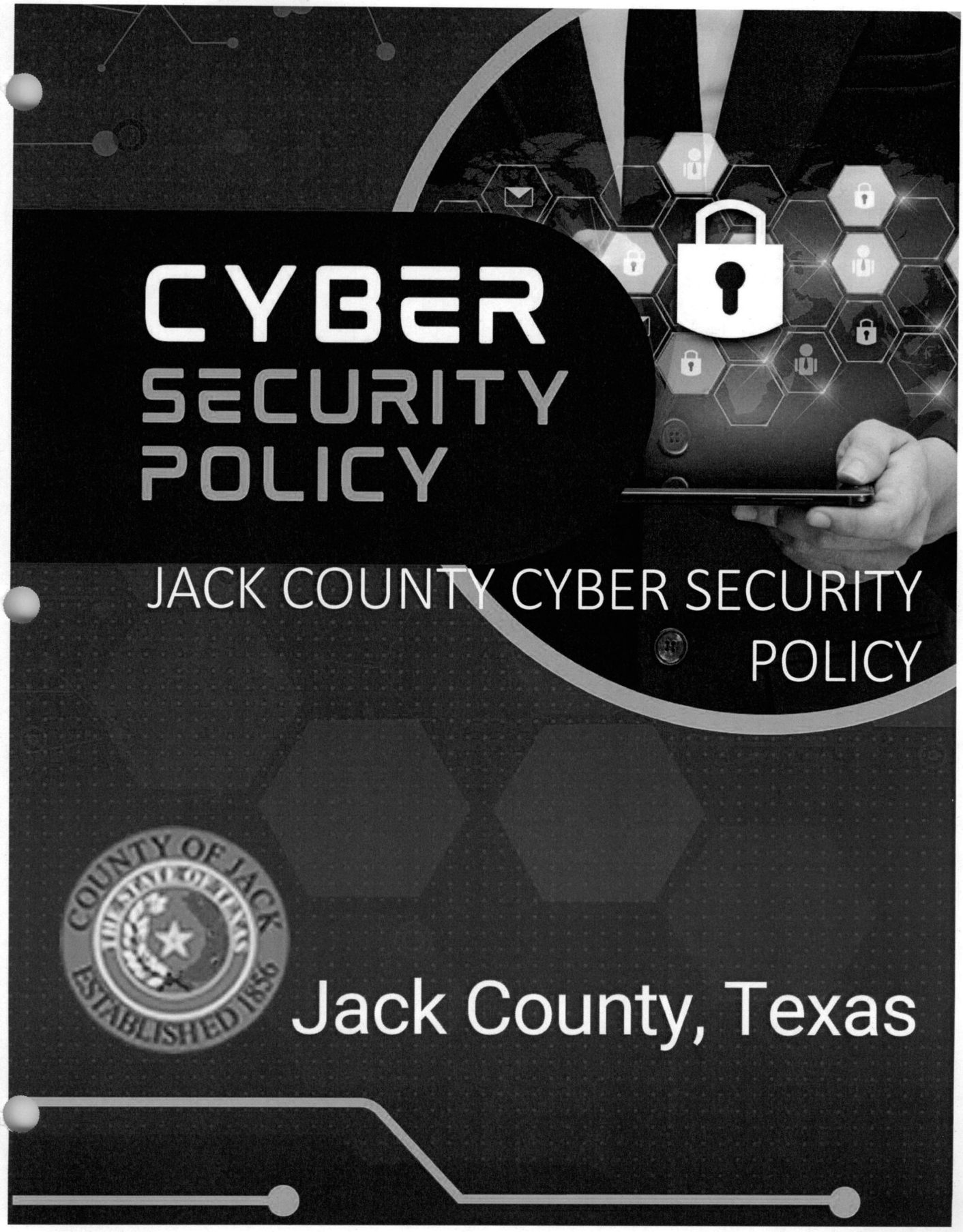
CYBER
SECURITY
POLICY
JACK COUNTY CYBER SECURITY
POLICY
COUNTY OF JACK
ESTABLISHED 1856
Jack County, Texas

Table of Contents

Acceptable Use Policy (AUP)

1. Introduction and Purpose:

This Acceptable Use Policy (AUP) outlines the guidelines and rules for the appropriate and responsible use of the information technology resources and networks provided by Jack County. This policy aims to ensure a safe and productive computing environment for all users and protect the interests of Jack County, its employees, and its constituents.

2. Scope:

This AUP applies to all individuals who have authorized access to Jack County's information technology resources, including employees, contractors, volunteers, and visitors.

3. Acceptable Use:

Users are permitted to use Jack County's information technology resources for legitimate business purposes, including but not limited to:

a. Conducting official county business and accessing county-provided applications and services.

b. Communicating and collaborating with colleagues, constituents, and authorized external parties.

c. Conducting research, accessing educational materials, and gathering information relevant to work responsibilities.

d. Storing, processing, and sharing files and data necessary for official county activities.

e. Participating in training programs and professional development related to county operations.

Personal use of Jack County's information technology resources may be permitted within reasonable limits, provided it does not interfere with work responsibilities, violate any other section of this AUP, or incur excessive costs for the county.

4. Unacceptable Use:

The following activities are strictly prohibited and constitute a violation of this AUP:

a. Unauthorized access: Attempting to access, modify, or use any information, system, or network without proper authorization.

b. Malicious software: Intentionally introducing or spreading viruses, malware, or other destructive software.

c. Harassment: Engaging in any form of harassment, discrimination, or intimidation through electronic means.

d. Illegal activities: Using Jack County's resources for any unlawful activities or violating any local, state, or federal laws.

e. Intellectual property violations: Infringing on copyrights, trademarks, patents, trade secrets, or other intellectual property rights.

f. Unauthorized disclosure: Sharing confidential or sensitive information without proper authorization or consent.

g. Network interference: Intentionally disrupting or compromising the operation, performance, or security of the county's networks and systems.

h. Unauthorized hardware or software installation: Installing or using unauthorized hardware or software that may pose security risks or violate licensing agreements.

i. Unauthorized sharing of credentials: Sharing usernames, passwords, or other authentication credentials with unauthorized individuals.

j. Misuse of resources: Consuming excessive network bandwidth, storage, or computing resources without legitimate business reasons.

k. Unauthorized monitoring: Engaging in unauthorized monitoring or interception of network traffic or communications.

5. User Responsibilities:

Users are responsible for adhering to this AUP and are expected to:

a. Use Jack County's information technology resources in a responsible and ethical manner.

b. Safeguard usernames, passwords, and other access credentials and use them only for authorized purposes.

c. Protect confidential and sensitive information by following established data protection and security guidelines.

d. Report any suspected violations of this AUP or any potential security breaches to the designated IT department or supervisor.

e. Cooperate with any investigations related to alleged violations of this AUP.

