Section 1: Purpose

This document provides policy, direction, procedures, and guidance to ensure the security, confidentiality, integrity, and availability of electronic information and the information systems that contain it.

Sarpy County shall provide only that access to computers, systems, and information that is required for that individual or agency to perform required tasks and duties. This policy includes both login access to computers, networks and servers, as well as physical access to workstations, systems, wiring closets, and data centers.

The overarching policy for information security is that everything that is not specifically permitted shall be denied. Access is granted or approved by the owner of the system or information, provided by employees of the Information Systems Department, and utilized by the employee or end-user for business purposes. Only authorized personnel are allowed to facilitate or provide access to systems. These include authorized employees of the Information Systems Department of Sarpy County Nebraska, or departmental employees who are authorized to create and administer application-level user accounts and passwords

Section 2: Scope

This policy applies to all automated resources, computers/computer systems, networks, hardware, software and all information, data, applications, functions, files and resources that are owned, paid for, or administered by Sarpy County. This policy applies to all County employees, appointed officials, elected officials, department heads, interns/externs, contractors, business partners, affiliated agencies, vendors, and volunteers.

Anyone using the computing resources of or accessing information from or through Sarpy County information systems or networks is required to abide by these procedures and guidelines. Failure to abide by the provisions of this document may result in disciplinary action up to and including termination of employment. Those not complying with these guidelines may also be subject to criminal prosecution or be held financially liable for damage to equipment, denial of needed resources, loss of data or harm or damage to an individual or entity caused by their action.

Section 3: Exceptions

Requests for exceptions will follow Policy 12: Exception Request Process.

Section 4: Roles and Responsibilities

4.1 Sarpy County

Sarpy County is the organizational entity that owns, secures and establishes policy for the security of all information, resources and facilities under its control, as well as for contractors, tenant organizations, and business partners. Policies may be based on existing laws, rules, regulations, administrative policies and commonly accepted business practices; and will be determined based on the best interests of Sarpy County and its constituents.

4.1.1 The Information Technology Security Policy and all policies within shall be audited for compliance per I.S. auditing procedure.

4.2 Elected Officials / Department Heads

Elected Officials / Department Heads are responsible for all electronic information in their areas, as well as all stored documents, and data archives. Elected Officials / Department Heads are typically Data Stewards (as defined in policy 1, section 4.8). As such, they determine who will be allowed to access their information, consistent with their written department policies, and any applicable laws and regulations. The Elected Official / Department Head may delegate this authority to other individuals within their department or organization. These individuals may act or sign on his or her behalf. He or she will be appointed in writing or via email and will be identified to the Sarpy County Information Systems Department. This individual will assist in disseminating policy and guidance, providing or coordinating training, supporting the Sarpy County Information Security Analyst in monitoring and achieving compliance, and notifying the Security Analyst of actual or suspected incidents. The final responsibility for establishing clear guidance for their data and enforcing security policy lies with the Elected Official / Department Head.

4.3 Information Systems Department

Information Systems Department houses, administers, and operates all servers, infrastructure and security equipment for Sarpy County agencies unless special exceptions are granted. The Information Systems Department is typically the Data Custodian (defined in section 4.7) of the County's information resources and implements the technical policies set forth in this document. The Information Systems Department acts on behalf of Sarpy County and Elected Officials /

Department Heads to secure information, applications, systems and networks, to provide authorized access to approved personnel, and to monitor, detect, investigate and report on actual or suspected security breaches or incidents.

4.4 End-Users/Employees

Employees of Sarpy County, and others accessing County information or computer services, play a key role in maintaining the integrity and security of all of our information systems. Each user of automated services is responsible to understand these rules and guidelines, to abide by them, as well as to identify and report issues and problems. Departments, offices and employees are responsible for training interns/externs, contractors, business partners, affiliated agencies, vendors, and volunteers on the security policies of the County.

4.5 Information Security Advisory Group

Policies are the heart of any compliance program. They form the baseline of organizational will and intent, and in this case, as they pertain to Information Security. The County's information security policies will be created by the Information Security Advisory Group, and approved by the County Board. Policies will be reviewed at least annually, or as often as may be required to respond to changes in laws, technology or other requirements.

4.5.1 The Information Security Advisory Group shall include the following five (5) County permanent members: an Information Security Analyst, the County Information Systems Operations Manager, an Administration Representative, the Information Systems Director, and a Human Resources representative.

4.5.2 The Information Security Advisory Group shall also include the following invited members: no more than two (2) Elected Officials/Department Heads or their designated representatives, as invited by the permanent members.

