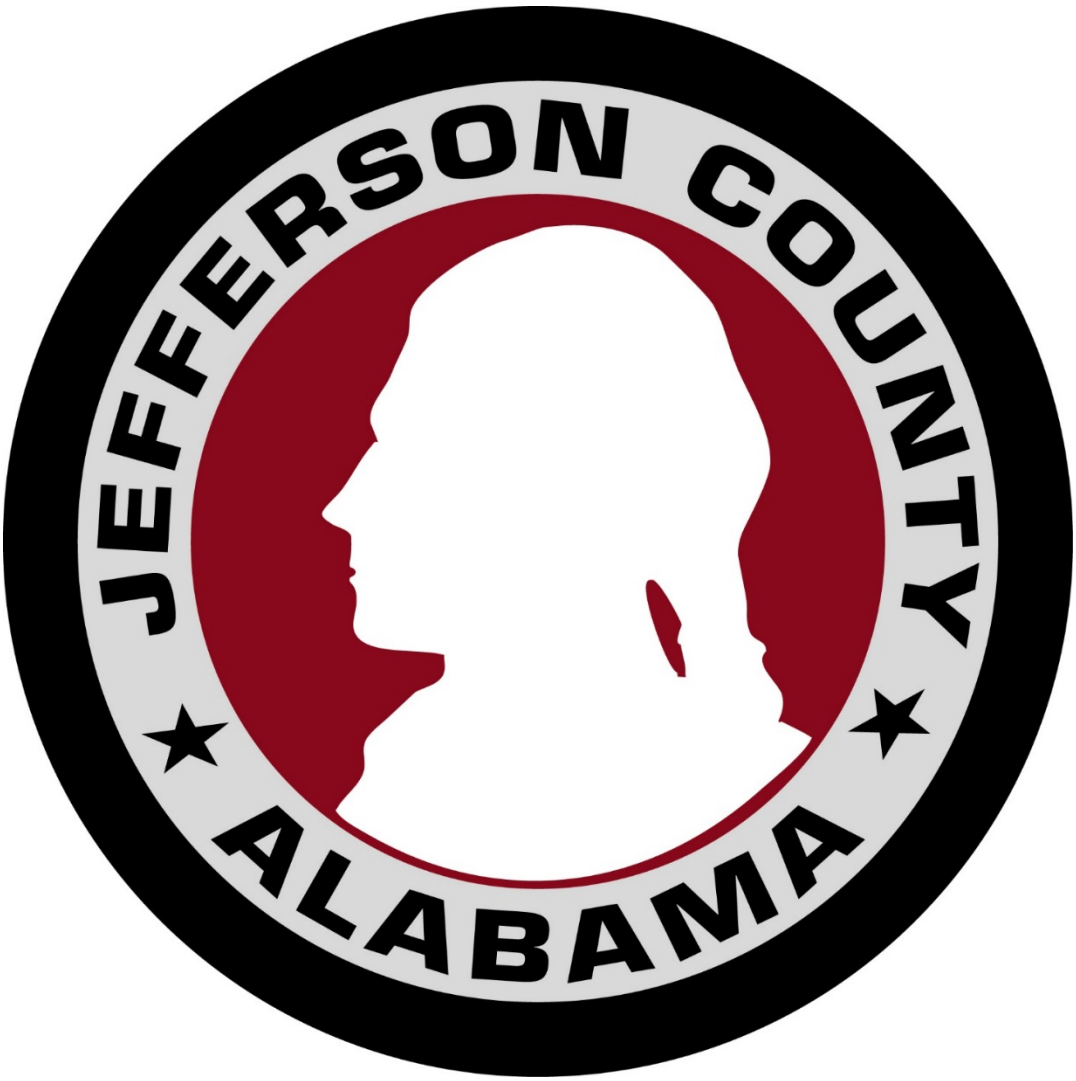
Jefferson County Commission
Department of Information Technology Services
Information Security Rules & Regulations



Prepared by the

Jefferson County Commission Department of Information Technology Services

Version 3.0

TABLE OF CONTENTS

18. Risk Assessment Information Security Rules & Regulations

19. Roles & Responsibilities Information Security Rules & Regulations

20. Software Application Development Information Security Rules & Regulations

21. User Access Management Information Security Rules & Regulations

22. Wireless Networking Access Information Security Rules & Regulations

JEFFERSON COUNTY COMMISSION

Information Technology Services Department

Acceptable Use Security Rules & Regulations

1.0 Overview

Throughout this document the use of the term policy refers to the strategy, procedures, rules, and regulations defined and encapsulated within each section of this document to achieve the stated information security goals. The Jefferson County Commission's ("JCC") intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to its established culture of openness, trust and integrity. The JCC is committed to protecting its employees, partners and the county from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, Internet, and FTP, are the property of Jefferson County. These systems are to be used for business purposes in serving the interests of the County, and of our clients and customers in the course of normal operations.

Effective security is a team effort involving the participation and support of every Jefferson County employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of JCC computer equipment, systems, and networks. These rules are in place to properly use and protect information resources and to respect the rights of other employees and Jefferson County. Inappropriate use exposes Jefferson County to risks including virus attacks, compromise of network systems and services, and legal issues.

3.0 Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at JCC, including all personnel affiliated with third parties. This policy also applies to those who avail themselves of the visitor wireless network access service, and to those who register their computers and other devices through Conference and Event Services programs or through other offices or by other means, for use of the JCC network. This policy applies to all equipment that is owned or leased by JCC and to personally owned devices connected by wire or wireless service to the JCC network (Collectively, "Users").

4.0 Policy

4.1 General Use and Ownership

4.1.1 While JCC desires to provide a reasonable level of privacy, users should be aware that the data they create on the County systems remains the property of JCC.

Management cannot guarantee the confidentiality of information stored on any network device belonging to JCC.

4.1.2 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

4.1.3 Jefferson County recommends that any information that users consider sensitive or vulnerable be encrypted. For guidelines on information classification, see JCC's Data Classification and Encryption Policies.

4.1.4 For security and network maintenance purposes, authorized individuals within JCC may monitor equipment, systems and network traffic at any time, per the JCC Audit Logging Policy.

4.1.5 JCC reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

4.2.1 The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by County classification guidelines, details of which can be found in the JCC Data Classification Policy. Examples of confidential information include but are not limited to county private specifications, security configurations, Personally Identifiable Information (PII), Financial Information, and HIPAA data. Employees should take all necessary steps to prevent unauthorized access to this information.

4.2.2 Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly.

4.2.3 All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 15 minutes or less, or by logging-off (control-alt-delete for Windows users) when the device will be unattended.

4.2.4 Use encryption of information in compliance with JCC Encryption policy.

4.2.5 Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the JCC Mobile Device Policy.

4.2.6 Postings to social networking platforms not limited to social media, chat rooms, blogs, and forums from a Jefferson County device and/or email address is prohibited with exception of the JCC Public Information Office and/or a explicit approval by Department Head or designee.

4.2.7 All devices that are connected to JCC's Internet/Intranet/Extranet, whether owned by the user or JCC, shall be continually executing approved virus-scanning software with a current virus database unless overridden by departmental or group policy.

4.2.8 Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, malwares or trojans.

4.3 Unacceptable Use

4.3.1 The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

4.3.2 Under no circumstances a user is authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing JCC owned or leased resources.

4.3.3 The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

4.4 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

4.4.1 Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by JCC.

4.4.2 Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which JCC or the end user does not have an active license is strictly prohibited.

4.4.3 Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

4.4.4 Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

4.4.5 Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

4.4.6 Using a JCC computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the local jurisdiction.

4.4.7 Making fraudulent offers of products, items, or services originating from any Jefferson County account.

4.4.8 JCC is prohibited from participating or intervening in any political campaign on behalf of or in opposition to a candidate for public office, and no substantial part of the JCC activities may be directed to influencing legislation (i.e. lobbying). Individuals may not use JCC technological resources for political purposes in a manner that suggests the JCC itself is participating in campaign or political activity or fundraising, or for influencing legislation.

4.4.9 Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

4.4.10 Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

4.4.11 Port scanning or security scanning is expressly prohibited unless prior notification and approval by JCC is made.

4.4.12 Executing any form of network monitoring which will intercept data not intended for the user's host, unless this activity is a part of the user's normal job/duty.

4.4.13 Circumventing user authentication or security of any host, network or account.

4.4.14 Interfering with or denying service to any user other than one’s host (for example, denial of service attack).

4.4.15 Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

4.4.16 Providing personal information about any employee or other person to unauthorized parties.

4.5 Email and Communications Activities

4.5.1 Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
4.5.2 Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
4.5.3 Unauthorized use, or forging, of email header information.
4.5.4 Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
4.5.5 Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
4.5.6 Use of unsolicited email originating from within JCC's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by JCC or connected via JCC's network.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Any other person or entity found to have violated this policy may subject to any or all remedies available at law or in equity. Any disciplinary action taken by the ITS Department to discipline a user who has violated this policy, will follow Jefferson County Commission's Disciplinary process.

6.0 Policy Owner

Jefferson County Commission

6.0a Policy Administrator

Chief Information Officer, Information Technology Services

7.0 Policy Approval Date

March 20, 2020

8.0 Policy Effective Date

March 20, 2020

9.0 Definitions

Term	Definition
Blogging	Writing a blog. A blog (short for weblog) is a personal online journal that is frequently updated and intended for general public consumption. For the purposes of this policy, blog includes posting to any social media sites.
Spam	Unauthorized and/or unsolicited electronic mass mailings.

Revision History

Initial Author	ITS Governance
Created On	August 13, 2019
Last Modified By	ITS Governance
Last Modified On	March 20, 2020
Revision Number	3
Approver	County Manager's Review Committee

Version	Changed By	Changed On	Notes / Comments
2	Information Technology	March 13, 2013	
3	Information Technology Services	March 20, 2020	

JEFFERSON COUNTY COMMISSION

Information Technology Services Department

Anti-Virus Security Rules & Regulations

1.0 Overview

Throughout this document the term policy refers to the strategy, procedures, rules, and regulations defined and encapsulated within each section of this document to achieve the stated information security goals. A virus is a piece of self-replicating code, most often a malicious software program designed to destroy or corrupt information, steal user data, or adversely impact the usage of Jefferson County Commission (JCC) Department of Information Technology Services (ITS) systems. Potential sources of viruses include shared media such as USB memory sticks, electronic mail (including, but not limited to, files attached to messages), malicious code embedded in websites and software or documents copied over networks such as the internal network or the internet. An infection by malicious software is almost always costly to the County's mission whether through the loss of data, staff time to recover a system, or adversely affect public safety systems.

2.0 Purpose

The purpose of this policy is to establish requirements for deploying, using and supporting anti-virus software for systems connected to the JCC network. This document contains the Antivirus (AV) policy details including actions to be taken if non-compliance occurs. A definition of the terms 'virus', 'malware' and 'spam' are listed in section 9.0 Definitions.

3.0 Scope

All computing devices (for example, laptops, workstations, servers, etc.) that are connected to the JCC data network must be protected against viruses and malware. This shall be accomplished through the use of anti-virus/malware software, where possible. This policy applies to all JCC staff authorized to use/access ITS systems and communications networks whether they are employed directly by JCC, partner organizations, contractors, voluntary organizations or vendors granted access for support purposes.

4.0 Policy

JCC Information Technology Services Department sets the standards as to what anti-virus software suite will be utilized through out the enterprise. Anti-virus software must be correctly installed and configured on all supported endpoint and servers across the JCC data network.

2.1 Configuration Standards

- 2.1.1 Anti-virus software must be kept up to date including the definitions files.
- 2.1.2 Anti-virus software updates must be deployed across the network automatically following their receipt from the vendor and it must be configured to check for these updates every 60 minutes daily.
- 2.1.3 Virus and malware signature updates must be deployed across the network automatically following their receipt from the vendor and it must be configured to check for signature updates every 10 minutes daily. All the endpoints must be configured with the secondary anti-virus update server so if a device is not checked

in on the corporate network then updates will be installed from the secondary server.

2.1.4 Anti-virus software must be configured for real time scanning and regular scheduled scans.

2.1.5 On-access scanning must be configured within Anti-virus software for removable media and websites.

2.1.6 Anti-virus server must be monitored on a daily basis by a nominated staff members within Technology Management and Architecture team for virus alerts and any issues which cannot be resolved remotely via centralized management console must be escalated to the ITS Help Desk where an incident will be raised and a technician assigned to immediately investigate.

2.1.7 In the event of a virus infection which infects multiple devices (more than 3 devices) at the same time. A root cause analysis report should be completed by the technician for the ITS Information Security Officer and/or Information Security Team.

2.1.8 Monthly Anti-Virus compliance reports must be provided to the ITS Information Security Officer and/or Information Security Team by the third working day of the month. In the event that systems are found to be non-compliant a report including suggested remediation will be created by the ITS Information Security Officer and/or Information Security Team for the Chief Information Officer.

2.1.9 Tamper protection must be enabled to prevent end users or malware altering the anti-virus software's configuration or disabling the protection.

2.2 User Responsibilities

2.2.1 All ITS networked devices and removable media must be scanned for viruses and malware before being introduced or prior use on the enterprise network, system or device.

2.2.2 Users must not accept, or run, software from non-trusted sources.

2.2.3 Users must not undertake any activities with the intention to create and/or distribute malicious programs (e.g. viruses, worms, Trojans, e-mail bombs, etc.) into enterprise network(s) or system(s).

2.2.4 Users must inform the ITS Help Desk immediately if a virus is detected on their system

2.2.5 ITS system(s) infected with a malware/virus that the anti-virus software has not been able to deal with must be disconnected/quarantined from the enterprise network until virus free.

2.3 Exceptions

2.3.1 Exceptions to the anti-virus policy require a formal documented risk assessment including steps taken to mitigate the risk and formal approval from the Chief Information Officer. Once approved exceptions will be implemented via ITS Change Management Process.

2.3.2 Any server or workstation that do not comply with policy must have an approved exception recorded in the Anti-virus exceptions file detailing the reason for the exception and the steps taken to mitigate the risk.

2.3.3 Systems will only have exception to the policy if scheduled updates or patches are deemed likely to cause major disruption to the system, resident software or service functionality or to facilitate problem diagnosis. All systems recorded within the Anti-virus exceptions file must be reviewed on a quarterly basis by the ITS Information Security Officer and/or Information Security Team and the risk will be re-evaluated.

2.4 Monitoring and Compliance

Anti-virus compliance level refers to the percentage of servers, workstations and laptops that have been successfully protected by an up to date Anti- virus product against virus or malware threats.

2.4.1 Jefferson County Commission ITS Department will endeavor to achieve 100% compliance for all the end points under its management. For monitoring and compliance assessment the following levels must be maintained at all times.

2.4.1 100% of all servers must be protected with up to date anti-virus software and virus signatures installed no more than 2 days of signatures being released by the vendor.

2.4.2 97% of all Desktops/laptops/tablets must be compliant with up to date anti-virus software and virus signatures installed within 2 days of the release

5.0 Enforcement

Any system or workstation found to be without adequate protection as defined by this policy will be removed from the network until adequate protection is implemented. Any user being found to be willfully violating the anti-virus policy may be subject to one or more of the following sanctions:

- Removal of any equipment used from the network until adequate protection is implemented
- Revocation of rights to access ITS systems
- Any costs incurred by the IT department to remove the virus may be passed on to the department or organization responsible for the outbreak.
- Subject to disciplinary action up to and including termination of employment. Any disciplinary action taken by the ITS Department to discipline a user who has violated this policy, will follow Jefferson County Commission's Disciplinary process.

6.0 Policy Owner

Jefferson County Commission

6.0a Policy Administrator

Chief Information Officer, Information Technology Services Department

7.0 Policy Approval Date

March 20, 2020

8.0 Policy Effective Date

March 20, 2020

9.0 Definitions

Term Definition

Adware: Software that automatically plays, displays, or downloads advertisements to a computer, often in exchange for the right to use a program without paying for it. The advertisements seen are based on monitoring of browser habits. Most adware is safe to use, but some can serve as spyware, gathering information about you from your hard drive, the websites you visit, or even your keystrokes. Certain types of adware have the capability to capture or transmit personal information.

Antivirus Software: A type of software that scans a computer's memory and disk drives for viruses. If it finds a virus, the application informs the user and may clean, delete, or quarantine any files, directories, or disks affected by the virus. The term antimalware is preferred because it covers more threats.

Browser Hijacker: A type of malware that alters your computer's browser settings so that you are redirected to websites that you had no intention of visiting. Most browser hijackers alter browser home pages, search pages, search results, error message pages, or other browser content with unexpected or unwanted content.

Dat Files: Also known as a data file, these files are used to update software programs, sent to users via the Internet. .DAT files contain up-to-date virus signatures and other information antivirus products use to protect your computer against virus attacks. .DAT files are also known as detection definition files and signatures.

Keylogger: Software that tracks or logs the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored. This is usually done with malicious intent to collect information including instant messages, email text, email addresses, passwords, credit card and account numbers, addresses, and other private data.

Malware: A generic term used to describe any type of software or code specifically designed to exploit a computer or the data it contains, without consent. Malware includes viruses, trojan horses, spyware, adware, most rootkits, and other malicious programs.

Phishing: A form of criminal activity using social engineering techniques through email or instant messaging. Phishers attempt to fraudulently acquire other people's personal information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an apparently official electronic communication. Typically, phishing emails request that recipients click on the link in the email to verify or update contact details or credit card information. Like spam, phishing emails are sent to a large number of email addresses, with the expectation that someone will act on the information in the email and disclose their personal information. Phishing can also happen via text messaging or phone.

Ransomware: Malicious software created by a hacker to restrict access to the computer system that it infects and demand a ransom paid to the creator of the malicious software for the restriction to be removed. Some forms of ransomware may encrypt files on the system's hard drive, while others may simply lock the system and display messages to coax the user into paying.

Spam: An unwanted electronic message, most commonly unsolicited bulk email. Typically, spam is sent to multiple recipients who did not ask to receive it. Types include email spam, instant messaging spam, web search-engine spam, spam in blogs, and mobile phone-messaging spam. Spam includes legitimate advertisements, misleading advertisements, and phishing messages designed to trick recipients into giving up personal and financial information. Email messages are not considered spam if a user has signed up to receive them.

Spyware: Software that can capture information like web browsing habits, email messages, usernames and passwords, and credit card information. Just like viruses, spyware can be installed on a computer through an email attachment containing malicious software.

Trojan: Malicious programs disguised as legitimate software. Users are typically tricked into loading and executing it on their systems. One key factor that distinguishes a Trojan from viruses and worms is that Trojans don't replicate.

Revision History

Initial Author	ITS Governance
Created On	August 13, 2019
Last Modified By	ITS Governance
Last Modified On	March 20, 2020
Revision Number	3
Approver	County Manager's Review Committee

Version	Changed By	Changed On	Notes / Comments
2	Information Technology	March 13, 2013	
3	Information Technology Services	March 20, 2020	

JEFFERSON COUNTY COMMISSION

Information Technology Services Department

Audit Logging Security Rules & Regulations

1.0 Overview

Throughout this document the term policy refers to the strategy, procedures, rules, and regulations defined and encapsulated within each section of this document to achieve the stated information security goals. Logging from Jefferson County Commission ("JCC") critical systems, applications and services can provide key information and potential indicators of compromise. Although logging information may not be viewed on a daily basis, it is critical to have from a forensics standpoint.

2.0 Purpose

The purpose of this document is to ensure that routine and random audits are utilized as oversight tools for recording and examining access to information and integrating that information into an enterprise's log management function. This will facilitate the Department of Information Technology Services (ITS) verification process for compliance with access controls and administrative and other safeguards developed and implemented to prevent/limit inappropriate access to data.

3.0 Scope

This policy applies to information technology resources administered centrally; personally-owned computing devices connected by wire or wireless to the JCC network; and to off-site computing devices that connect remotely to JCC network. ITS resources include all JCC owned, licensed, leased, or managed hardware and software, and use of the JCC network via a physical or wireless connection, regardless of the ownership of the computing device connected to the network.

4.0 Policy

Audit Policy:

- To ensure that appropriate safeguards are in place and effective, ITS shall audit, log, and monitor access and events to detect, report, and guard against:
    - o Network vulnerabilities and intrusions
    - o Performance problems and flaws in applications
    - o Security violations
    - o Data loss
    - o Unauthorized access to confidential data, attorney-client privileged information, etc.
    - o Breaches in confidentiality and security of confidential data
    - o Degradation or loss of information integrity (e.g., improper alteration or destruction of confidential data)

- Auditable Events:
  - ITS shall develop and implement an Audit Event Plan to identify which systems, applications, and processes carry out auditing activities.
  - The Audit Event Plan shall define what types of events are subject to auditing. At a minimum, the following events may be audited:
    - Normal system events (e.g., startup, shutdown, login attempts, errors, security policy changes, software installations, etc.).
    - Information changes (e.g., create, read, update, delete) including confidential data.
    - Unauthorized access to confidential data for non-permitted purposes.
    - System management activities including execution of privileged functions.
    - Information exchanges containing confidential data.

  - The Audit Event Plan shall provide a rationale for why the list of auditable events are deemed to be adequate to support after-the-fact investigations of security incidents.
  - The Information Security Officer and/or Information Security Team shall periodically review and update the Audit Event Plan. This review shall include consideration of events that require auditing on a continuous basis, and events that require auditing in response to specific situations based upon an assessment of risk. Note: The specifics of the Audit Event Plan are not outlined in this policy but would be covered in the ITS procedures to allow greater flexibility because the auditable event process could change with time.
  - ITS shall coordinate the security audit function with Third Party Service Providers requiring audit-related information to enhance mutual support and to help guide the selection of auditable events.

- Content of Audit Records:
  - ITS shall define the content for each type of audit record in the Audit Event Plan. Audit record content shall provide sufficient detail to determine whether a Given individual took a particular action.
  - Audit records of information exchanges containing confidential data shall include the date, time, origin and destination of the message, but not its contents.
  - All disclosures of confidential data within or outside of the ITS shall be logged including type of disclosure, date and time of the event, recipient, and sender.
  - Perimeter devices additionally log packet denials.

- Audit Record Retention:
  - Audit Records shall be retained and archived in accordance with the Data Retention & Disposal Policy to meet regulatory and organizational record retention requirements.

- Audit Record Storage Capacity:
  - ITS shall allocate sufficient audit record storage capacity to reduce the likelihood of such capacity being exceeded.
  - ITS shall configure auditing processes to reduce the likelihood of the audit record storage capacity being exceeded.
  - Systems shall alert System Administrators when the allocated audit record storage reaches 80% of its capacity.

- Audit Record Generation:
  - Systems shall provide audit record generation capability as defined in the Audit Event Plan.
  - Systems shall allow System Administrators to select which auditable events are audited by specific components of the system.
  - Systems shall generate audit records that contain sufficient information to Establish what events occurred, the sources of the events, and the outcomes of the events. Audit record content shall also provide sufficient detail to determine whether a given individual took a particular action associated with an event.
  - Systems shall generate audit records that contain the activities of privileged users as defined in the Audit Event Plan.