6. Consequences of Violations:

Violations of this AUP may result in disciplinary actions, up to and including:

a. Verbal or written warnings.

b. Temporary or permanent suspension of access privileges.

c. Termination of employment or contractual agreements.

d. Legal action, if necessary.

Jack County reserves the right to monitor and audit the use of its information technology resources to enforce this AUP and ensure compliance.

7. Reporting and Compliance:

Users should report suspected violations of this AUP or any concerns related to information security to the designated IT department or supervisor. All reports will be handled promptly and confidentially.

Jack County will investigate reported violations in a fair and impartial manner and take appropriate action to address the situation.

8. Policy Enforcement:

Jack County's IT department is responsible for the enforcement of this AUP. They may employ monitoring and auditing mechanisms to ensure compliance with the policy.

This AUP will be reviewed periodically, and updates will be communicated to all users as necessary.

9. Legal Disclaimer:

This AUP does not create any contractual rights or obligations beyond what is required by law. Jack County reserves the right to amend or modify this AUP at any time without prior notice.

Antivirus Management Policy

1. Introduction and Purpose:

This Antivirus Management Policy outlines the guidelines and procedures for the installation, configuration, and management of antivirus software across Jack County's information technology infrastructure. The purpose of this policy is to ensure the protection of the county's systems, networks, and data from malware and other security threats.

2. Scope:

This policy applies to all devices, including desktops, laptops, servers, and mobile devices, that are owned or operated by Jack County or connected to its networks.

3. Antivirus Software Installation:

a. All devices connected to Jack County's networks must have up-to-date antivirus software installed and activated.

b. Only approved and licensed antivirus software provided by the county's designated IT department may be installed on devices.

c. Antivirus software installations should be performed according to the manufacturer's guidelines and recommendations.

4. Antivirus Software Updates:

a. Antivirus software on all devices must be kept up to date with the latest virus definitions, program updates, and security patches.

b. Devices should be configured to receive automatic updates from the antivirus software vendor.

c. If automatic updates are not available, regular manual updates must be performed according to a defined schedule.

5. Real-Time Scanning:

a. Real-time scanning features of antivirus software must be enabled on all devices to provide continuous protection against malware.

b. Real-time scanning should be configured to scan files, email attachments, web downloads, and other relevant sources of potential threats.

6. Regular System Scans:

a. Scheduled system scans should be performed on all devices to proactively detect and remove malware.

b. The frequency and timing of system scans should be determined based on risk assessment and organizational needs.

c. System scans should cover all files, directories, and storage devices.

7. Quarantine and Removal:

a. Detected malware should be automatically or manually quarantined and isolated from the rest of the system to prevent further spread and damage.

b. Infected files should be promptly removed or cleaned, following the recommended procedures provided by the antivirus software vendor.

c. The IT department should be notified of any detected malware for appropriate action and further investigation.

8. Reporting and Incident Response:

a. Any suspected or confirmed malware infections should be promptly reported to the IT department.

b. Users should cooperate with the IT department during incident response and provide necessary information or access for investigation and remediation.

c. The IT department will document and track antivirus-related incidents and take appropriate actions to prevent future occurrences.

9. User Education and Awareness:

a. Users should be educated on the importance of antivirus software and the role they play in maintaining a secure computing environment.

b. Training programs and awareness campaigns should be conducted periodically to educate users about safe browsing habits, avoiding suspicious downloads, and recognizing potential malware threats.

10. Policy Compliance:

a. All users are required to comply with this Antivirus Management Policy.

b. Non-compliance with this policy may result in disciplinary actions, including warnings, suspension of network access, or termination, as determined by Jack County's policies and procedures.

11. Policy Review:

This policy will be reviewed periodically and updated as necessary to ensure its effectiveness and compliance with evolving security requirements.

Backup and Disaster Recovery Policy

1. Policy Statement

The purpose of this policy is to establish guidelines and procedures for the backup and disaster recovery of critical data and systems within Jack County. The policy aims to ensure the availability, integrity, and confidentiality of data, as well as the quick recovery and resumption of services in the event of a disaster or system failure.

2. Scope

This policy applies to all departments, employees, and systems within Jack County that handle or process critical data. It encompasses all hardware, software, and data stored within Jack County's infrastructure, whether on-premises or in the cloud.

3. Backup Procedures

3.1 Data Classification

Data within Jack County shall be classified based on its criticality and importance. A classification system shall be established, designating data as high, medium, or low priority for backup and recovery purposes.

3.2 Regular Backup Schedule

A regular backup schedule shall be established, taking into consideration the criticality of data and the frequency of changes. All critical data shall be backed up at least daily, while less critical data may be backed up less frequently.

3.3 Backup Storage

Backed-up data shall be stored securely in on-site and off-site locations to protect against physical damage or loss. Suitable storage media, such as tapes or cloud-based solutions, shall be utilized to ensure data integrity and accessibility.

3.4 Testing and Verification

Regular testing and verification of backup data shall be conducted to ensure its integrity and recoverability. Test restorations shall be performed periodically to validate the backup process and the restoration of critical systems and data.

4. Disaster Recovery Procedures

4.1 Disaster Recovery Plan

A comprehensive disaster recovery plan (DRP) shall be developed and maintained. The DRP should include detailed procedures and guidelines for responding to different types of disasters, including natural disasters, system failures, cyber-attacks, and other emergencies.

4.2 Roles and Responsibilities

Clear roles and responsibilities shall be assigned to designated personnel within each department to ensure a coordinated and efficient response during a disaster. Key personnel should be trained regularly on their roles and responsibilities and kept up to date on the DRP.

4.3 Alternative Facilities and Infrastructure

Alternative facilities, such as a backup data center or a secondary site, shall be identified and maintained to support the recovery of critical systems and services. These facilities should have the necessary infrastructure, power, connectivity, and resources to resume operations.

4.4 Communication Plan

A communication plan shall be established to ensure effective and timely communication during a disaster. Contact lists, emergency notification systems, and backup communication channels should be in place to facilitate communication among key personnel, stakeholders, and relevant authorities.

4.5 Documentation and Updates

All disaster recovery procedures, plans, and contact information shall be documented, reviewed periodically, and updated as needed. Changes to the infrastructure, systems, or critical data should be reflected in the DRP to ensure its accuracy and effectiveness.

5. Training and Awareness

Regular training and awareness programs shall be conducted for all employees to ensure they are familiar with backup and disaster recovery procedures, their roles, and their responsibilities. Training should cover emergency response, data backup, restoration, and business continuity practices.

6. Compliance and Auditing

Compliance with this policy shall be periodically audited to ensure adherence to the established procedures. Any deviations or non-compliance shall be addressed promptly, and corrective actions taken to maintain the effectiveness of the backup and disaster recovery capabilities.

7. Review and Revision

This policy shall be reviewed annually or as needed to account for changes in technology, infrastructure, or regulatory requirements. Any updates or revisions shall be communicated to all relevant personnel and stakeholders.

