ADMINISTRATIVE ORDER
OF THE
JEFFERSON COUNTY COMMISSION
04-3

PURSUANT to the authority vested in the Jefferson County Commission by law, the following Administrative Order is hereby issued:

PURPOSE

To establish a uniform policy and procedure for the protection of the County's information and technology resources.

I. POLICY

The policies in the attached Jefferson County Information Technology Security Policy are hereby adopted as if fully set out herein.

II. PROCEDURES

The procedures in the attached Jefferson County Information Technology Security Policy are hereby adopted as if fully set out herein.

III. DISCIPLINARY ACTION

Employees who fail to comply with the Jefferson County Information Technology Security Policy are subject to disciplinary action which may include termination of employment for a first offense.

ORDERED at the Jefferson County Courthouse this 9th day of November, 2004.

LARRY P. LANGFORD, President
Jefferson County Commission

APPROVED BY THE
JEFFERSON COUNTY COMMISSION
DATE: 11-9-04
MINUTE BOOK: 146
PAGE(S): 361-379

Jefferson County
Information Technology
Security Policy

Prepared by the

Jefferson County Department of Information Technology

Version 1.0

TABLE OF CONTENTS

Section 1: Establishment of Security Program

1.1 *Policy Intent:*

This Jefferson County *Information Technology Security Program* will assign responsibility and clarify behavioral expectations to safeguard technology-related information and tools. It also provides guidance for administering the Jefferson County Information Technology Security Policy. This policy is designed to protect Jefferson County's internal and external information resources.

This policy was created to comply with Section 5, Paragraph B, Item 6 of **Administrative Order 92-2** which directs the IT Department to "Develop and implement security policies and procedures pertaining to the County's wide area network, local area networks, and central computer platforms … ".

1.2 *Scope:*

This policy applies to all Jefferson County organizations, employees, and contractors, and any other individuals or organizations that use Jefferson County technology resources. Jefferson County technology resources include, but are not limited to: networks, servers, data, applications, and information. It applies to all Jefferson County facilities.

1.3 *Policy:*

It will be the policy of the Jefferson County Commission to establish and maintain an *Information Technology Security Program* to create policy and procedures to protect Jefferson County's information and technology resources.

The Commission is the final authority for policy and procedures relating to technology security.

The Department of Information Technology will act as the Commission's controlling authority in matters of data security, internet security, security policy development, security standards, security services, and compliance.

The Department of Information Technology will create standards and procedures, consistent with sound business practices that support and enforce the Jefferson County Information Technology Security Policy.

Standards and procedures will consist of usual, customary, and reasonable security practices, and should not inflict undue hardship on the Jefferson County computing community.

Because an item or activity is not expressly prohibited does not mean the item or activity is permitted. The security of such items or activities will be decided by the Department of Information Technology on a case-by-case basis.

Like **Administrative Order 92-2**, violations of Jefferson County's security policy shall subject the responsible individual or user to disciplinary action, up to and including termination.

This policy will be reviewed twice a year by the Department of Information Technology, and changes will be recommended that keep it current as information technology evolves and changes.

1.4 *Policy Owner:*

Jefferson County Commission

1.4a *Policy Administrator:*

Chief Information Officer, Department of Information Technology

1.5 *Policy Approval Date:*

1.6 *Policy Effective Date:*

April 5, 2004

1.7 *Terms and Definitions:*

Section 2: Backup and Recovery

2.1 *Policy Intent:*

The intent of this policy is to establish responsibility and accountability for maintaining the ability to recover and restore data/information.

2.2 *Scope:*

This policy applies to all Jefferson County organizations, employees, and contractors, and any other individuals or organizations that use Jefferson County technology resources. Jefferson County technology resources include, but are not limited to: networks, servers, data, applications, and information. It applies to all Jefferson County facilities.

2.3 *Policy:*

The Department of Information Technology will execute regularly scheduled backups of data resident in the data center, and for other organizations with whom the Department of Information Technology has an approved Backup & Recovery Agreement.

The Department of Information Technology will not be responsible for backup or recovery of data not stored in the data center, nor for any organization with whom the Department of Information Technology does not have an approved Backup & Recovery Agreement.

Configurations of network transport equipment will be backed up regularly.

The process of restoring data will be tested and confirmed on at least a semi-annual basis.

The Department of Information Technology will develop and maintain a disaster recovery plan. This plan will be tested at least annually.

User requests to restore data must be in writing from a supervisor or other manager, and all requests will be verified for appropriateness.

Backup media will be stored at a secure offsite location.

2.4 *Policy Owner:*

Jefferson County Commission

2.4a *Policy Administrator:*

IT Infrastructure Manager, Department of Information Technology

2.5 *Policy Approval Date:*

2.6 *Policy Effective Date:*

April 5, 2004

2.7 *Terms and Definitions:*

Network Transport equipment – routers, switches, and hubs used to move information through the County's network.

Backup Media – tapes, discs, optical platters, or any other media used in the backup process.

Section 3: User Accountability

3.1 *Policy Intent:*

This policy section is intended to communicate Jefferson County's commitment to information security, and to define the individual user's responsibility for ensuring information security policies are adhered to and enforced.

3.2 *Scope:*

This policy applies to all Jefferson County organizations, employees, and contractors, and any other individuals or organizations that use Jefferson County technology resources. Jefferson County technology resources include, but are not limited to: networks, servers, data, applications, and information.