4.5.3 The Information Security Advisory Group may invite or ask guidance of other departmental or technical representatives and subject matter experts.

4.5.4 The Information Security Advisory Group will be chaired by the Information Security Analyst, who will make meeting notifications to participants, set up room arrangements, and prepare an agenda.

4.5.5 The Information Security Advisory Group will have meetings on a quarterly basis, or more often as needs arise.

4.5.6 The Information Security Advisory Group will receive guidance from Elected Officials/Department Heads for security, in general, and for specific areas of concern in the area of information security.

4.5.7 The Information Security Advisory Group will recommend procedures for training, investigations, monitoring, compliance, enforcing these policies, and any other areas that would prove beneficial to Elected Officials / Department Heads in the area of information security.

4.5.8 The Information Security Advisory Group will act in a consultative or advisory capacity to Elected Officials / Department Heads in all areas pertaining to information security.

4.5.9 The Information Security Advisory Group will act as an advisory organization and information resource in the area of security to County departments.

4.5.10 The Information Security Advisory Group itself is not an enforcement entity. It is strictly advisory in nature.

4.6 Affiliated Agencies or Business Partner

Affiliated agencies or business partners are departments or agencies who are members of, or occupying space within, the Sarpy County Campus area, but whose networking and/or computer support comes from an external entity. Examples of this are the Courts and the Department of Motor Vehicles. Entities in this category shall abide by these policies when utilizing County resources and networks and shall follow their security policies on their networks.

4.7 Data Custodian

A Data Custodian is an employee of the County who has administrative and/or operational responsibility over County Data. Generally, the Information Technology Department is the Data Custodian. A Data Custodian is responsible for the following:

4.7.1 **Understanding and reporting on how County Data is stored, processed and transmitted by the County and by third-party Agents of the County.** Understanding and documenting how County Data is being stored, processed and transmitted is the first step toward safeguarding that data. Without this knowledge, it is difficult to implement or validate safeguards in an effective manner. One method of performing this assessment is to create a data flow diagram for a subset of data that illustrates the system(s) storing the data, how the data is being processed and how the data traverses the network. Data flow diagrams can also illustrate security controls as they are implemented. Regardless of approach, documentation should exist and be made available to the appropriate Data Steward. (See Illustration 4.7.1 Data Flow diagram example, herein.)

4.7.2 **Implementing appropriate physical and technical safeguards to protect the confidentiality, integrity and availability of County Data.** The Information Security Advisory Group has published guidance on implementing reasonable and appropriate security controls for three (3) classifications of data: public, private and restricted. Contractual obligations, legal or regulatory requirements, and industry standards also play an important role in implementing appropriate safeguards. Data Custodians should work with Data Stewards to gain a better understanding of these requirements. Data Custodians should also document what security controls have been implemented and where gaps exist in current controls. This documentation should be made available to the appropriate Data Steward.

4.7.3 **Documenting and disseminating administrative and operational procedures to ensure consistent storage, processing and transmission of County Data.** Documenting administrative and operational procedures goes hand in hand with understanding how data is stored, processed and transmitted. Data Custodians should document as many processes as possible. This will help ensure that County Data is handled in a consistent manner. This will also help ensure that safeguards are being effectively leveraged.

4.7.4 **Provisioning and de-provisioning access to County Data as authorized by the Data Steward.** Data Custodians are responsible for applying and removing access based on criteria established by the appropriate Data Steward. As specified above, standard procedures for applying and removing access should be documented and made available to the appropriate Data Steward.

4.7.5 **Understanding and reporting on security risks and how they impact the confidentiality, integrity and availability of Institutional Data.** Data Custodians should have a thorough understanding of security risks impacting data. For example, storing or transmitting restricted data in an unencrypted form is a security risk. Protecting access to data using a weak password and/or not patching a vulnerability in a system or application are both examples of security risks. Security risks should be documented and reviewed with the appropriate Data Steward so that he or she can determine whether greater resources need to be devoted to mitigating these risks. The Information Security Analyst can assist Data Custodians with gaining a better understanding of their security risks.

4.8 Data Stewards

A Data Steward is usually an Elected Official / Department Head who oversees the lifecycle of one or more sets of County Data. Responsibilities of a Data Steward include the following:

4.8.1 **Assigning an appropriate classification to County Data.** All County data shall have a particular classification assigned to it. The County has adopted three (3) primary classifications: public, private and restricted. (See *Policy 3 Data Classification* for more information.)