By adhering to this Backup and Disaster Recovery Policy, Jack County aims to safeguard its critical data, minimize downtime, and ensure the continuity of essential services during emergencies or system failures.

Cryptography Usage Policy

1. Introduction

This Cryptography Usage Policy outlines the guidelines and requirements for the use of cryptographic methods and tools within Jack County. Cryptography plays a crucial role in ensuring the confidentiality, integrity, and authenticity of sensitive information and communications. This policy aims to promote secure and responsible use of cryptography while safeguarding the interests and assets of Jack County.

2. Policy Scope

This policy applies to all employees, contractors, and third-party entities that have access to Jack County's information systems, networks, and data. It encompasses the use of both symmetric and asymmetric encryption algorithms, cryptographic keys, digital signatures, and related cryptographic technologies.

3. Encryption Requirements

a. Encryption of Sensitive Data: All sensitive information stored or transmitted by Jack County shall be encrypted using approved cryptographic algorithms and key lengths appropriate for the level of sensitivity.

b. Encryption for Mobile Devices: All mobile devices, including laptops, smartphones, and tablets, that store or access Jack County's sensitive information must employ strong encryption for data at rest and data in transit.

c. Encryption for Network Traffic: Encryption protocols such as SSL/TLS must be utilized for secure transmission of data across public or untrusted networks.

d. Encryption for Remote Access: Remote access to Jack County's networks and systems must employ secure VPN connections or other approved encryption mechanisms.

4. Key Management

a. Key Generation: Cryptographic keys must be generated using approved methods and cryptographic algorithms.

b. Key Storage: Keys must be stored securely and protected from unauthorized access, theft, loss, or disclosure.

c. Key Exchange: Key exchange protocols should be employed to establish secure communication channels and protect against unauthorized interception or tampering.

d. Key Lengths and Algorithms: The use of strong cryptographic algorithms and key lengths in accordance with industry best practices and standards is mandatory.

e. Key Rotation: Keys used for encryption and digital signatures should be rotated periodically to mitigate the risk of compromise.

5. Cryptographic Operations

a. Cryptographic Module Standards: All cryptographic modules, including hardware and software, must comply with recognized industry standards and certifications.

b. Cryptographic Protocols: Only approved cryptographic protocols and algorithms should be used, avoiding weak or deprecated algorithms known to have vulnerabilities.

c. Digital Signatures: Digital signatures shall be used to ensure the authenticity, integrity, and non-repudiation of critical information and documents.

d. Cryptographic Hash Functions: Cryptographic hash functions must be used to verify the integrity of data and protect against unauthorized modifications.

6. Key Escrow

a. Escrow for Encryption Keys: Encryption keys used to protect Jack County's sensitive information must be escrowed or otherwise safeguarded against key loss to prevent data loss.

b. Escrow for Digital Certificates: Digital certificates used for encryption, digital signatures, or other cryptographic purposes must be securely managed and backed up.

7. Compliance Monitoring

Jack County reserves the right to monitor and audit all cryptographic activities to ensure compliance with this policy. Any violations or suspected breaches of this policy shall be reported immediately to the appropriate authority.

8. Policy Review

This policy will be reviewed regularly to ensure its effectiveness and compliance with evolving cryptographic standards, industry best practices, and legal or regulatory requirements.

9. Non-Compliance

Failure to comply with this Cryptography Usage Policy may result in disciplinary actions, including but not limited to revocation of access privileges, employment termination, and legal consequences in accordance with applicable laws and regulations.

It is recommended to involve legal and cybersecurity experts in the policy development and review process.

Data and Asset Classification Policy

1. Purpose

The purpose of this policy is to establish guidelines for the classification and protection of data and assets within Jack County. This policy ensures the appropriate handling, access, and security measures are implemented to safeguard sensitive information.

2. Scope

This policy applies to all employees, contractors, vendors, and any other individuals or entities accessing, processing, or storing data and assets belonging to Jack County.

3. Data Classification

3.1. Confidential Data: This category includes information that, if disclosed, could have a significant adverse impact on the operations, reputation, or legal compliance of Jack County. Examples include personally identifiable information (PII), financial data, trade secrets, and sensitive internal communications.

3.2. Internal Data: This category includes information that is intended for internal use within Jack County. Although the impact of disclosure may not be as severe as confidential data, it is still essential to protect this information from unauthorized access. Examples include internal reports, policies, and non-public project information.

3.3. Public Data: This category includes information that is intended for public dissemination and does not require any special protection measures. Examples include press releases, publicly available reports, and information on the Jack County website.

4. Asset Classification

4.1. Critical Assets: These assets are essential to the operations of Jack County and require the highest level of protection. They may include servers, network infrastructure,

databases, and any other assets that, if compromised, could significantly impact the county's operations and security.

4.2. Sensitive Assets: These assets may not be critical to operations but still require protection to prevent unauthorized access. Examples include desktops, laptops, mobile devices, and removable media.

4.3. General Assets: These assets have no specific sensitivity requirements and are subject to standard security practices. Examples include office furniture, general-use equipment, and publicly accessible systems.

5. Responsibilities

5.1. Data Owners: Each data asset within Jack County shall have an assigned data owner who is responsible for classifying the data, identifying appropriate protection measures, and ensuring compliance with this policy.

5.2. Asset Owners: Each asset within Jack County shall have an assigned asset owner who is responsible for classifying the asset, implementing security controls, and maintaining its integrity and availability.

5.3. Employees and Users: All employees and users must adhere to the classification and protection requirements as defined by this policy. They should only access and handle data and assets that are necessary for their job functions, and report any suspected or actual breaches or security incidents promptly.

6. Security Controls

6.1. Access Controls: Access to classified data and assets shall be granted based on the principle of least privilege. Access permissions should be reviewed periodically and revoked when no longer necessary.

6.2. Data Encryption: Confidential and sensitive data should be encrypted when stored, transmitted, or accessed remotely to ensure its confidentiality and integrity.

6.3. Physical Security: Critical and sensitive assets should be physically secured in locked rooms, cabinets, or racks. Access to these areas should be restricted and monitored.

6.4. Network Security: Robust network security measures, including firewalls, intrusion detection systems, and encryption protocols, should be implemented to protect classified data and assets from unauthorized access or tampering.

6.5. Data Disposal: When data or assets are no longer required, they should be disposed of securely using approved methods, such as shredding documents or securely wiping electronic storage media.

7. Training and Awareness

Jack County shall provide regular training and awareness programs to employees and users regarding the classification and protection of data and assets. Training should cover the policy guidelines, security best practices, and procedures for reporting security incidents.

8. Compliance and Monitoring

Compliance with this policy shall be monitored through regular audits, assessments, and incident tracking. Non-compliance may result in disciplinary action, up to and including termination of employment or contractual relationships.

