

SOCORRO COUNTY
BOARD OF COUNTY COMMISSIONERS
RESOLUTION 2011-25

INFORMATION SYSTEMS POLICY

1.0 PURPOSE

- 1.1 The Socorro County Manager's Office is charged with coordinating vendors to manage the County's computer network, personal computers used by the county employees and officials, and services and support for those machines.

2.0 RESPONSIBILITIES & ACCESS

- 2.1 All County employees with access to the County's local area network (LAN) for the purpose of electronic communications, software usage, and electronic research shall have a record of access permissions kept in the Manager's office. Electronic communication will include that with other county employees and officials and individuals and organizations outside of Socorro County as needed. Software will include timekeeping software, an electronic mail application, word processing and spreadsheet software, office-specific software (i.e. Data Now, Tyler) and other applications as needed for each employee to effectively perform tasks.
- 2.2 All computer systems users' identities will be protected from fraudulent use by password access. Passwords shall be required to include seven to fourteen characters, should not contain words in any language, and must contain alphanumeric characters and symbols. Passwords shall be routinely changed at least every six months.
- 2.3 The Manager's Office shall take extra effort to ensure that all County computer systems have security measures that meet or exceed local government audit standards and ensure that these measures are appropriately implemented.
- 2.4 The County's IT vendor shall keep a log of equipment failures and downtime, network audit logs, and network activity reports to be reviewed by auditors and for system evaluation.

3.0 BACKUPS

- 3.1 Any network servers shall have complete backups performed nightly after every business day. One week of daily backups shall be performed on a singular tape and daily backup tapes shall be retained for two months then rotated through the cycle.
- 3.2 Monthly server backups shall be performed on the last business day of each month. Monthly backup tapes shall be retained for four months as a secondary or point in time recovery method.
- 3.3 It is the goal of Socorro County to implement server mirroring for real time backup between the County Courthouse and Annex buildings in the future.
- 3.4 All vital information shall not be kept on the PC's, but on the servers instead, alleviating the need to backup PC's. Any vital software installed on PC's in the County shall be stored in an appropriate storage facility with the County's IT vendor.

3.5 Personal Computers (PC's) shall not be backed up unless they do not have server access. It is the responsibility of the department head to ensure those PC's not integrated with County servers are backed up weekly using alternate storage such as an independent hard drive or USB drive.

4.0 IMPLEMENTING & TESTING NEW SOFTWARE

- 4.1 New software shall first be installed and tested in a non-production test environment. After the IT vendor is satisfied with the operation of the software it can be implemented across County system.
- 4.2 New software that will only be used by a small group will be installed first on a test machine. Once the County's IT vendor is satisfied, the software will then be deployed to County users.
- 4.3 If the software is an upgrade that doesn't require all users to upgrade immediately, one user will be upgraded to test the software. Once the IT Vendor is satisfied the software will be deployed.
- 4.4 If the software is an upgrade that requires all users to upgrade simultaneously the upgrade will be deployed to all users with the option of uninstalling the software and reinstalling the previous version.

5.0 E-MAIL BACKUPS

- 5.1 All County email data will be backed up nightly and backup tapes shall be retained for at least two weeks (14 days).
- 5.2 Any email or e-messaging records that include any of the following items must be archived in searchable database maintained by the individual department/office OR a hardcopy must be printed and retained. This includes email or e-messaging records that are:
 - 1. Policies and directives;
 - 2. correspondence or memoranda that contain final directives, determinations, instructions or guidance regarding public business;
 - 3. minutes of governing boards, advisory groups, ad-hoc committees or work groups developing programs;
 - 4. messages that authorize, establish or complete a business transaction; or
 - 5. final reports or recommendations such as to legislative committees or produced by task forces or study groups.

6.0 USER TERMINATION

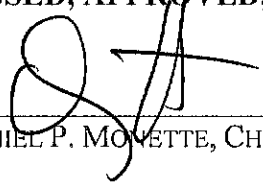
- 6.1 All department heads and elected officials will complete the exit worksheet for the Manager's Office. The Manager's Office will contact the IT vendor to remove system access for any terminated employee.
- 6.2 All data shall be deleted along with user access. No retention of data is planned once a county employee has been terminated.

7.0 INHERITANCE PROGRAM

7.1 The County will develop a formal PC inheritance program for those machines that have a long use life. In order to ensure proper compliance and compatibility with current systems as well as uniformity within County offices, the County implementation of a PC inheritance program for other equipment is not recommended.


7.2 Any outdated or decommissioned PC's will be removed from service. Hard drives and all RAM will be removed and permanently destroyed by the County's IT Vendor and a statement of destruction will be given to the County Manager's office. The remaining computer is then placed in the County's disposal list or transported to the appropriate landfill for disposal or recycling.


PASSED, APPROVED, and ADOPTED this 25th day of January, 2011.


DANIEL P. MONETTE, CHAIR


PAULINE JARAMILLO, VICE-CHAIR


PHILLIP ANAYA


RUMALDO J. GRIEGO


JUAN JOSE GUTIERREZ



ATTEST BY:

REBECCA (BECKY) VEGA, COUNTY CLERK