- Protection of Audit Records:
  - Access to audit logging systems and system audit tools shall be limited to those With a job-related need according to the Roles & Responsibilities for Security Personnel Policy to protect against possible misuse of the tools or compromise to the audit records.
  - Access to audit records shall be limited to those with a job-related need according to the Roles & Responsibilities for Security Personnel Policy to prevent misuse or compromise of audit records.
  - Audit records shall be immutable and shall be protected against modification and deletion by anyone regardless of access privilege according to the Roles & Responsibilities for Security Personnel Policy.
  - Attempts to access the audit logging systems and audit records shall be logged and the audit records shall be protected from modification and deletion.
  - ITS shall implement file-integrity monitoring (or change detection software) to ensure that modifications to existing audit records generate an alert to the System Administrator. Note that the creation of new audit records should not trigger an alert.
  - Audit records for external-facing technologies (e.g., wireless, firewalls, DNS, etc.) shall be stored on a server located on the internal network. If third party security information management and security event management team (SIEM) is engaged, system logs are permitted to moved offsite for SIEM analysis.

- Audit Monitoring, Review, Analysis and Reporting:
  - ITS and/or SIEM managed service provider shall review and analyze audit records for evidence of suspicious, unusual, and inappropriate activity on an ongoing basis.
  - ITS and/or SIEM managed service provider shall report anomalous auditable events and related security incidents to the Information Security Officer and/or Information Technology Services Security Team, who shall be responsible for reporting security and compliance issues to senior leadership as appropriate.
  - ITS and/or SIEM managed service provider shall adjust the level of audit review, analysis, and reporting within systems when there is a change in risk to operations, assets, individuals, and other organizations based on law enforcement information, intelligence information, or other credible sources of information.
  - ITS shall establish procedures for monitoring the use of systems and facilities to test the effectiveness of access control and security mechanisms. The results of the monitoring activities shall be reviewed on a regular basis.
  - ITS shall review any unauthorized access to the network and information systems at least once every quarter, with appropriate action being taken upon discovery of unauthorized access.
  - Monitoring activities shall include execution of privileged operations, authorized access, unauthorized access attempts, and system alerts or failures.

- ITS shall meet all applicable legal requirements related to monitoring authorized access and unauthorized access attempts.
- Monitoring shall include inbound and outbound information exchanges and file integrity monitoring.
- ITS shall analyze and correlate audit records across different repositories and correlate this information with input from non-technical sources.
- ITS will conduct analyses to detect trends and/or patterns of use.
- System Administrator activities shall be logged and reviewed on a regular basis.

- Audit Reduction and Report Generation:
  - ITS shall utilize audit reduction, review, and reporting techniques while ensuring that original audit records needed to support after-the-fact investigations are not altered.
  - ITS Systems and/or SIEM managed service provider shall provide audit reduction and report generation capability.
  - Auditing and monitoring systems shall have the capability to automatically process audit records for events of interest based upon selectable event criteria.

- Response to Alerts:
  - ITS Systems and/or SIEM managed service provider shall alert System Administrators in the event of an audit processing failure and System Administrators shall take remediation action.
  - ITS Systems and/or SIEM managed service provider shall generate alerts for suspicious activity and security alerts. System Administrators shall analyze the alerts and investigate suspicious activity or suspected violations.
  - Automated Systems (e.g., IDS, IPS) shall support near real-time analysis and Alerting of adverse events (e.g., malicious code, potential intrusions, etc.) and Integrate intrusion detection into access and flow control mechanisms. The events that trigger real-time alerts shall be defined in the Audit Event Plan.
  - System faults shall be logged and analyzed, and System Administrators shall take appropriate remediation action.

5.0 Enforcement

The Information Security Officer and/or Information Technology Services Security Team shall be responsible for enforcing compliance with this policy under the direction of the Chief Information Officer. Any disciplinary action taken by the ITS Department to discipline a user who has violated this policy, will follow Jefferson County Commission's Disciplinary process.

6.0 Policy Owner

Jefferson County Commission

6.0a Policy Administrator

Chief Information Officer, Information Technology Services Department

7.0 Policy Approval Date

March 20, 2020

8.0 Policy Effective Date

March 20, 2020

9.0 Definitions

Term **Definition**

Revision History

Initial Author	ITS Governance
Created On	August 13, 2019
Last Modified By	ITS Governance
Last Modified On	March 20, 2020
Revision Number	3
Approver	County Manager's Review Committee

Version	Changed By	Changed On	Notes / Comments
2	Information Technology	March 13, 2013	
3	Information Technology Services	March 20, 2020	

JEFFERSON COUNTY COMMISSION

Information Technology Services Department

Change Management Security Rules & Regulations

1.0 Overview

Throughout this document the term policy refers to the strategy, procedures, rules, and regulations defined and encapsulated within each section of this document to achieve the stated information security goals. Change Management refers to a formal process for making changes to information technology systems. The goal of change management is to increase awareness and understanding of proposed changes across an organization and ensure that all changes are made in a thoughtful way that minimize negative impact to services and customers.
Change management generally includes the following steps:

- Planning: Plan the change, including the implementation design, schedule, plan, communication plan, test plan, and roll back plan.
- Evaluation: Evaluate the change, including determining the risk based in priority level of service and the nature of the proposed change, determining the change type and the change process to use.
- Review: Review change plan with peers and/or Change Control Board as appropriate to the change type.
- Approval: Obtain approval of change by management or other appropriate change authority as determined by change type.
- Communication: Communicate about changes with the appropriate parties (targeted or campus-wide).
- Implementation: Implement the change.
- Documentation: Document the change and any review and approval information.
- Post-change review: Review the change with an eye to future improvements.

2.0 Purpose

The objective of this policy is to define formal requirements to manage changes to Jefferson County Commission ("JCC") Department of Information Technology Service ("ITS") systems and applications, in order to prevent unscheduled disruption, data corruption or loss.

3.0 Scope

Because the Change Management Policy deals with the management of changes in the production environment, it is imperative that both users and ITS understand the events that are considered within the scope of the policy. The intent of this Policy is to ensure the effective management of change while reducing risk. In this section, the scope is described and includes areas which are both within and outside of the change management scope. The intended scope

of the Change Management Policy is to cover all of the County's computing systems and platforms. The primary functional components covered in the Change Management process include:

- SDLC – Changes handled through the formal software development life cycle will be included within the County's change management program.
- Hardware – Installation, modification, removal or relocation of computing equipment.
- Software – Installation, patching, upgrade or removal of software products including operating systems, access methods, commercial off-the-shelf (COTS) packages, internally developed packages and utilities packages and utilities.
- Database – Changes to databases or files such as additions, reorganizations and major maintenance.
- Application – Application changes being promoted to production as well as the integration of new application systems and the removal of obsolete elements.
- Moves, Adds, Changes and Deletes – Changes to system configuration.
- Schedule Changes - Requests for creation, deletion, or revision to job schedules, back-up schedules or other regularly scheduled jobs managed by the Information Technology Services Department.

There are many information technology tasks performed at the County, either by ITS staff or by the end users that do not fall under the policies and procedures of Change Management. Tasks that require an operational process, but are outside the initial scope of the County's Change Management Policy includes:

- Contingency/Disaster Recovery
- Changes to non-production elements or resources
- Changes made within the daily administrative process. Examples of daily administrative tasks are:
  - Password resets
  - User adds/deletes
  - User modifications
  - Adding, deleting or revising security groups
  - Rebooting machines when there is no change to the configuration of the system
  - File permission changes

The Change Control Board (CCB) may modify the scope periodically to include items in the scope of the County's overall Change Management process.

4.0 Policy

JCC Department of Information Technology Service formally manages changes to its information technology resources to prevent disruptions to the stability or integrity of hardware/software systems, applications, and data.

4.1 Responsibilities

a) ITS Staff - ITS staff are responsible for entering change requests into the Change Management system for review and approval prior to implementing any changes in production environments, except for emergency requests.

b) Change Control Board (CCB) - Review and either approve or deny change requests based on the propose change request documentation to ensure the change is aligned with best practices.

4.2 Principles
All change requests must be:

4.2.1 Classified before being processed. The level of analysis, approval and testing must be aligned with the change classification level in order to address potential risks.

4.2.2 Approved prior to commencing the change or development, and prior to implementing the fully tested change into the live environment.

4.2.3 Must have a quantifiable reason why change is necessary such as new functionality, enhancement, bug fix, etc....

4.2.4 Must have change description that conveys the significance of the change as well as the components that will be changed.

4.2.5 Must include impact analysis that provides a deterministic view of the potential effects to the subject system resulting from the proposed change.

4.2.6 Must include a communication plan that details the communication protocol for communicating change events to stake holders and Information Technology Services management team.

4.2.7 Must have a priority level (Emergency, High, Medium, Low) to specify the importance of the request to the stake holder or organization.

4.2.8 Must include a contingency plan that thoroughly communicate technical measures that will be taken to enable the system to be recovered from any failed change to quickly and effectively recover from a disruption of service.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Any disciplinary action taken by the ITS Department to discipline a user who has violated this policy, will follow Jefferson County Commission's Disciplinary process.

6.0 Policy Owner

Jefferson County Commission

6.0a Policy Administrator

Chief Information Officer, Information Technology Services Department

7.0 Policy Approval Date

March 20, 2020

8.0 Policy Effective Date

March 20, 2020

9.0 Definitions

Term **Definition**

Change Control Board: Group of individuals including but not limited to CIO, Deputy CIO, and others appointed by the CIO who are responsible for making the ultimate decision as to when and if any particular changes are to be made in regards to production systems.

Revision History

Initial Author	ITS Governance
Created On	August 13, 2019
Last Modified By	ITS Governance
Last Modified On	March 20, 2020
Revision Number	3
Approver	County Manager's Review Committee

Version	Changed By	Changed On	Notes / Comments
2	Information Technology	March 13, 2013	
3	Information Technology Services	March 20, 2020	

JEFFERSON COUNTY COMMISSION

Information Technology Services Department

Clear Desk & Screen Security Rules & Regulations

1.0 Overview

Throughout this document the term policy refers to the strategy, procedures, rules, and regulations defined and encapsulated within each section of this document to achieve the stated information security goals. The overall purpose of this policy is to ensure Jefferson County Commission ("JCC") Users have an awareness of the importance of keeping both paper and electronic documents and records safe when they are working at their desk/workstation or on their screen and that they have knowledge of how to protect them. A "User" shall mean all JCC employees, including temporary staff, contractors, sub-contractors, and any person with access to JCC information and information systems and services. This ensures that all sensitive and confidential information, whether it be on paper, a storage device, or a hardware device is properly locked away or disposed of when a workstation is not in use. This policy will reduce the risk of unauthorized access, loss of, and damage to information during and outside of normal business hours or when workstations are left unattended.

2.0 Purpose

The purpose of this policy is to ensure users have an awareness of the importance of keeping both paper and electronic documents and records safe when they are working at their desk/workstation or on their screen and that they have knowledge of how to protect them. This policy will minimize the risk of unauthorized access, loss of and damage to sensitive information, and provides a positive image for visiting customers and potential customers.

3.0 Scope

This policy applies to all JCC employees including temporary staff, sub-contractors, contractors and third parties with access to Jefferson County Commission information and information systems and services. The reference to desks includes any place where printed material containing confidential data or information is being or has been worked upon (i.e. Jefferson County Commission office, site or home desk area). This policy is intended to supplement any and all applicable local, state, and federal laws that may apply, including but not limited to:

3.1 Confidential Information

All users have the responsibility to use information and data in a secure and confidential way. Staff who have access to information about individuals (whether patients, employees, customers, and/or others) need to use it effectively, whilst maintaining appropriate levels of confidentiality. This information sets out the key principles and main '"do's" and "don'ts"' that everyone should follow to achieve this for both electronic and paper records.

4.0 Policy

JCC Users are expected to secure all information by keeping their workspace clear of sensitive and confidential information at all times. The following guidelines shall be implemented.

4.1 Clear Desk Policy

4.1.1 When leaving a desk for a short period of time, users must ensure printed matter containing information that is confidential is not left in view.
4.1.2 When leaving a desk for a longer period of time / overnight, users must ensure printed matter containing confidential information is securely locked away.

4.1.3 Whiteboards and flipcharts should be wiped / removed of all confidential information when finished with.

4.2 Clear Screen Policy

4.2.1 When leaving the workstation for any period of time, the user must ensure they lock their computer session to prevent unauthorized access to the network and stored information.

4.2.2 All users must ensure their screens cannot be overlooked by members of the public, or people without the necessary authority when confidential data and/or information is displayed. Where appropriate, privacy filters should be used to protect the information.

4.2.3 Following (up to a maximum of) 15 minutes of inactivity, the session will be automatically locked as a failsafe measure.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Any disciplinary action taken by the ITS Department to discipline a user who has violated this policy, will follow Jefferson County Commission's Disciplinary process.

6.0 Policy Owner

Jefferson County Commission

6.0a Policy Administrator

Chief Information Officer, Information Technology Services Department

7.0 Policy Approval Date

March 20, 2020

8.0 Policy Effective Date

March 20, 2020

Revision History

Initial Author	ITS Governance
Created On	August 13, 2019
Last Modified By	ITS Governance
Last Modified On	March 20, 2020

Revision Number	3
Approver	County Manager's Review Committee

Version	Changed By	Changed On	Notes / Comments
2	Information Technology	March 13, 2013	
3	Information Technology Services	March 20, 2020	

JEFFERSON COUNTY COMMISSION

Information Technology Services Department

Data Classification Security Rules & Regulations

1.0 Overview

Throughout this document the term policy refers to the strategy, procedures, rules, and regulations defined and encapsulated within each section of this document to achieve the stated information security goals. Jefferson County Commission ("JCC") Information Technology Services Department assigns data sensitivity levels based on who should have access to it and how much harm would be done if it were disclosed. This assignment of sensitivity is called "data classification." JCC Information Technology Services Department (ITS) will maintain a data classification system designed to enable the use of data so that information will be protected from unauthorized disclosure, use or modification, and deletion. The determinations to be made in accordance with this policy are subject to the requirements of state and federal law, rules, and regulations.

2.0 Purpose

Protecting data generated, accessed, transmitted and stored by any JCC resources; and to promote compliance with local, state, and federal regulations regarding privacy and sensitivity of information. Sensitive, Restricted and Public data types will be the three data types that are appropriately chosen. ITS will maintain a data classification system designed to enable the use of data so that information will be protected from unauthorized disclosure, use or modification, and deletion. The determinations will be made in accordance with this policy and are subject to the requirements of state and federal law, rules, and regulations.

3.0 Scope

This data classification policy is applicable to all County owned data which is generated, accessed, transmitted, or stored on systems and networks owned and managed by JCC, or approved vendors, and/or hosted in a cloud environment.

4.0 Policy

4.1.1 All JCC information and information entrusted to JCC from third parties falls into one of three sensitivity classifications. Classifying data is the process of categorizing data according to its sensitivity. If no designation has been assigned, information must be handled as though it is **Sensitive**, **Restricted,** or **Public** data.

4.1.2 Legally protected information, or what's called Restricted and Sensitive at JCC (e.g., SSNs, heath information, etc.), requires a greater level of protection, while lower risk data (e.g., published information, publicly available information, etc.), requires proportionately less protection. This policy describes JCC information classifications and appropriate processes and procedures that should or, where noted, must be applied based on the sensitivity of the information.

4.1.3 Prior to releasing, publishing, or disclosing any information, the owner of the information should classify the information according to its need for sensitivity. Consult applicable policies before tagging the data under any classification.

4.1.4 The owner of the information should ensure that disclosure controls and procedures are implemented to afford the degree of protection required by the assigned classification. Each member will use this classification standard as their baseline standard. If a member requires a more restrictive classification for a particular class of information due to state, federal or other agreements, the more restrictive classification will apply.

5.0 Classification Level and Descriptions

5.1.1 Sensitive

Sensitive information is information whose unauthorized disclosure, compromise or destruction would result in severe damage to the County, its citizens, or employees (e.g., social security numbers, dates of birth, medical records, credit card or bank account information, information regarding minors). The examples given are not intended to be all-inclusive. Additional types of information may be deemed Sensitive. Sensitive is intended solely for use within JCC and is limited to those with a “business need-to-know.”

5.1.2 Restricted

Restricted information is internal use information that must be guarded due to custody, ethical or privacy considerations. Although not specifically protected by statute, regulations, or other legal obligations or mandates, unauthorized use, access, disclosure, acquisition, modification, loss or deletion of information at this level could cause monetary loss, damage to the County’s reputation, or violate an individual’s privacy rights (e.g., educational records, employment history, and biographical information). The examples given are not intended to be all-inclusive. Additional types of information may be deemed Restricted. Restricted information is intended for use by JCC employees, contractors, and vendors covered by a non-disclosure agreement.

5.1.3 Public

Public information is information that is not publicly disseminated, but accessible to the public. These data values are either explicitly defined as public information (e.g., employee salary ranges), intended to be readily available to individuals both on and off premises (e.g., an

employee's work email addresses), or not specifically classified elsewhere in the protected data classification standard. The examples given are not intended to be all-inclusive. Additional types of information may be deemed Public. Knowledge of public information does not expose JCC to financial or reputational loss or jeopardize the security of County data. Publicly available data may be subject to appropriate review or disclosure procedures to mitigate potential risks of inappropriate disclosure of data or to organize it according to its risk of loss or harm from disclosure.

6.0 Data Classification Examples

3	***RESTRICTED:* Information that would likely cause serious harm to individuals or the JCC if disclosed.** • Individually identifiable medical records • Personally identifiable information (PII), banking or financial information or medical information (ePHI). • Information commonly used to establish identity that is protected by state, federal, or foreign privacy laws and regulations • National security information (subject to specific government requirements) • Credentials (Usernames/Passwords) and JCC PINs that can be used to access sensitive information
2	**SENSITIVE: Information that could cause risk of material harm to individuals or the JCC if disclosed.** • JCC personnel records (employees may discuss terms and conditions of employment with each other and third parties) • Institutional financial records • Building plans and information about the JCC physical security plans • Other personal information protected under state, federal and foreign privacy laws.
1	**Public information.** • Data that has been de-identified in accordance with applicable rules • Published information about the JCC

7.0 Data Classification Standards and Process

7.1.1 The Risk Assessment will be performed annually which will recommend safeguards or security controls and describe the expected level of risk that would remain if these controls were put in place. Following are minimum security controls that must be considered based on the three data classification levels. Departments may assign more stringent requirements based on the results of their risk assessment. Departments that receive data from other agencies must adhere to any security controls agreed to by the originating department and the receiving department.

7.1.2 JCC recognizes that many types of information may be classified as JCC sensitive. This classification may vary by department or business unit. The dissemination of such information may be limited only to those individuals that have a "Need to Know" to perform their job responsibilities. However, there may be instances where it is cost prohibitive and/or technically complicated to limit information based on the Need-to-Know model. In these cases, the Information Owner and Information Manager determine the associated risk of potential information loss. This balance of cost, technology, and risk are then used to define the security access model.

7.1.3 Information classification is required to determine the relative sensitivity and criticality of information technology resources, which provide the basis for protection efforts and access control. The Data Classification and Protection Standard establishes a baseline derived from federal laws, state laws, regulations, and County policies that govern the privacy and sensitivity of data.

7.1.4 The Data Classification and Protection Standard applies to all data (e.g., research, financial, employee data collected in electronic or hard copy form that is generated, maintained, and entrusted to JCC except where a different standard is required by grant, contract, or law.

7.1.5 All institutional data must be classified into one of three data classifications that JCC has identified, which are referred to as Sensitive, Restricted, and Public. Although all the enumerated data values require some level of protection, some data values are considered more sensitive and correspondingly tighter controls are required for these values.

7.1.6 All County data is to be reviewed on a periodic basis and classified according to its use, sensitivity, and importance to the County and in compliance with federal and/or state laws.

7.1.7 The ITS department has pre-defined several types of sensitive data. The level of security required depends in part on the effect that unauthorized access or disclosure of those data values would have on County operations, functions, image or reputation, assets, or the privacy of individual members of the JCC Community.

8.0 Roles and Responsibilities

8.1.1 County Attorney's Office – Responsible for issuing, reviewing, and removing JCC wide classification data types.

8.1.2 Department Heads - Responsible for reviewing data types and identifying the data storage location(s) for the impacted records that their department is the "official data owner". Also responsible for communicating the data type to all impacted parties that store records, all departmental employees, and departmental management. Responsible to identify the data flow diagrams and impact on the data if exposed. Communicate that risk to the risk management and legal team asap.

8.1.3 ITS Department – Responsible for ensuring that technology systems have the adequate controls in place to manage data. Upon receiving proper authorization from department(s) designated as the official data owner, will execute data security controls for electronic data keeping systems that they manage.

9.0 More Data Type examples

Governance: Non-public financial or other material information, anti-trust, strategic plans, and other such information.

Citizen: Information gathered on citizens, medical data, name and address of citizens, and other similar citizen information.

Financial: JCC financial contributions, business profitability, actual, financial planning, financial reporting, internal audit, legal entities, shareholder information, Tax, Treasury, project forecasts, and other such financial information.

Other: Computer account/access information, contract services, corporate security incidents, litigation.

Person: Sensitive employee information such as background checks, benefits, credit card, and employment information, medical records, organizational, financial, payroll, skills, and another similar employee information.

Supplier: Capacity, business forecasts, contracts and prices, financial data, purchases made, and other such supplier data.

Technology: Export restricted data, product logics, IT systems designs, lab notebooks, software design, security design, research reports and information, information received from outside parties under nondisclosure agreements and technical agreements, and other similar technology information.

10.0 Policy Owner

Jefferson County Commission

10.0a Policy Administrator

Chief Information Officer, Information Technology Services Department

11.0 Policy Approval Date

March 20, 2020

12.0 Policy Effective Date

March 20, 2020

Revision History

Initial Author	ITS Governance
Created On	August 13, 2019
Last Modified By	ITS Governance
Last Modified On	March 20, 2020
Revision Number	3
Approver	County Manager's Review Committee

Version	Changed By	Changed On	Notes / Comments
2	Information Technology	March 13, 2013	
3	Information Technology Services	March 20, 2020	

JEFFERSON COUNTY COMMISSION

Information Technology Services Department

Data Retention & Disposal Security Rules & Regulations

1.0 Overview

Throughout this document the term policy refers to the strategy, procedures, rules, and regulations defined and encapsulated within each section of this document to achieve the stated information security goals. One of Jefferson County Commission ("JCC") Information Technology Services Department's primary objectives is to ensure that all necessary electronic records and documents are adequately protected and maintained and that records that are no longer needed or are of no value are discarded at the proper time. This Policy should be read in conjunction with other policies that have as their objectives the protection and security of data such as the Network Security Policy, Information Security Policy, and Data Classification Policy.