9. Policy Review

This policy will be reviewed and updated annually or as needed to ensure its effectiveness and alignment with evolving security threats and regulatory requirements.

10. Policy Acceptance

All employees, contractors, vendors, and other users who access Jack County's data and assets must read, understand, and comply with this policy. By accessing the county's resources, they acknowledge their acceptance of this policy.

This Data and Asset Classification Policy is effective as of the date of approval and supersedes any previous policies or guidelines related to data and asset classification within Jack County.

Data Support and Operations Policy

1. Purpose

The purpose of this policy is to establish guidelines and procedures for data support and operations within Jack County. This policy aims to ensure the availability, integrity, and confidentiality of county data, as well as define roles and responsibilities for data management and operations.

2. Scope

This policy applies to all county employees, contractors, and third-party vendors who have access to Jack County data, including data stored on local servers, cloud platforms, and mobile devices.

3. Data Governance

3.1 Data Ownership and Stewardship

a. Each department head or designated representative shall be responsible for the data generated, collected, or maintained within their respective departments.

b. Data stewards shall be appointed for critical data sets, who will ensure data quality, access control, and compliance with relevant regulations and policies.

3.2 Data Classification

a. All data within Jack County shall be classified based on its sensitivity and criticality, following an established data classification framework.

b. Data classification shall determine appropriate security controls, access privileges, and retention periods.

3.3 Data Retention and Disposal

a. Jack County shall maintain a data retention schedule that defines the duration for which different types of data must be retained.

b. When data is no longer required, it shall be securely disposed of using approved methods, ensuring the destruction of any personal or sensitive information.

4. Data Security

4.1 Access Control

a. Access to Jack County data shall be granted on a need-to-know basis, following the principle of least privilege.

b. User access privileges shall be reviewed regularly and revoked or modified when job roles change or personnel leave the county.

4.2 Data Transmission

a. Sensitive data transmitted over public networks shall be encrypted using industry-standard encryption protocols.

b. Mobile devices used to access or store county data shall be protected with strong passwords or biometric authentication.

4.3 Data Storage

a. County data shall be stored in secure, controlled environments, with appropriate physical and logical access controls in place.

b. Backup and recovery procedures shall be established and regularly tested to ensure data integrity and availability in the event of a disaster.

4.4 Incident Response

a. Jack County shall maintain an incident response plan to address data breaches, unauthorized access, or other security incidents.

b. Security incidents shall be reported promptly to the designated authorities, and appropriate measures shall be taken to mitigate the impact and prevent future occurrences.

5. Data Privacy and Compliance

5.1 Privacy Protection

a. Jack County shall comply with applicable privacy laws and regulations to protect the privacy rights of individuals whose data is collected and processed.

b. Privacy impact assessments shall be conducted for new projects or initiatives involving personal information.

5.2 Compliance Monitoring

a. Regular audits and reviews shall be conducted to ensure compliance with this policy, relevant regulations, and industry best practices.

b. Any identified non-compliance issues shall be promptly addressed, and corrective actions shall be implemented.

6. Training and Awareness

Jack County shall provide training and awareness programs to educate employees about their responsibilities and obligations regarding data management, security, and privacy.

7. Policy Review

This policy shall be reviewed annually or whenever significant changes occur in technology, regulations, or county operations. Amendments to the policy shall be approved by the appropriate county authorities.

By adhering to this Data Support and Operations Policy, Jack County aims to maintain the confidentiality, integrity, and availability of its data while ensuring compliance with relevant laws and regulations.

Data Usage Policy

Introduction

This Data Usage Policy outlines the guidelines and practices for the collection, storage, processing, and usage of data by Jack County. This policy applies to all employees, contractors, and any individual or entity that accesses or utilizes Jack County's data resources. It is designed to ensure the protection, integrity, and responsible use of data in compliance with relevant laws and regulations.

1. Data Collection and Storage

1.1. Jack County will collect and store data only for legitimate and lawful purposes directly related to its official functions and responsibilities.

1.2. The County will collect data in a fair and transparent manner, informing individuals about the purpose and scope of data collection, and obtaining consent when required by applicable laws and regulations.

1.3. Data collected by Jack County shall be accurate, relevant, and limited to what is necessary for the intended purpose. Efforts will be made to minimize the collection of personally identifiable information (PII) unless required for a specific purpose.

1.4. The County will implement appropriate security measures to safeguard the data against unauthorized access, disclosure, alteration, or destruction. Access to data will be granted on a need-to-know basis, and regular assessments will be conducted to identify and address potential vulnerabilities.

2. Data Processing and Usage

2.1. Data processing activities carried out by Jack County shall be consistent with the purpose for which the data was collected. Any additional processing beyond the original purpose will require proper authorization and compliance with relevant legal requirements.

2.2. The County will ensure that data processing is performed in a manner that respects individuals' rights to privacy and data protection, in accordance with applicable laws and regulations.

2.3. Personal data will not be disclosed, sold, rented, or otherwise shared with third parties without the explicit consent of the individuals concerned, except as required by law or when necessary for legitimate purposes directly related to Jack County's functions.

2.4. Jack County will retain data only for as long as necessary to fulfill the purpose for which it was collected, or as required by law or legal obligations. Once data is no longer needed, it will be securely disposed of or anonymized to protect individuals' privacy.

3. Data Access and Rights

3.1. Individuals whose data is collected by Jack County have the right to access, correct, and update their personal information held by the County, subject to legal and regulatory restrictions.

3.2. Requests for accessing or amending personal data should be submitted in writing to the designated contact person within the office in which the data is held at Jack County. The County will respond to such requests promptly and in accordance with applicable laws.

3.3. Jack County will provide appropriate training and resources to its employees and contractors regarding data protection, privacy, and the responsible use of data resources.

4. Compliance and Accountability

4.1. Jack County is committed to complying with all applicable laws, regulations, and standards relating to data protection, privacy, and security.

4.2. The County will regularly review and update this Data Usage Policy to reflect changes in the legal and regulatory landscape or the County's data management practices.

4.3. Any breaches or suspected breaches of this policy, data breaches, or non-compliance with data protection regulations must be promptly reported to the appropriate authority within Jack County.

4.4. Violations of this policy may result in disciplinary actions, up to and including termination of employment or contractual agreements, and legal consequences as per applicable laws.

Conclusion

This Data Usage Policy is intended to ensure the responsible and ethical use of data by Jack County, promoting transparency, privacy, and security. By adhering to this policy, all individuals accessing or utilizing Jack County's data resources contribute to the protection of individuals' privacy rights and the overall integrity of the data managed by the County.

Email Usage Policy

1. Introduction and Purpose:

The county email usage policy helps employees use their county email addresses appropriately. Email is essential to our everyday jobs. We want to ensure that our employees understand the limitations of using their county email accounts.

Our goal is to protect our confidential data from breaches and safeguard our reputation and technological property.