4.8.2 **Assigning day-to-day administrative and operational responsibilities for County Data to one or more Data Custodians.** Data Stewards may assign administrative and operational responsibility to specific employees or groups of employees (usually Information Systems). A Data Steward could also serve as a Data Custodian. In some situations, multiple groups will share Data Custodian responsibilities. If multiple groups share responsibilities, the Data Steward should understand what functions are performed by what group.

4.8.3 **Approving standards and procedures related to day-to-day administrative and operational management of County Data.** While it is the responsibility of the Data Custodian to develop and implement operational procedures for County Data, it is the Data Steward's responsibility to review and approve these standards and procedures. A Data Steward should consider the classification of the data and associated risk tolerance when reviewing and approving these standards and procedures. For example, high risk and/or highly sensitive data may warrant more comprehensive documentation and, similarly, a more formal review and approval process. A Data Steward should also consider his or her relationship with the Data Custodian(s). For example, different review and approval processes may be appropriate based on the relationship of the Data Custodian(s) and/or Data Steward(s).

4.8.4 **Determining the appropriate criteria for obtaining access to County Data.** Provisioning access to County data is the responsibility of a Data Custodian. A Data Steward is accountable for determining who has access to County Data. This does not imply that a Data Steward is responsible for the day-to-day provisioning of access. A Data Steward may decide to review and authorize each access request individually or a Data Steward may define a set of rules that determine who is eligible for access based on business function, support role, etc. For example, a simple rule may be that all employees are permitted access to their own personnel file, or all staff members are permitted access to their own health benefits information. These rules should be documented in a clear and concise manner so that they can be easily understood by a Data Custodian.

4.8.5 **Ensuring that Data Custodians implement reasonable and appropriate security controls to protect the confidentiality, integrity and availability of County Data.** The Information Security Advisory Group has published guidance on implementing reasonable and appropriate security controls based on three classifications of data: public, private and restricted. Data Stewards will often have their own security requirements specified in contractual language and/or based on various industry standards. Data Stewards should be familiar with their own unique requirements and ensure that Data Custodians are also aware of and can demonstrate compliance with these requirements.

4.8.6 **Understanding and approving how County Data is stored, processed and transmitted by the County and by third-party Agents of the County.** In order to ensure reasonable and appropriate security controls are implemented, a Data Steward must understand how data is stored, processed and transmitted. This can be accomplished through review of data flow documentation maintained by a Data Custodian. In situations where County Data is being managed by a third-party, the contract or service level agreement should require documentation of how data is or will be stored, processed and transmitted.

4.8.7 **Defining risk tolerance and accepting or rejecting risk related to security threats that impact the confidentiality, integrity and availability of County Data.** Information security requires a balance between security, usability and available resources. Risk management plays an important role in establishing this balance. Understanding what classifications of data are being stored, processed and transmitted will allow Data Stewards to better assess risks. Understanding legal obligations and the cost of non-compliance will also play a role in this decision making.