3.3 *Policy:*

Officials, employees, contractors, and vendors providing information technology services will abide by and follow Jefferson County's information security policies, and adhere to all security standards and guidelines.

Officials, employees, contractors, and vendors will protect information from unauthorized disclosure or interception.

Officials, employees, contractors, and vendors will safeguard the accuracy and completeness of information stored and processed by Jefferson County's computer systems.

Officials, employees, contractors, and vendors will ensure that information is available to authorized users with the least impact on their productivity and the least costs to Jefferson County.

Officials, employees, contractors, and vendors will protect and maintain the confidentiality of jurisdictional and citizen information.

Users will report any security violations to their supervisor or manager.

Employees, contract personnel and vendors will sign an agreement indicating they have read Jefferson County's information security policies and they are committed to comply with those policies and the supporting procedures and standards.

3.4 *Policy Owner:*

Jefferson County Commission

3.4a *Policy Administrator:*

Chief Information Officer, Department of Information Technology

3.5 *Policy Approval Date:*

3.6 *Policy Effective Date:*

April 5, 2004

3.7 *Terms and Definitions:*

Section 4: Operational Health

4.1 *Policy Intent:*

This policy section establishes guidelines for maintaining the operational health of Jefferson County's computing environment.

4.2 *Scope:*

This policy applies to all Jefferson County organizations, employees, and contractors, and any other individuals or organizations that use Jefferson County technology resources. Jefferson County technology resources include, but are not limited to: networks, servers, data, applications, and information. It applies to all Jefferson County facilities.

4.3 *Policy:*

The Department of Information Technology will ensure monitoring and logging are in place on all critical systems, servers, and applications.

The Department of Information Technology will periodically verify the level and viability of system monitoring.

Audit logs will be initiated and will contain adequate information to construct an appropriate review of system activities, track the sequence of events, and detect suspicious activities or system failures.

The Department of Information Technology will monitor network and computer operations to detect suspicious or unauthorized activities.

4.4 *Policy Owner:*

Jefferson County Commission

4.4a *Policy Administrator:*

IT Infrastructure Manager, Department of Information Technology

4.5 *Policy Approval Date:*

4.6 *Policy Effective Date:*

April 5, 2004

4.7 *Terms and Definitions*

Systems (in this context) - an automated process or function made up of multiple computer applications.

Audit Log – a record of events which chronicles the changes that occurred while a computer program was running.

Section 5: Access Control

5.1 *Policy Intent:*

The intent of this policy section is to ensure access to systems and data is assigned, approved, and removed in an appropriate manner.

5.2 *Scope:*

This policy applies to all Jefferson County organizations, employees, and contractors, and any other individuals or organizations that use Jefferson County technology resources. Jefferson County technology resources include, but are not limited to: networks, servers, data, applications, and information. It applies to all Jefferson County facilities.

5.3 *Policy:*

Every user of computerized information will have a unique system account and a unique identification assigned.

All user accounts for access to Jefferson County computing resources will be created by the Department of Information Technology organization.

Every user, when signing-on, will be required to provide a means of authentication such as a password, in order to gain access to the network.

Access to the network will be requested and approved by a manager or supervisor. This authorization shall be consistent with the level of access required for the user to perform their assigned responsibilities.

All local area networks connecting to the wide area network must comply with the security guidelines for authorization and authentication.

Access to hosts by vendors and service providers will be granted for specific purposes only, for a limited time frame, and all activities will be logged, recorded and supervised by a manager.

When an employee resigns or is terminated, takes a long-term leave, or when a contract person completes their assignment, the Department of Information Technology will be notified immediately by the appropriate department head or his/her representative. Immediately system access will be removed and all access to data will be removed.

The Department of Information Technology will review user accounts that have had no activity for 30 days to determine their status.

The Department of Information Technology will periodically review user accounts to insure all terminated and inactive users are disabled or removed from the system.

User accounts that are inactive for 30 days will be disabled, and after 60 days shall be reviewed for possible deletion.

Users, when terminated, will have account access disabled with complete account removal from the system after 60 days.

See Section 12 for policy on password management.

5.4 *Policy Owner:*

Jefferson County Commission

5.4a *Policy Administrator:*

System Administrators, Department of Information Technology

5.5 *Policy Approval Date:*

5.6 *Policy Effective Date:*

April 5, 2004

5.7 *Terms and Definitions:*

Host – any computer or equipment containing or accessing Jefferson County information.

Section 6: Acceptable System Usage (Security)

6.1 *Policy Intent:*

The purpose of this policy section is to reinforce the secure use of computing and telecommunications equipment and software at Jefferson County.

6.2 *Policy Scope:*

This policy applies to all Jefferson County organizations, employees, and contractors, and any other individuals or organizations that use Jefferson County technology resources. Jefferson County technology resources include, but are not limited to: networks, servers, data, applications, and information. It applies to all Jefferson County facilities.

6.3 *Policy:*

Under no circumstances is a Jefferson County official, employee, contractor, or vendor authorized to engage in any activity that is illegal under local, state, federal or international law, while utilizing Jefferson County-owned computing resources.

Jefferson County officials, employees, contractors, and vendors will comply with Jefferson County security policies while utilizing Jefferson County-owned computing resources.