2. Scope:

This policy applies to all employees, vendors and partners who are assigned (or given access to) a county email. This email may be assigned to an individual (e.g. employeename@countydomain) or department (e.g. hr@countydomain.)

3. Email Usage

County emails are powerful tools that help employees in their jobs. Employees should use their county email primarily for work-related purposes. However, we want to provide employees with some freedom to use their emails for personal reasons.

We will define what constitutes appropriate and inappropriate use.

3.1 Inappropriate use of county email

Our employees represent our company whenever they use their corporate email address. They must not:

- Sign up for illegal, unreliable, disreputable or suspect websites and services.
- Send unauthorized marketing content or solicitation emails.
- Register for a non-county business unless authorized.
- Send insulting or discriminatory messages and content.
- Intentionally spam other people's emails, including their coworkers.

The County has the right to monitor and archive corporate emails.

3.2 Appropriate use of county email

Employees are allowed to use their county email for work-related purposes without limitations. For example, employees can use their email to:

- Communicate with current or prospective customers and partners.
- Log in to online accounts they have legitimate access to.
- Give their email address to people they meet at conferences, or other county events for business purposes.
- Sign up for newsletters, platforms and other online services that will help them with their jobs or professional growth.

3.3 Personal Use

Employees are allowed to use their county email for some personal reasons. For example, employees can use their county email to:

- Register for classes.
- Send emails to friends and family as long as they don't spam or disclose confidential information.

Employees must adhere to this policy at all times.

3.4 Email Security

Email is often the medium of hacker attacks, confidentiality breaches, viruses and other malware. These issues can compromise our reputation, legality and security of our equipment.

Employees must:

- Select strong passwords with at least eight characters (capital and lower-case letters, symbols and numbers) without using personal information (e.g. birthdays.)
- Remember passwords instead of writing them down and keep them secret.
- Change their email password on a regular basis.

Also, employees should always be vigilant to catch emails that carry malware or phishing attempts. We instruct employees to:

- Avoid opening attachments and clicking on links when content is not adequately explained (e.g. "Watch this video, it's amazing.")
- Be suspicious of clickbait titles.

- Check email and names of unknown senders to ensure they are legitimate.
- Look for inconsistencies or style red flags (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)

If an employee isn't sure that an email they received is safe, they can ask the IT Department.

We remind our employees to keep their anti-virus programs updated.

4. Disciplinary Action

Employees who don't adhere to the present policy will face disciplinary action up to and including termination. Example reasons for termination are:

- Using a county email address to send confidential data without authorization.
- Sending offensive or inappropriate emails.
- Using a county email for an illegal activity.

Cyber Incident Response Policy

1. PURPOSE

The purpose of this Cyber Incident Response Policy is to establish guidelines and procedures for Jack County to effectively detect, respond to, and mitigate cyber incidents that may pose a threat to the County's information technology infrastructure, data, and operations. This policy aims to minimize the impact of cyber incidents and ensure a prompt, coordinated, and consistent response to safeguard the County's digital assets and maintain the confidentiality, integrity, and availability of critical information.

2. SCOPE

This policy applies to all employees, contractors, and authorized users who have access to Jack County's information technology systems, network resources, and data.

3. DEFINITIONS

a) Cyber Incident: Any unauthorized or unexpected event that may have an adverse effect on the confidentiality, integrity, or availability of information and/or the County's IT resources.

b) Incident Response Team (IRT): A designated team responsible for coordinating the response to cyber incidents.

c) Incident Severity Levels:

- Level 1: Low impact, localized incident with minimal immediate risk.
- Level 2: Moderate impact, potentially affecting multiple systems or users.
- Level 3: High impact, widespread incident with significant risk to critical systems or data.

4. CYBER INCIDENT REPORTING

a) All personnel are required to report any suspected or confirmed cyber incidents immediately to the designated Incident Response Team (IRT) via the County's incident reporting channels.

b) Incident reporting channels shall be well-publicized and readily accessible to all County employees and users.

5. INCIDENT RESPONSE TEAM (IRT)

a) The County shall establish an Incident Response Team (IRT) comprising representatives from IT, law enforcement, legal, communications, relevant department head, and Texas Association of Counties Risk Management Team. The IRT shall be responsible for leading the response to cyber incidents.

b) The IRT members shall undergo regular training and drills to ensure their readiness in responding to cyber incidents.

6. INCIDENT HANDLING PROCEDURE

a) The IRT shall categorize each reported incident based on its severity level.

b) For each incident, the IRT shall follow predefined procedures for containment, eradication, recovery, and lessons learned, considering the specific incident type.

c) The IRT shall document all actions taken during the incident response process, including communications and outcomes.

7. COMMUNICATIONS

a) The IRT shall be responsible for coordinating all internal and external communications regarding the cyber incident.

b) External communication shall be carefully managed to avoid disclosing sensitive information that may jeopardize the investigation or pose additional risks.

c) Communications with the media and the public shall be centralized and conducted by authorized personnel only.

8. LESSONS LEARNED

a) After resolving a cyber incident, the IRT shall conduct a thorough post-incident analysis to identify weaknesses and areas of improvement in the incident response process.

b) Lessons learned from each incident shall be documented and incorporated into future incident response planning and training.

9. REVIEW AND UPDATES

This policy shall be reviewed annually or as needed and may be updated to reflect changes in technology, regulations, or organizational requirements.

Insider Threat Protection Policy

1. Introduction

This Insider Threat Protection Policy outlines the measures and guidelines that must be followed by all employees, contractors, and vendors of Jack County to protect against potential insider threats. Insider threats pose a significant risk to the organization's security, privacy, and integrity of sensitive information. This policy aims to ensure the identification, prevention, detection, and response to such threats to maintain the confidentiality, availability, and integrity of county resources and data.

2. Definition of Insider Threat

An insider threat refers to any potential or actual harm to Jack County's information systems, data, or operations arising from individuals within the organization who misuse their access, privileges, or knowledge to compromise security and violate county policies or laws.

3. Responsibilities

3.1. County Administration: The County Administration is responsible for overseeing the implementation and enforcement of this policy. They will designate a designated individual or team responsible for managing insider threat prevention efforts.

3.2. Employees, Contractors, and Vendors: All personnel with access to Jack County's systems, data, and facilities are responsible for understanding and complying with this policy. They should report any suspicious activities or potential insider threats they encounter.

4. Insider Threat Prevention Measures

4.1. Security Awareness Training: All employees, contractors, and vendors must undergo regular security awareness training, emphasizing the significance of insider threats, recognizing potential warning signs, and reporting suspicious activities.

4.2. Access Controls: Limit access privileges to the minimum necessary for individuals to perform their job duties effectively. Regularly review and update access rights based on job roles and responsibilities.

4.3. Separation of Duties: Implement separation of duties where feasible to prevent any single individual from having excessive control over critical systems or sensitive data.