2.0 Purpose

The purpose of this Data Retention and Disposal Policy is to ensure that JCC retains its official records in accordance with the requirements of all applicable laws and to ensure that official records no longer needed by JCC are discarded at the proper time. This Policy provides guidelines concerning the length of time official records should be retained under ordinary business circumstances.

3.0 Scope

This policy specifies the retention and destruction requirements that apply to all Information Assets that are held by JCC Information Technology Services information systems and are classified as either Public Data (Open Data), Sensitive Data, or Restrictive Data, as defined in the Data Classification & Disposal Policy. This policy governed by the Local Government Records Commission Alabama County Commissions Functional Analysis & Records Disposition Authority Document revised October 23, 2013. Cooper Green Health Services records and the Youth Detention Center records are governed by separate policies.

4.0 Policy

To provide the comprehensive range of services to the citizens of Jefferson County Alabama, the retention, storage and disposal of data will be undertaken at appropriate times, with adequate methods to meet our legislative, regulative and any other significant obligations.

JCC needs to process data and use documentation to be able to provide its services. This requires information to be stored in systems that enable it to honor contracts and other agreements. JCC Information Technology Services Department (ITS) will only hold data and documentation for as long as required and will deploy an effective review mechanism to ensure that this works in practice based on the Data Classification Policy. ITS will ensure compliance with all necessary regulatory and legislative requirements regarding data and document retention, storage and disposal.

4.1 Data Retention

As stated above, the ITS shall not retain data for any longer than is necessary in

light of the purpose(s) for which that data is collected, held, and processed. When establishing and/or reviewing retention periods, the following shall be taken into account:

1. Alabama County Records Retention, Recommendations and Disposition
2. The objectives and requirements of the Jefferson County Commission;
3. The class of data in question;
4. The purpose(s) for which the data in question is collected, held, and processed;
5. The County's legal basis for collecting, holding, and processing that data;
6. Anticipated or pending litigation under which the data may be discoverable or subject to a litigation hold.

4.1.2 If a precise retention period cannot be fixed for a particular type of data, criteria shall be established by which the retention of the data will be determined, thereby ensuring that the data in question, and the retention of that data, can be regularly reviewed against those criteria.

4.1.3 Notwithstanding the following defined retention periods, certain data may be deleted or otherwise disposed of prior to the expiry of its defined retention period where a decision is made within the County to do so (whether in response to a request by a data subject or otherwise) so long as the disposal does not violate any local, state, or federal laws or evidentiary rules.

4.1.4 In limited circumstances, it may also be necessary to retain data for longer periods where such retention is for archiving purposes that are in the public interest, for historical purposes, for legal reasons, or for statistical purposes. All such retention will be subject to the implementation of appropriate technical and organizational measures to protect the rights and freedoms of data subjects.

Data Retention Schedule

Data Class	*Retention Period*
Public Data (Open Data)	See Alabama County Commissions Functional Analysis & Records Disposition Authority
Sensitive Data	See Alabama County Commissions Functional Analysis & Records Disposition Authority
Restrictive Data	See Alabama County Commissions Functional Analysis & Records Disposition Authority

4.2 Data Disposal

4.2.1 Removal Classification

A) Clearing

If comprehensive data removal from the media is not required, then non-specialist staff or contractors may carry out clearing. Typical clearing programs use sequential writes of patterned data, ensuring that data is not easily recovered using standard techniques and programs. To ensure that historical data is thoroughly removed it is advisable to make as many passes as is practicable.

B) Purging

Purging is a more advanced level of sanitization that renders media unreadable even through an advanced laboratory. After removal of media from its current security context, there must be sufficient care taken to ensure that data is irretrievable. If

purging of the media is required, a minimum of seven passes qualifies as a purging process.

C) Destroying

Destroying renders media unusable. Destruction techniques include but are not limited to disintegration, incineration, pulverizing, shredding and melting.

4.2.2 Media Destruction

A) Hard Disk Destruction

Degaussing is a simple method that permanently destroys all data and disables the drive. Degaussing uses a high-powered magnetic field that permanently destroys data on the platters. The recommended specification for data destruction is the SEAP 8500 Type II standard used for classified government material.

C) Solid-State Devices

Solid-state devices normally require the complete physical destruction of the device to ensure that any recovery of data is impossible. Incineration will melt SD cards. Devices such as USB thumb drives should be physically destroyed using brute force methods. As long as appropriate safety methods are in use, non-specialist staff can destroy these devices.

D) Cloud Based (Azure/AWS) Devices

"When cloud providers determine that media has reached the end of its useful life, or it experiences a hardware fault, they shall follows the techniques detailed in Department of Defense (DoD) 5220.22-M ("National Industrial Security Program Operating Manual") or NIST SP 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process.

4.2.3 Data Removal and Destruction Management

Once a specialist company or contractor has processed the media, there should be a procedure for verification of data removal. It is important to maintain an effective method of managing the process of data destruction. This ensures that all media requiring cleaning or destruction is correctly organized and properly audited. Tracking of hard disk serial numbers should be used a bare minimum for individual component tracking.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Any disciplinary action taken by the ITS Department to discipline a user who has violated this policy, will follow Jefferson County Commission's Disciplinary process.

6.0 Policy Owner

Jefferson County Commission

6.0a Policy Administrator

Chief Information Officer, Information Technology Services Department

7.0 Policy Approval Date

March 20, 2020

8.0 Policy Effective Date

March 20, 2020

Revision History

Initial Author	ITS Governance
Created On	August 13, 2019
Last Modified By	ITS Governance
Last Modified On	March 20, 2020
Revision Number	3
Approver	County Manager's Review Committee

Version	Changed By	Changed On	Notes / Comments
2	Information Technology	March 13, 2013	
3	Information Technology Services	March 20, 2020	

JEFFERSON COUNTY COMMISSION

Information Technology Services Department

Email Security Rules & Regulations

1.0 Purpose

Throughout this document the term policy refers to the strategy, procedures, rules, and regulations defined and encapsulated within each section of this document to achieve the stated information security goals. All emails internally and externally will be properly identified per Jefferson County Commission ("JCC") Data Classification policy and any internal or external emails will only be distributed to properly authorized recipients. Spam, Phishing, Chain and other non-business emails will be in violation of this policy. Automated email surveillance systems are in place to identify data that appear malicious in nature (e.g., viruses, spyware) or contain confidential information (e.g., protected health information and personally identifiable information) for further investigation.

All emails containing classified information will be properly encrypted and secured and proper authentication measures should be applied. To prevent tarnishing the public image of JCC, emails that are sent to the general public should be considered an official announcement and be treated as an official statement. Additionally, information such as protected health information (PHI), personally identifiable information (PII), or financial records are either classified or confidential and must be treated with extreme care to avoid inappropriate disclosure that could lead to exposure of risk to JCC and its affiliates. A complete list of all data considered confidential and classified by JCC is available in Data Classification policy and everyone should adhere the same document. All emails are the official property of JCC if they are sent or received by JCC Department of Information Technology Services (ITS) Network Infrastructure.

2.0 Scope

This policy covers appropriate use of any email sent from a JCC email address whether internally or externally and applies to all employees, vendors, and agents operating on behalf of Jefferson County.

3.0 Policy

3.1 Email Account Owner Responsibility

Email accounts are personal Except in cases approved by JCC Information Security team or General Counsel, these email accounts are not transferrable to other users. Access to JCC email system requires certain responsibilities for the account holder, including, but not limited to, the following:

3.1.1 Do not share your email account password with anyone, including ITS or ITS Information Security Officer and/or ITS Information Security Team (They will never ask you for your password). Use delegation, where appropriate, if another user needs access to your email.

3.1.2 Email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, appearance, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national

origin. Employees who receive any emails with this content from any JCC employee should report the matter to their supervisor immediately.

3.1.3 Do not falsify email accounts to send out email as another person.

3.1.4 Do not flood/spam people with email in an attempt to disrupt their service.

3.1.5 Do not accept credit card numbers sent in email for payment purposes.

3.1.6 Do not create rules that enable automated forwarding to non-JCC email accounts.

3.1.7 Do not send confidential or classified data to any party via email without using approved encryption standards and tools.

3.1.8 Do not use personal email addresses, such as Gmail or Yahoo!, for work-related communications.

3.1.9 Use of electronic communications to intimidate others or to interfere with the ability of others to conduct JCC business.

3.1.10 "Spoofing," i.e., constructing electronic communication so it appears to be from someone else.

3.1.11 "Snooping," i.e., obtaining access to the files or communications of others for the purpose of satisfying idle curiosity, with not substantial JCC business purpose.

3.1.12 Attempting unauthorized access to data or attempting to breach any security measures on any electronic communication system, or attempting to intercept any electronic communication transmissions without proper authorization.

3.2 Personal Use - Using a reasonable amount of JCC systems for personal emails is acceptable, but non work-related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from a JCC email account is prohibited. Virus warnings and/or other malware warnings and mass mailings from JCC shall be approved by JCC Chief Information Officer (CIO) before sending. These restrictions also apply to the forwarding of email received by any JCC employee.

3.3 Monitoring - JCC employees shall have no expectation of privacy in anything they store, send or receive on the county's email system. JCC may monitor and inspect messages without prior notice in the course of an investigation triggered by indications of misconduct or on random basis however JCC is not obliged to monitor email messages. The contents of electronic communications, properly obtained for legitimate business or legal purposes, may be disclosed without permission of or notice to the employee. JCC will attempt to refrain from disclosure of particular messages if disclosure could create personal embarrassment, unless such disclosure is required to serve a business purpose or satisfy a legal obligation.

3.4 Forwarding - Employees must exercise utmost caution when sending any email from inside JCC to an outside network. Unless approved by the employee's departmental manager and ITS, JCC email will not be automatically forwarded to an external destination. Sensitive information, as defined in JCC's Data Classification Policy, will not be forwarded via any means, unless that email is critical to business and is encrypted in accordance with JCC's Encryption Policy.

3.5 Administrative Correspondence - JCC Administrative Correspondence includes, though is not limited to clarification of established county policy, including holidays, timecard information, dress code, workplace behavior and any legal issues such as intellectual property violations. To ensure Administrative Correspondence is properly retained, the emails retention will be administered by ITS and adhere to JCC's Retention Policy.

3.6 Fiscal Correspondence - JCC Fiscal Correspondence is all information related to revenue and expense for JCC. To ensure Fiscal Correspondence is properly retained, the emails retention will be administered by ITS and adhere to JCC's Retention Policy.

3.7 Email Retention

Email is a business record if there exists a legitimate and ongoing business or legal reason to preserve the information contained in the email. All emails that are identified as a JCC business record shall be retained according to JCC Retention Policy for potentially relevant information even if users delete/purge their JCC emails or attachments or any important information from their email client/mobile devices.

3.8 General Correspondence - JCC General Correspondence covers information that relates to general employee interaction and the operational decisions of the business.

3.9 Ephemeral Correspondence - JCC Ephemeral Correspondence is by far the largest category and includes personal email, requests for recommendations or review, email related to county development, updates and status reports. All emails considered Ephemeral Correspondence will adhere to JCC Data Classification and Retention Policies.

3.10 Instant Messenger Correspondence - JCC Instant Messenger General Correspondence may be saved with logging function of Instant Messenger, or copied into a file and saved. Instant Messenger conversations that are Administrative or Fiscal in nature should be copied into an email message and sent to the appropriate email retention address. All information considered classified per JCC Data Classification Policy shall be strictly prohibited.

3.11 Encrypted Communications - JCC encrypted communications should be stored in a manner consistent with JCC's Data Classification and Encryption Policies.

3.12 Recovering Deleted Email via Backup Media - JCC email data is maintained within secure cloud infrastructure that allows the County to enable system wide save lock on all users email accounts. This functionality effectively saves all emails sent from and sent to all users for a minimum for 7 years. Therefore, emails are effectively retained once they have been sent from or received by a JCC employee/affiliate email account. The system provides email administrators the capability to recall messages that users have accidentally and/or knowingly deleted.

3 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Any disciplinary action taken by the ITS Department to discipline a user who has violated this policy, will follow Jefferson County Commission's Disciplinary process.

4 Policy Owner

Jefferson County Commission

4.0a Policy Administrator

Chief Information Officer, Information Technology Services Department

5 Policy Approval Date

March 20, 2020

6 Policy Effective Date

March 20, 2020

7 Definitions

Term **Definition**

Email - The electronic transmission of information through a mail protocol such as SMTP or IMAP.

Forwarded email - Email resent from an internal network to an outside point.

Chain email or letter - Email sent to successive people. Typically, the body of the note has direction to send out multiple copies of the note and promises good luck or money if the direction is followed.

Sensitive information - Information is considered sensitive if it can be damaging to Jefferson County or its citizens.

Virus warning - Email containing warnings about virus or malware.

Unauthorized Disclosure - The intentional or unintentional revealing of restricted information to people, both inside and outside Jefferson County, who do not have a need to know that information.

Approved Electronic Mail - Includes all mail systems supported by the Information Technology Services Team.

Approved Instant Messenger - The CISCO Jabber Secure IM Client and Microsoft Business Skype are the only IM clients approved for use on Jefferson County computers.

Individual Access Controls - Individual Access Controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner.

Insecure Internet Links - Insecure Internet Links are all network links that originate from a locale or travel over lines that are not totally under the control of Jefferson County.

Revision History

Initial Author	ITS Governance
Created On	August 13, 2019
Last Modified By	ITS Governance
Last Modified On	March 20, 2020
Revision Number	3
Approver	County Manager's Review Committee

Version	Changed By	Changed On	Notes / Comments
2	Information Technology	March 13, 2013	
3	Information Technology Services	March 20, 2020	

JEFFERSON COUNTY COMMISSION

Information Technology Services Department

Employee Information Security Rules & Regulations

1.0 Overview

Throughout this document the term policy refers to the strategy, procedures, rules, and regulations defined and encapsulated within each section of this document to achieve the stated information security goals. The Jefferson County Commission ("JCC") Employee Information Security Policy serves to be consistent with best practices associated with organizational Information Security management. It is the intention of this policy to establish a general Information Security requirement for all JCC employees and track acknowledgement.

2.0 Purpose

- JCC is committed to protecting the security and privacy of county, citizen, and employee information in accordance with applicable laws and regulatory requirements. Information security is the protection of information from unauthorized use, circumvention, neglect, disclosure, modification or destruction, whether accidental or intentional.
- The confidentiality and protection of citizens information is one of JCC's fundamental responsibilities. While information is critical to providing quality service, we recognize that our most important asset is the trust of our citizens. Thus, the safekeeping of citizen information is a priority for JCC.
- Protecting JCC and citizen information is the responsibility of all employees. All employees who have access to systems that store and/or access such information are required to understand and comply with any and all specific policies, procedures, standards and guidelines established in support of the Information Security Program.
- This policy is intended to establish a framework for JCC policies related to information security and provide a straightforward communication to all employees. All detailed Information Security policies, procedures, and guidance will follow this framework and be available to all employees.
- Questions regarding implementation of this policy should be directed to the Department of Information Technology Services ("ITS") or Human Resources.

3.0 Scope

This policy encompasses all JCC employees and contractors, volunteers and visitors or any one with authorized access to JCC assets or information systems.

Security controls must be used regardless of:

- The media on which the information is stored (including, but not limited to, paper, hard drives, servers, databases, mobile and handheld devices, transparencies, email systems, web or Audit/Video systems or voice mail systems, etc.).
- The systems that process the information (including, but not limited to workstations, laptops, handheld devices, servers, email systems, web/audio/video systems, voice mail systems, databases, etc.).
- The methods by which the information is moved (including, but not limited to wireless, electronically, written, telephone, face-to-face conversation, removable media, etc.).

4.0 Policy

All JCC information security policies, standards, guidelines, and practices shall be coordinated through the ITS and shall be consistent with the enterprise-wide approach in developing, implementing, and managing information systems security.

- 4.1 All JCC personnel who have access to county or citizen information are expected to exercise discretion and due diligence in connection with their use of information created, stored, transmitted or disposed in the course of their job duties, regardless of the medium in which that information is maintained.
- 4.2 All JCC personnel should use due care in the course of their job duties to protect the confidentiality, integrity, and availability of data created, received, stored, transmitted, or used by the County and citizen.
- 4.3 Take precautions against theft of or damage to information resources.
- 4.4 JCC personnel are prohibited from attempting to circumvent or subvert any JCC information security control.
- 4.5 No authorized user may install, remove, or otherwise modify any information security controls for the purpose of bypassing, avoiding, or defeating any filtering, monitoring, or other security controls JCC may have in place.
- 4.6 Conversations shall not be recorded or monitored without advising all participants, unless a court has explicitly ordered such monitoring or recording to occur without notice.
- 4.7 All authorized users must create and use strong passwords that are in compliance with the ITS Password Policy. These passwords should be kept confidential and not written down or shared with anyone.
- 4.8 Users must not intentionally seek or provide information on, obtain copies of, or modify data files, programs, passwords or other digital materials belonging to other users, without the specific permission of those other users.
- 4.9 Users must not encroach, disrupt or otherwise interfere with access or use of the JCC's information or information resources.
- 4.10 All authorized users must participate in the provided Security Training and be re-certified on an annual basis.
- 4.11 All authorized users shall read and comply with JCC Clear Desk & Screen policy.
- 4.12 All authorized users that access JCC information remotely must read and comply with the documented Remote Access Policy.
- 4.13 All authorized users will read and comply with the complete JCC Information Security Policy.
- 4.14 All authorized users will immediately notify and report defects in system accounting, concerns with system security, or suspected unlawful or improper system activities or any indications or suspicions of a breach or violation of security.

5.0 ENFORCEMENT

All JCC personnel must comply with this policy, including all detailed JCC Information Security Policies and implemented procedures. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Any disciplinary action taken by the ITS Department to discipline a user who has violated this policy, will follow Jefferson County Commission's Disciplinary process.

6.0 Policy Owner

Jefferson County Commission

6.0a Policy Administrator

Chief Information Officer, Information Technology Services Department

7.0 Policy Approval Date

March 20, 2020

8.0 Policy Effective Date

March 20, 2020

Revision History

Initial Author	ITS Governance
Created On	August 13, 2019
Last Modified By	ITS Governance
Last Modified On	March 20, 2020
Revision Number	3
Approver	County Manager's Review Committee

Version	Changed By	Changed On	Notes / Comments
2	Information Technology	March 13, 2013	
3	Information Technology Services	March 20, 2020	

JEFFERSON COUNTY COMMISSION

Information Technology Services Department

Encryption Security Rules & Regulations

1.0 Overview

Throughout this document the term policy refers to the strategy, procedures, rules, and regulations defined and encapsulated within each section of this document to achieve the stated information security goals. For Jefferson County Commission (JCC), encryption is a critical tool for managing and protecting confidential, restricted, and/or sensitive information. The use of encryption technology significantly limits unauthorized access to critical data.

2.0 Purpose

The purpose of this policy is to provide JCC guidance on the use of encryption to protect information resources that contain, process, or transmit confidential, restricted, and/or sensitive information.

3.0 Scope

This policy applies to all information classified as confidential, restricted, and/or sensitive that may be transmitted by electronic means. Electronic information is defined as data, stored electronically, copied, and/or transmitted from JCC information systems, employees, business partners, or customers.

4.0 Policy

All JCC data that's classified as restricted and/or sensitive in accordance with the Data Classification Policy shall not be stored and/or transmitted across any communication mechanism unless it is protected via encryption.

4.1 Principles of Encryption

- Where possible confidential, restricted, and/or sensitive information must be stored on a secure Information Technology Services (ITS) network server with restricted access.

- All confidential and restricted information transmitted via email internally and externally must be encrypted.

4.2 Servers

Severs that store confidential/restricted/sensitive data must be located within JCC ITS data centers and/or within ITS cloud partners secure cloud infrastructure.

4.3 Desktop Computers

JCC desktop computers are generally accepted as having a lower risk of being stolen and as such most will not need to have disk encryption. However, where possible the following types of JCC desktop computers will need to have disk encryption:

1) Desktop computers assigned to Jefferson County Commissioners and staff.

2) Desktop computers assigned to Jefferson County Commission's County Manager and staff.
3) Desktop computers assigned to Jefferson County Commission's County Attorney and staff.
4) Desktop computers assigned to Jefferson County Commission department heads and deputies.

4.4 Laptop and Tablet

Newly purchased laptops and tablet computers must have disk encryption if assigned to the following areas:

1) Commissioners and/or staff
2) County Manager and/or staff
3) County Attorneys
4) Department Heads and Deputy Directors

4.5 Removeable Storage Devices

All restricted and sensitive information stored on removable storage devices must be encrypted. In addition to being encrypted, removable storage devices must be stored in a locked cabinet or drawer when not in use.

4.6 Transmission Security

- All confidential, restricted, and/or sensitive information transmitted via email to must be encrypted. The transfer of such information outside of the Jefferson County Commission's domain must be authorized by sender's management and/or apart of sender's role and responsibilities (i.e. vendor correspondence).

- Where confidential, restricted, and/or sensitive information is transmitted through a public network (for example the internet) to an external third party the information must be encrypted first or sent via a secure channel (for example: Secure FTP, TLS, VPN etc.).

- All confidential, restricted, and/or sensitive information transmitted via wireless networks must be encrypted using WEP (Wired Equivalent Privacy) protocol or better. All new wireless networks installations must be encrypted using WPA (Wi-Fi Protected Access) or latest wireless security protocol.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Any disciplinary action taken by the ITS Department to discipline a user who has violated this policy, will follow Jefferson County Commission's Disciplinary process.

6.0 Related Policies

Data Classification Policy

7.0 Policy Owner

Jefferson County Commission

7.0a Policy Administrator

Chief Information Officer, Information Technology Services Department

8.0 Policy Approval Date

March 20, 2020

9.0 Policy Effective Date

March 20, 2020

10.0 Definitions

Term **Definition**

Revision History

Initial Author	ITS Governance
Created On	August 13, 2019
Last Modified By	ITS Governance
Last Modified On	March 20, 2020
Revision Number	3
Approver	County Manager's Review Committee

Version	Changed By	Changed On	Notes / Comments
2	Information Technology	March 13, 2013	
3	Information Technology Services	March 20, 2020	

JEFFERSON COUNTY COMMISSION

Information Technology Services Department

Information Security Rules & Regulations

1.0 Overview

Throughout this document the term policy refers to the strategy, procedures, rules, and regulations defined and encapsulated within each section of this document to achieve the stated information security goals. Jefferson County Commission ("JCC") Information Security Policy serves to be consistent with best practices associated with organizational Information Security management. It is the intention of this policy to ensure the protection of JCC information resources from accidental or intentional unauthorized access or damage and establish a general Information Security requirement for all JCC employees and resources.

2.0 Purpose

The contents of this document specify JCC Department of Information Technology Services ("ITS") overall policies for information security. The Information Security Program and policies were designed to meet industry standards.