Jefferson County officials, employees, contractors, and vendors will not knowingly take any action that would jeopardize the security of Jefferson County-owned computing resources, including but not limited to:

- Circumventing user authentication or security of any host, network or account,
- Port scanning or security scanning,
- Revealing your account password to others or allowing use of your account,
- Packet spoofing,
- Using an account you are not authorized to use,
- Providing list of or information about Jefferson County employees to parties outside Jefferson County,
- Network sniffing,
- Accessing information to which you are not entitled,

- Disabling security features on any workstation or server.

6.4 *Policy Owner:*

Jefferson County Commission

6.4a *Policy Administrator:*

Shared by:
Chief Information Officer, Department of Information Technology
Appropriate department managers

6.5 *Policy Approval Date:*

6.6 *Policy Effective Date:*

April 5, 2004

6.7 *Terms and definitions:*

Port scanning or security scanning – the process of probing a network looking for exploitable communications channels.

Packet spoofing – the act of assuming the identity (IP address) of another network user, generally for malicious or illegal purposes.

Network sniffing – the process of capturing and decoding network traffic in search of passwords, credit card numbers, user accounts, or other information to which one would not normally be entitled.

Section 7: Information Security and Protection

7.1 *Policy Intent:*

This policy section establishes standards for the protection of Jefferson County's computer network.

7.2 *Scope:*

This policy applies to all Jefferson County organizations, employees, and contractors, and any other individuals or organizations that use Jefferson County technology resources. Jefferson County technology resources include, but are not limited to: networks, servers, data, applications, and information. It applies to all Jefferson County facilities.

7.3 *Policy:*

The Department of Information Technology has responsibility for the security and protection of Jefferson County's network.

Appropriate authentication, logging, and restrictions will be instituted and maintained to ensure Jefferson County's network is secured.

An intrusion protection system will be instituted and maintained to protect the County from malicious code and would-be interlopers.

Gateways and/or other filters will be installed and maintained to protect the County's network from viruses, worms, and other forms of malicious code.

Incoming email attachments and other file downloads will be limited to those files that have a low probability of containing malicious code.

Firewalls will be used where appropriate to maintain safe communications into and out of the County computer network.

No publicly accessible web server will be connected to the backbone of Jefferson County's network. All web servers will be isolated from the backbone using appropriate firewall technology.

Usual, customary, and reasonable encryption standards will be used. Encryption key management will be utilized to insure the safe and secure exchange of encryption keys.

7.4 *Policy Owner:*

Jefferson County Commission

7.4a *Policy Administrator:*

IT Infrastructure Manager, Department of Information Technology

7.5 *Policy Approval Date:*

7.6 *Policy Effective Date:*

April 5, 2004

7.7 *Terms and Definitions:*

Intrusion protection system – a system for detecting inappropriate, incorrect, malicious, or anomalous activity on a network.

Malicious code – a computer program or other resource that intentionally causes harm.

Gateway – a computer application through which network traffic passes for purposes of auditing, monitoring, blocking, testing, or filtering.

Firewall – a network security device or program used primarily to separate a private network from the Internet, and to help control and manage access for Internet users.

Backbone – that private portion of Jefferson County's network to which Jefferson County users and hosts are attached.

Section 8: Internet Access and Usage

8.1 *Policy Intent:*

This policy establishes standards of acceptable Internet usage, and identifies controls and constraints that will be applied.

8.2 *Scope:*

This policy applies to all Jefferson County organizations, employees, and contractors, and any other individuals or organizations that use Jefferson County technology resources. Jefferson County technology resources include, but are not limited to: networks, servers, data, applications, and information. It applies to all Jefferson County facilities.

8.3 *Policy:*

An Internet Service Provider (ISP) can attach to Jefferson County's network only with the approval of the Department of Information Technology.

Access to the Internet is provided to accommodate County business. Limited personal use is not inherently a violation of this policy, provided such use may be restricted or terminated by a supervisor for abuse, or for jeopardizing the security of Jefferson County's computing environment.

Internet access from Jefferson County's network will be granted only to individuals who complete a Memorandum of Understanding (MoU) and have it signed by a sponsoring Commissioner.

All inbound and outbound Internet traffic will go through a proxy server maintained by the IT department.

Bypassing the proxy server is not permitted, except by approval of the IT Department. Users who are authorized to bypass the proxy server should do so only for those operations for which they were granted approval to bypass the proxy server.

Inappropriate web sites will be blocked from access. Examples include pornography, gambling, and entertainment.

Internet usage that poses a security threat will be blocked. Examples of such usage include instant messaging, peer-to-peer, and public email.

Spyware, and other stealth information gathering programs should not be knowingly installed on networked workstations, and will be blocked from Internet access.

8.4 *Policy Owner:*

Jefferson County Commission

8.4a *Policy Administrator:*

Network Manager, Department of Information Technology

8.5 *Policy Approval Date:*

8.6 *Policy Effective Date:*

April 5, 2004

8.7 *Terms and Definitions*

Internet Service Provider - a company who provides the connection that allows a person or organization to access the Internet.

Proxy server – a device or program which communications with the Internet on behalf of users, generally providing increased security.

Spyware – any technology that aids in gathering information about a person or organization without their knowledge. On the Internet, it is used to secretly gather information about the user and relay it to advertisers or other interested parties.