4.4. Monitoring and Auditing: Regularly monitor and audit user activities, network traffic, and system logs to identify and investigate abnormal behavior or unauthorized access attempts.

4.5. Reporting Mechanism: Establish a confidential reporting mechanism for employees to report potential insider threats without fear of retaliation.

4.6. Incident Response Plan: Develop and maintain an insider threat incident response plan that outlines the steps to be taken in the event of a suspected or confirmed insider threat incident.

4.7. Background Checks: Conduct thorough background checks for new hires (when applicable), contractors, and vendors with access to sensitive information or critical systems.

4.8. Third-Party Oversight: Implement a comprehensive vendor management program to assess and monitor the security posture of third-party vendors handling county data.

5. Incident Response and Investigation

5.1. Incident Reporting: Any suspected insider threat or unusual behavior must be promptly reported to the designated authority or the IT department.

5.2. Investigation: Upon receiving a report, the designated authority will initiate a thorough investigation following the incident response plan.

5.3. Preservation of Evidence: Preserve all relevant evidence to aid in the investigation process.

5.4. Legal and HR Involvement: Engage legal and human resources departments to address legal and personnel-related aspects of the incident.

6. Policy Compliance and Enforcement

6.1. Compliance Monitoring: Regularly review and assess compliance with this policy and associated procedures.

6.2. Consequences of Non-Compliance: Violations of this policy may result in disciplinary action, up to and including termination of employment or contract.

7. Policy Review

This policy will be subject to periodic review and updates as necessary to adapt to changing technology, security threats, and organizational requirements.

Adhering to this Insider Threat Protection Policy is critical for maintaining the security and trust of Jack County's resources and information. All individuals associated with the organization must be vigilant, cooperative, and proactive in preventing and responding to insider threats.

Internet Usage Policy

1. Purpose

The purpose of this Internet Usage Policy is to establish guidelines and rules for the appropriate and responsible use of the Internet and other network resources in Jack County. This policy aims to ensure the security, reliability, and ethical use of internet services and to protect the County's information technology infrastructure.

2. Scope

This policy applies to all employees, contractors, vendors, volunteers, and any other individuals granted access to Jack County's internet and network resources.

3. Acceptable Use

3.1. Internet and network resources provided by Jack County are to be used solely for official County business purposes. Incidental and occasional personal use is permitted as long as it does not interfere with job duties, consume excessive resources, or violate any other provision of this policy.

3.2. Employees are expected to use the Internet responsibly and in compliance with all applicable laws and regulations, including but not limited to copyright laws, software licensing agreements, and data protection laws.

3.3. Employees should not access, download, or distribute any materials that are offensive, inappropriate, discriminatory, defamatory, or that violate any County policies or laws.

4. Prohibited Activities

4.1. Unauthorized Access: Attempting to access, or actually accessing, any unauthorized systems, accounts, or data is strictly prohibited.

4.2. Malicious Software: Downloading, installing, or distributing any form of malicious software, including viruses, worms, spyware, or ransomware, is strictly prohibited.

4.3. Hacking and Intrusion: Engaging in any activities that compromise the security or integrity of Jack County's information systems or networks is prohibited.

4.4. Unauthorized Sharing: Sharing or disclosing sensitive County information without proper authorization is strictly prohibited.

4.5. Network Disruption: Any actions that disrupt or degrade the performance of the County's network or internet services are prohibited.

4.6. Bandwidth-Intensive Activities: Employees should refrain from bandwidth-intensive activities (e.g., streaming, file sharing) that could negatively impact the overall network performance.

4.7. Personal Gain: Using the County's internet or network resources for personal financial gain or any illegal activities is strictly prohibited.

5. Social Media Usage

5.1. Employees representing Jack County through official social media accounts should adhere to the County's Social Media Policy.

5.2. Employees should exercise caution when using personal social media accounts to ensure they do not post any information that may reflect negatively on the County or violate any confidentiality obligations.

6. Enforcement

6.1. Violations of this Internet Usage Policy may result in disciplinary action, up to and including termination of employment or contract, and potential legal consequences.

6.2. The County reserves the right to monitor internet and network activities to ensure compliance with this policy.

7. Reporting

7.1. Employees who become aware of any violations or security incidents related to the County's internet usage should report them to their immediate supervisor or the IT department.

8. Policy Review

8.1. This policy will be reviewed periodically and updated as needed to reflect changes in technology, regulations, and business needs.

By using Jack County's internet and network resources, individuals agree to comply with this policy and all applicable laws and regulations. Failure to adhere to this policy may result in disciplinary action.

Mobile Device Policy

1. Purpose

The purpose of this Mobile Device Policy is to establish guidelines for the appropriate use and management of mobile devices owned by Jack County and issued to its employees, contractors, and authorized users. This policy aims to protect sensitive information, maintain network security, and ensure responsible and productive use of mobile devices.

2. Scope

This policy applies to all employees, contractors, and authorized users who have been provided with mobile devices owned by Jack County or those who access the organization's network using personal mobile devices.

3. Acceptable Use

3.1. Mobile devices provided by Jack County are intended for official business use only. Users are expected to exercise responsible and professional behavior while using these devices.

3.2. Users must not use mobile devices for personal activities that are unrelated to work, except during authorized break times.

3.3. The installation of unauthorized applications or software on Jack County-issued mobile devices is prohibited.

3.4. Users are responsible for safeguarding their mobile devices from loss, theft, or damage and must report any incidents promptly to their supervisors or IT support.

4. Data Security

4.1. Users must adhere to all data security policies, including but not limited to those related to data classification, access control, and data encryption.

4.2. Confidential and sensitive information must not be stored on mobile devices unless explicitly authorized and encrypted appropriately.

4.3. In case of a lost or stolen mobile device, the user must immediately report the incident to IT support to initiate remote wipe procedures if necessary.

5. Passwords and Authentication

5.1. Users must set a strong password or PIN to protect access to their mobile devices. Devices should be configured to automatically lock after a reasonable period of inactivity.

5.2. Biometric authentication methods, if available, should be encouraged for an added layer of security.

6. Mobile Device Management (MDM)

6.1. Jack County may implement Mobile Device Management (MDM) solutions to monitor, manage, and secure mobile devices. Users must comply with all MDM policies and settings.

6.2. Jack County reserves the right to remotely manage and wipe devices if there is a breach of security or a violation of this policy.

7. Reporting Security Incidents

7.1. Users must report any suspected security incidents, lost devices, or unauthorized access to mobile devices promptly to the IT support team.

7.2. If an employee leaves Jack County or loses possession of their issued mobile device, they must return the device and any associated accessories immediately.

8. Training and Awareness

8.1. Jack County will provide training and awareness programs on mobile device security and this policy to all employees and authorized users.

9. Policy Non-Compliance

9.1. Failure to comply with this policy may result in disciplinary actions, which may include temporary or permanent revocation of mobile device privileges, or other appropriate consequences as determined by Jack County.