3.0 Scope

The scope of this policy is applicable to all employees, contractors, and vendors of JCC. All users including JCC employees, contractors, vendors or others that access JCC assets (but not limited to all computer and communication facilities owned, leased, operated, or contracted by JCC. This includes networking devices, personal digital assistants, telephones, wireless devices, personal computers, workstations, mainframes, minicomputers, and any associated peripherals and software, regardless of whether used for administration, development, research or other purposes) and data are responsible for adhering to this policy.

4.0 Policy

JCC management expects all personnel, contractors, and business partners of JCC to ensure all critical information used and held by the County is protected to assure its confidentiality, integrity and availability. In particular, this information security program shall apply to safeguarding sensitive, personal and citizen information regardless of storage location, medium and form (in both paper and electronic records) from anticipated threats and hazards to the security and integrity of this information including unauthorized access, abuse, theft or inadvertent or unauthorized destruction.

4.1 Information Security Management Framework

4.1.1 This information security policy provides management direction and support for information security across JCC. Specifically, subsidiary

information security policies shall be considered part of this County Information Security Policy and shall have equal standing.

4.1.2 This policy has been approved by JCC leadership and forms part of its policies and procedures. It is applicable to and will be communicated to staff, partners, contractors and other relevant parties.

4.1.3 This policy shall be reviewed and updated regularly, or at least annually, to ensure that it remains applicable and effective in the light of any relevant changes to the environment, law, JCC policies, or contractual obligations. The implementation of the information security policy shall be reviewed independently of those charged with its implementation.

4.1.4 All JCC information security documentation including, but not limited to, policies, standards, and procedures, must be classified as "Internal Use Only," unless expressly created for external business processes or partners.

4.2 Organization of Information Security Management

4.2.1 To manage information security within Jefferson County, ITS shall ensure there is clear direction and visible management support for security initiatives.

4.2.2 ITS is charged with the prevention of serious loss or compromise of critical, valuable, and sensitive information resources by coordinating and directing specific actions that will provide a secure and stable information systems environment consistent with goals and objectives.

4.2.3 The ITS Security Team must perform risk assessments, prepare action plans, evaluate vendor products, assist with control implementations, investigate information security breaches, train other staff members, and perform other activities which are necessary to assure a secure information handling environment.

4.2.4 The ITS Security Team has top management authorization to complete regular assessment of the configuration, programming, operation, maintenance, documentation, training, and any other aspect of any operated information systems.

4.2.5 The ITS Security Team has the authority to create and periodically modify both technical standards and standard operating procedures that support this information security policy. When approved by appropriate management, these new requirements will have the same scope and authority as if they were included in this policy document.

4.2.6 Each year, ITS Security Team must facilitate a enterprise risk assessment. The report resulting from this project must include a detailed description of the information security risks currently facing JCC, and specific recommendations for preventing or mitigating these risks.

4.3 Outsourcing and Third-Party Access Policy

4.3.1 All third-party access to JCC or citizen information or any JCC systems requires approval through the formal Access Control Request process that includes a risk assessment and security review before providing access.

4.3.2 All third parties who are given access to JCC information systems, whether suppliers, or otherwise, must agree to follow JCC information security policies. A summary of the information security policies and the third party's role in ensuring compliance will be provided to any such third party, prior to their being granted access.

4.3.3 JCC will assess the risk to its information and, where deemed appropriate because of the confidentiality, sensitivity or value of the

information being disclosed or made accessible, Jefferson County will require external suppliers of services to sign a confidentiality agreement to protect its information assets.

4.3.4 Persons responsible for agreeing to maintenance and support contracts will ensure that the contracts being signed are in accord with the content and spirit of JCC information security policies and right to audit compliance with these policies.

4.3.5 All contracts with external suppliers for the supply of services to JCC must be monitored and reviewed to ensure that information security requirements are being satisfied. Contracts must include appropriated provisions to ensure the continued security of information and systems in the event that a contract is terminated or transferred to another supplier.

4.3.6 Any facilities management, outsourcing or similar company with which JCC may do business must be able to demonstrate compliance with JCC information security policies and enter into binding service level agreements that specify the performance to be delivered and the remedies available in case of non-compliance.

4.3.7 All disclosures of confidential, employee, or citizen information to third parties must be accompanied by an explicit statement describing exactly what information is restricted and how this information may and may not be used. In no case may JCC disclose any information about its citizens without the citizen's written approval.

4.3.8 If JCC terminates its contract with any third-party organization that is handling private information, this same third-party organization must immediately destroy (and certify destruction) or return all of JCC's private data in its possession.

4.4 Terms and conditions of Employment

4.4.1 All employees must comply with the information security policies of JCC. Any information security incidents resulting from non-compliance should result in appropriate disciplinary action.

4.4.2 If, after investigation, a user is found to have violated JCC's information security policy and/or procedures, they may be disciplined in line with JCC's formal disciplinary process.

4.4.3 All employees are required to be compliance with confidentiality rules/guidelines concerning the restricted and/or sensitive of information, during their employment with JCC.

4.5 Recruitment and contracts

4.5.1 All external suppliers who are contracted to supply services to JCC must agree to follow the information security policies of JCC. An appropriate summary of the information security policies must be formally delivered to any such supplier, prior to any supply of services.

4.6 Training and awareness

4.6.1 All staff will be provided with information security awareness tools to enhance awareness and educate them regarding the range of threats,

the appropriate safeguards, and the need for reporting suspected problems.

4.6.2 An appropriate summary of the information security policies must be formally delivered to any contractor, prior to any supply of services.

4.6.3 An appropriate summary of the information security policies must be formally delivered to, and accepted by, all temporary staff, prior to their starting any work for JCC.

4.6.4 JCC is committed to providing training to all users of new systems to ensure that their use is both efficient and does not compromise information security. Periodic training for the Information Security Team is to be prioritized to educate and train in the latest threats and information security techniques.

4.6.5 All new staff, rehires, and transfers are to receive mandatory Information Security Awareness Training as part of induction. Where staff change jobs, their information security needs must be reassessed, and any new training provided as a priority by their department.

4.7 Termination of Employment

4.7.1 Management must respond quickly yet discreetly to indications of staff termination, interacting as necessary with Human Resources management and the Information Security Officer and/or Information Technology Services Security Team.

4.7.2 Upon notification of staff resignations, Human Resources management must notify the ITS designated team member to revoke all access rights.

4.7.3 Departing staff must return all information assets and equipment belonging to JCC to their department.

4.8 Physical & Environmental Security Policy

4.8.1 Areas and offices where sensitive or critical information is processed shall be given an appropriate level of physical security and access control. Staff with authorization to enter such areas are to be provided with information on the potential security risks and the measures used to control them.

4.8.2 A Physical Security Policy shall be developed and enforced that includes controls for access control, monitoring, protection against human and natural events.

4.9 Operations Policy

4.9.1 The procedures for the operation and administration of JCC business systems and activities must be documented with those procedures and documents being regularly reviewed and maintained.

4.9.2 Duties and areas of responsibility shall be segregated to reduce the risk and consequential impact of information security incidents that might result in financial or other material damage to Jefferson County.

4.9.3 Procedures shall be established and widely communicated for the reporting of security incidents and suspected security weaknesses in JCC business operations and information processing systems. Mechanisms shall be in place to monitor and learn from those incidents.

4.9.4 Procedures shall be established for the reporting of software malfunctions and faults in JCC information processing systems. Faults

and malfunctions shall be logged and monitored, and timely corrective action taken.

4.9.5 Changes to operational procedures must be controlled to ensure ongoing compliance with the requirements of information security and must have management approval.

4.9.6 Development and testing facilities for business-critical systems shall be separated from operational facilities and the migration of software from development to production status shall be subject to formal change control procedures.

4.9.7 Acceptance criteria for new information systems, upgrades and new versions shall be established and suitable tests of the system carried out prior to migration to production status. Tests involving live data or periods of parallel running may only be permitted where adequate controls for the security of the data are in place.

4.9.8 Procedures shall be established to control the development or implementation of all operational software. All systems developed for or within JCC must follow a formalized development process.

4.9.9 The security risks to the information assets of all system development projects shall be assessed and access to those assets shall be controlled.

4.10 Information Handling Policy

4.10.1 Inventory shall be maintained of all JCC major information assets and the ownership of each asset will be clearly stated.

4.10.2 Classified information and outputs from systems handling classified data must be appropriately labeled according to the output medium.

4.10.3 When permanently disposing of equipment containing storage media, all sensitive data and licensed software will be irretrievably deleted before the equipment is moved off site using procedures authorized by the ITS Security Team.

4.10.4 Damaged storage devices containing sensitive data will undergo appropriate risk assessment, to determine if the device should be destroyed, repaired or discarded. Such devices will remain the property of the JCC and only be removed from site with the permission of the ITS Security Team.

4.10.5 JCC advocates a clear desk and screen policy particularly when employees are absent from their normal desk and outside normal working hours. In addition, screens on which confidential or sensitive information is processed or viewed should be sited in such a way that they cannot be viewed by unauthorized persons.

4.10.6 Offsite removal of the JCC sensitive information assets, either printed or held on computer storage media, should be properly authorized by the ITS Security Team. Prior to authorization, a risk assessment based on the criticality of the information asset should be carried out.

4.10.7 JCC must ensure that appropriate backup and system recovery procedures are in place. A Back-up policy will be created and enforced that includes a review of frequency, content, location, copies, and testing.

4.10.8 JCC shall ensure that safeguards are in place to protect the integrity of information during the recovery and restoration of data files; especially where such files may replace files that are more recent.

4.10.9 The archiving of information and documents must take place with due consideration for legal, regulatory and business issues, with liaison

between technical and business staff, and in keeping with Jefferson County's Retention Policy.

4.10.10 Storage media used for the archiving of information must be appropriate to its expected longevity. The format in which the data is stored must also be carefully considered, especially where proprietary formats are involved.

4.10.11 All users of information systems must manage the creation, storage, amendment, copying and deletion or destruction of data files in a manner which safeguards and protects the confidentiality, integrity and availability of such files. The degree to which software techniques and disciplined user procedures are necessary should be applied by management and determined by the classification of the information in question.

4.10.12 Day to day data storage must ensure that current information is readily available to authorized users and that archives are both created and accessible in case of need.

4.10.13 Hard copies of sensitive or classified material must be protected and handled according to the distribution and authorization levels specified for those documents.

4.10.14 All employees should be aware of the risk of breaching confidentiality associated with the photocopying (or other duplication) of sensitive documents. Authorization from the document owner should be obtained where documents are classified.

4.10.15 All information used for, or by JCC, must be filed appropriately and according to its classification. All signatures authorizing access to systems or release of information must be properly authenticated.

4.10.16 All hardcopy documents of a sensitive nature are to be shredded or similarly destroyed when no longer required. The document owner must authorize or initiate this destruction.

4.10.17 Any third party used for external disposal of JCC obsolete information bearing equipment or hardcopy material must be able to demonstrate compliance with JCC information security policies and also, where appropriate, provide a service level agreement which documents the performance expected and the remedies available in case of non-compliance.

4.10.18 Prior to sending sensitive information or documents to third parties, not only must the intended recipient be authorized to receive such information, but the procedures and information security measures adopted by the third party must also be reviewed to continue to assure the confidentiality and integrity of the information.

4.10.19 Sensitive data or information may only be transferred across networks, or copied to other media, when the confidentiality and integrity of the data can be reasonably assured throughout the transfer.

4.10.20 Staff participating in conference and videoconference must be made aware of the information security issues involved.

4.10.21 All parties are to be notified in advance whenever telephone conversations or videoconference events, such as lectures, are to be recorded.

4.10.22 Any fax received in error is to be returned to the sender or destroyed. Its contents must not be disclosed to other parties without the sender's permission. Unsolicited or unexpected faxes should be treated with great care until the sender has been identified.

4.11 User Management Policy

4.11.1 Procedures for the provisioning and de-provisioning of users and for managing access to all information systems shall be established to ensure that all users' access rights match their authorizations. These procedures shall be role based and implemented based on the principle of least privilege.

4.11.2 All users shall have a unique identifier (user ID) for their personal and sole use for access to all JCC information services. The user ID must not be used by anyone else and associated passwords shall not be shared with any other person for any reason.

4.11.3 Password management procedures shall be put into place to ensure the implementation of the requirements of the information security policies and to assist users in complying with best practice guidelines.

4.11.4 Access control standards must be established for all information systems, at an appropriate level for each system, which minimizes information security risks yet allows JCC business activities to be carried out without undue hindrance. A review period will be determined for each information system and access control standards will be reviewed regularly at those intervals.

4.11.5 Access to all systems must be authorized and record must be maintained of such authorizations, including the appropriate access rights or privileges granted.

4.11.6 Procedures shall be established for all information systems to ensure that users' access rights are adjusted appropriately, and in a timely manner, whenever there is a change in business need, staff change their role, or staff leave JCC. Users' access rights will be reviewed at regular intervals.

4.11.7 Segregation of duties will be part of the access control roles in areas of access request (HR), access authorization (InfoSec), and access administration (ITS).

4.12 Acceptable Use Policy

4.12.1 An Acceptable Use Policy that includes rules for the acceptable use of information and other assets associated with information processing facilities shall be identified, documented and implemented.

4.12.2 Files downloaded from the internet, including mobile code and files attached to electronic mail, must be treated with the utmost care to safeguard against both malicious code and inappropriate material. Such files, or any others not known to come from a trusted source, must be scanned for possible malicious code before being opened.

4.12.3 Electronic mail must not be used to communicate confidential or sensitive information unless appropriate measures have been taken to ensure authenticity and confidentiality, that it is correctly addressed and that the recipients are authorized to receive it.

4.12.4 Any essential information stored on a laptop or on a PC's local disk must be backed up regularly. It is the responsibility of the user to ensure that this takes place on a regular basis.

4.12.5 Sensitive or confidential data should only be accessed from equipment in secure locations and files must never be printed on a networked printer that does not have adequate protection or security.

4.12.6 All media from outside sources must be screened and scanned by the ITS before being used on any other office computer.

4.12.7 Employees are not permitted to load unapproved software onto JCC PCs, laptops and workstations.

4.13 System Planning Policy

4.13.1 New information systems, or enhancements to existing systems, must be authorized jointly by the business manager(s) and the Chief Information Officer. The business requirements of all authorized systems must specify requirements for security controls.

4.13.2 The implementation of new or upgraded software must be carefully planned and managed, to ensure that the information security risks associated with such changes are mitigated using a combination of procedural and technical controls.

4.13.3 The information assets associated with any proposed new or updated systems must be identified, classified and recorded, and a risk assessment undertaken to identify the probability and impact of security failure.

4.13.4 Equipment shall be correctly maintained, and equipment supporting business systems shall be given adequate protection from unauthorized access, environmental hazards and failures of electrical power or other utilities.

4.13.5 Access controls for all information and information systems are to be set at appropriate levels in accordance with the value and classification of the information assets being protected.

4.13.6 Access to operating system commands and application system functions is to be restricted to those persons who are authorized to perform systems administration or management functions. Where appropriate, use of such commands should be logged and monitored.

4.13.7 Prior to acceptance, all new or upgraded systems shall be tested to ensure that they comply with JCC information security policies, access control standards and requirements for ongoing information security management.

4.14 System Management Policy

4.14.1 JCC systems shall be managed by suitably trained and qualified staff to oversee their day to day running and to preserve security and integrity.

4.14.2 All systems management staff shall be given relevant training in information security issues.

4.14.3 Access controls shall be maintained at appropriate levels for all systems by ongoing proactive management and any changes of access permissions must be authorized and a record of access permissions granted must be maintained.

4.14.4 All access to information services is to be logged and monitored to identify potential misuse of systems or information. Inactive connections to JCC systems shall shut down after a defined period of inactivity to prevent access by unauthorized persons.

4.14.5 Password management procedures shall be put into place to ensure the implementation of the requirement of the information security policies and to assist users in complying with best practice guidelines.

4.14.6 The implementation of new or upgraded software must be carefully planned and managed. Formal change control procedures, with audit trails, shall be used for all changes to systems. All changes must be properly tested and authorized before moving to the production environment.

4.14.7 Capacity demands of systems supporting business processes shall be monitored and projections of future capacity requirements made to

enable adequate processing power, storage and network capacity to be made available.

4.14.8 Security event logs, operational audit logs and error logs must be properly reviewed and managed by qualified staff.

4.14.9 System clocks must be regularly synchronized between all JCC's processing platforms.

4.15 Network Management Policy

4.15.1 JCC network shall be managed by suitably authorized and qualified staff to oversee its day to day running and to preserve its security and integrity. All network management staff shall be given relevant training in information security issues.

4.15.2 The network must be designed and configured to deliver high performance and reliability to meet JCC needs while providing a high degree of access control and a range of privilege restrictions.

4.15.3 The network must be segregated into separate logical domains with routing and access controls operating between the domains. Appropriately configured firewalls shall be used to protect the networks supporting JCC business systems.

4.16 Intrusion Detection / Prevention Systems will be utilized on all perimeter firewalls.

4.16.1 Access to the resources on the network must be strictly controlled to prevent unauthorized access and access control procedures must provide adequate safeguards through robust identification and authentication techniques. Access to all computing and information systems and peripherals shall be restricted unless explicitly authorized.

4.16.2 Remote access to the network will be subject to robust authentication and VPN connections to the network are only permitted for authorized users ensuring that use is authenticated, and data is encrypted during transit across the network.

4.16.3 The implementation of new or upgraded software or firmware must be carefully planned and managed. Formal change control procedures, with audit trails, shall be used for all changes to critical systems or network components. All changes must be properly tested and authorized before moving to the production environment.

4.16.4 Moves, changes and other reconfigurations of users' network access points will only be carried out by staff authorized by Information Technology Services and according to documented procedures.

4.16.5 Networks and communication systems must all be adequately configured and safeguarded against both physical attack and unauthorized intrusion.

4.17 Software Management Policy

4.17.1 JCC business applications are to be managed by suitably trained and qualified staff to oversee their day to day running and to preserve security and integrity.

4.17.2 All Software Development staff shall be given relevant training in information security issues.

4.17.3 The procurement or implementation of new, or upgraded, software must be carefully planned and managed and any development for or by JCC must always follow a formalized development process. Information

security risks associated with such projects must be mitigated using a combination of procedural and technical controls.

4.17.4 Business requirements for new software or enhancement of existing software shall specify the requirements for information security controls.

4.17.5 Formal change control procedures, with comprehensive audit trails, must be used for all changes or upgrades to business software. All changes must be properly authorized and all software, including that which interacts with the modified software, must be tested before changes are moved to the production environment.

4.17.6 The need for systems to support mobile code (applets, scripts, etc.) shall be reviewed. Where the use of mobile code is necessary, the environment shall be configured so as to restrict its ability to harm information or other applications.

4.18 Mobile Computing Policy

4.18.1 Persons accessing information systems remotely to support business activities must be authorized to do so by an appropriate authority within JCC. A risk assessment, based on the criticality of the information asset being used, must be carried out.

4.18.2 JCC will publish guidelines for users of mobile computing equipment advising them on how these should be used to conform to JCC's information security policy and other good practices.

4.19 Cryptography Policy

4.19.1 A policy on cryptographic controls shall be developed with procedures to provide appropriate levels of protection to sensitive information while ensuring compliance with statutory, regulatory and contractual requirements.

4.19.2 Confidential information shall not be taken for use outside of JCC's hosted environment without previous permission from Information Technology Services Security Team.

4.19.3 Procedures shall be established to ensure that authorized staff may gain access, when needed, to any important business information being held in encrypted form.

4.19.4 The confidentiality of information being transferred on portable media or across networks, must be protected by use of appropriate encryption techniques.

4.19.5 Encryption shall be used whenever appropriate on all remote access connections to JCC's network and resources.

4.19.6 A procedure for the management of electronic keys, to control both the encryption and decryption of sensitive documents or digital signatures, must be established to ensure the adoption of best practice guidelines and compliance with both legal and contractual requirements.

4.20 Business Continuity Management Policy

4.20.1 ITS Information Security Officer (ISO) and/or ITS Security Team will initiate a project to assess business continuity requirements and to identify appropriate areas for further action.

4.20.2 A formal risk assessment exercise will be conducted to classify all systems according to their level of criticality to Jefferson County and to determine where business continuity planning is needed.

4.20.3 A business continuity plan will be developed for each system or activity. The nature of the plan and the actions it contains will be commensurate with the criticality of the system or activity to which it relates.

4.20.4 The business continuity plan will be periodically tested. The frequency of testing will be as defined for the appropriate criticality level and will include tests to verify whether management and staff are able to put the plan into operation.

4.20.5 All relevant staff will receive appropriate training to be able to carry out their roles with respect to business continuity plans.

4.20.6 The business continuity plan will be reviewed and, if necessary, updated on a regular basis, but at a minimum on an annual basis.

4.21 Compliance Policy

4.21.1 Relevant statutory, regulatory, and compliance requirements will be identified and documented. Compliance approach to meeting these requirements will be defined and documented.

4.21.2 Appropriate policies will be developed and enforced to ensure the confidentiality, integrity, and availability of sensitive data.

4.21.3 JCC data retention policy defines the appropriate length of time for different types of information to be held. data will not be destroyed prior to the expiration of the relevant retention period and will not be retained beyond that period. During the retention period appropriate technical systems will be maintained to ensure that the data can be accessed.

4.21.4 JCC will only process personal data in accordance with the requirements of the data protection legislation. Personal or confidential information will only be disclosed or shared where authorized to do so.

4.21.5 Where it is necessary to collect evidence from the information systems, it shall be collected and presented in its original format without change or alteration of metadata to conform to the relevant rules of evidence. Expert guidance will normally be sought.

4.21.6 All of JCC systems will be operated and administered in accordance with the documented procedures. Regular reviews and audits will be carried out to verify this compliance.

5.0 Enforcement

Penalties for Non-Compliance: Non-compliance with any policy or standard may expose the Company to unacceptable risk. Any deviation can subject the offender to disciplinary action, including dismissal. If adherence to any policy or standard is believed to be unwarranted, documentation substantiating that assessment must be forwarded to the Information Technology Services Security Team and Human Resources. Any disciplinary action taken by the ITS Department to discipline a user who has violated this policy, will follow Jefferson County Commission's Disciplinary process.

6.0 Policy Owner

Jefferson County Commission

6.0a Policy Administrator

Chief Information Officer, Information Technology Services Department

7.0 Policy Approval Date

March 20, 2020

8.0 Policy Effective Date

March 20, 2020

Revision History

Initial Author	ITS Governance
Created On	August 13, 2019
Last Modified By	ITS Governance
Last Modified On	March 20, 2020
Revision Number	3
Approver	County Manager's Review Committee

Version	Changed By	Changed On	Notes / Comments
2	Information Technology	March 13, 2013	
3	Information Technology Services	March 20, 2020	

JEFFERSON COUNTY COMMISSION

Information Technology Services Department

Laptop Security Rules & Regulations

1.0 Overview

Throughout this document the term policy refers to the strategy, procedures, rules, and regulations defined and encapsulated within each section of this document to achieve the stated information security goals. Corporate laptops are often the biggest data security threat for companies or governmental agencies. Laptops contain highly sensitive information, but are extremely vulnerable to theft
or loss. This policy aims to address laptop security vulnerabilities.

