice that §154.061 of the Valencia County Zoning Code provides that the proposed zone change should be consistent with the goals, policies and any other applicable provisions of the Comprehensive Plan. As further delineated below, the Board's decision herein is consistent with the Comprehensive Plan.

I. The Board takes notice that the Valencia County Comprehensive Land Use Plan of October 7, 2005, ("Comprehensive Plan") is the comprehensive plan applicable to this matter, and was properly adopted according to New Mexico statutory authority.

J. Land Use and Housing Development Goal A of the Comprehensive Plan encourages the County to "guide development in a manner that balances the patterns of urban development with the rural character and natural resources of the County."

K. Economic Development Goal P of the Comprehensive Plan encourages the County to "strengthen the economic base of the County, expand employment opportunities, and improve local workforce skills and abilities."

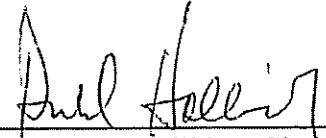
L. Section 154.061 (C) (2) of the Zoning Ordinance provides that "The proposed change [be] appropriate considering...the surrounding land uses, density and pattern of development in the area..." The future land use intended by the Applicant is consistent with the Zoning Ordinance.


**Decision**

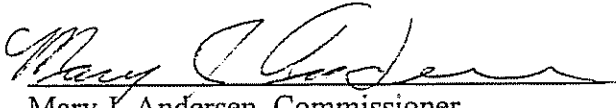
**IT IS, THEREFORE, ORDERED** that the zone change from Rural Residential (RR-2) zoning designation to a Community Commercial (C-2) zoning designation. This zone change is requested by applicant Simon and Catrina Montano in their application to Amend the Zoning Map on the property commonly described as: T6N, R2E, Section 3, Map 79; NMPM; Lands of Gabaldon Kids, LLC; Tracts 27-1, 27-C & Lot 17; Zoned RR-2; Filed in book 361, page 7151; of the office of the Valencia County Clerk; Also known as 3165 Highway 47, Los Lunas, NM. is hereby granted by a vote of 5-0.


**BOARD OF COUNTY COMMISSIONERS OF VALENCIA COUNTY**

P.O. Box 1119 / 444 Luna Ave  
Los Lunas, NM 87031

  
Donald E. Holliday, Chair

  
Georgia Otero-Kirkham, Vice-Chair

  
Mary J. Andersen, Commissioner

  
Lawrence R. Romero, Commissioner

  
Ron Gentry, Commissioner

ATTEST BY:

  
Sally Perea, County Clerk

Date: 12-5-28/2



BEFORE THE BOARD OF COUNTY COMMISSIONERS  
OF VALENCIA COUNTY

In the matter of Amending the Zone Map  
from P-D to I-3, Valencia County, New  
Mexico, application by PNM.

**FINDINGS OF FACT, CONCLUSIONS OF LAW AND DECISION**

**THIS MATTER** came before the Board of County Commissioners of Valencia County ("the Board") on November 14<sup>th</sup>, 2012, and was held pursuant to PNM's application to Amend the Zoning Map from a Planned Development (P-D) zoning designation to a Heavy Industrial (I-3) zoning designation on the lot commonly described as: T6N, R3E, Section 18; NMPM; Sierra Vista Subdivision; Filed in Cabinet J, Page 288-229; of the office of the Valencia County Clerk.

The Board, having considered the documents in the record before it, testimony of staff, applicants and members of the public, and argument by the parties and/or their legal representatives, **FINDS:**