10. Policy Review

10.1. This policy will be reviewed regularly to ensure relevance and compliance with changing security requirements and technology.

By adopting and adhering to this Mobile Device Policy, Jack County aims to protect its information assets, maintain network security, and promote responsible mobile device usage among its employees and authorized users.

Network Security Policy

1. Introduction

This Network Security Policy outlines the guidelines and procedures for ensuring the security and integrity of Jack County's computer network and information systems. The policy aims to safeguard sensitive data, prevent unauthorized access, and protect against potential security threats and breaches.

2. Scope

This policy applies to all employees, contractors, vendors, and any other individuals granted access to Jack County's network and information systems.

3. Access Controls

3.1 User Authentication

Users must authenticate themselves using unique, strong passwords to access the network resources.

Multi-factor authentication (MFA) will be implemented for privileged accounts and remote access.

Passwords must be changed periodically and should not be shared with anyone.

User accounts of former employees and contractors must be promptly disabled or removed.

3.2 Privileged Access

Privileged access will be granted only on a need-to-know basis.

System administrators will have separate privileged accounts for administrative tasks.

Privileged sessions must be logged and monitored.

4. Network Infrastructure Security

4.1 Firewalls and Intrusion Detection/Prevention Systems (IDS/IPS)

Firewalls will be deployed to control traffic and block unauthorized access.

IDS/IPS will be employed to detect and prevent intrusions and malicious activities.

4.2 Network Segmentation

The network will be divided into separate segments based on sensitivity and access requirements.

Access between segments will be strictly controlled and monitored.

4.3 Wireless Network Security

Wireless networks will be secured using strong encryption methods (WPA2/WPA3).

Wireless access points will be regularly patched and monitored for unauthorized access.

5. Data Protection

5.1 Data Classification

All data will be classified based on its sensitivity level (e.g., confidential, internal use, public).

Access controls and encryption will be applied based on data classification.

5.2 Data Encryption

Sensitive data, especially when transmitted over public networks, will be encrypted using approved encryption methods.

5.3 Backup and Recovery

Regular backups of critical data will be performed and stored in secure locations.

Backup integrity and recovery procedures will be periodically tested.

6. Software Security

6.1 Patch Management

All software, including operating systems and applications, will be promptly patched and updated.

Critical security patches will be prioritized for immediate implementation.

6.2 Antivirus and Anti-Malware

Antivirus and anti-malware solutions will be deployed on all networked devices.

Definitions will be kept up to date, and regular scans will be conducted.

7. Incident Response

7.1 Incident Reporting

Employees must report any suspected or confirmed security incidents to the IT department immediately.

The incident response team will promptly investigate and take appropriate action.

7.2 Incident Handling

A detailed incident response plan will be maintained and reviewed regularly.

The goal will be to minimize the impact of incidents, restore services, and prevent recurrence.

8. Employee Training and Awareness

8.1 Security Awareness Training

All employees will receive regular training on network security best practices.

Training will cover topics such as phishing awareness, password security, and social engineering.

9. Compliance and Monitoring

9.1 Compliance

The network security policy will comply with all applicable laws, regulations, and industry standards.

9.2 Monitoring

Network activity will be continuously monitored for security breaches, anomalies, and unauthorized access.

10. Policy Review

This Network Security Policy will be reviewed annually or as needed to address emerging security threats and changes in the county's network infrastructure.

By adhering to this Network Security Policy, Jack County aims to protect its sensitive information, maintain the integrity of its systems, and ensure a secure computing environment for all authorized users.

Patch Management Policy

1. Purpose

This Patch Management Policy outlines the procedures and guidelines for maintaining the security and stability of Jack County's information technology (IT) infrastructure. The purpose of this policy is to ensure that all software and systems within the county are up-to-date with the latest security patches and updates, reducing the risk of security breaches and ensuring the efficient operation of county services.

2. Policy Scope

This policy applies to all departments, employees, contractors, and third-party vendors with access to Jack County's IT systems and infrastructure.

3. Patch Management Responsibilities

3.1. IT Department: The IT department is responsible for overseeing the patch management process and ensuring its proper implementation. This includes:

a. Identifying critical systems and software that require regular patching.

b. Testing patches in a controlled environment before deploying them to production systems.

c. Developing a patch deployment schedule and adhering to it.

d. Maintaining records of patch application and system update history.

3.2. Department Heads: Department heads are responsible for ensuring that all systems and software used within their respective departments comply with the patch management policy. They must promptly report any patch-related issues or concerns to the IT department.

3.3. Employees: All employees must cooperate with the IT department in applying patches promptly on their workstations and devices. They must also report any unusual behavior or issues related to software or systems immediately.

4. Patch Management Process

4.1. Patch Identification: The IT department will regularly monitor software vendors' security advisories and official sources to identify patches and updates. Critical patches will be given priority.

4.2. Testing: Before deploying any patches to production systems, the IT department will thoroughly test them in a non-production environment to ensure compatibility and assess potential impacts on existing systems.

4.3. Patch Deployment: The IT department will schedule regular maintenance windows for patch deployment. This will be communicated in advance to all relevant parties. Urgent security patches may be deployed outside of regular maintenance windows when necessary.

4.4. Backup and Rollback: Prior to patch deployment, a complete backup of critical systems will be taken to allow for rollbacks in case of any unforeseen issues during the patching process.

4.5. Monitoring and Reporting: The IT department will monitor the status of all deployed patches and system updates. Any failed or incomplete patches will be addressed promptly. Patch management reports will be generated periodically for review by management.

5. Exceptions

5.1. In exceptional circumstances, temporary exemptions from the patch management policy may be granted by the IT department. Such exceptions must be properly documented, and a timeline for compliance with the policy must be established.

6. User Awareness and Training

6.1. Regular user awareness sessions will be conducted to educate employees about the importance of patching and the role it plays in maintaining the security and integrity of the county's IT infrastructure.

7. Policy Review

7.1. This Patch Management Policy will be reviewed annually or as needed by the IT department to ensure it remains effective and aligned with best practices and security standards.

8. Policy Compliance and Enforcement

8.1. Non-compliance with this policy may result in disciplinary action, which may include but is not limited to, warnings, suspension of IT system access, or termination of employment or contractual agreements.

By following this Patch Management Policy, Jack County aims to minimize security risks and maintain a stable and efficient IT environment.

Ransomware Detection Policy

Policy Statement:
This Ransomware Detection Policy outlines the procedures and guidelines for detecting, preventing, and responding to ransomware threats within Jack County. Ransomware poses a significant risk to the security and continuity of our operations, and it is crucial to have a robust framework in place to identify and mitigate these threats promptly.

1. Purpose:
The purpose of this policy is to establish a clear framework for the detection of ransomware threats within Jack County, ensuring the protection of sensitive data, the continuity of services, and the preservation of our reputation.