Stealth – computer programs that operate without the knowledge of the computer user. Many spyware programs operate in a stealth mode.

Section 9: e-Mail Use and Accountability

9.1 *Policy Intent:*

The intent of this policy section is to establish acceptable e-mail use within Jefferson County's networked environment.

9.2 *Scope:*

This policy applies to all Jefferson County organizations, employees, and contractors, and any other individuals or organizations that use Jefferson County technology resources. Jefferson County technology resources include, but are not limited to: networks, servers, data, applications, and information. It applies to all Jefferson County facilities.

9.3 *Policy:*

E-mail is provided to accommodate County business. Limited personal use is not inherently a violation of this policy, provided such use may be restricted or terminated by a supervisor for abuse, or for jeopardizing the security of Jefferson County's computing environment.

All e-mail systems and services will be approved by the Department of Information Technology prior to installation or operation.

The size of e-mail attachments will be limited.

The amount of storage allocated to individuals for the storage of e-mail messages will be limited.

Requests for e-mail for a Jefferson County employee will be submitted in writing and will be approved by the appropriate supervisor. Requests for e-mail for service providers will be submitted in writing and will be approved by an Information Technology manager.

See **Administrative Order 04-1** (04/27/04) for additional email usage policies and prohibitions.

9.4 *Policy Owner:*

Jefferson County Commission

9.4a *Policy Administrator:*

Systems Administrator, Department of Information Technology

9.5 *Policy Approval Date:*

9.6 *Policy Effective Date:*

April 5, 2004

9.7 *Terms and Definitions:*

Section 10: Security Incident Management and Response

10.1 *Policy Intent:*

This policy section will establish the creation of a team to respond to security incidents.

10.2 *Scope:*

This policy applies to all Jefferson County organizations, employees, and contractors, and any other individuals or organizations that use Jefferson County technology resources. Jefferson County technology resources include, but are not limited to: networks, servers, data, applications, and information. It applies to all Jefferson County facilities.

10.3 *Policy:*

A Computer Incident Response Team (CIRT) will be established and maintained by the Department of information Technology to respond to security incidents.

The Computer Incident Response Team (CIRT) will develop and maintain appropriate responses and take appropriate action when a technology security incident occurs.

The Computer Incident Response Team (CIRT) will recommend revisions to processes, guidelines, and procedures that will help prevent future security incidents.

10.4 *Policy Owner:*

Jefferson County Commission

10.4a *Policy Administrator:*

Chief Information Officer, Department of Information Technology

10.5 *Policy Approval Date:*

10.6 *Policy Effective Date:*

April 5, 2004

10.7 *Terms and Definitions:*

Incident - an event that produces actual or potent adverse impact on computer or network operations.

Section 11: Security Approvals

11.1 *Policy Intent:*

The intent of this policy section is to ensure all activity by information technology administrators is properly monitored and reviewed.

11.2 *Scope:*

This policy applies to all Jefferson County information technology administrators, and any other individuals or organizations that might perform in that capacity.

11.3 *Policy:*

Information technology administrators will be granted only those rights required to carry out their assigned roles and responsibilities.

All requests for administrator rights will be documented with the requested rights properly defined and justified.

An appropriate manager will approve the rights and privileges of all information technology administrators.

All activity by information technology administrators will be properly monitored and reviewed.

Administrator accounts will not be used when a non-privileged account will suffice.

11.4 *Policy Owner:*

Jefferson County Commission

11.4a *Policy Administrator:*

IT Infrastructure Manager, Department of Information Technology

11.5 *Policy Approval Date:*

11.6 *Policy Effective Date:*

April 5, 2004

11.7 *Terms and Definitions:*

Information Technology Administrator – a person trained in the configuration and management of networks or computer hardware and software, and charged with maintaining networks or computer systems in good working order.

Administrator Rights – the authority and access privileges granted to those responsibility for maintaining computer systems or networks in good working order.

Section 12: Passwords and Password Aging

12.1 *Policy Intent:*

The intent of this policy section is to establish standards for the effective use of passwords to access information technology solutions.

12.2 *Scope:*

This policy applies to all Jefferson County organizations, employees, and contractors, and any other individuals or organizations that use Jefferson County technology resources. Jefferson County technology resources include, but are not limited to: networks, servers, data, applications, and information. It applies to all Jefferson County facilities.

12.3 *Policy:*

Every user is required to provide a password to verify his/her identity to the system, and to receive authorization for access to the network, applications, servers, and data.

Each user will be personally accountable for all activities and transactions associated with his/her user identification (password).

Individuals will change their passwords every 30 days, or other appropriate frequency as specified by the Department of Information Technology security guidelines.

Jefferson County Department of Information Technology shall develop and maintain guidelines and tools for the effective management of passwords.

12.4 Policy Owner:

Jefferson County Commission

12.4a Policy Administrator:

IT Infrastructure Manager, Department of Information Technology

12.5 Policy Approval Date:

12.6 Policy Effective Date:

April 5, 2004

12.7 Terms and Definitions:

Section 13: Single Sign-On

13.1 Policy Intent:

The intent of this policy section is to enhance security and facilitate use of business applications through a primary authentication, single identity-based access system.