**Findings of Fact**

1. Notice of the regularly scheduled meeting of the Board of Commissioners of Valencia County, New Mexico (the "Board") on November 14<sup>th</sup>, 2012, at which was had the public hearing of the Application to Amend Zoning Maps, was published according to New Mexico Statutes and the Valencia County Interim Comprehensive Zoning Ordinance, Ordinance 2004-05, as amended ("Zoning Ordinance").
2. The applicant's request is for an amendment to the Zoning Map from a Planned Development (P-D) zoning designation to a Heavy Industrial (I-3) zoning designation on the property commonly described as: T6N, R3E, Section 18; NMPM; Sierra Vista Subdivision; Filed in Cabinet J, Page 288-229; of the office of the Valencia County Clerk.
3. Approval of the application will result in allowing for the development of a solar generating facility.
4. The property for which the zone change is requested has a Planned Development (P-D) zoning designation.
5. The purpose of the Planned Development District (PD) is to allow and encourage comprehensive development rather than traditional parcel-by-parcel development.
6. The proposed use is not permitted in the P-D District.
7. The purpose of the I-3 District is to provide for industrial uses with high nuisance characteristics that are incompatible with adjacent urban residential uses or for industrial uses where space or performance characteristics demand a specialized locale. The proposed use is for a solar generating facility.
8. The proposed use is permitted in the Heavy Industrial (I-3) zone district.
9. The Planning and Zoning Commission heard this request at the monthly P&Z hearing on October 24, 2012. After hearing testimony from the applicant and taking public comments on the matter, the P&Z Commission voted 5-0 to recommend approval of the zone change.
10. The Planning and Zoning Commission Found:
  - a. The development as described by the applicant (solar energy generation station) is appropriate considering the surrounding land use and pattern development in the area.
  - b. The development as described by the applicant (solar energy generation station) enhances the County's protection of public health, safety and welfare.
  - c. The development as described by the applicant (solar energy generation station) provides quality public utility that will steer urbanizing development to areas with adequate infrastructure and utility.

(EXHIBIT C)

- d. The development as described by the applicant (solar energy generation station) strengthens the economic base of the County.
11. The Board finds the findings of the Planning and Zoning Commission well taken, and adopts them in part.
12. The Board of County Commissioners held a Public Hearing on this request on November 14, 2012. After hearing testimony from the applicant and taking public comments on the matter, the Board of County Commissioners voted 5-0 to approve this request on November 26, 2012.
13. The findings made by the Board are each independent reasons for the decision of the Board in conditionally approving the zone change.

### Conclusions of Law

The following conclusions of law are cumulative, but are severable and independent of each other.

A. The County is a zoning authority with the power to regulate and restrict use of land. NMSA 1978, § 3-21-1 (1995).

B. The Board of County Commissioners is the body that exercises the powers of a county as a body politic and corporate. NMSA 1978, § 4-38-1 (1876).

C. The Board takes notice that the Zoning Ordinance was adopted according to New Mexico statutory authority and duly recorded in the records of the Clerk of Valencia County.

D. The Board has discretion in making zoning decisions. *See Singleterry v. City of Albuquerque*, 96 N.M. 468, 471, 632 P2d 345, 348 (1981).

E. The Board has authority and jurisdiction over the Petition for Zone Change filed by Manzano Solar Energy Center.

F. All parties entitled to notice were afforded notice in accordance with the applicable Valencia County Ordinances, New Mexico State Statutes, and common law.

G. The applicant and the public were afforded due process pursuant to the United States Constitution, the New Mexico Constitution, and in accordance with the applicable Valencia County Ordinances.

H. The Board takes notice that §154.061 of the Valencia County Zoning Code provides that the proposed zone change should be consistent with the goals, policies and any other applicable provisions of the Comprehensive Plan. As further delineated below, the Board's decision herein is consistent with the Comprehensive Plan.

I. The Board takes notice that the Valencia County Comprehensive Land Use Plan of October 7, 2005, ("Comprehensive Plan") is the comprehensive plan applicable to this matter, and was properly adopted according to New Mexico statutory authority.

J. Land Use and Housing Development Goal A of the Comprehensive Plan encourages the County to "guide development in a manner that balances the patterns of urban development with the rural character and natural resources of the County."

K. Regional Infrastructure Goal K of the Comprehensive Plan encourages the County to "Promote regional facilities and services that meet health and safety needs of the County."

L. Economic Development Goal P of the Comprehensive Plan encourages the County to "Strengthen the economic base of the County, expand employment opportunities, and improve local workforce skills and abilities."