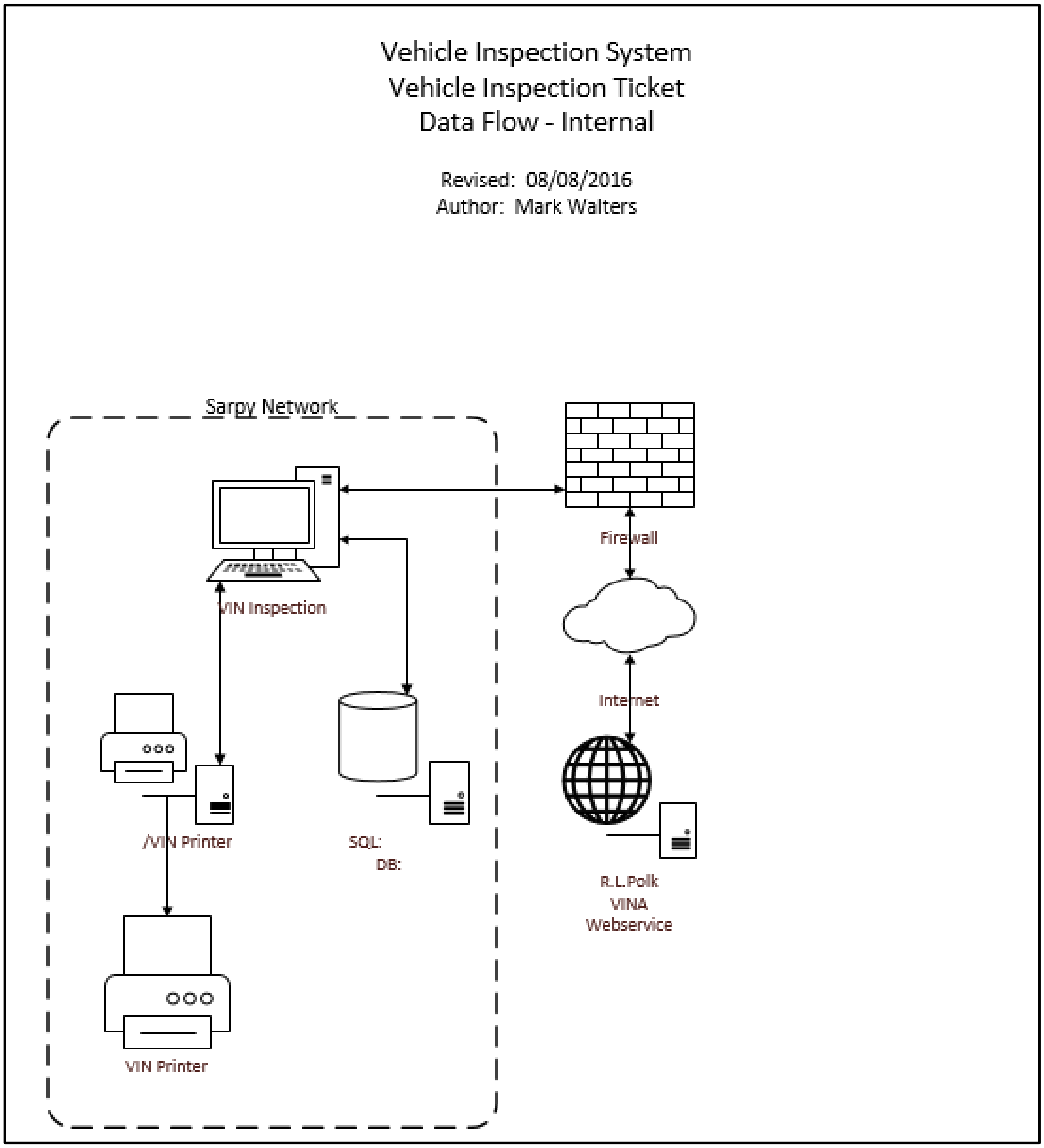
4.9 Application Administrator, and Application Steward / Owner

Applications many times will have an Administrator and/or an Application Steward. These roles play important parts in security and security decisions. In multi-office applications there may be more than one Application Administrator or Application Steward.

4.9.1 An Application Administrator is a person or group that has elevated rights to an application and can manage accounts within the application.

4.9.2 An Application Steward is a person or group that is tasked with the responsibility of making decisions about an application. This position may also be referred to as the application owner. Usually an application steward is an Elected Official / Department Head for which the application is primarily used or the Elected Official / Department Head of the office that purchased the application.

Illustration 4.7.1 – Data Flow Diagram Example



Section 1: Purpose

This document provides policy, direction, procedures and guidance to properly access County information technology equipment, networks, data and resources.

Section 2: Scope

This policy applies to all automated resources, computers/computer systems, networks, hardware, software and all information, data, applications, functions, files and resources that are owned, paid for, or administered by Sarpy County. This policy applies to all County employees, appointed officials, elected officials, department heads, interns/externs, contractors, business partners, affiliated agencies, vendors, and volunteers.

Section 3: Exceptions

Requests for exceptions will follow Policy 12: Exception Request Process.

Section 4: Access Establishment Details

4.1 Access to systems is established through the use of the User Account Request form which is posted on the Intranet. Special consideration should be given to ensure that each Elected Official / Department Head or their designee is following the least privilege rule. The “least privilege rule” means that an individual should be given only that access required to perform his or her assigned tasks and responsibilities.

4.2 Each user will have his or her own unique account credentials, normally defined as the combination of both a username and password. This information is used for determining audits and securing systems.

4.3 When practical, role-based access shall be used to provide consistent, least-privilege access to applications and systems. Elected Officials / Department Heads or their designee shall be responsible for determining application access roles and requirements, and for enforcing, reviewing and managing them.

4.4 Users will not share or be required to share individual or assigned account credentials. On occasion, this may be necessary in which case a policy exception request shall be submitted.

4.5 Special attention should be given when providing access to information that may require written authorization or special training. This is generally referred to as "restricted" data (See Policy 3 – "Data Classification").

4.6 I.S. will audit all user accounts annually. All accounts will be reviewed for currency and applicability. Users who have moved, departed, or no longer require access will be removed from the system or have their accounts updated appropriately.