13.2 Scope:

This policy applies to all Jefferson County organizations, employees, and contractors, and any other individuals or organizations that use Jefferson County technology resources. Jefferson County technology resources include, but are not limited to: networks, servers, data, applications, and information. It applies to all Jefferson County facilities.

13.3 Policy:

The Department of Information Technology will implement and maintain a user identification and authorization system based on a single user sign-on.

Single sign-on will support existing production business applications, and future production business applications will be required to work with Jefferson County's single sign-on system.

Single sign-on will support and comply with requirements for password length and complexity. (See Section 12)

13.4 Policy Owner:

Jefferson County Commission

13.4a Policy Administrator:

IT Infrastructure Manager, Department of Information Technology

13.5 Policy Approval Date:

13.6 Policy Effective Date:

April 5, 2004

13.7 Terms and Definitions:

Single Sign-On – a system whereby a users signs on once via a single authentication to obtain access to all authorized resources.

Section 14: Hardware and Software Installation Standards

14.1 *Policy Intent:*

The intent of this policy section is to establish guidelines for the installation, configuration, maintenance, and management of the software and hardware on the Jefferson County network.

14.2 *Scope:*

This policy applies to all Jefferson County organizations, employees, and contractors, and any other individuals or organizations that use Jefferson County technology resources. Jefferson County technology resources include, but are not limited to: networks, servers, data, applications, and information. It applies to all Jefferson County facilities.

14.3 *Policy:*

Users and department managers, with the help of the Department of Information Technology, will ensure their software and hardware are in compliance with all license agreements.

All servers and workstations will be configured to insure the installation of effective security measures.

Only software authorized by the Department of Information Technology will be installed on Jefferson County computers and communications equipment. All authorized software will be installed under the supervision of the Department of Information Technology.

All software acquisitions and upgrades will be reviewed by the Department of Information Technology for verification of available technical support and appropriate security features.

All new software and upgrades must be tested prior to installation in a production environment.

The Department of Information Technology must approve all internal servers deployed on Jefferson County's network.

Software installed on workstations will comply with the standard software configuration for workstations developed by the Department of Information Technology.

Users may use only those versions of software licensed to Jefferson County and supported by the Department of Information Technology.

Freeware and shareware will not be downloaded from the Internet or otherwise installed unless approved by the Department of Information Technology.

Computers attached to Jefferson County's network will have their operating systems configured to fully utilize appropriate security features.

14.4 *Policy Owner:*

Jefferson County Commission

14.4a *Policy Administrator:*

Help Desk Manager, Department of Information Technology

14.5 *Policy Approval Date:*

14.6 *Policy Effective Date:*

April 5, 2004

14.7 *Terms and Definitions:*

Section 15: Application Security Standards

15.1 *Policy Intent:*

The intent of this policy section is to establish standards for application security for Jefferson County's production applications.

15.2 *Scope:*

This policy applies to all Jefferson County organizations, employees, and contractors, and any other individuals or organizations that use Jefferson County technology resources. Jefferson County technology resources include, but are not limited to: networks, servers, data, applications, and information. It applies to all Jefferson County facilities.

15.3 *Policy:*

Jefferson County production applications will provide security features and options that ensure the protection of the information and data within the specific application.

Jefferson County production applications will provide a level of security and access controls that are appropriate to the confidentiality and risk inherent in the data being processed.

Jefferson County production application users will be granted application access and authorization commensurate with their informational needs, job roles, and responsibilities. See Section 11 for additional information.

Jefferson County production applications will incorporate processes to ensure that activities of the application are appropriately monitored and logged.

15.4 *Policy Owner:*

Jefferson County Commission

15.4a *Policy Administrator:*

Manager of Application Development, Department of Information Technology

15.5 *Policy Approval Date:*

15.6 *Policy Effective Date:*

April 5, 2004

15.7 *Terms and Definitions*

Production Applications – Operational computer programs routinely used in the normal process of conducting business.

Section 16: Security Awareness and Training

16.1 *Policy Intent:*

The intent of this policy section is to establish guidelines for employee technology security awareness and training.

16.2 *Scope:*

This policy applies to all Jefferson County organizations, employees, and contractors, and any other individuals or organizations that use Jefferson County technology resources. Jefferson County technology resources include, but are not limited to: networks, servers, data, applications, and information.

16.3 *Policy:*

Information security training and orientation will be provided to all new employees.

Information security will be emphasized through a security awareness program that reminds users on an on-going basis of their responsibilities and accountability. All employees will participate in this program.

Security administrators will receive on-going security training appropriate to their responsibilities.

16.4 *Policy Owner:*

Jefferson County Commission

16.4a *Policy Administrator:*

Training Administrator, Department of Information Technology

16.5 *Policy Approval Date:*

16.6 *Policy Effective Date:*

April 5, 2003

16.7 *Terms and Definitions:*

Section 17: Change Management – Network and Systems Accountability

17.1 *Policy Intent:*

The intent of this policy section is to ensure security practices are sustained during network and system changes.

17.2 *Scope:*

This policy applies to all Jefferson County organizations, employees, and contractors, and any other individuals or organizations that use Jefferson County technology resources. Jefferson County technology resources include, but are not limited to: networks, servers, data, applications, and information. It applies to all Jefferson County facilities.

17.3 *Policy:*

The Department of Information Technology will develop and maintain a technology change management process that ensures security is addressed during all changes to systems and networks.