2.0 Purpose

The purpose of this policy is to provide guidance for laptop security for Jefferson County Commission ("JCC") laptops in order to ensure the security of information on the laptop and information the laptop may have access to. Additionally, the policy provides guidance to ensure the requirements of the HIPAA guidelines are met.

3.0 Scope

This policy applies to all JCC employees, contractors, workforce members, vendors and agents with a JCC owned or personal-laptop connected to the JCC data network.

4.0 Policy

Appropriate measures must be taken when using laptops conducting JCC business, ensuring the confidentiality, integrity and availability of sensitive information, including protected health information (PHI) and that access to sensitive information is restricted to authorized users in order to protect JCC sensitive and PHI data. Appropriate measures must also be taken to reduce the likelihood of physical loss or damage to laptops in order to protect JCC capital assets.

4.1 Employees

Employees using laptops shall consider the sensitivity of the information that may be accessed and minimize the possibility of unauthorized access.

4.2 Safeguards

JCC Department of Information Technology Services ("ITS") will implement physical and technical safeguards for all laptops that have network
access via authorized users.

4.3 Appropriate Measures

01. Restricting physical access to laptops to only authorized personnel.

02. Ensuring laptops are not left unattended in public places on or off JCC property.
03. Securing laptops (screen lock or logout) prior to leaving area to prevent unauthorized access.
04. Enabling a password-protected screen saver with a short timeout period to ensure that laptops that were left unsecured will be protected.
05. Complying with all applicable password policies and procedures.
06. A software firewall (such as Windows Firewall) should be turned on and configured for the minimal access necessary to perform normal work.
07. All operating system and application security related hotfixes, service packs and patches should be applied as early as possible after they have been made available.
08. Antivirus definitions should be kept up to date.
09. Laptops are to be used for authorized business purposes only.
10. Never installing unauthorized software on laptops.
11. All sensitive information, including protected health information (PHI) should be stored on network servers.
12. Keeping food and drink away from laptops in order to avoid accidental spills.
13. Securing laptops that contain sensitive information by using cable locks or locking laptops up in drawers or cabinets.
14. Complying with the Encryption Policy.
15. Complying with the Anti-Virus policy.
16. Ensuring that view screen/monitors are positioned away from public view. If necessary, install privacy screen filters or other physical barriers to public viewing.
17. When left at JCC facilities, ensuring laptops are left on but logged off in order to facilitate after-hours updates. Exit running applications and close open documents.
18. Ensuring, when possible, that all laptops use a surge protector (not just a power strip).
19. If wireless network access is used, ensure access is secure by following the Wireless Networking/Access Policy.
20. If remote access is used to connect to the JCC network, ensure the Remote Access Policy is followed.
21. Ensuring laptops are transported and stored in a padded, protective case, bag, backpack, or other similar luggage. Locks should be employed whenever possible.
22. When transported by car, laptops should be stowed in the trunk or some other area where it will not be easily seen or attract attention.
23. When traveling by air or train, the laptop should never become checked baggage and should always be kept as carry-on luggage.
24. During hotel stays, laptops should not be left unsecured in the room. If the user cannot take the laptop with them when leaving the hotel, it should be secured with a cable lock or left in the hotel safe.
25. If network connectivity is required during hotel stays, the user should opt for a wired connection if one is available.
26. When used away from JCC facilities, wireless and bluetooth should be turned off whenever possible to reduce the likelihood of unauthorized access.
27. Public Wi-Fi hotspots should be avoided if at all possible. Great caution should be used when connecting to non-JCC operated networks.
28. Lost or stolen laptops should be reported to ITS as soon as possible. ITS Help Desk and the Jefferson County Sheriff's Department should also be notified.
29. For a laptop that is used to conduct JCC's business that is ready to be retired or, repurposed, the data must be destroyed using secure data disposal tools and methods.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Any disciplinary action taken by the ITS Department to discipline a user who has violated this policy, will follow Jefferson County Commission's Disciplinary process.

6.0 Related Policies

Antivirus Policy
Encryption Policy
Wireless Networking/Access Policy
Remote Access Policy

7.0 Policy Owner

Jefferson County Commission

7.0a Policy Administrator

Chief Information Officer, Information Technology Services Department

8.0 Policy Approval Date

March 20, 2020

9.0 Policy Effective Date

March 20, 2020

10.0 Definitions

Term	Definition
Laptop	A computer that is portable and suitable for use while traveling.
Protective, Sensitive Data	Data Classification and Data Retention policies define Protective and Sensitive data which includes but not limited to Personally Identifiable Information, SSN, Protected Health Information, Protected Financial Information.

Revision History

Initial Author	ITS Governance
Created On	August 13, 2019
Last Modified By	ITS Governance
Last Modified On	March 20, 2020
Revision Number	3
Approver	County Manager's Review Committee

Version	Changed By	Changed On	Notes / Comments
2	Information Technology	March 13, 2013	
3	Information Technology Services	March 20, 2020	

JEFFERSON COUNTY COMMISSION

Information Technology Services Department

Mobile Device Security Rules & Regulations

1.0 Overview

Throughout this document the term policy refers to the strategy, procedures, rules, and regulations defined and encapsulated within each section of this document to achieve the stated information security goals. Mobile devices, such as smartphones and tablet computers, are important tools for Jefferson County Commission ("JCC") employees and the JCC Department of Information Technology Services ("ITS") supports their use to achieve legislative, community, and business goals for the citizens of Jefferson County Alabama. However, mobile devices also represent a significant risk to data security as, if the appropriate security applications and procedures are not applied, they can be a conduit for unauthorized access to the County's data and ITS infrastructure. This can subsequently lead to data leakage and system infection. This policy document addresses this threat by formalizing provisioning and access guidelines to reduce the risk to data security.

2.0 Purpose

The purpose of this policy is to establish a framework for consistent decision-making regarding the provision of essential, business-related mobile devices to JCC staff and employees. Also, this policy serves to protect information assets and to safeguard citizens' and employees' personal and sensitive information.

3.0 Scope

All mobile devices, whether owned by JCC or owned by employees, inclusive of smartphones and tablet computers, that have access to the County's networks, data and/or systems are governed by this mobile device security policy. The scope of this policy does not include laptops managed by ITS (see Laptop Security Policy).

Exemptions: Where there is a business need to be exempted from this policy (too costly, too complex, adversely impacting other business requirements) a risk assessment authorized by security management must be conducted.

Applications used by employees on their own personal devices which store or access corporate data, such as cloud storage applications, are also subject to this policy.

4.0 Policy

4.1 Technical Requirements

a) Devices must use the following Operating Systems: Android 7.0 or later, iOS 10.3.3 or later.

b) Devices must store all user-saved passwords in an encrypted password store.

c) Devices must be configured with a secure password that complies with ITS Password Policy.

d) Only devices managed by ITS will be allowed to connect directly to the internal corporate network.

e) These devices will be subject to the valid compliance rules on security features such as encryption, password, key lock, etc. These policies will be enforced by ITS using Mobile Device Management software.

4.2 User Requirements

a) Users may only load corporate data that is essential to their role onto their mobile device(s).

b) Users must report all lost or stolen devices to ITS immediately.

c) If a user suspects that unauthorized access to the County's data has taken place via a mobile device, they must report the incident in alignment with ITS incident handling process.

d) Devices must not be "jailbroken" or "rooted"* or have any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the user.

e) Users must not load pirated software or illegal content onto their devices.

f) Applications must only be installed from official platform-owner approved sources. Installation of code from untrusted sources is forbidden. If you are unsure if an application is from an approved source contact ITS.

g) Devices must be kept up to date with manufacturer or network provided patches. As a minimum patch should be checked for weekly and applied at least once a month.

h) Devices must not be connected to a PC which does not have up to date and enabled anti-malware protection and which does not comply with the County's Antivirus Policy.

i) Where possible devices must be encrypted in accordance with ITS Encryption Policy.

j) Users must be cautious about the merging of personal and work email accounts on their devices. Users must take particular care to ensure that County data is only sent through the enterprise email system. If a user suspects that data has been sent from a personal email account, either in body text or as an attachment, they must notify ITS immediately.

k) The above requirements will be checked regularly, and should a device be non-compliant that may result in the loss of access to email, a device lock, or in particularly severe cases, a device wipe.

l) The user is responsible for the backup of their own personal data and the County will accept no responsibility for the loss of files due to a non-compliant device being wiped for security reasons.

m) Users must not use County workstations to backup or synchronize device content such as media files, unless such content is required for legitimate business purposes.

4.3 Actions which may result in a full or partial wipe of the device, or other interaction by ITS.

a) A device is jailbroken/rooted

b) A device contains an app known to contain a security vulnerability (if not removed within a given time-frame after informing the user)

c) A device is lost or stolen

d) A user has exceeded the maximum number of failed password attempts

4.4 Use of particular applications which have access to corporate data

a) Cloud storage solutions: ITS supports the use of the following cloud storage solutions:

1) Microsoft One Drive (GCC Tenant)
2) Apple iCloud

b) The use of solutions other than the above will lead to a compliance breach and the loss of access to the corporate network for the user

5 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Any disciplinary action taken by the ITS Department to discipline a user who has violated this policy, will follow Jefferson County Commission's Disciplinary process.

6 Related Policies

Acceptable Use Policy
Laptop Security Policy
Antivirus Policy

7 Policy Owner

Jefferson County Commission

7.0a Policy Administrator

Chief Information Officer, Information Technology Services Department

8 Policy Approval Date

March 20, 2020

9 Policy Effective Date

March 20, 2020

10 Definitions

Term	Definition
Jailbroken	Refers to the process of removing all restrictions imposed on a mobile device.
Rooted	Refers to the process that allows a user to attain root access to a mobile device

Revision History

Initial Author	ITS Governance
Created On	August 13, 2019
Last Modified By	ITS Governance
Last Modified On	March 20, 2020
Revision Number	3
Approver	County Manager's Review Committee

Version	Changed By	Changed On	Notes / Comments
2	Information Technology	March 13, 2013	
3	Information Technology Services	March 20, 2020	

JEFFERSON COUNTY COMMISSION

Information Technology Services Department

Network Access & Authentication Security Rules & Regulations

1.0 Overview

Throughout this document the term policy refers to the strategy, procedures, rules, and regulations defined and encapsulated within each section of this document to achieve the stated information security goals. Consistent standards for network access and authentication are critical to the Jefferson County Commission's information security and are often required by regulations or third-party agreements. Any user accessing the County's computer systems has the ability to affect the security of all users of the network. An appropriate Network Access and Authentication Policy reduces risk of a security incidents by requiring consistent application of authentication and access standards across the network.

2.0 Purpose

The purpose of this policy is to describe what steps must be taken to ensure that users connecting to Jefferson County Commission ("JCC") data network are authenticated in an appropriate manner, in compliance with information technology standards, and are given the least amount of access required to perform their job function. This policy specifies what constitutes appropriate use of network accounts and authentication standards.

3.0 Scope

The scope of this policy includes all users who have access to county-owned or county-provided computers or require access to the data network and/or systems. This policy applies not only to employees, but also to guests, contractors, and anyone requiring access to the county network. Public access to the County's externally-reachable systems, such as its website or public web applications, are specifically excluded from this policy.

4.0 Policy

4.1 Account Setup
During initial account setup, certain checks must be performed in order to ensure the integrity of the process. The following policies apply to account setup:

- Positive ID and coordination with Human Resources is required.
- Users will be granted least amount of network access required to perform his or her job function in accordance with the User Access Management Policy.
- Users will be granted access only if he or she accepts the Acceptable Use Policy.
- Access to the network will be granted in accordance with the Acceptable Use Policy.

4.2 Account Use
Network accounts must be implemented in a standard fashion and utilized consistently across the organization. The following policies apply to account use:

- Accounts must be created using a standard format (i.e., lastnamefirst initial) in accordance with the User Access Management Policy.

- Accounts must be password protected (refer to the Password Policy for more detailed information).

- Accounts must be for individuals only. Account sharing and group accounts are not permitted.

- User accounts must not be given administrator or 'root' access

- Occasionally guests will have a legitimate business need for access to the County's network. When a reasonable need is demonstrated, temporary guest access is allowed. This access, however, must be severely restricted to only those resources that the guest needs at that time, and disabled when the guest's work is completed.

- Individuals requiring access to confidential data must have an individual, distinct account. This account may be subject to additional monitoring or auditing at the discretion of the Chief Information Officer or Department of Information Technology Services ("ITS") executive team, or as required by applicable regulations or third-party agreements.

4.3 Account Termination
When managing network and user accounts, it is important to stay in communication with JCC Human Resources Department so that when an employee is no longer employed, that employee's account can be disabled based on the User Access Management Policy. Human Resources must create a process to notify ITS in the event of a staffing change, which includes employment termination, employment suspension, or a change of job function (promotion, demotion, suspension, etc.).

4.4 Authentication
User machines must be configured to request authentication against the domain at startup. If the domain is not available or authentication for some reason cannot occur, then the machine should not be permitted to access the network. Some machines operating as public information kiosks will not require this authentication, the such machines will have no access to the County's network.

4.5 Use of Passwords
When accessing the network locally, username and password is an acceptable means of authentication. Usernames must be consistent with the requirements set forth in this document, and passwords must conform to the County's Password Policy.

4.6 Remote Network Access
Remote access to the network can be provided for convenience to users but this comes at some risk to security. For that reason, ITS encourages additional scrutiny of users remotely accessing the network. The County's standards dictate that username and password is an acceptable means of authentication as long as appropriate policies are followed. Remote access must adhere to the Remote Access Policy.

4.7 Screensaver
Screensaver offer an easy way to strengthen security by removing the opportunity for a malicious user, curious employee, or intruder to access network resources through an idle computer. For this reason, screensavers are required to be activated after 15 minutes of inactivity.

4.8 Minimum Configuration for Access
Any system connecting to the network can have a serious impact on the security of the entire network. A vulnerability, virus, or other malware may be inadvertently introduced in this manner. For this reason, antivirus software should be updated in accordance with the Antivirus Policy.

4.9 Encryption
Industry best practices state that username and password combinations must never be sent as plain text. If this information were intercepted, it could result in a serious security incident. Therefore, authentication credentials must be encrypted in accordance with the Encryption Policy during transmission across any network, whether the transmission occurs internal to the county's network or across a public network such as the Internet.

4.10 Failed Logons
Repeated logon failures can indicate an attempt to 'crack' a password and surreptitiously access a network account. In order to guard against password-guessing and brute-force attempts, ITS must lock a user's account after 5 unsuccessful logins. This can be implemented as a time-based lockout or require a manual reset, at the discretion of the Chief Information Officer. In order to protect against account guessing, when logon failures occur the error message transmitted to the user must not indicate specifically whether the account name or password were incorrect. The error can be as simple as "the username and/or password you supplied were incorrect."

4.11 Non-Business Hours
While some security can be gained by removing account access capabilities during non-business hours, the County does not mandate time-of-day lockouts. This may be either to encourage working remotely, or because the County's business requires all-hours access.

4.12 Applicability of Other Policies
This document is part of ITS cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Any disciplinary action taken by the ITS Department to discipline a user who has violated this policy, will follow Jefferson County Commission's Disciplinary process.

6.0 Related Policies

User Access Management Policy
Acceptable Use Policy
Password Policy
Antivirus Policy
Encryption Policy

7.0 Policy Owner

Jefferson County Commission

7.0a Policy Administrator

Chief Information Officer, Information Technology Services Department

8.0 Policy Approval Date

March 20, 2020

9.0 Policy Effective Date

March 20, 2020

10.0 Definitions

Term Definition

Revision History

Initial Author	ITS Governance
Created On	August 13, 2019
Last Modified By	ITS Governance
Last Modified On	March 20, 2020
Revision Number	3
Approver	County Manager's Review Committee

Version	Changed By	Changed On	Notes / Comments
2	Information Technology	March 13, 2013	
3	Information Technology Services	March 20, 2020	

JEFFERSON COUNTY COMMISSION

Information Technology Services Department

Network Security Rules & Regulations

1.0 Overview

Throughout this document the term policy refers to the strategy, procedures, rules, and regulations defined and encapsulated within each section of this document to achieve the stated information security goals. Jefferson County Commission ("JCC") resources, such as Internet/Intranet-related systems, are to be used for JCC business purposes in serving the interests of the citizens of Jefferson County Alabama. The participation and support of every employee and affiliate who deals with information and/or information systems is necessary to achieve effective security.

2.0 Purpose

The purpose of this policy is to establish administrative direction, procedural requirements, and technical guidance to ensure the appropriate protection of JCC information handled by its enterprise networks. Inappropriate use exposes JCC to risks including virus attacks, compromise of network systems and services, and legal issues.

3.0 Scope

This policy applies to all JCC enterprise networks. The policy also applies to all computer and data communication systems owned by or administered by Jefferson County Commission Information Technology Services Department (ITS).

4.0 Policy

The data network is a shared resource used by the entire County and its affiliates in support of the business processes and departments missions. JCC Departments must protect the network by securing computers and network devices in order to secure access. In addition, they must certify that the devices connecting to the business unit's network are in compliance with the policies and procedures as established by the ITS Department. This policy is designed to help protect JCC central and distributed data networks and computing environment from accidental, or intentional damage, and from alteration or theft of data while preserving appropriate access and use.

The following rules define the ITS Department policy regarding access to the County's network:

4.1 Only authorized people can gain access to JCC data networks. Positive identification is required for system usage. All users must have their identities positively identified with user-IDs and secure passwords--or by other means that provide equal or greater security--prior to being permitted to use Jefferson County Commission -owned computers.

4.2 User-IDs must each uniquely identify a single user. Each computer user-ID must uniquely identify only one user, so as to ensure individual accountability in system logs. Shared or group user-IDs are not permitted.

4.3 Use of service accounts for local log-ins by any individual is prohibited. This rule is designed to prevent unauthorized changes to production data by accounts that allow groups of users to employ the same password. In cases where users require account privileges inherent in service accounts, the user's manager must obtain approval from ITS Department. Those privileges may be assigned to individual users on as-needed basis and must be revoked when they are no longer necessary.

4.4 Access controls are required for remote systems connecting to production systems. All computers that have remote real-time dialogs with ITS Department production systems must run an access control package approved by ITS.

4.5 Multiple simultaneous remote external network connections are prohibited. Unless special permission has been granted by the Jefferson County Commission Chief Information Officer, computer systems must not allow any user to conduct multiple simultaneous remote network connections.

4.6 All log-in banners must include security notice. Every log-in screen for multi- user computers must include a special notice. This notice must state: (1) the system may only be accessed by authorized users, (2) users who log-in represent that they are authorized to do so, (3) unauthorized system usage or abuse is subject to penalties, and (4) system usage will be monitored and logged.

4.7 Security notice in log-in banner must not disclose system information. All log-in banners on network-connected JCC computer systems must simply ask the user to log-in, providing terse prompts only where essential. Identifying information about the organization, operating system, system configuration, or other internal matters must not be provided until a user's identity has been successfully authenticated.

4.8 Users must log off before leaving sensitive systems unattended. If the computer system to which users are connected or which they are currently using contains sensitive information, and especially if they have special access rights, such as domain admin or system administrator privileges, users must not leave their computer, workstation, or terminal unattended without first logging-out, locking the workstation, or invoking a password-protected screen saver.

4.9 Employees, and ITS staff must:

a. Follow policies and procedures, as established by ITS, to validate firewall activation, operating system installation, application software security patches and virus protection updates for all devices in the unit's areas of physical or administrative control that are to be, or are configured to utilize network resources that are controlled and managed by Information Technology Services Department.

b. Follow policies and procedures, as established by ITS, for using automated tools to test devices connected to the business unit's local wired or wireless data network for compliance. Noncompliant devices are to be disconnected, disabled or quarantined until the device is brought into compliance. When devices are not compliant, operating units, or individuals and their information technology staff must employ compensating controls. Units must document compensating controls and/or any exceptions. These must be reviewed, tested, and approved by Information Security.

The operating business unit or individual must retain the approved documentation for audits as long as the device is in operation. Any connection to the Internet, or to a national or regional network from a private network operated by an administrative, or support unit, must be made via JCC data

network resources. The Chief Information Officer must approve any exceptions to this requirement.

4.10 All network access attempts (success or failure) must be logged and retained for auditing.

4.11 Servers
JCC embraces an open information technology environment to encourage the use of technology in pursuit of the County's missions in supporting the citizens of Jefferson County Alabama. However, within this open environment, the County must also preserve and safeguard its electronic information resources and comply with applicable laws and regulations, while facilitating activities the support the County's missions. In a highly distributed technological environment, operation and management of electronic information resources is broadly distributed. This policy applies to all servers that ITS is responsible to manage. This explicitly includes any system for which ITS has an obligation to administer. This also includes all server systems setup for internal use by JCC regardless of whether ITS retains administrative obligation or not.

ITS is responsible for system administration and must manage all internal servers. Approved server configuration guides must be established and maintained by the ITS Infrastructure Division, based on business needs and approved by ITS. ITS Infrastructure Division should monitor configuration compliance and implement an exception policy tailored for each exception.

4.11.1 Servers must be registered within ITS Asset Management System. At a minimum, the following information is required to positively identify server characteristics:

- Server contact(s) and location, and a backup contact
- Hardware and Operating System/Version
- Main functions and applications, if applicable
- Information in the Asset Management System must be kept up-to-date.

4.11.2 Each device must meet the following minimum standards prior to, and after connecting to the data network or support infrastructure:

- The device must be guarded by an up-to-date and active firewall set to protect it from unauthorized network traffic.
- Current operating system and application software with current security patches must be installed.
- The device must be protected against malicious or undesired software such as viruses, spyware, or adware.
- Access to the device must require appropriate authentication controls such as account identifiers and robust passwords.
- The device must be certified and registered by ITS as equipment that has met all security criteria, prior to connecting to the network.

4.11.3 SERVER GENERAL CONFIGURATION GUIDELINES
The following items serve as provisioning configuration guidelines for the servers that are managed by ITS staff:

- Operating System configuration should be in accordance with ITS - approved guidelines.
- Services and applications that will not be used must be disabled where practical.

• Access to services should be logged and/or protected through access-control methods.
• The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
• Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication is available.
• Do not use root account when a non-privileged account can perform the task.
• If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH).
• Servers should be physically located in an access-controlled environment.
• Servers are specifically prohibited from being operated in uncontrolled cubicle areas.

4.11.4 Internal network addresses must not be publicly released.
The internal system addresses, configurations, and related system design information systems and users outside the ITS internal network cannot access this information.