4.7 Contractors and support personnel may be issued credentials on County systems when sponsored by a County Employee or Department. Care must be taken to ensure they are closely monitored and have access to only the systems authorized. The Contractor shall also be provided any required training and a copy of this security policy to read and review. The County employee, or the department or office sponsoring the individual requesting access, remains responsible for the Contractor until access is terminated.

4.8 Contractors and other non-County personnel will have an expiration date established on their User Account Request form. The expiration date will be the expected ending date of work or 365 days from the creation of the account, whichever is less. The sponsoring County employee, department or office is responsible for providing at least 24 hours' prior written notice to I.S. of when the final date of work for the contractor is expected. This will allow proper scheduling of the deactivation and removal of the user account.

4.9 Elected Officials, County and non-County Department Heads or their designees are required to inform Information Systems of any changes in employee status which could impact access to information. This includes, but is not limited to retirements, termination, transfer, or any personnel investigations or actions which may modify a particular user's access.

Section 5: External Accounts

Most departments or offices have various needs for accounts that exist on external sites (systems not on County hardware). These accounts may be Software as a Service (SaaS), Cloud Computing, or a website that contains information or support resources. Examples of these types of accounts are: ADP, Payroll processing; Microsoft, Licensing information; Cisco, Licensing and Hardware Inventory, etc.…

5.1 Each Elected Official / Department Head should keep an inventory of all employee external accounts that are used for business purposes. Information recorded should include the following (please note a password is not requested):

- **External Resource Name**: The name of the resource that the account is for.
- **Employee Name**: The name of the employee that has the account.
- **Username**: Usually the part of the credentials to log into the account.
- **Email or Phone**: The email address or phone number used to create account.
- **Access type**: Level of access of the external resource (e.g. Admin, Read-only).
- **Description of External Service**: A description of what the service is (e.g. Payroll, Inventory).
- **Any required authentication devices**: A list of the devices that may be needed for secondary (multi-factor) authentication (cell phone, SMS aka texting, application, token, FOB, etc.).

5.2 All external accounts will use an authorized business (work) email address. These addresses are typically username@sarpy.com.

5.3 Each Elected Official / Department Head is responsible for removing access to external accounts for any users separating service.

5.4 Each Elected Official / Department Head will review and update these records on an annual basis and provide the folder location where their external account list is stored to the Information Security Analyst.

Section 6: Electronic Record Access

The following items do not apply to I.T. staff performing authorized support services.

6.1 Access to another user's data, including email, **with** the user's knowledge or approval, shall be executed by a request to the I.S. Department by the Elected Official / Department Head or their designee of that user. I.S. will make a record of the request to ensure proper controls have been followed.

6.2 Access to another user's data, including email, **without** the user's knowledge or approval, shall be executed by a request to the I.S. Department by the Elected

Official / Department Head or their designee of that user and approval of the request by the County Attorney’s Office. I.S. will make a record of the request to ensure proper controls have been followed.

6.3 Access to data of a separated user (e.g. resigned, retired, quit, terminated) shall be executed by a request to the I.S. Department by the Elected Official / Department Head or their designee of that user. I.S. will make a record of the request to ensure proper controls have been followed.

6.4 In the case of a public records request, the County’s Policy on Public Records Requests will be followed. In the absence of a County Public Records Policy, statutory requirements prescribed by the Nebraska Public Records law, and any other applicable law, rule or regulation will be followed.

6.5 In the case of a legal request for data, including email, the County Attorney’s office will review the request and advise I.S. and the appropriate offices what steps need to be taken to fulfill the request. I.S. will make a record of the request to ensure proper controls have been followed. The parties involved in the legal request will be notified at the discretion of the County Attorney’s office.

Section 1: Purpose

The purpose of this Policy is to establish a framework for classifying data based on its level of sensitivity, value and criticality to the County. Classification of data will aid in determining baseline security controls for the protection of data.

Section 2: Scope

This policy applies to all County employees, appointed officials, elected officials, department heads, interns/externs, contractors, business partners, vendors, and volunteers.

Section 3: Exceptions

Requests for exceptions will follow Policy 12: Exception Request Process.

Section 4: Data Classification Details

Data classification, in the context of information security, is the classification of data based on its level of sensitivity and the impact to the County should that data be disclosed, altered or destroyed without authorization. The classification of data helps determine what baseline security controls are appropriate for safeguarding that data. All County data should be classified into one of three sensitivity classifications:

4.1 **Restricted Data.** Data should be classified as “restricted” when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to the County or its affiliates. Examples of restricted data include data protected by state or federal privacy laws or regulations and data protected by confidentiality agreements. The highest level of security controls should be applied to restricted data.