Managers within the Department of Information Technology will review and approve any changes affecting security.

Primary stakeholders will be notified of any network or system changes that affect security.

The date and time of all technical changes will be negotiated based on security considerations and other business conditions.

Changes to systems and networks will be validated for completion and achievement of desired security objectives.

17.4 *Policy Owner:*

Jefferson County Commission

17.4a *Policy Administrator:*

Project Management Officer, Department of Information Technology

17.5 *Policy Approval Date:*

17.6 *Policy Effective Date:*

April 5, 2004

17.7 *Terms and Definitions:*

Change Management Process – a documented practice whereby changes to systems, applications, or procedures are closely monitored and managed to ensure the desired outcome.

Section 18: Security Risk Assessment

18.1 *Policy Intent:*

The intent of this policy section is to ensure that systematic and appropriate information security risk assessment is applied to Jefferson County systems and applications.

18.2 *Scope:*

This policy applies to all Jefferson County organizations, employees, and contractors, and any other individuals or organizations that use Jefferson County technology resources. Jefferson County technology resources include, but are not limited to: networks, servers, data, applications, and information. It applies to all Jefferson County facilities.

18.3 *Policy:*

The Department of Information Technology will periodically conduct an across-the-board information risk assessment to determine the sufficiency of current security measures, and to identify security vulnerabilities.

A security assessment will be completed by the Department of Information Technology for any computer hardware being considered for purchase and installation, for any business application being considered for in-house development, or for any software packages being considered for purchase and installation, in Jefferson County.

18.4 *Policy Owner:*

Jefferson County Commission

18.4a *Policy Administrator:*

Network Manager, Department of Information Technology

18.5 *Policy Approval Date:*

18.6 *Policy Effective Date:*

April 5, 2004

18.7 *Terms and Definitions:*

Risk Assessment - A study of vulnerabilities, threats, likelihood, loss or impact, and theoretical effectiveness of technology security measures.

Section 19: Data Security Levels

19.1 *Policy Intent:*

This policy section is intended to establish the basis for assigning appropriate levels of security to the retention, transmission and handling of data created, retained, and transmitted by Jefferson County.

19.2 *Scope:*

This policy applies to all Jefferson County organizations, employees, and contractors, and any other individuals or organizations that use Jefferson County technology resources. Jefferson County technology resources include, but are not limited to: networks, servers, data, applications, and information. It applies to all Jefferson County facilities.

19.3 *Policy:*

The Department of Information Technology, in partnership with data owners, will develop guidelines for the classification and disclosure of Jefferson County information.

All information created, retained, and transmitted by Jefferson County will be classified according to classification guidelines.

All Jefferson County information will be retained, transmitted, and otherwise handled according to its classification.

Portable storage devices containing Jefferson County information will be handled consistent with appropriate classification guidelines. In such cases the information will be deleted or the portable media will be destroyed when the purpose of the portable copy is completed.

Care will be taken when emailing Jefferson County information to comply with classification guidelines.

Any public disclosure of Jefferson County information will be consistent with **Administrative Order 03-01**, and will comply with **Code of Alabama (1975), § 36-12-40.**

19.4 *Policy Owner:*

Jefferson County Commission

19.4a *Policy Administrator:*

Shared by:
Chief Information Officer, Department of Information Technology
Information Owners

19.5 *Policy Approval Date:*

19.6 *Policy Effective Date:*

April 5, 2004

19.7 *Terms and Definitions:*

Section 20: Physical Security Standards and Personal Asset Management

20.1 *Policy Intent:*

The intent of this policy section is to establish physical security standards for Jefferson County's computer and communications assets as well as Jefferson County's network computing and telecommunications assets.

20.2 *Scope:*

This policy applies to all Jefferson County organizations, employees, and contractors, and any other individuals or organizations that use Jefferson County technology resources. Jefferson County technology resources include, but are not limited to: networks, servers, data, applications, and information. It applies to all Jefferson County facilities.

20.3 *Policy:*

Computing assets used in the transmission, processing, and storage of Jefferson County data will be physically secured at all times.

Jefferson County employees are responsible to exercise reasonable care to prevent the theft of or damage to Jefferson County assets.

Access to secure areas will be limited to authorized users.

Visitors to secure areas will be escorted at all times.

No unauthorized users will be allowed access to Jefferson County computers. Jefferson County employees have primary responsibility for preventing unauthorized access to their workstations.

Unattended computers will be properly secured and will be logged out, or have a keyboard/screen locking program that automatically invokes after a brief period of inactivity.

20.4 *Policy Owner:*

Jefferson County Commission

20.4a *Policy Administrator:*

Shared by:
Appropriate departmental managers
Manager, Human Resources Department
IT Infrastructure Manager, Department of Information Technology

20.5 *Policy Approval Date:*

20.6 *Policy Effective Date:*

April 5, 2004

20.7 *Terms and Definitions:*

Asset Owner or Manager – A Jefferson County employee or an agent of Jefferson County who has physical possession of, or has responsibility for an asset.

Users – For the purposes of this policy, users are defined as team members, vendors, and contractors who have been granted access to Jefferson County computer networks and/or have been provided with a Jefferson County asset.

Computing Asset - A hardware item, a software item, a technology capability, electronic information, or technical knowledge possessed by an organization.