2. Scope:
This policy applies to all employees, contractors, vendors, and anyone with access to Jack County's information systems and data.

3. Definitions:
- Ransomware: Malicious software that encrypts data and demands a ransom in exchange for the decryption key.

- Detection: The process of identifying ransomware threats and unauthorized access to data and systems.

4. Ransomware Detection Measures:
4.1. Endpoint Protection:
- All endpoints, including computers and mobile devices, shall have up-to-date antivirus and antimalware software installed and enabled.

- Regularly schedule automatic scans of all endpoints to identify potential ransomware infections.

4.2. Email Security:
- Implement email filtering solutions to detect and quarantine suspicious attachments and links.

- Educate employees on recognizing phishing emails and reporting them promptly.

4.3. Network Monitoring:

- Employ intrusion detection and prevention systems (IDS/IPS) to monitor network traffic for suspicious activities and ransomware signatures.

- Regularly review logs and alerts to identify potential threats.

4.4. Data Backup and Recovery:

- Maintain regular and secure backups of all critical data and systems.

- Test data restoration procedures to ensure timely recovery in case of a ransomware incident.

4.5. User Awareness:

- Provide ransomware awareness training to all employees, emphasizing the importance of safe online practices and the dangers of downloading or opening suspicious files.

5. Incident Response:

- Establish an incident response plan that outlines the steps to take in case of a ransomware incident, including containment, investigation, recovery, and reporting.

- Notify appropriate authorities and stakeholders, such as law enforcement, affected individuals, and the County Commissioners, in the event of a significant ransomware incident.

6. Reporting:

- All employees, contractors, and vendors shall promptly report any suspected ransomware activity to the IT department or the designated IT security contact.

7. Compliance and Enforcement:

- Non-compliance with this policy may result in disciplinary actions, including but not limited to warnings, suspension, or termination.

- Periodic audits and assessments shall be conducted to ensure compliance with this policy.

8. Review and Updates:
- This policy shall be reviewed annually and updated as needed to reflect changes in technology, threats, or organizational requirements.

9. Training and Awareness:
- Conduct regular training and awareness programs to ensure that all staff are informed and up-to-date on ransomware detection best practices.

10. Communication:
- Communicate this policy to all employees, contractors, and relevant third parties and ensure they acknowledge their understanding and commitment to compliance.

System Update Policy

Policy Statement:
Jack County is committed to maintaining the security, functionality, and efficiency of its information technology systems. To achieve this goal, the county shall implement a System Update Schedule Policy to ensure that all hardware and software systems receive regular updates and patches to address security vulnerabilities, improve performance, and enhance functionality.

Scope:
This policy applies to all Jack County information technology systems, including servers, workstations, laptops, mobile devices, network equipment, and software applications.

Policy Objectives:
1. To minimize security risks by promptly applying security updates and patches.

2. To improve system performance and reliability through regular updates.

3. To maintain compliance with software licensing agreements.

4. To enhance the functionality of systems and applications.

Responsibilities:
1. IT Department:
- The IT department shall be responsible for planning, scheduling, and implementing system updates and patches.

- The IT department shall maintain an inventory of all hardware and software systems to track update requirements.

- The IT department shall perform regular vulnerability assessments to identify critical update needs.

2. System Owners:
- Each department or division shall designate a system owner responsible for coordinating with the IT department regarding system updates.

- System owners shall report any system-related issues to the IT department promptly.

System Update Schedule:

1. Security Updates:
   - Critical security updates shall be applied within 30 days of release.
   - High-priority security updates shall be applied within 60 days of release.
   - Regular security updates shall be applied within 90 days of release.

2. Software Updates:
   - Operating system updates shall be applied within 60 days of release.
   - Application software updates shall be applied within 90 days of release.

3. Hardware Updates:
   - Firmware and driver updates for hardware components shall be applied within 90 days of release.

4. Testing:
   - All updates shall be tested in a controlled environment before deployment to production systems to minimize disruptions.

5. Notification:
   - System owners shall be notified at least one week in advance of scheduled updates that may impact their operations.
   - Users shall be informed of any expected downtime.

6. Exceptions:
   - Any deviation from the update schedule shall require prior approval from the IT department, with documentation of the reason for the delay.

7. Reporting:
   - The IT department shall maintain records of all system updates, including dates, descriptions, and any issues encountered during the update process.
   - Regular reports on the status of system updates shall be provided to county management.

Wireless Network and Guest Access Policy

Policy Statement:
Jack County recognizes the importance of providing secure and reliable wireless network access to authorized personnel while also accommodating the needs of guests and visitors. This policy outlines the guidelines and procedures for the use of the county's wireless network and guest access.

Scope:
This policy applies to all county employees, contractors, and visitors who access or use the county's wireless network.

Policy Objectives:
1. To ensure the security and integrity of the county's wireless network.
2. To provide authorized employees with reliable and secure wireless access.
3. To accommodate guests and visitors with limited and controlled access.
4. To establish guidelines for acceptable use of the wireless network.

Policy Guidelines:

1. Wireless Network Access for Employees:
   - County employees shall have access to the secure wireless network using their county-issued credentials.
   - The IT department shall enforce strong security measures, including WPA3 encryption and authentication protocols, to protect the wireless network.

2. Guest Access:
   - Guest access to the wireless network shall be provided for authorized visitors and contractors.
   - Access for guests shall be granted through a separate guest network with limited privileges.

- Guests must obtain approval from the appropriate department head or sponsor to access the guest network.

3. Guest Access Procedures:

- County employees sponsoring guest access shall provide the guest access via preestablish guest network credentials.

4. Acceptable Use:

- Users, including employees and guests, shall adhere to the county's acceptable use policy when using the wireless network.

- Unauthorized access or any misuse of the network is strictly prohibited.

5. Security Measures:

- Employees and guests are responsible for maintaining the security of their devices connected to the network.

- Anti-virus software and operating system updates must be kept up to date on all devices.

6. Monitoring:

- Network traffic may be monitored for security and performance purposes.

- The IT department reserves the right to investigate any suspicious or unauthorized activity on the network.

7. Reporting Security Incidents:

- Any security incidents or breaches must be reported immediately to the IT department.

8. Compliance:

- Non-compliance with this policy may result in the revocation of network access privileges and may lead to disciplinary action for county employees.

Date: September 25, 2023

Re: Jack County Cyber Security Policy

The Commissioners Court of Jack County, Texas hereby approves the Cyber Security Policy as outlined in this policy manual until revisions are needed.

County Judge

Pct. 1 Commissioner

Pct. 2 Commissioner

Pct. 3 Commissioner

Pct. 4 Commissioner

FILED FOR RECORD

_____ O'CLOCK _____M

SEP 25 2023

VANESSA JAMES, County Clerk
JACK COUNTY, TEXAS

BY_____ DEPUTY