4.2 **Private Data.** Data should be classified as “private” when the unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk to the County or its affiliates. By default, all County Data that is not explicitly classified as restricted or public data should be treated as private data. A reasonable level of security controls should be applied to private data.

4.3 **Public Data.** Data should be classified as “public” when the unauthorized disclosure, alteration or destruction of that data would result in little or no risk to the County and its affiliates. Examples of public data include press releases, County Board minutes and finalized County contracts. While little or no controls are required to protect the confidentiality of public data, some level of control is required to prevent unauthorized modification or destruction of public data.

Section 5: Data Steward

Classification of data should be performed by an appropriate Data Steward using classification guidelines published by the Information Security Advisory Group. Data Stewards are usually Elected Officials / Department Heads who oversee the lifecycle of one or more sets of Data. See Policy 1 - Security Policy for more information on the Data Steward's role and responsibilities.

Section 6: Data Collections

Data Stewards may wish to assign a single classification to a collection of data that is common in purpose or function. When classifying a collection of data, the most restrictive classification of any of the individual data elements should be used. For example, if a data collection consists of an employee's name, address and social security number, the data collection should be classified as restricted even though the employee's name and address may be considered public information.

Section 7: Reclassification

On a periodic basis, it is important to reevaluate the classification of data to ensure the assigned classification is still appropriate based on changes to legal and contractual obligations as well as changes in the use of the data or its value to the County. This evaluation should be conducted by the appropriate Data Steward. Conducting an evaluation on an annual basis is encouraged; however, the Data Steward should determine what frequency is most appropriate based on available resources. If a Data Steward determines that the classification of a certain data set has changed, an analysis of security controls should be performed to determine whether existing controls are consistent with the new classification. If gaps are found in existing security controls, they should be corrected in a timely manner, commensurate with the level of risk presented by the gaps.

Section 8: Calculating Classification

There is no perfect quantitative system for calculating the classification of a particular data element. In some situations, the appropriate classification may be more obvious, such as when federal or state laws require the County to protect certain types of data (e.g. personally identifiable information).

Consideration for data classification should include the following security objectives:

8.1 **Confidentiality.** This involves preserving authorized restriction on information access and disclosure, including means for protecting personal privacy and proprietary information.

8.2 **Integrity.** This means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

8.3 **Availability.** This ensures timely and reliable access to, and use of, information.

Further guidance on the topic of data classification can be found in *NIST Publication 800-60 Guide for Mapping Types of Information and Information Systems to Security Categories*.

Section 1: Purpose

The purpose of this document is to establish policies and procedures for the consistent and correct handling and sanitization of storage mediums.

It shall be the mission of Sarpy County to provide for the security (confidentiality, integrity, availability) of all information systems and resources. Storage of data on both removable and non-removable media is a fundamental part of our systems and infrastructure. Appropriate handling, storage, security and destruction of these media are essential and required. All media will be protected and secured in accordance with the highest level of information stored in any one of its files. Thus, if a single file on a drive contains restricted information, the entire drive must be classified restricted. Media will be physically protected from harm or loss whether or not it is installed or inserted into a target device, workstation or server. Media shall not be left in unprotected or public access locations. This policy will be reviewed annually.

Section 2: Scope

This policy applies to all systems owned by, or connected to, Sarpy County computers or networks. Remote systems are also included, such that equipment in remote locations, employees who are working remotely, contractors, and business-to-business partners may also be covered within the scope of this policy.

Section 3: Exceptions

Requests for exceptions will follow Policy 12: Exception Request Process.

Section 4: Media Sanitization

4.1 Sarpy County will generally adhere to the most current version of the guidelines for media sanitization published by the National Institute of Standards and Technology (NIST). Special Publication 800-88 Guidelines for Media Sanitization.

4.2 Types of Sanitization:

4.2.1 **Clear** applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques; typically applied through the standard Read and Write commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported). An example of this would be to use a secure wipe software on a hard drive.

4.2.2 **Purge** applies physical or logical techniques that render Target Data recovery infeasible using state of the art laboratory techniques. An example of this would be to degauss a hard drive.

4.2.3 **Destroy** renders Target Data recovery infeasible using state of the art laboratory techniques and results in the subsequent inability to use the media for storage of data. An example of this would be to shred a hard drive.