Section 21: Operating System Security Standards

21.1 *Policy Intent:*

The intent of this policy section is to establish information security standards for workstations and server operating systems.

21.2 *Scope:*

This policy applies to all Jefferson County organizations, employees, and contractors, and any other individuals or organizations that use Jefferson County technology resources. Jefferson County technology resources include, but are not limited to: networks, servers, data, applications, and information. It applies to all Jefferson County facilities.

21.3 *Policy:*

Computers attached to Jefferson County's network will have their operating systems configured to fully utilize appropriate security features.

All OS accounts will have non-blank passwords.

User accounts will not be shared.

Guest accounts will be disabled.

The Department of Information Technology will have administrator rights to all computers for which the Department of Information Technology provides support.

Users and vendors will not have administrator rights to computers supported by the Department of Information Technology except in cases deemed necessary by the Department of Information Technology.

On an on-going basis, the Department of Information Technology will identify the appropriate service packs, security patches, and updates that should be installed on workstations and servers.

Network accounts will be locked out after consecutive unsuccessful login attempts.

21.4 *Policy Owner:*

Jefferson County Commission

21.4a *Policy Administrator:*

Chief Information Officer, Department of Information Technology

21.5 *Policy Approval Date:*

21.6 *Policy Effective Date:*

April 5, 2004

21.7 *Terms and Definitions:*

Operating Systems (OS) - the supervising program that manages input/output and other computer resources. Examples are Windows, UNIX, and Linux.

User Account – a catalog of workstation and network resources which an authenticated individual is entitled to use.

Guest Account – a user account with limited rights that come standard with an operating system.

Network Account – a User ID and password that authenticates a user to the network and permits access to network-based resources. Often used interchangeably with User Account.

Section 22: Remote Access

22.1 *Policy Intent:*

This policy section establishes standards for remotely accessing other computers from inside the County's network, and for remotely access County computers from outside Jefferson County's computer network.

22.2 *Scope:*

This policy applies to all Jefferson County organizations, employees, and contractors, and any other individuals or organizations that use Jefferson County technology resources. Jefferson County technology resources include, but are not limited to: networks, servers, data, applications, and information. It applies to all Jefferson County facilities.

22.3 *Policy:*

Remote access from a computer attached to Jefferson County's network to computers or networks outside Jefferson County's network must be approved by the Department of Information Technology.

Internet access from Jefferson County's network will be granted only to individuals who complete a Memorandum of Understanding (MoU) and have it signed by a sponsoring Commissioner.

Legitimate Internet access to/from Jefferson County's network using regular communications channels will be provided. Other communications channels will be opened on an exception basis only.

Anyone desiring access into Jefferson County's network from outside Jefferson County's network by means other than regular communications channels must be sponsored by a member of the Department of Information Technology.

Any workstation used to access Jefferson County's network from outside Jefferson County's network by means other than regular communications channels must meet configurations standards established by the Department of Information Technology.

Any computer that can be connected to Jefferson County's network, and has wireless dial-up capability must meet configurations standards established by the Department of Information Technology.

22.4 *Policy Owner:*

Jefferson County Commission

22.4a *Policy Administrator:*

Network Manager, Department of Information Technology.

22.5 *Policy Approval Date:*

22.6 *Policy Effective Date:*

April 5, 2004

22.7 *Terms and Definitions:*

Remote Access – communicating with distant computers and/or networks, using communications techniques and protocols other than the World Wide Web.

Memorandum of Understanding – a form requesting Internet access that states the requestor will comply with County policies for Internet usage.

Sponsor – a person willing to confirm the legitimacy of the request for access and assume responsibility for the requestor's actions.

Regular communications channels – techniques for accessing publicly available Internet services, i.e. World Wide Web

Section 23: LAN Attachment and Wireless Usage

23.1 *Policy Intent:*

This policy section establishes standards for attaching equipment to Jefferson County's computer network, and for the installation, configuration, and operation of wireless access to Jefferson County's computer network.

23.2 *Scope:*

This policy applies to all Jefferson County organizations, employees, and contractors, and any other individuals or organizations that use Jefferson County technology resources. Jefferson County technology resources include, but are not limited to: networks, servers, data, applications, and information. It applies to all Jefferson County facilities.

23.3 *Policy:*

All equipment attached to Jefferson County's network must be approved by the Department of Information Technology prior to attachment.

All workstations attached to Jefferson County's network will meet configuration criteria established by the Department of Information Technology.

Any device attached to Jefferson County's network is subject to audit at any time for proper configuration and usage.

The Department of Information Technology is responsible for the network addresses assigned to equipment attached to Jefferson County's network.

Any equipment that is causing abnormal operation of the County's network, or that is being used contrary to County security policy, may be temporarily disabled until corrective action can be taken.

All wireless communications with the County's network must be configured to meet the security standards established by the Department of Information Technology.

All workstations and other equipment communicating wirelessly with the County's network must be examined and approved by the Department of Information Technology.

23.4 *Policy Owner:*

Jefferson County Commission

23.4a *Policy Administrator:*

Network Manager, Department of Information Technology

23.5 *Policy Approval Date:*

23.6 *Policy Effective Date:*

April 5, 2004

23.7 *Terms and Definitions:*

Section 24: Network Equipment

24.1 *Policy Intent:*

This policy section establishes standards for the installation, configuration, and operation of wired network infrastructure equipment in Jefferson County's computer network.