4.11.5 All Internet Web servers must be firewall protected.
All connections between JCC's internal networks and the Internet (or any other publicly-accessible computer network) must be protected by a router, firewall, or related access controls approved by ITS.

4.11.6 Public facing servers on Internet must be placed on separate subnets.
Public Internet servers must be placed on subnets separate from internal ITS networks. Routers or firewalls must be employed to restrict traffic from the public servers to internal networks.

4.11.7 All sever configuration changes/virtual provisioning/deprovisioning must be approved via the change management process. See Change Management Policy.

4.12. MALWARE PROTECTION
ITS is entrusted with the responsibility to provide professional management of the County's servers as outlined in this policy. Inherent in this responsibility is an obligation to provide appropriate protection against malware threats, such as viruses and spyware applications. Effective implementation of this policy will limit the exposure and effect of common malware threats to the systems they cover.

This policy applies to all servers/desktops/laptops/tablets that ITS is responsible for managing. This explicitly includes any system for which ITS has an obligation to administer.

4.12.1. ANTI-VIRUS
All servers MUST have an anti-virus application installed that offers real-time scanning protection to files and applications running on the target system.

4.12.2 MAIL SERVER SPAM/MALWARE FILTERS
If the target system is a mail server it MUST have spam/malware anti-virus scanning/filters that scans all mail destined to and from the electronic mail

appliance. This also applies to electronic mail appliance(s) hosted in cloud platform such as Microsoft, Google, and AT&T.

4.12.3 Enforcement:
The responsibility for implementing this policy belongs to ITS. Responsibility for ensuring that new and existing systems remain in compliance with this policy resides with the Information Security Officer/and or Security Team. Any employee, guest, or contractors found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

4.13. ROUTER/SWITCH CONFIGURATIONS
This section describes a required minimal security configuration for all routers and switches connecting to the production network at all JCC facilities. Every router and switch must meet the following configuration standards:

4.13.1. No local user accounts are configured on the router. Routers and switches should use Terminal Access Controller Access Control System (TACACS+) for all user authentication or some form of authentication that allows for individual user accounts for each network administrator and encrypts the entire TCP payload including username and password.

4.13.2. The enable password on the router or switch must be kept in a secure encrypted form. The router or switch must have the enable password set to the current production router/switch password from the device's support organization.

4.13.3. The following services or features must be disabled:
- a. IP directed broadcasts
- b. Incoming packets at the router/switch sourced with invalid addresses such as RFC1918 addresses
- c. TCP small services
- d. UDP small services
- e. All source routing and switching
- f. All web services running on router
- g. Discovery protocols on Internet connected interfaces
- h. Telnet, FTP, and HTTP services
- i. Auto-configuration

4.13.4. The following services should be disabled unless a business justification is provided:
- a. Discovery protocols
- b. Dynamic trunking
- c. Scripting environments, such as the TCL shell

4.13.5. The following services must be configured:
- a. Password-encryption
- b. NTP configured to a corporate standard source

4.13.6. All routing updates shall be done using secure routing updates.

4.13.7. Use corporate standardized SNMP community strings. Default strings, such as public or private must be removed. SNMP must be configured to use the most secure version of the protocol allowed for by the combination of the device and management systems.

4.13.8. Access control lists must be used to limit the source and type of traffic that can terminate on the device itself.

4.13.9. Access control lists for transiting the device are to be added as business needs arise.

4.13.10. The router must be included in the corporate enterprise management system with a designated point of contact.

4.13.11. Each router must have the following statement presented for all forms of login whether remote or local:

"UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement. There is no right to privacy on this device. Use of this system shall constitute consent to monitoring."

4.13.12. Telnet may never be used across any network to manage a router, unless there is a secure tunnel protecting the entire communication path. SSH version 2 is the preferred management protocol.

4.13.13. Dynamic routing protocols must use authentication in routing updates sent to neighbors. Password hashing for the authentication string must be enabled when supported.

4.13.14. The corporate router configuration standard will define the category of sensitive routing and switching devices, and require additional services or configuration on sensitive devices including:

a. IP access list accounting
b. Device logging
c. Incoming packets at the router sourced with invalid addresses, such as RFC1918 addresses, or those that could be used to spoof network traffic shall be dropped.
d. Router console and modem access must be restricted by additional security controls

4.13.15 All configuration changes must be approved via the change management process. See Change Management Policy.

4.14. FIREWALL

The firewall policy dictates how the firewall should handle application traffic such as web, email, or telnet. Generally, firewalls should block all inbound and outbound traffic that has not been expressly permitted by the firewall policy—traffic that is not needed by the organization. This practice, known as deny by default, decreases the risk of attack and can also reduce the volume of traffic carried on the organization's networks. Because of the dynamic nature of hosts, networks, protocols, and applications, deny by default is a more secure approach than permitting all traffic that is not explicitly forbidden.

This section provides details on what types of traffic should be blocked. Section 4.14.1 discusses policies for packet filtering and stateful inspection based on IP addresses and other IP characteristics. Section 4.14.2 covers policies relating to application-specific traffic. Section 4.14.3 covers access based on user identity, and Section 4.14.4 describes policies triggered by network activity.

4.14.1 POLICIES BASED ON IP ADDRESSES AND PROTOCOLS

Firewall policies should only allow necessary IP protocols through. Examples of commonly used IP protocols, with their IP protocol numbers,17 are ICMP (1), TCP (6), and UDP (17). Other IP protocols, such as IPsec components Encapsulating Security Payload (ESP) (50) and Authentication Header (AH) (51) and routing protocols, may also need to pass through firewalls. These necessary protocols should be restricted whenever possible to the specific hosts and networks within the organization with a need to use them. By permitting only necessary protocols, all unnecessary IP protocols are denied by default.

Some IP protocols are rarely passed between an outside network and an organization's LAN, and therefore can simply be blocked in both directions at the firewall. For example, IGMP is a protocol used to control multicast networks, but multicast is rarely used, and when it is, it is often not used across the Internet. Therefore, blocking all IGMP traffic in both directions is feasible if multicast is not used.

4.14.1.1 IP ADDRESSES AND OTHER IP CHARACTERISTICS

Firewall policies should only permit appropriate source and destination IP addresses to be used. Specific recommendations for IP addresses include:

- Traffic with invalid source or destination addresses should always be blocked, regardless of the firewall location. Examples of relatively common invalid IPv4 addresses are 127.0.0.0 to 127.255.255.255 (also known as the localhost addresses) and 0.0.0.0 (interpreted by some operating systems as a localhost or a broadcast address). These have no legitimate use on a network. Also, traffic using link-local addresses (169.254.0.0 to 169.254.255.255) should be blocked.

- Traffic with an invalid source address for incoming traffic or destination address for outgoing traffic (an invalid "external" address) should be blocked at the network perimeter. This traffic is often caused by malware, spoofing, denial of service attacks, or misconfigured equipment. The most common type of invalid external addresses is an IPv4 address within the ranges in RFC 1918, Address Allocation for Private Internets, that are reserved for private networks. These ranges are 10.0.0.0 to 10.255.255.255 (10.0.0.0/8 in Classless Inter-Domain Routing [CIDR] notation), 172.16.0.0 to 172.31.255.255 (172.16.0.0/12), and 192.168.0.0 to 192.168.255.255 (192.168.0.0/16).

- Traffic with a private destination address for incoming traffic or source address for outgoing traffic (an "internal" address) should be blocked at the network perimeter. Perimeter devices can perform address translation services to permit internal hosts with private addresses to communicate through the perimeter, but private addresses should not be passed through the network perimeter.

- Outbound traffic with invalid source addresses should be blocked (this is often called egress filtering). Systems that have been compromised by attackers can be used to attack other systems on the Internet; using invalid source addresses makes these

kinds of attacks more difficult to stop. Blocking this type of traffic at an organization's firewall helps reduce the effectiveness of these attacks.

- Incoming traffic with a destination address of the firewall itself should be blocked unless the firewall is offering services for incoming traffic that require direct connections—for example, if the firewall is acting as an application proxy.

- Traffic containing IP source routing information, which allows a system to specify the routes that packets will employ while traveling from source to destination. This could potentially permit an attacker to construct a packet that bypasses network security controls. IP source routing is rarely used on modern networks, and valid applications are even less common on the Internet.

- Traffic from outside the network containing broadcast addresses that is directed to inside the network. Any system that responds to the directed broadcast will then send its response to the system specified by the source, rather than to the source system itself. These packets can be used to create huge "storms" of network traffic for denial of service attacks. Regular broadcast addresses, as well as addresses used for multicast IP, may or may not be appropriate for blocking at an organization's firewall. Multicast and broadcast networking is seldom used in normal networking environments, but when it is used both inside and outside of the organization, it should be allowed through firewalls.

Firewalls at the network perimeter should block all incoming traffic to networks and hosts that should not be accessible from external networks. These firewalls should also block all outgoing traffic from the organization's networks and hosts that should not be permitted to access external networks. Deciding which addresses should be blocked is often one of the most time-consuming aspects of developing firewall IP policies. It is also one of the most error-prone, because the IP address associated with an undesired entity often changes over time.

4.14.1.2 IPv6

IPv6 is a new version of IP that is increasingly being deployed. Although IPv6's internal format and address length differ from those of IPv4, many other features remain the same—and some of these are relevant to firewalls. For the features that are the same between IPv4 and IPv6, firewalls should work the same. For example, blocking all inbound and outbound traffic that has not been expressly permitted by the firewall policy should be done regardless of whether or not the traffic has an IPv4 or IPv6 address. As of this writing, some firewalls cannot handle IPv6 traffic at all; others are able to handle it but have limited abilities to filter IPv6 traffic; and still others can filter IPv6 traffic to approximately the same
extent as IPv4 traffic. Every organization, whether or not it allows IPv6 traffic to enter its internal network, needs a firewall that is capable of filtering this traffic. These firewalls should have the following capabilities:

- The firewall should be able to use IPv6 addresses in all filtering rules that use IPv4 addresses.

- The administrative interface should allow administrators to clone IPv4 rules to IPv6 addresses to make administration easier.

- The firewall needs to be able to filter ICMPv6, as specified in RFC 4890, Recommendations for Filtering ICMPv6 Messages in Firewalls.

- The firewall should be able to block IPv6-related protocols such as 6-to-4 and 4-to-6 tunneling, Teredo, and Intra-site Automatic Tunnel Addressing Protocol (ISATAP) if they are not required.

- Many sites tunnel IPv6 packets in IPv4 packets. This is particularly common for sites experimenting with IPv6, because it is currently easier to obtain IPv6 transit from a tunnel broker through a v6-to-v4 tunnel than to get native IPv6 transit from an Internet service provider (ISP). A number of ways exist to do this, and standards for tunneling are still evolving. If the firewall is able to inspect the contents of IPv4 packets, it needs to know how to inspect traffic for any tunneling method used by the organization. A corollary to this is that if an organization is using a firewall to prohibit IPv6 coming into or going out of its network, that firewall needs to recognize and block all forms of v6-to-v4 tunneling.

Note that the above list is short and not all the rules are security-specific. Because IPv6 deployment is still in its early stages, there is not yet widespread agreement in the IPv6 operations community about what an IPv6 firewall should do that is different from IPv4 firewalls.

For firewalls that permit IPv6 use, traffic with invalid source or destination IPv6 addresses should always be blocked—this is similar to blocking traffic with invalid IPv4 addresses. Since much more effort has been spent on making lists of invalid IPv4 addresses than on IPv6 addresses, finding lists of invalid IPv6 addresses can be difficult. Also, IPv6 allows network administrators to allocate addresses in their assigned ranges in different ways. This means that in a particular address range assigned to an organization, there can literally be trillions of invalid IPv6 addresses and only a few that are valid. By necessity, listing which IPv6 addresses are invalid will have to be less fine-grained than listing invalid IPv4 addresses, and the firewall rules that use these lists will be less effective than their IPv4 counterparts.

Organizations that do not yet use IPv6 should block all native and tunneled IPv6 traffic at their firewalls. Note that such blocking limits testing and evaluation of IPv6 and IPv6 tunneling technologies for future deployment. To permit such use, the firewall administrator can selectively unblock IPv6 or the specific tunneling technologies of interest for use by the authorized testers.

4.14.1.3 TCP AND UDP

Application protocols can use TCP, UDP, or both, depending on the design of the protocol. An application server typically listens on one or more fixed TCP or UDP ports. Some applications use a single port, but many applications use multiple ports. For example, although SMTP uses TCP port 25 for sending mail, it uses TCP port 587 for mail submission. Similarly, FTP uses at least two ports, one of which can be unpredictable, and while most web servers use only TCP port 80, it is common to have web sites that also use additional ports such as TCP port 8080. Some applications use both TCP and UDP; for example, DNS lookups can occur on UDP port 53 or TCP port 53. Application clients typically use any of a wide range of ports.

As with other aspects of firewall rulesets, deny by default policies should be used for incoming TCP and UDP traffic. Less stringent policies are generally used for outgoing TCP and UDP traffic because most organizations permit their users to access a wide range of external applications located on millions of external hosts. In addition to allowing and blocking UDP and TCP traffic, many firewalls are also able to report or block malformed UDP and TCP traffic directed towards the firewall or to hosts protected by the firewall. This traffic is frequently used to scan for hosts, and may also be used in certain types of attacks. The firewall can help block such activity—or at least report when such activity is happening.

4.14.1.4 ICMP

Attackers can use various ICMP types and codes to perform reconnaissance or manipulate the flow of network traffic. However, ICMP is needed for many useful things, such as getting reasonable performance across the Internet. Some firewall policies block all ICMP traffic, but this often leads to problems with diagnostics and performance. Other common policies allow all outgoing ICMP traffic, but limit incoming ICMP to those types and codes needed for Path Maximum Transmission Unit (PMTU) discovery (ICMP code 3) and destination reachability.

To prevent malicious activity, firewalls at the network perimeter should deny all incoming and outgoing ICMP traffic except for those types and codes specifically permitted by the organization. For ICMP in IPv4, ICMP type 3 messages should not be filtered because they are used for important network diagnostics. The ping command (ICMP code 8) is an important network diagnostic, but incoming pings are often blocked by firewall policies to prevent attackers from learning more about the internal topology of the organization's network. For ICMP in IPv6, many types of messages must be allowed in specific circumstances to enable various IPv6 features. See RFC 4890, Recommendations for Filtering ICMPv6 Messages in Firewalls, for detailed information on selecting which ICMPv6 types to allow or disallow for a particular firewall type.

ICMP is often used by low-level networking protocols to increase the speed and reliability of networking. Therefore, ICMP within an organization's network generally should not be blocked by firewalls that are not at the perimeter of the network, unless security needs outweigh network operational needs. Similarly, if an organization has more than one network, ICMP that comes from or goes to other networks within the organization should not be blocked.

4.14.1.5 IPsec PROTOCOLS

An organization needs to have a policy whether or not to allow IPsec VPNs that start or end inside its network perimeter. The ESP and AH protocols are used for IPsec VPNs, and a firewall that blocks these protocols will not allow IPsec VPNs to pass. While blocking ESP can hinder the use of encryption to protect sensitive data, it can also force users who would normally encrypt their data with ESP to allow it to be inspected—for example, by a stateful inspection firewall or an application-proxy gateway.

Organizations that allow IPsec VPNs should block ESP and AH except to and from specific addresses on the internal network—those addresses belong to IPsec gateways that are allowed to be VPN endpoints. Enforcing this policy will require people inside the organization to obtain the appropriate policy approval to open ESP and/or AH access to their IPsec routers. This will also reduce the amount of encrypted traffic coming from inside the network that cannot be examined by network security controls.

4.14.2 POLICIES BASED ON APPLICATIONS

Most early firewall work involved simply blocking unwanted or suspicious traffic at the network boundary. Inbound application firewalls or application proxies take a different approach—they let traffic destined for a particular server into the network, but capture that traffic in a server that processes it like a port-based firewall. The application-based approach provides an additional layer of security for incoming traffic by validating some of the traffic before it reaches the desired server. The theory is that the inbound application firewall's or proxy's additional security layer can protect the server better than the server can protect itself—and can also remove malicious traffic before it reaches the server to help reduce server load. In some cases, an application firewall or proxy can remove traffic that the server might not be able to remove on its own because it has greater filtering capabilities. An application firewall or proxy also prevents the server from having direct access to the outside network. If possible, inbound application firewalls and proxies should be used in front of any server that does not have sufficient security features to protect it from application-specific attacks. The main considerations when deciding whether or not to use an inbound application firewall or proxy are:

- Is a suitable application firewall available? Or, if appropriate, is a suitable application proxy available?
- Is the server already sufficiently protected by existing firewalls?
- Can the main server remove malicious content as effectively as the application firewall or proxy?
- Is the latency caused by an application proxy acceptable for the application?
- How easy it is to update the filtering rules on the main server and the application firewall or proxy to handle newly developed threats?

Application proxies can introduce problems if they are not highly capable. Unless an application proxy is significantly more robust than the server and easy to keep updated, it is usually best to stay with the application server alone. Application firewalls can also introduce problems if they are not fast enough to handle the traffic destined for the server. However, it is also important to consider the server's resources—if the server does not have sufficient resources to withstand attacks, the application firewall or proxy could be used as a shield.

When an inbound application firewall or proxy is behind a perimeter firewall or in the firewall's DMZ, the perimeter firewall should be blocking based on IP addresses, as described earlier in this section, to reduce the load on the application firewall or proxy. Doing this puts more of the address-specific policy in a single place—the main firewall—and reduces the amount of traffic seen by the application firewall or proxy, freeing more power to filter content. Of course, if the perimeter firewall is also the application firewall and an internal application proxy is not used, no such rules are needed. Outbound application proxies are useful for detecting systems that are making inappropriate or dangerous connections from inside the protected network. By far the most common type of outbound proxy is for HTTP. Outbound HTTP proxies allow an organization to filter dangerous content before it reaches the requesting PC. They also help an organization better understand and log web traffic from its users, and to detect activity that is being tunneled over HTTP. When an HTTP proxy filters content, it can alert the web user that the site being visited sent the filtered content. The most prominent non-security benefit of HTTP proxies is caching web pages for increased speed and decreased bandwidth use. Most organizations should employ HTTP proxies.

4.14.3 POLICIES BASED ON USER IDENTITY

Traditional packet filtering does not see the identities of the users who are communicating in the traffic traversing the firewall, so firewall technologies without more advanced capabilities cannot have policies that allow or deny access based on those identities. However, many other firewall technologies can see these identities and therefore enact policies based on user authentication. One of the most common ways to enforce user identity policy at a firewall is by using a VPN. Both IPsec VPNs and SSL VPNs have many ways to authenticate users, such as with secrets that are provisioned on a user-by-user basis, with multi-factor authentication (e.g., time-based cryptographic tokens protected with PINs), or with digital certificates controlled by each user. NAC has also become a popular method for firewalls to allow or deny users access to particular network resources. In addition, application firewalls and proxies can allow or deny access to users based on the user authentication within the applications themselves. Firewalls that enforce policies based on user identity should be able to reflect these policies in their logs. That is, it is probably not useful to only log the IP address from which a particular user connected if the user was allowed in by a user-specific policy; it is also important to log the user's identity as well.

4.14.4 POLICIES BASED ON NETWORK ACTIVITY

Many firewalls allow the administrator to block established connections after a certain period of inactivity. For example, if a user on the outside of a firewall has logged into a file server but has not made any requests during the past 15 minutes, the policy might be to block any further traffic on that connection. Time-based policies are useful in thwarting attacks caused by a logged-in user walking away from a computer and someone else sitting down and using the established connections (and therefore the logged-in user's credentials). However, these policies can also be bothersome for users who make connections but do not use them frequently. For instance, a user might connect to a file server to read a file and then spend a long time editing the file. If the user does not save the file back to the file server before the firewall-mandated timeout, the timeout could cause the changes to the file to be lost. Some organizations have mandates about when firewalls should block connections that are considered to be inactive, when applications should disconnect sessions if there is no activity, etc. A firewall used by such an organization should be able to set policies that

match the mandates while being specific enough to match the security objective of the mandates.

4.14.5 All configuration changes must be approved via the change management process. See Change Management Policy.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Any disciplinary action taken by the ITS Department to discipline a user who has violated this policy, will follow Jefferson County Commission's Disciplinary process.

6.0 Related Policies, Processes, and Standards

Change Management Policy

7.0 Policy Owner

Jefferson County Commission

7.0a Policy Administrator

Chief Information Officer, Information Technology Services Department

8.0 Policy Approval Date

March 20, 2020

9.0 Policy Effective Date

March 20, 2020

10.0 Definitions

Term **Definition**

Revision History

Initial Author	ITS Governance
Created On	August 13, 2019
Last Modified By	ITS Governance
Last Modified On	March 20, 2020
Revision Number	3
Approver	County Manager's Review Committee

Version	Changed By	Changed On	Notes / Comments
2	Information Technology	March 13, 2013	

3	Information Technology Services	March 20, 2020	

JEFFERSON COUNTY COMMISSION

Information Technology Services Department

Password Security Rules & Regulations

1.0 Overview

Throughout this document the term policy refers to the strategy, procedures, rules, and regulations defined and encapsulated within each section of this document to achieve the stated information security goals. Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Jefferson County Commission ("JCC") entire telecommunication's network. As such, all JCC employees (including contractors and vendors with access to JCC systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.0 Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change. Additionally, this policy ensures JCC's compliance with legal and regulatory standards such as the Health Insurance Portability and Accountability Act (HIPAA).

3.0 Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any JCC facility, has access to JCC's network, or stores any non-public JCC information.

4.1 Policy

4.2 General

- **4.2.1** All system-level passwords (e.g., root, sudo, local, enterprise, domain, database and application administration accounts, etc.) must be changed on at least a quarterly basis.
- **4.2.2** All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least quarterly.
- **4.2.3** User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
- **4.2.4** Passwords must not be inserted into email messages or other forms of electronic communication.
- **4.2.5** All user-level and system-level passwords must conform to the guidelines described below.

5.1 Guidelines

5.2 General Password Construction Guidelines

Passwords are used for various purposes. Some of the more common uses include user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords. All user-level and system-level passwords must conform to the Password Construction complexity requirements outlined in this policy. Passwords must be changed regularly, as outlined in this policy, at the regularly scheduled time interval or sooner if there is suspicion of a compromise.