Section 5: Tape

5.1 Tapes will be handled according to the highest level of data classification that they may contain.

5.2 Tapes will be stored in secure locations that meet the manufacturers’ recommended environmental conditions.

5.3 Tape will generally have the “Destroy” method of sanitization.

Section 6: Universal Serial Bus (USB) Storage (e.g. thumb drive, flash drive, external hard drive)

6.1 Use of removable USB drives on Sarpy County equipment should be avoided.

6.2 USB Storage devices used or provided by contractors or vendors for system updates are authorized after the devices are scanned for malware by an air-gapped system.

6.3 USB Storage devices from an unknown origin must be scanned for malware on an air-gapped system prior to using on Sarpy County equipment.

6.4 All USB Storage devices that are no longer needed should be turned into the Information Systems Department for proper sanitization.

Section 7: Optical and Magnetic Media

7.1 Optical media (e.g. CD, DVD, Blu-ray) and magnetic media (e.g. floppy disk, zip disk) should be stored in a controlled environment. Care should be taken to not expose optical media to direct sunlight or heat.

7.2 Optical and magnetic media typically have a short life span and should not be used for archival storage purposes.

7.3 Optical and magnetic media used or provided by contractors or vendors for system updates are authorized after the devices are scanned for malware by an air-gapped system.

7.4 All optical and magnetic media no longer needed should be turned into the Information Systems Department for proper sanitization.

Section 8: Mobile Devices (e.g. Smart Phone, Smart Watch, Activity Tracker, Tablet)

8.1 Mobile devices used for Sarpy County business purposes will be locked when idle and require the use of a passcode/password or biometrics to unlock at all times.

8.2 Mobile devices used for Sarpy County business purposes will not be shared with non-county employees.

8.3 Sarpy County employees will immediately report any lost or stolen mobile devices used for Sarpy County business to Information Systems via the Help Desk line 402-593-4357.

8.4 All mobile devices used for Sarpy County business will be required to maintain current updates within the last 30 days.

8.5 All mobile devices used for Sarpy County business purposes will not be “jail-broken” unless authorized by Information Systems.

8.6 All mobile devices used for Sarpy County business should have County data erased or the device reset to factory default settings prior to trading in or transferring to a third-party. Sarpy County Information Systems is available to assist via the Help Desk line at 402-593-4357.

Section 9: Printer, Multi-function Device, Copier, Fax Machine

9.1 Any device being decommissioned must have all network and/or system settings removed or deleted from the device.

9.2 Copiers or other devices with hard-drives must have a data security system on it to automatically overwrite information on the hard-drive.

9.3 Devices with hard-drives that are decommissioned must have the hard-drive removed and immediately given to the Information Systems Security Analyst for proper destruction.

9.4 Fax machines that have ribbons or film for operation must have those items removed and properly destroyed before decommissioning. Please check with Information Systems for the proper media destruction process.

Section 10: Other

10.1 Due to the ever changing nature of technology in media storage, any electronic device (other than those covered in this policy) that communicates, disseminates or stores data will require authorization from Sarpy County Information Systems Department prior to use.

Section 1: Purpose

The purpose of this policy is to provide guidance on security and use of Sarpy County systems from a remote location.

The County provides the capability to remotely access networks and systems for business-related purposes ONLY. Remote access requests must be made to Sarpy County Information Systems.

It is the responsibility of all authorized users to strictly control remote access from any device that connects from outside the Sarpy County network to a desktop, server or network device inside the Sarpy County network, and ensure that employees, contractors, vendors and any other agent granted remote access privileges to any Sarpy County network follow the practices outlined in this policy.

The practices set forth by this policy are designed to minimize potential damages which may result from unauthorized use of resources, including loss of sensitive or confidential information, intellectual property and damage to public image or critical internal systems.

Section 2: Scope

This policy applies to all County employees, appointed officials, elected officials, department heads, interns, contractors, business partners, affiliated agencies, vendors and volunteers.

Section 3: Exceptions

Requests for exceptions will follow Policy 12: Exception Request Process.

Section 4: Remote Access Practices

The following measures will be followed by, and enforced for, remote access users:

4.1 Remote access is defined as connections to County networks and or systems from a non-direct connection on the County network. This includes, but is not limited to dial-up (modem), client-based VPN, router-based VPN, screen sharing, or access to an application through the Internet.

4.2 VPN Access will be established through the use of a User Account Request form.

4.3 When a business-to-business connection is needed, an Elected Official, Department Head or their designee must send a written request with documentation of the need to the I.S. Director, Operations Manager, and Information Security Analyst.