24.2 *Scope:*

This policy applies to all Jefferson County organizations, employees, and contractors, and any other individuals or organizations that use Jefferson County technology resources. Jefferson County technology resources include, but are not limited to: networks, servers, data, applications, and information. It applies to all Jefferson County facilities.

24.3 *Policy:*

All network transport equipment attached to Jefferson County's network must be owned and operated by the Department of Information Technology.

Network transport equipment will be accessed and operated only by the County's network administrators and their designated representatives.

Passwords for accessing network transport equipment will be encrypted, and will be changed at regular intervals.

Network transport equipment have internal clocks that will be synchronized using a nationally recognized, Internet accessible source.

An authentication server (process) will provide password authentication for accessing network transport equipment.

Network transport equipment will be secured from physical access, accept by authorized persons.

Configurations of network transport equipment will be backed up regularly.

SNMP access to network infrastructure equipment will be secured with passwords, which will be changed at regular intervals.

Information about Jefferson County's network is proprietary and confidential. Disclosure of information about Jefferson County's network will only be made by the Department of Information Technology.

24.4 *Policy Owner:*

Jefferson County Commission

24.4a *Policy Administrator:*

Network Manager, Department of Information Technology

24.5 *Policy Approval Date:*

24.6 *Policy Effective Date:*

April 5, 2004

24.7 *Terms and Definitions:*

Network Transport equipment – routers, switches, and hubs used to move information through the County's network.

SNMP - (Simple Network Management Protocol) – a protocol that facilitates the exchange of management information between network devices. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

Authentication server – a device or program used to determine whether someone or something is, in fact, who or what it is declared to be. In computer networks, authentication is commonly done through the use of passwords. Knowledge of the password is assumed to guarantee that the user is authentic.

Section 25: Communications Line Procurement

25.1 *Policy Intent:*

This policy section establishes requirement for obtaining data communications lines.

25.2 *Scope:*

This policy applies to all Jefferson County organizations, employees, and contractors, and any other individuals or organizations that use Jefferson County technology resources. Jefferson County technology resources include, but are not limited to: networks, servers, data, applications, and information. It applies to all Jefferson County facilities.

25.3 *Policy:*

All requests for communications lines that will be connected to a device attached to Jefferson County's computing network will be approved by the Department of Information Technology prior to installation.

25.4 *Policy Owner:*

Jefferson County Commission

25.4a *Policy Administrator:*

Network Manager, Department of Information Technology

25.5 *Policy Approval Date:*

25.6 *Policy Effective Date:*

April 5, 2004

25.7 *Terms and Definitions:*

Communications Line - A connection between computers (and/or peripherals) enabling data transfer. Examples of communications lines are network cables, telephone (modem) cables, or data transmission cables.

Section 26: Technology Services and Service Providers

26.1 *Policy Intent:*

This policy section establishes security standards of submitting technology offerings to Jefferson County, and requirements of providers who supply technology to Jefferson County.

26.2 *Scope:*

This policy applies to all Jefferson County organizations, employees, and contractors, and any other individuals or organizations that use Jefferson County technology resources. Jefferson County technology resources include, but are not limited to: networks, servers, data, applications, and information. It applies to all Jefferson County facilities.

26.5 *Policy:*

All offerings to Jefferson County that include information technology services or equipment will require the provider to address security requirements, and their ability and intent to comply with Jefferson County's security policies.

The Department of Information Technology will evaluate all offerings to Jefferson County that contain information technology services or equipment to ensure compliance with Jefferson County's security policies.

All service providers who access confidential information will sign a non-disclosure agreement on behalf of their personnel.

Service provider's access shall be limited to only those privileges and access levels required to complete their tasks.

26.4 *Policy Owner:*

Jefferson County Commission

26.4a *Policy Administrator:*

Chief Information Officer, Department of Information Technology

26.5 *Policy Approval Date:*

26.6 *Policy Effective Date:*

April 5, 2004

26.7 *Terms and Definitions:*

Section 27: Information/Equipment Access and Usage

27.1 Policy Intent:

The purpose of this policy section is to reinforce the principle of predominant denial of access to computers and information.

27.2 Policy Scope:

This policy applies to all Jefferson County organizations, employees, and contractors, and any other individuals or organizations that use Jefferson County technology resources. Jefferson County technology resources include, but are not limited to: networks, servers, data, applications, and information. It applies to all Jefferson County facilities.

27.3 Policy:

No Jefferson County official, employee, contractor, or vendor will use another Jefferson County agent's computer, or access information controlled by another Jefferson County agent without the express consent of that agent, or an appropriate supervisor or manager.

27.4 Policy Owner:

Jefferson County Commission

27.4a Policy Administrator:

Shared by:
Chief Information Officer, Department of Information Technology
Appropriate department managers

27.5 Policy Approval Date:

27.6 Policy Effective Date:

April 5, 2004

27.7 Terms and definitions:

A **Jefferson County agent** may be an official, an employee, a contractor, a vendor, a department, or an agency. A **Jefferson County agent** may also be an organization that has a fiduciary or contractual arrangement with the Jefferson County Commission.

End of

Jefferson County Information Technology Security Policy