Strong passwords have the following characteristics:

5.2.1 Contain both upper- and lower-case characters (e.g., a-z, A-Z)
5.2.2 Have digits and punctuation characters as well as letters e.g., 0-9,!@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
5.2.3 Are at least 8 alphanumeric characters long and is a passphrase (Ohmy1stubbedmyt0e)
5.2.4 Are not words in any language, slang, dialect, jargon, etc.
5.2.5 Are not commonly used words such as:
5.2.6 names of family, pets, friends, co-workers, fantasy characters, etc.,
5.2.7 computer terms and names, commands, sites, companies, hardware, software,
5.2.8 contains the name "Jefferson County" or "Jefferson" or "County" or any derivation,
5.2.9 birthdays and other personal information such as address and phone numbers,
5.2.10 word or number patterns like aaabbb, qwerty, zyxwvuts, 123321 etc.,
5.2.11 any of the above spelled backwards or preceded or followed by a digit (e.g., secret1, 1secret)
5.2.12 Are not based on personal information, names of family, etc.
5.2.13 Try to create passwords that can be easily remembered. One way to do this is creating a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way to Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

5.3 Password Protection Standards

Do not use the same password for JCC accounts as for other non-JCC access (e.g., personal accounts, option trading, benefits, etc.). Where possible, don't use the same password for various JCC access needs. For example, select one password for personnel systems and a separate password for IT systems. Also, select a separate password to be used for a Windows account and a UNIX account.

Do not share Jefferson County passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as "**confidential"** Jefferson County information.

Here is a list of what users should not do:

5.3.1 Don't reveal a password over the phone to ANYONE
5.3.2 Don't reveal a password in an unencrypted email or voice or text message.
5.3.3 Don't reveal a password to the manager, higher management, IT/Information Security Officer and/or Information Security Team, staff or colleagues.
5.3.4 Don't talk about a password in front of others.
5.3.5 Don't hint at the format of a password. (e.g., "my family name")
5.3.6 Don't reveal a password on questionnaires or security forms.
5.3.7 Don't share a password with family members or friends or acquaintances
5.3.8 Don't reveal a password to co-workers while on vacation.
5.3.9 If someone demands a password, refer them to this document or have them call the Department of Information Technology ("ITS").
5.3.10 Do not use the "Remember Password" feature of applications.
5.3.11 Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.
5.3.12 Change passwords at least once every 90 days.
5.3.13 passwords must not be same as usernames.

5.3.14 passwords must be changed immediately upon issuance for the first use. Initial passwords must be securely transmitted to the individual, either via the individual's supervisor or Human Resources at New Hire Orientation.

5.3.15 Individuals must never leave themselves logged into an application or system where someone else can knowingly or unknowingly use their account.

5.3.16 In the event that a password needs to be issued to a remote user or service provider, the password must never be sent without the use of proper safeguards (e.g., do not send passwords through email without encryption).

5.4 Password Storage

5.4.1 Do not use the "Remember Password" feature of applications (e.g., IE, Chrome, Outlook, Firefox).

5.4.2 Passwords must never be written down and left in a location easily accessible or visible to others.

5.4.3 Do not store passwords in a file on any computer system (including Palm Pilots, Blackberry's, iPhones, iPads, or similar devices) without encryption.

5.4.4 Password cracking or guessing may be performed on a periodic or random basis by the Information Security group or its delegates to test that password policies are being followed. If a password is guessed or cracked during one of these scans, the user will be required to change it.

5.4.5 ITS approved Privileged Account Management (PAM) solutions must be considered for storing privileged credentials for vaulting in encrypted manner.

5.5 Reporting a Compromise of credentials

5.5.1 In the event a breach or compromise is suspected, the incident must be reported to ITS Information Security Officer and/or ITS Information Security Team immediately and change all passwords.

Note: Filing or reporting a security incident can be done without fear or concern for retaliation.

5.6 Application Development Standards

Application developers must ensure their programs, applications, microservices, scripts, tools and databases contain the following security precautions. Applications:

5.6.1 Should support authentication of individual users, not groups.

5.6.2 Should not store passwords in clear text or in any easily reversible form.

5.6.3 Should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

5.6.4 should support TACACS+, RADIUS and/or X.509 with LDAP security retrieval, wherever possible

5.6.5 Passwords must be prohibited from being displayed when entered.

5.6.6 Passwords must never be stored in clear, readable format (encryption must always be used).

5.6.7 Passwords must never be stored as part of a login script, program, or automated process.

5.6.8 Systems storing or providing access to confidential data or remote access to the internal network should be secured with multifactor authentication.

5.6.9 Encrypted password hashes must never be accessible to unauthorized individuals.

5.6.10 Where possible, salted hashes should be used for password encryption. Exceptions should be filed and reviewed on a regular basis.

5.6.11 Where any of the above items are not supported, appropriate authorizations and access control methods must be implemented to ensure only a limited number of authorized individuals have access to readable passwords.

5.6.12 Implementation of/or activation multi-factor authentication/ token-based authentication or one-time password systems must be approved by Information Security Officer and/or Information Security Team.

5.6.13 The use of token-based authentication or one-time passwords (e.g., SecurID, Authenex) is required when supported by the platform.

5.6.14 When one-time passwords are in use, the local device password does not require password rotation on the ninety (90) day schedule dictated in the Access Control Policy. Reliance on local fixed passwords must be avoided, if possible.

5.7 Use of Passwords and Passphrases for Remote Access Users

Access to JCC's network via remote access is to be controlled Access to JCC data network via the methods outlined in the Remote Access Policy and a multi-factor authentication tool or a public/private key system with a strong passphrase.

"Multi-Factor authentication" is a security process in which the user provides two means of identification. One identification is typically a physical token such as a card and the other identification is typically something memorized such as a PIN or password. These two identification factors are sometimes referred to as something you have and something you know.

- A simple username/password combination will not be acceptable as strong authentication.
- Server modem "dial back" to a pre-determined and authorized phone number in combination with a username and password is acceptable for IT administrative staff that must perform remote administration

Examples of authentication are:

- Something the user has (e.g., ID card, security token, software token, or a cell phone for SMS messaging)
- A physical security token that contains a tamper resistance authentication code or responds to an authentication
- challenge and requires the user to input a PIN or password.
- A digital certificate or logical access token that is pre-installed on a system and requires a PIN or password. All
- logical access tokens must be encrypted.
- Something the user knows (e.g., a password, pass phrase, or personal identification number (PIN))
- Something the user is or does (e.g., fingerprint or retinal pattern, signature or voice recognition, unique bio-electric signals,
- or another biometric identifier)
- Biometric authentication systems may be used in combination with these systems to replace the requirement for
- a PIN or password.

5.8 Passphrases

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

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

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. Pass phrases should be at least 15 to 25 characters in length. An example of a good passphrase:

"The*?#>*@TrafficOnI65NBWas*&#!#ThisMorning"

pizzawithcrispyspaniels mangledpersimmontherapy
Pizzaw/6krispySpaniels! mangl3dPersimmonTh3rapy?

Note: Do not adopt any of the sample passphrases shown above. All of the rules above that apply to passwords also apply to passphrases.

5.9 Password Lockout & Reset

Jefferson County is providing various options to assist users with changing a forgotten or expired password.

Password Management System (Self Service Portal)
The preferred method is through the use the Password Self Service using the password management system. Users will setup Personalized security questions in order to use Password management system to reset their password.

Phone
In the event your password cannot be reset via the password management system, you must contact IT/Information Security Officer and/or Information Security Team's Helpdesk team over the phone for changing a forgotten or expired password.

Following will be considered for every request made on Password Management solution or over the phone:

5.9.1 Multiple Failed attempts shall be monitored by the HIPAA sub-committee.

5.9.2 System administrators receiving requests for password changes shall positively identify the individual requesting the change.

5.9.3 Users requesting password changes shall provide their identity by providing their name, UserID and/or other information that can be verified by the System Administrator.

5.9.4 If there is reason to suspect deception on the part of the caller, the request shall be refused pending further investigation.

5.9.5 ITS Information Security Officer and/or Information Security Team reserves the right to reset a user's password in the event a compromise is suspected or reported.

5.9.6 The HIPAA/Privacy officer shall be notified in order that they may investigate.
If the user cannot provide proper identification, the request shall be refused.
The required frequency at which passwords must be changed varies based on the type of user, as defined below:

5.9.7.1 Standard Users

Standard users consist of Jefferson County employees and contractors (including temporary, permanent contractors and consultants), and employees who are not performing privilege functions or processing credit card payments.

- Passwords must be changed every three (3) months.
- Passwords must not be reused for at least five (5) generations.
- Passwords must not be changed more than one (1) time per day.
- New passwords must comply with the password requirements defined in the previous section.
- Accounts will lockout after five (5) invalid password attempts in fifteen (15) minutes.

- Accounts will remain locked for a duration of fifteen (15) minutes, unless the Jefferson County Service Desk is contacted, and the user's identity is verified in order for the account to be unlocked sooner.

5.9.7.2 Privileged Users and Service Account

Privileged users consist of users or service accounts with elevated access to manage and administer information systems, data and applications.
Such users have administrator access and these accounts are at a higher risk for compromise.

- Jefferson County approved Privileged Account Management (PAM) solutions must be considered for Privileged credentials vaulting in encrypted manner.
- Passwords must be changed every sixty (60) days for Privileged Users accounts and 180 days for service accounts.
- Passwords must not be reused for at least eight (8) generations.
- Passwords must not be changed more than one (1) time per day.
- New passwords must comply with the password requirements defined in the previous section.
- Accounts will lockout after three (3) invalid password attempts in fifteen (15) minutes.
- Accounts will remain locked for a duration of fifteen (15) minutes, unless the Jefferson County Service Desk is contacted, and the user's identity is verified in order for the account to be unlocked sooner.

6.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Any disciplinary action taken by the ITS Department to discipline a user who has violated this policy, will follow Jefferson County Commission's Disciplinary process.

7.0 Policy Owner

Jefferson County Commission

7.0a Policy Administrator

Chief Information Officer, Information Technology Services Department

8.0 Policy Approval Date

March 20, 2020

9.0 Policy Effective Date

March 20, 2020

10.0 Definitions

Term	Definition
Application Administration Account	- Any account that is for the administration of an application (e.g., Oracle database administrator).

Revision History

Initial Author	ITS Governance
Created On	August 13, 2019
Last Modified By	ITS Governance

Last Modified On	March 20, 2020
Revision Number	3
Approver	County Manager's Review Committee

Version	Changed By	Changed On	Notes / Comments
2	Information Technology	March 13, 2013	
3	Information Technology Services	March 20, 2020	

JEFFERSON COUNTY COMMISSION

Information Technology Services Department

Remote Access Security Rules & Regulations

1.0 Overview

Throughout this document the term policy refers to the strategy, procedures, rules, and regulations defined and encapsulated within each section of this document to achieve the stated information security goals. Remote access to Jefferson County Commission ("JCC") enterprise network is essential to maintain each departments productivity, but in many cases this remote access originates from networks that may already be compromised or are at a significantly lower security posture than the County's network. While these remote networks are beyond the control of JCC policies and procedures, the external risks must be mitigated on a continual basis.

2.0 Purpose

The purpose of this policy is to define rules and requirements for connecting to JCC's network from any host. These rules and requirements are designed to minimize the potential exposure to JCC from damages which may result from unauthorized use of JCC resources. Damages include the loss of sensitive or citizens confidential data, intellectual property, damage to public image, damage to critical JCC internal systems, and fines or other financial liabilities incurred as a result of those losses.

3.0 Scope

This policy applies to all JCC employees, contractors, vendors and agents with a JCC-owned or personally-owned computer or workstation used to connect to the JCC network. This policy applies to remote access connections used to do work on behalf of JCC, including reading or sending email and viewing intranet web resources. This policy covers any and all technical implementations of remote access used to connect to JCC networks.

4.0 Policy

It is the responsibility of JCC employees, contractors, vendors and agents with remote access privileges to JCC's enterprise network to ensure that their remote access connection is given the same consideration as the user's on-site connection to JCC data network. General access to the Internet for personal use through the JCC network is strictly limited to JCC employees, contractors, vendors and agents (hereafter referred to as "Authorized Users"). When accessing the JCC network from a personal computer, Authorized Users are responsible for preventing access to any JCC computer resources or data by non-Authorized Users. Performance of illegal activities through the JCC network by any user (Authorized or otherwise) is prohibited. The Authorized User bears responsibility for and consequences of misuse of the Authorized User's access. For further information and definitions, see the Acceptable Use Policy.

Authorized Users will not use JCC networks to access the Internet for outside business interests.

4.1 Requirements

4.1.1 Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs)) and strong pass-phrases. For further information see the Acceptable Use Policy, Encryption Policy, and Password Policy.

4.1.2 Authorized Users shall protect their login and password, even from family members.

4.1.3 While using a JCC-owned computer to remotely connect to JCC's data network, Authorized Users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an Authorized User or Third Party.

4.1.4 Use of external resources to conduct JCC business must be approved in advance by the JCC Department of Information Technology Services and the appropriate department business unit manager.

4.1.5 All hosts that are connected to JCC internal networks via remote access technologies must use the most up-to-date anti-virus software, this includes personal computers. Third party connections must comply with requirements as stated in the Third-Party Agreement.

4.1.6 Personal equipment used to connect to JCC's networks must meet the requirements of JCC-owned equipment for remote access.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Any disciplinary action taken by the ITS Department to discipline a user who has violated this policy, will follow Jefferson County Commission's Disciplinary process.

6.0 Related Policies

Acceptable Use Policy
Encryption Policy
Password Policy

7.0 Policy Owner

Jefferson County Commission

7.0a Policy Administrator

Chief Information Officer, Department of Information Technology Services

8.0 Policy Approval Date

March 20, 2020

9.0 Policy Effective Date

March 20, 2020

10.0 Definitions

Term Definition

Revision History

Initial Author	ITS Governance
Created On	August 13, 2019
Last Modified By	ITS Governance
Last Modified On	March 20, 2020
Revision Number	3
Approver	County Manager's Review Committee

Version	Changed By	Changed On	Notes / Comments
2	Information Technology	March 13, 2013	
3	Information Technology Services	March 20, 2020	

JEFFERSON COUNTY COMMISSION

Information Technology Services Department

Risk Assessment Security Rules & Regulations

1.0 Purpose

Throughout this document the term policy refers to the strategy, procedures, rules, and regulations defined and encapsulated within each section of this document to achieve the stated information security goals. The objective of performing risk management is to enable Jefferson County Commission ("JCC") to evaluate, in an ongoing fashion, the county security posture. The resulting risk assessment provides management with the necessary information on which to base ongoing information security decisions within the network environment. Risk assessments provide the foundation for JCC's Information Security Program by guiding the selection and implementation of security controls and the timing and nature of testing those controls. Testing results, in turn, provide the evidence to the Risk Assessment Process that the controls selected and implemented are achieving their intended purpose.

2.0 Scope

This policy applies to all of JCC applications, databases, servers, clients and networks within the network environment.

3.0 Policy

JCC utilizes a risk-based approach to determine information security requirements to ensure that security is commensurate with the risk and magnitude of harm that can result from the loss, misuse, unauthorized access to, or modification of, cardholder information.

Risk Management procedures are integrated into JCC Change Management and Information Systems Security meetings. Meaning, assessment of risk is part of all Change Request reviews and is also included in the review of current vulnerabilities

JCC will also include a formal risk assessment during the purchasing of any new hardware or software and any acquisitions that may occur to ensure all potential threats and vulnerabilities are properly identified and documented.

JCC will also conduct a risk assessment for all Emergency Response, Disaster Recovery and Business Continuity plans which is an inherent part of a thorough Business Impact Analysis which is the basis for any ER, DR and BC plan.

JCC will also conduct annual risk assessments and security assessments enterprise wide on their security programs to help understand and identify all current threats, vulnerabilities and gaps within their process that may create critical risks to the environment. This assessment is conducted via completion of a formal checklist which is based on information assurance best practices.

The annual risk assessment also includes vulnerability scanning and penetration testing in concert with vulnerability analyses of all clients, networks, applications, databases and systems associated with any sensitive county data.

Additionally, the formal risk assessment documentation is reviewed, and updated if necessary, during the annual requirements and documentation review process.

4.0 Risk Management Approach

The Risk Assessment process will be conducted and documented on an annual basis under the direction of the JCC Department of Information Technology Services ("ITS") Governance & Information Security Division. The assessment process will also be repeated any time changes occur in the classification, controls, environment or operation that could significantly impact the confidentiality, integrity, or availability of resources.

4.1 Key Roles and Responsibilities

Risk Committee (RC) / Security Review Board

- Governs overall Risk Management process that includes:
  - Strategic risks.
  - Tactical risks.
  - ITS Architecture risks.
  - Cybersecurity Architecture risks.
  - Operational/Business Continuity risks.
  - Technology risks.
  - Reputational risks.
  - Transactional risks.
  - Employee risks.
  - Third-Party risks.
  - Compliance risks,
- Making critical decisions related to risks in protecting JCC's ITS assets, business operations, and information.
- Reviews presented Risk Assessment Reports
- Approves risk treatment plan or recommended controls
- Meets quarterly and is attended by the CIO/s, Cybersecurity Staff, CIO, ITS Staff, business management, and others listed in a formal RC Charter.

Senior Management

- Sponsorship and support of the Risk Management Plan and process.
- Participation on the Security Review Board
- Review and approval of risk assessments and control recommendations
- Reporting to the board what mitigation actions have been taken.
- Ensuring that responsible personnel are formally assigned and trained on the Cybersecurity Risk Management Program aspects that relate to their assigned roles and integrated into the Cybersecurity Training and Awareness Program.

Information Security Office

- Conducts the Risk Assessments
- Integration of Risk Management activities with other ITS and Cybersecurity processes that include, but are not limited to:
  - System Administration and Operations,
  - Configuration Management,
  - Change Control,
  - Vulnerability Management,
  - Business Continuity Planning,

- Disaster Recovery,
- Continuous Monitoring, and
- Security Awareness and Training; and

- Analyzes Risk and recommends controls
- Presents for approval
- Documents the process
- Manages and facilitates implementation of recommended controls

Information Technology Services

- Participates in the Identification and Analysis process
- Participates on the Security Review Board
- Implementation of technical controls

Business and Functional Managers

- Participates in the risk identification and analysis process
- Some participation on the Security Review Board
- Implementation of administrative controls

4.2 Records to be kept

All information collected or used as part of the risk assessment process will be formally documented and securely maintained.

4.3 Risk Levels

4.3.1 The level of risk will be determined by combining the impact level and likelihood, as shown in the table below. Table below assists with determination of Overall Risk Level

	Level of Impact				
Likelihood	**Very Low**	**Low**	**Moderate**	**High**	**Very High**
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

4.3.2 Identify and evaluate additional controls that will reduce the identified risk to acceptable levels:

- Evaluate both technical (access control systems, firewalls, etc.) and non-technical (policies and procedures) controls.
- Evaluate both detective (those that warn of violations) and preventative (those that inhibit violations) controls.
- Perform a cost-benefit analysis for each control to narrow the selection of controls to those that mitigate risk cost effectively.

4.4 Risk Register and Action Plan

As Risks are identified and quantified, they are entered into the Risk Register in a matrix form. All risks are reported based on type of risk, probability, impact and overall risk. JCC shall maintain a Risk Register and Action Plan outlining existing risks, approved policy exceptions and accepted residual risk. This register should contain:

- Date entered.
- Responsible party for the risk (risk owner).
- Risk Identifier (unique)
- A detailed description of the risk.
- Any predisposing conditions or identified vulnerabilities that contribute to the risk.
- What system/hardware/application/location/etc. the risk applies to.
- Asset Value ($$$).
- Expected Loss ($$$)
- An estimate of the risks impact on confidentiality, integrity and availability.
- An estimate of the overall risk.
- An estimate of the likelihood that and attempt will be made to exploit the vulnerability.
- An estimate of the likelihood of success in exploiting the vulnerability.
- An estimate of overall likelihood.
- An estimate of the impact of a successful exploitation of the vulnerability.
- An overall risk rating.
- A detailed description of controls in place.
- An estimate of control effectiveness.
- Proposed additional controls.
- Responsible parties for additional controls.
- Proposed date when additional controls must be in place.
- Residual risk with additional controls in place.
- Date residual risk was accepted.
- Approver of acceptance of risk.
- Proposed re-review date.
- Issue history notes and milestones.
- Risk Status
- Risk Response will be formally documented by Jefferson County in the Risk Register as one of the following:
    - Remediated.
    - Mitigated/Reduced.
    - Accepted and Monitored.
    - Avoided.
    - Transferred

4.5 Review Process

Results and control recommendations will be presented to the Security Review Board for review at periodic and regular formal or informal meetings.

4.6 Risk Factors to be considered (Not limited to)

The following provides a summary of the potential risk factors that are to be analyzed during the Risk Assessment process to determine the security risk profile of a specific information resource:

- Internal networks that are connected to the resource
- External networks that are connected to the resource
- Hardware that supports the resource Software that supports the resource
- Applications that reside on the resource
- Physical location of the resource and related physical controls that are in place
- Interdependencies between the items documented above

- Business disruptions that could affect the resource (including natural disasters, failures of interdependent infrastructures such as power, telecommunications, etc.)
- Fraud that could be enacted on the resource
- Breach of legal, regulatory, or contractual obligations relating to the resource (e.g. privacy regulations)
- Risk to students or personal employee information residing on the resource
- Loss of public confidence if the resource was compromised
- Organizational vulnerabilities that could affect the resource - weak management support, ineffective training, inadequate expertise or resource allocation and inadequate policies, standards or procedures
- Additional costs being incurred
- Need to help mitigate risk through insurance coverage

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Any disciplinary action taken by the ITS Department to discipline a user who has violated this policy, will follow Jefferson County Commission's Disciplinary process.

6.0 Policy Owner

Jefferson County Commission

6.0a Policy Administrator

Chief Information Officer, Information Technology Services Department

7.0 Policy Approval Date

March 20, 2020

8.0 Policy Effective Date

March 20, 2020

Revision History

Initial Author	ITS Governance
Created On	August 13, 2019
Last Modified By	ITS Governance
Last Modified On	March 20, 2020
Revision Number	3
Approver	County Manager's Review Committee

Version	Changed By	Changed On	Notes / Comments
2	Information Technology	March 13, 2013	
3	Information Technology Services	March 20, 2020	

JEFFERSON COUNTY COMMISSION

Information Technology Services Department

Roles & Responsibilities for Security Personnel Rules & Regulations

1.0 Overview

Throughout this document the term policy refers to the strategy, procedures, rules, and regulations defined and encapsulated within each section of this document to achieve the stated information security goals. Jefferson County Commission ("JCC") Departments rely heavily on information technology components to run their daily operations and deliver products and services. With an increasing reliability on information technology, a growing complexity of information technology infrastructure, and a constantly changing information security threat and risk environment, information security has become a mission-essential function. This function must be managed and governed to reduce the risks to JCC operations and to ensure the County's ability to do business and serve the citizenry.

2.0 Purpose

The purpose of this policy is to ensure that JCC Information Technology Services Department (ITS) information security roles are clearly defined with specific responsibilities that are essential to the implementation of ITS Governance and Security Framework program.

3.0 Scope

This policy covers all JCC ITS information systems. Also, this policy applies to all JCC employees, contractors, and all other users of JCC ITS information systems that support the operations and citizens of Jefferson County.