M. Section 154.061 (C) (2) of the Zoning Ordinance provides that "The proposed change [be] appropriate considering...the surrounding land uses, density and pattern of development in the area..." The future land use intended by the Applicant is consistent with the Zoning Ordinance.

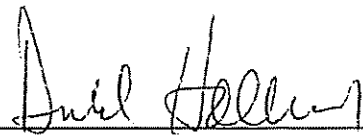
**Decision**

**IT IS, THEREFORE, ORDERED** that zone change from Planned Development (P-D) zoning designation to a Heavy Industrial (I-3) zone designation is conditionally approved with the following conditions:


1. Applicant recognizes and agrees that it shall submit proof of financing to County Planning and Zoning and start on actual site preparation within five years of approval of this quasi-judicial district change, in addition to the other requirements set forth in the County's zoning ordinance, and recognizes and agrees that if Applicant fails to submit proof of financing to County Planning and Zoning and start actual land preparation within five years of approval of this quasi-judicial district change, or otherwise fails to satisfy the other requirements set forth in the County's zoning ordinance, the property will automatically and without action by the County or applicant revert back to P-D by operation of law and/or the agreement of the parties.
2. Applicant further recognizes and agrees that if the use of the property as a Solar Energy Facility ever shall cease, the property will automatically and without action by the County or applicant revert back to P-D by operation of law and/or the agreement of the parties.
3. Applicant further recognizes and agrees that this property will not be utilized for any other purpose permitted in an I-3 zone except that provided above, and that should the property be used for any other such purpose, the property will automatically and without action by the County or applicant revert back to P-D by operation of law and/or the agreement of the parties.

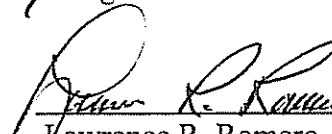
**BOARD OF COUNTY COMMISSIONERS OF VALENCIA COUNTY**

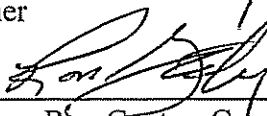
P.O. Box 1119 / 444 Luna Ave  
Los Lunas, NM 87031

  
Donald E. Holliday, Chair

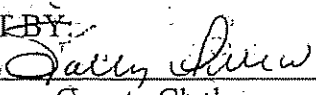
  
Georgia Otero-Kirkham, Vice-Chair

  
Mary J. Andersen, Commissioner

  
Lawrence R. Romero, Commissioner

  
Ron Gentry, Commissioner

ATTEST BY:

  
Sally Perea, County Clerk

Date: 12-5-2012

I hereby acknowledge, represent, warrant and confirm that I have the authority to bind the applicant, Manzano Solar Energy Center, and that I have read and understand the conditions set forth above, that I have had the assistance of counsel, or the opportunity to obtain counsel, in reviewing, discussing, and considering the conditions set forth in these Findings of Fact and Conclusions of Law, and, if applicable, that counsel has read and considered the conditions and has advised me on these conditions, and I agree to be bound by these terms and conditions. These conditions shall be binding upon the parties and their heirs, executors, administrators, assigns, successors in interest, predecessors in interest, and anyone claiming by, through, or under any one of the parties.

**Manzano Solar Energy Center**

By: \_\_\_\_\_ Date: \_\_\_\_\_

Title: \_\_\_\_\_

**VALENCIA COUNTY  
BOARD OF COUNTY COMMISSIONERS  
ACCOUNTS PAYABLE AUTHORIZATION**

*Sally Perea*  
The attached computer printout lists all the checks issued by the Manager's Office on November 20, 2012 covering vendor bills processed on the above date.  
Check # 116060 to 116127 inclusive, for the total of \$249,998.74.

All have been reviewed for:

1. Appropriate documentation and approvals.
2. Authorized budget appropriations.
3. Compliance with New Mexico Statutes, and
4. DFA Rules and Regulations.

In recognition of the above, the Fiscal Office requests this action be officially recorded in the minutes of the regular county commission meeting before which body this matter came.


Recommended:

  
\_\_\_\_\_  
Nick Telles-Finance Director

Done this 5th day of December, 2012.