4.0 Policy

4.1 Principles

- JCC ITS is committed to ensuring the security and confidentiality of institutional data is maintained at all times, and that institutional data is only accessed appropriately.
- Employees are individually responsible for any breaches that occur as a direct result of non-compliance.
- Access to non-public data may only be granted to Authorized Users on a need to know basis. The Data Steward of any non-public data, as defined below, must approve and verify Authorized User access.
- Employees who access data for which they are not authorized and/or commit breaches of confidentiality may be subject to disciplinary action up to and including discharge and/or termination of contract/relationship.
- Authorized Users shall be provided training on the expectations, knowledge, and skills related to information security.
- Authorized Users must maintain the confidentiality of all non-public data even if technical security mechanisms fail or are absent. A lack of security measures to protect the confidentiality of information does not imply that such information is public.
- Authorized Users are responsible for enforcing security controls whenever they place Jefferson County Commission data onto non-JCC managed devices or services.

- All users' access to citizens and/or employee data or managed digital and or physical assets will comply with applicable standards, controls, and regulations (e.g.,HIPAA, FISMA, PII, etc.).
- Non-compliance shall be reported to the Information Security Officer and/or Information Services Department Security Team.

4.2 Roles and Responsibilities for Information Security

Responsibility for JCC ITS comprehensive enterprise information security program is delegated to the groups and individuals as defined below. Note that an individual may function within more than one role.

Enterprise Level Roles:

Information Services Department Security Team
Information Security Officer
Data Trustee

Unit Level Roles:

Data Steward
Network Security Contact
Data Custodian
Authorized User

4.2.1 Enterprise Level Roles

4.2.1.1 Information Services Department Security Team

The ITS Security Team is responsible for governance and oversight of the enterprise information security program. The ITSST will:

1. Analyze and manage institutional risks.
2. Review and recommend policies, procedures, and standards.
3. Ensure consistency in disciplinary processes for violation.

4.2.1.2 Information Security Officer

The official responsible for directing implementation of the enterprise Security Framework program. The Information Security Officer will:

1. Coordinate the development and maintenance of information security policies and standards.
2. Investigate security incidents and coordinate their resolution by incorporating incident response management best practices.
3. Advise Data Stewards in classifying their data and recommend Available controls as defined in the Data Classification Policy.
4. Implement an information security awareness program.
5. Serve as liaison to the ITSST, Law Enforcement, Internal Audit, and County Attorney's Office.
6. Provide consulting services for information security throughout the enterprise.

4.2.1.3 Data Trustee

Data Trustees are senior County employees, or their designees, who have planning and policy level responsibility for data within their functional areas and management responsibility for defined segments of the County data. Data Trustees work with the Chief Information Officer (CIO) to ensure that the appropriate resources (staff, technical infrastructure, etc.) are available to support the data needs of the entire County.

Data Trustee responsibilities include:

1. Assigning and overseeing Data Stewards.
2. Overseeing the establishment of data policies in their areas.
3. Determining legal and regulatory requirements for data in their areas.
4. Promoting appropriate data use and data quality.

4.2.2 Unit Level Roles

4.2.2.1 Data Steward

The senior official within a departmental unit (or his/her designee) accountable for managing information assets. The Data Steward will:

1. Approve business use of information.
2. Identify Data Custodian(s) (see below) for each segment of information under his/her control.
3. Ensure implementation of policies, and documentation of process and procedures for guaranteeing availability of systems, including:
    - Risk assessment
    - Disaster recovery
    - Business Continuity
    - Software testing and revision controls
4. Determine appropriate classification of each segment of data as described In the Data Classification Policy.
5. Define departmental access roles and assign access for individuals based On their business need to know.
6. Ensure that all department/unit personnel with access to information Assets are trained in relevant security and confidentiality policies and procedures.
7. Ensure applicable protection of health information assets under his/her control, including:
    - Identify all health information assets containing individually identifiable health information (e.g., Protected Health Information, or "PHI") to ensure HIPPA compliance.
    - Ensure that validated corrections to health information are implemented.
    - Ensure compliance with federal and state laws and Jefferson County Commission Policies regarding the use of individually identifiable health information in directed communication or solicitation.
    - Require the completion of an information sharing agreement before access to health information assets is granted to external entities.
    - Ensure similar, applicable protection for non-health information assets.

4.2.2.2 Network Security Contact (NSC)

The individual within a unit who acts as a liaison for timely and relevant information flow between central networking and information technology security personnel and the unit.

The NSC will:

1. Receive vulnerability reports for unit computer systems and disseminate such information to appropriate technical staff for resolution.
2. Receive network alerts, outage notifications, or other networking issues affecting the unit and disseminate such information to appropriate staff.
3. Coordinate unit response to computer security incidents.

4.2.2.3 Data Custodian

Functional or technical user that has operational responsibility for the capture, maintenance, and dissemination of a specific segment of information, including the installation, maintenance, and operation of computer hardware and software

platforms. The data custodian may or may not be Information Technology Services staff.
The Data Custodian will:

1. Define and implement processes for assigning User access, revoking User Access privileges and setting file protection parameters.
2. Implement system protection, data protection and access controls conforming to the Data Classification Policy.
3. Define and implement procedures for backup and recovery of information.
4. Ensure processes are in place for the detection of security violations.
5. Monitor compliance with information security policy and standards.
6. Limit physical and logical access to information assets, including:
    - Equipment control (inventory and maintenance records), and physical security of equipment.
    - Authorization procedures prior to physical access to restricted areas, such as data centers, with sign-in or escort of visitors, as appropriate.
    - Implement a system for software change management and revision controls.
    - Maintain appropriate internal audits, which record system activity such as log-ins, file accesses, and security incidents.
    - Maintain records of those granted physical access to restricted areas (e.g., key card access lists).
    - Provide appropriate handling and physical protection for health information assets
    - Ensure operation and maintenance personnel are given access only as necessary to perform system maintenance responsibilities.
    - Ensure authorized Information Technology Services staff supervise all external personnel performing maintenance activities.
    - Some of the above requirements may be delegated to others, when hosting within an institutional data center or when in the cloud. The data custodian will take appropriate steps to monitor these delegated requirements.

4.2.2.4 Authorized User

Individuals who have been granted access to information assets in the performance of their assigned duties are considered Authorized Users ("Users"). Users include, but are not limited to: employees, vendors, volunteers, contractors, or other affiliates of Jefferson County Commission.

Authorized Users will:

1. Seek access to data only through established authorization and access control processes.
2. Access only that data for which they have a business need to know to carry out job responsibilities.
3. Disseminate data to others only when authorized by the Data Steward.
4. Report access privileges inappropriate to job duties to the Data Steward for correction.
5. Complete training in information security and confidentiality policies and procedures.
6. Acknowledge or sign annual confidentiality statements for access to restricted and critical data.
7. Perform all responsibilities necessary to protect data when placing

County data on personally owned or managed devices.

5.0 Enforcement

Any employee, contractors, and vendors found to have violated this policy may be subject to disciplinary action, up to and including termination of employment and or contract. In cases where vendors or contractors are involved the ITS Department will consult with Legal to officially terminate any agreement with the vendor or contractor.

6.0 Policy Owner

Jefferson County Commission

6.0a Policy Administrator

Chief Information Officer, Information Technology Services Department

7.0 Policy Approval Date

March 20, 2020

8.0 Policy Effective Date

March 20, 2020

Revision History

Initial Author	ITS Governance
Created On	August 13, 2019
Last Modified By	ITS Governance
Last Modified On	March 20, 2020
Revision Number	3
Approver	County Manager's Review Committee

Version	Changed By	Changed On	Notes / Comments
2	Information Technology	March 13, 2013	
3	Information Technology Services	March 20, 2020	

JEFFERSON COUNTY COMMISSION

Information Technology Services Department

Software / Application Development Security Rules & Regulations

1.0 Overview

Throughout this document the term policy refers to the strategy, procedures, rules, and regulations defined and encapsulated within each section of this document to achieve the stated information security goals. Software application development is a complex endeavor, susceptible to failure, unless undertaken with a deliberate and systematic methodology. The integration of Project Management and Software Quality Controls into the Software Development Life Cycle (SDLC) provides a robust framework for successful application development process for Jefferson County Commission ("JCC") Information Technology Services Department (ITS).

2.0 Purpose

The purpose of this Policy is to standardize software development for all enterprise-level centrally-managed mission critical applications through the use of industry leading practices. These applications and services typically deal with critical data and / or HR-, finance-, geographic information systems, land records management, etc.., and due diligence in protecting this data is required. Standardizing the development approach and coding techniques for critical systems will ensure their maintainability, security, and protection against cyber-attacks and accessibility.

3.0 Scope

This Policy applies to all employees, consultants and / or contractors involved in the development or modification of enterprise-level centrally-managed mission critical applications that support JCC.

4.0 Policy

ITS is responsible for developing, maintaining, and participating in a Software Development Life Cycle for all Jefferson County Commission software development projects. All software developed in-house which runs on production systems must be developed according to the SDLC. At a minimum, this Policy addresses the areas of preliminary analysis or feasibility study; risk identification and mitigation; systems analysis; design specification; development; quality assurance and acceptance testing; implementation; and post-implementation maintenance and review. This methodology ensures that the software will be adequately documented and tested before production implementation.

All enterprise-level centrally-managed applications developed by ITS staff, consultants, and/or contractors must adhere to development standards and procedures in the ITS Application Development Standards. These standards include: coding techniques, testing strategies, documentation requirements and software release processes that align with industry standards, regulatory requirements and any contractually specified obligation.

There must be a separation between the production, development and test environments. This will ensure that security is rigorously maintained for the production system, while the

development and test environments can maximize productivity with fewer security restrictions. Where these distinctions have been established, development and test staff must not be permitted to have access to production systems.

5.0 Enforcement

ITS enforces this Policy and the related Standards at all times. Anyone who has reason to suspect a deliberate and / or significant violation of this Policy is encouraged to promptly report it to the Manager of Systems Analysis. The Manager of Systems Analysis will review, investigate and document any actions that violate this policy to substantiate further corrective actions that need to be taken. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Any disciplinary action taken by the ITS Department to discipline a user who has violated this policy, will follow Jefferson County Commission's Disciplinary process.

6.0 Policy Owner

Jefferson County Commission

6.0a Policy Administrator

Chief Information Officer, Information Technology Services Department

7.0 Policy Approval Date

March 20, 2020

8.0 Policy Effective Date

March 20, 2020

Revision History

Initial Author	ITS Governance
Created On	August 13, 2019
Last Modified By	ITS Governance
Last Modified On	March 20, 2020
Revision Number	3
Approver	County Manager's Review Committee

Version	Changed By	Changed On	Notes / Comments
2	Information Technology	March 13, 2013	
3	Information Technology Services	March 20, 2020	

JEFFERSON COUNTY COMMISSION

Information Technology Services Department

User Access Management Security Rules & Regulations

1.0 Overview

Throughout this document the term policy refers to the strategy, procedures, rules, and regulations defined and encapsulated within each section of this document to achieve the stated information security goals. Information security is important to Jefferson County Commission ("JCC") daily operational duties and responsibilities to the citizens of Jefferson County Alabama, driven in part by changes in the regulatory environment and advances in technology. Information security ensures that JCC Department of Information Technology Services ("ITS") systems, data, and infrastructure are protected from risks such as unauthorized access, manipulation, destruction or loss of data, as well as unauthorized disclosure or incorrect processing of data.

2.0 Purpose

The purpose of this policy is to ensure ITS reduces risks to information security by managing accounts that provide access, limiting access to authorized users and preventing unauthorized access to information systems.

3.0 Scope

The policy applies to every user account within JCC domain, including its service providers/vendors. This policy is regarded as being crucial to the operation and security of ITS systems.

The policy covers the following elements of user access management:

- New user account;
- Terminated user removal;
- User permission/role change request;
- User access rights assignment for networks, operating systems, databases and applications;
- Reviewing user access permissions; and
- User and administrator activity monitoring.

4.0 Policy

Protecting access to JCC's systems and applications is critical to maintain the integrity of the County's technology and data to prevent unauthorized access to such resources. Access to the County's technology systems must be restricted to only authorized users or processes, based on the principle of strict need to know and least privilege.

4.1. General

ITS shall develop procedures for the effective implementation of security controls covering access control and information system account management. Information system accounts are used to provide access to information technology assets and physical access, in cases where physical access is tied to information system accounts.

Information system account types include, for example, individual, shared, group, system, guest/anonymous, and service. As set forth below, Information Technology Services Department access control processes are supported through the use of the controls set forth in: (i) business requirements (Section 4.2 below); (ii) user access management (see Section 4.3 below); (iii) system and application access control (see Section 4.4 below); (iv) segregation of duties (see Section 4.5 below); and (v) additional security controls (see Section 4.6 below).

4.2. Business Requirements of Access Control

4.2.1. ITS shall:

a. Provide access based on business and information security requirements;
b. Determine appropriate access control rules, access rights and restrictions for specific user roles towards their assets, with the amount of detail and the strictness of the controls reflecting the associated information security risks;
c. Consider both logical and physical access controls together, where applicable;
d. Give users and service providers a clear statement of the business requirements to be met by access controls that have been provided.

Two of the frequent principles directing the access control policy are:
a. Need-to-know: you are only granted access to the information you need to perform your tasks (different tasks/roles mean different need-to-know and hence different access profile);
b. Need-to-use: you are only granted access to the information processing facilities (Information Technology Services Department equipment, applications, procedures, rooms) you need to perform your task/job/role.

4.2.2. Access to Networks and Network Services

ITS shall provide users with only the access to the network and network services that they have been specifically authorized to use. Unauthorized and insecure connections to network services can affect the whole organization. This control is particularly important for network connections to sensitive or critical business applications or to users in high-risk locations, e.g. public or external areas that are outside the organization's information security management and control. ITS shall utilize appropriate technical controls to protect the internal JCC network from external networks.

4.2.3. Least Privilege

ITS shall employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

4.3. User Access Management

ITS shall include possible impacts to access controls when assessing changes to the information technology environment.

4.3.1. User OnBoarding and OffBoarding

ITS shall implement a formal user onboarding (new employee) and offboarding process (separated employee) to enable assignment of access rights and the provisioning technology services. Providing or revoking access to information or information processing facilities is usually a two-step procedure:

- assigning and enabling, or revoking, a user ID;
- providing, or revoking, access rights to such user ID.

4.3.2. User Access Provisioning

ITS shall implement formal user access provisioning to assign or revoke access rights for all user types to all systems and services. Ideally, consideration should be given to

establishing user access roles based on business requirements that summarize a number of access rights into typical user access profiles.

4.3.3. Management of Privileged Access Rights

ITS shall implement processes for restricting and controlling the allocation and use of "privileged access rights". These privileged access rights are generally referred to as "administrative rights". Inappropriate use of administrative rights (any feature or facility of an information system that enables the user to override system or application controls) is a major contributory factor to failures or breaches of systems.

4.3.4. Review of User Access Rights

ITS shall include a review of users' access rights at regular defined intervals as part of access control procedures.

4.3.5. Removal or Adjustment of Access Rights

4.3.5.1. Removal

ITS shall confirm that the access rights of all Users to information assets be removed upon termination of their employment, contract or agreement, or adjusted upon change. Upon termination, the access rights of an individual to information and assets associated with information processing facilities and services should be removed or suspended.

4.3.5.2. Modifications

ITS shall confirm that changes of User employment or role is reflected in removal of all access rights that were not approved for the new employment. The access rights that should be removed or adjusted include those of physical and logical access. Removal or adjustment can be done by removal, revocation, or replacement of keys, identification cards, information processing facilities or subscriptions. Any documentation that identifies access rights of employees and contractors should reflect the removal or adjustment of access rights. If a departing employee or external party user has known passwords for user IDs remaining active, these should be changed upon termination or change of employment, contract or agreement.

4.3.5.3. Additional Considerations

Access rights for information and assets associated with information processing facilities should be reduced or removed before the employment terminates or changes, depending on the evaluation of risk factors such as:

- whether the termination or change is initiated by the employee, the external party user, or by management, and the reason for termination;
- the current responsibilities of the employee, external party user or any other user;
- the value of the assets currently accessible.
- In certain circumstances access rights may be allocated on the basis of being available to more people than the departing employee or external party user, e.g. group IDs. In such circumstances, departing individuals should be removed from any group access lists and arrangements should be made to advise all other employees and external party users involved to no longer share this information with the person departing. In cases of management-initiated termination, disgruntled employees or external party users can deliberately corrupt information or sabotage information processing facilities. In cases of persons resigning or being dismissed, they may be tempted to collect information for future use.

4.4. System and Application Access Control

ITS shall develop and document processes to prevent unauthorized access to systems and applications.

4.4.1. Information Access Restriction
Access to information and application system functions shall be restricted in accordance with this policy and shall be restricted based on individual business application requirements.

4.4.2. Secure Log-on Procedures
Access to systems and applications shall be controlled by a secure log-on procedure. A suitable authentication technique shall be chosen to substantiate the claimed identity of a user.

2.4.3. Password Management System
Password management systems shall be shall be utilized in accordance with the Password Policy to ensure quality passwords.
A password management system must:

- enforce the use of individual user IDs and passwords to maintain accountability;
- allow users to select and change their own passwords and include a confirmation procedure to allow for input errors;
- enforce a choice of quality passwords;
- force users to change their passwords at the first log-on;
- enforce regular password changes and as needed;
- maintain a record of previously used passwords and prevent re-use;
- not display passwords on the screen when being entered;
- store password files separately from application system data;
- and transmit passwords in protected form.

4.5. Segregation of Duties
Conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets. Segregation of duties is a method for reducing the risk of accidental or deliberate misuse of an organization's assets.

Care should be taken that no single person can access, modify or use assets without authorization or detection. The initiation of an event should be separated from its authorization. The possibility of collusion should be considered in designing the controls.

ITS shall work to implement segregation of duties, where applicable. Whenever it is difficult to segregate, other controls such as monitoring of activities, audit trails and management supervision shall be considered.

4.6. Additional Security Controls
ITS shall, where applicable:

4.6.1. Evaluate and impose additional usage restrictions to further limit access;

4.6.2. Identify parameters that define typical account usage and notify when use is outside those parameters;

4.6.3. Enforce a limit of invalid logon attempts and automatically lock account for a specified period of time;

4.6.4. Institute session lock and termination settings for a determined period of inactivity;

4.6.5. Require the creation and use of any “generic” account, an account used by multiple users and whose activity cannot be tracked to a unique user, to be approved via the security exception process.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Any disciplinary action taken by the ITS Department to discipline a user who has violated this policy, will follow Jefferson County Commission’s Disciplinary process.

6.0 Related Policies

Password Policy
Network Security Policy

7.0 Policy Owner

Jefferson County Commission

7.0a Policy Administrator

Chief Information Officer, Information Technology Services Department

8.0 Policy Approval Date

March 20, 2020

9.0 Policy Effective Date

March 20, 2020

10.0 Definitions

Term	Definition
OnBoarding	Process of providing new employees with the necessary access methods to perform their responsibilities.
OffBoarding	Process of removing former employees’ access from all information technology system (user account, user file share, perimeter access, etc..,)

Revision History

Initial Author	ITS Governance
Created On	August 13, 2019
Last Modified By	ITS Governance
Last Modified On	March 20, 2020
Revision Number	3
Approver	County Manager’s Review Committee

Version	Changed By	Changed On	Notes / Comments
2	Information Technology	March 13, 2013	

3	Information Technology Services	March 20, 2020	

JEFFERSON COUNTY COMMISSION

Information Technology Services Department

Wireless Networking/Access Security Rules & Regulations

1.0 Overview

Throughout this document the term policy refers to the strategy, procedures, rules, and regulations defined and encapsulated within each section of this document to achieve the stated information security goals. With the mass explosion of Smart Phones and Tablets, pervasive wireless connectivity is almost a given at any organization. Insecure wireless configuration can provide an easy open door for malicious threat actors/activity.

2.0 Purpose

The purpose of this policy is to secure and protect the information assets of Jefferson County Commission ("JCC"). JCC provides computer devices, data networks, and other electronic information systems to meet missions, goals, and initiatives as well as the needs of the citizens. The County grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets.

This policy specifies the conditions that wireless infrastructure devices must satisfy to connect to JCC data network. Only those wireless infrastructure devices that meet the standards specified in this policy or are granted an exception by the Department of Information Technology Services ("ITS") are approved for connectivity to the JCC wireless network.

3.0 Scope

All employees, contractors, consultants, temporary and other workers at JCC, including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of the County must adhere to this policy. This policy applies to all wireless infrastructure devices that connect to the JCC network or reside on a JCC site that provide wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular phones, and tablets. This includes any form of wireless communication device capable of transmitting packet data.

4.0 Policy

4.1 General Requirements

All wireless infrastructure devices that reside at a JCC site or connect to a JCC network, or provide access to information classified as JCC Restricted and/or Sensitive, or all of the above must:

- Abide by the standards specified within this policy.
- Be installed, supported, and maintained by an approved support team.
- Use ITS approved authentication protocols and infrastructure.
- Use ITS approved encryption protocols.
- Maintain a hardware address (MAC address) that can be registered and tracked.
- Not interfere with wireless access deployments maintained by other support organizations.

4.2 Home Wireless Device Requirements

4.2.1 Wireless infrastructure devices that provide direct access to the JCC enterprise network, must conform to Remote Access, Antivirus, and Network Access & Authentication policies.

4.2.2 Wireless infrastructure devices that fail to conform to Remote Access, Antivirus, and Network Access & Authentication policies must be installed in a manner that prohibits direct access to the JCC enterprise network. Access to the JCC enterprise network through a non-conforming device must use standard remote access authentication.

5.0 Jefferson County WiFi Networks

5.1 JeffCo-Guest
5.2 JeffCo-Mobile
5.3 JeffCo-Connect

6.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Any exception to the policy must be approved by the ITS in advance. Any disciplinary action taken by the ITS Department to discipline a user who has violated this policy, will follow Jefferson County Commission's Disciplinary process.

7.0 Related Policies

Remote Access Policy
Antivirus Policy
Network Access & Authentication Policy

8.0 Policy Owner

Jefferson County Commission

8.0a Policy Administrator

Chief Information Officer, Information Technology Services Department

9.0 Policy Approval Date

March 20, 2020

10.0 Policy Effective Date

March 20, 2020

11.0 Definitions

Term	Definition
MAC Address	Stands for "Media Access Control Address". A MAC address is a hardware identification number that uniquely identifies each device on a network.
Packet Data	A unit of data made into a single package that travels along a given network path.

Revision History

Initial Author	ITS Governance
Created On	August 13, 2019
Last Modified By	ITS Governance
Last Modified On	March 20, 2020
Revision Number	3
Approver	County Manager's Review Committee

Version	Changed By	Changed On	Notes / Comments
2	Information Technology	March 13, 2013	
3	Information Technology Services	March 20, 2020	