**VALENCIA COUNTY BOARD OF COMMISSIONERS**

  
\_\_\_\_\_  
Donald E. Holliday, Chair

  
\_\_\_\_\_  
Lawrence R. Romero, Commissioner

  
\_\_\_\_\_  
Ron Gentry, Commissioner

  
\_\_\_\_\_  
Georgia Otero-Kirkham, Vice-Chair

  
\_\_\_\_\_  
Mary J. Andersen, Commissioner

ATTEST:

  
\_\_\_\_\_  
Sally Perea, County Clerk

(EXHIBIT D)

**VALENCIA COUNTY  
BOARD OF COUNTY COMMISSIONERS  
ACCOUNTS PAYABLE AUTHORIZATION**

*Sally Perea*  
The attached computer printout lists all the checks issued by the Manager's Office on November 28, 2012 covering vendor bills processed on the above date.  
Check # 116131 to 116200 inclusive, for the total of \$179,926.46.

All have been reviewed for:

1. Appropriate documentation and approvals.
2. Authorized budget appropriations.
3. Compliance with New Mexico Statutes, and
4. DFA Rules and Regulations.


In recognition of the above, the Fiscal Office requests this action be officially recorded in the minutes of the regular county commission meeting before which body this matter came.


Recommended:

  
\_\_\_\_\_  
Nick Telles-Finance Director

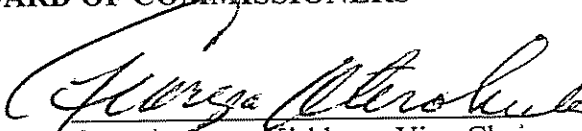
Done this 5th day of December, 2012.

**VALENCIA COUNTY BOARD OF COMMISSIONERS**

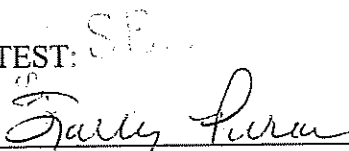
  
\_\_\_\_\_  
Donald E. Holliday, Chair

  
\_\_\_\_\_  
Lawrence R. Romero, Commissioner

  
\_\_\_\_\_  
Ron Gentry, Commissioner

  
\_\_\_\_\_  
Georgia Otero-Kirkham, Vice-Chair

  
\_\_\_\_\_  
Mary J. Andersen, Commissioner

ATTEST:   
\_\_\_\_\_  
Sally Perea, County Clerk

(EXHIBIT E)

Sally

VALENCIA COUNTY  
BOARD OF COUNTY COMMISSIONERS  
PAYROLL AUTHORIZATION

The attached computer printout lists all checks issued by the Managers Office on November 30, 2012 covering payroll process on the above date.  
Direct Deposit Check# 27999 through Direct Deposit Check # 28195 inclusive.  
Deduction Check # 0116201 through Deduction Check # 0116237 inclusive.  
Payroll Check #93665 through Payroll Check # 93727 inclusive.  
Listing total \$ 417,974.84

All have been reviewed for:

1. Appropriate documentation and approvals.
2. Authorized budget appropriations.
3. Compliance with New Mexico Statutes, and
4. DFA Rules and Regulations


In recognition of the above, the Manager's Office request this action be officially recorded in the minutes of the regular County Commission meeting before which body this matter came.


Recommended:

  
Nick Telles, Finance Director

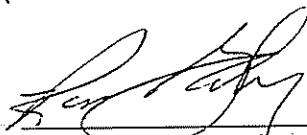
Done this 30<sup>th</sup> day of December, 2012

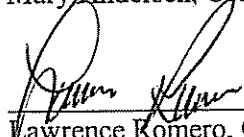
VALENCIA COUNTY BOARD OF COMMISSIONERS

  
Donald E. Holliday, Chair

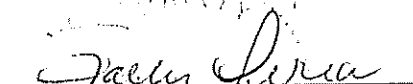
  
Georgia Otero-Kirkham, Vice Chair

  
Mary Andersen, Commissioner

  
Ron Gentry, Commissioner

  
Lawrence Romero, Commissioner

ATTEST:

  
Sally Perea, County Clerk

(EXHIBIT F)