4.4 Users who use remote access will ensure that their device contains adequate and updated anti-virus and/or anti-malware protection. If an end-point device appears to be virus infected or is behaving unpredictably it **shall not** be used to access County systems. Contact the Help Desk staff immediately at 402-593-4357.

4.5 Under no circumstances should family members be allowed to access an end-point device that is remotely connected to the County's network. Passwords will not be saved in remote access software/applications. Saved passwords may enable remote access without the user's knowledge.

4.6 County systems and networks are monitored. There should be no presumption of privacy when using them with remote access.

4.7 Contractor or business-to-business remote connections will be provided on an as-needed basis only. Accounts will be activated for the minimum practical duration and deactivated when not in use. Businesses desiring connections should complete a network access agreement, and a non-disclosure agreement if necessary, as a part of the contracting process.

4.8 Remote access capabilities will not be engineered or installed by anyone outside of the Systems and Operations Group of Information Systems Department. Remote access sessions, where system control is granted to a third party who has not signed the network access agreement, will be monitored by a member of the Information Systems Department. If the third party attempts to gain unauthorized access or misuses their privileges, the remote session will be terminated immediately to minimize any potential damage. Such an incident must be reported per Policy 9 "Incident Response and Reporting".

4.9 Under no circumstances will modems be directly attached to workstations, or will devices such as workstations or laptops be plugged into phone lines at the County, unless approval has been granted from the County Information Security Analyst. The County does monitor and audit for such devices and disciplinary action will be taken if unauthorized devices are found.

4.10 Remote access connections from a County device to a personal/private system, network, or personal cloud computing services is prohibited.

4.11 Sarpy County's "Electronic Communications" policies contained within the Sarpy County Personnel Rules & Regulations and Policies & Procedures Manual govern individuals during remote access.

INFORMATION TECHNOLOGY SECURITY POLICY

Policy 6: Passwords	Revision Date 11/15/2018 4:00 PM
	Page **1** of **3**

Section 1: Purpose

This policy is to establish and maintain standard parameters for passwords.

The combination of user account and password credentials is considered to be adequate and acceptable security measures for most of our systems. The fundamental philosophy of this policy is to ensure that the passwords we use are of a sufficient strength so as not to be easily cracked or broken by unauthorized individuals.

Section 2: Scope

This policy applies to all County employees, appointed officials, elected officials, department heads, interns/externs, contractors, business partners, vendors, and volunteers.

Section 3: Exceptions

Requests for exceptions will follow Policy 12: Exception Request Process.

Section 4: General Password Policy

The following measures will be followed and enforced on systems where possible:

4.1 Passwords will be a minimum of 8 characters in length.

4.2 Passwords shall contain an upper case, lower case, numeric, and special character.

4.3 Passwords shall be changed every 90 days.

4.4 Passwords shall have a minimum age of 1 day.

4.5 Passwords may not be reused for 10 iterations.

4.6 The password shall not be something that is easily guessed, such as the name of a pet, a child or other family member, or any part of a person’s name or their login ID. The password “password” is not acceptable, nor is a simple series of numbers like “12345678”.

4.7 Passwords shall not be standard dictionary words that can be acquired or cracked with automated password cracking programs and brute force dictionary attacks.

4.8 Passwords for personal or assigned credentials will not be asked of, or given to others. If someone requests an individual's password it should be reported to the Sarpy County Help Desk at 402-593-4357 (help). This policy does not include I.S. staff requesting passwords to perform setup or maintenance on equipment.

4.9 Requests to reset a user's password must come from that user. No other parties are authorized to request a password reset on behalf of another individual. This policy does not include I.S. staff performing password resets as part of their job duties.

Section 5: Specialized Accounts (See Policy 57 – Specialized Accounts)

5.1 Passwords are to be complex and should contain at least 12 characters.

5.2 Passwords should be documented but kept encrypted and protected.

5.3 Passwords may not be required to be changed.

Section 6: Technical Implementation

6.1 Passwords shall not be written down and stored on, or near, computer equipment.

6.2 Passwords shall never be stored in any application or system in a readable format (excluding password management software).

6.3 Passwords shall not be stored in database tables unless encrypted and not available to any account except the root, system, or administrator.

6.4 Whenever possible, passwords shall be encrypted in scripts or programs (code).

6.5 Passwords and password files may not be copied or transmitted across any means of communication in clear text. This does not include first use or temporary passwords that must be changed on first log-on.

6.6 It is the responsibility of technical staff, including systems administrators, developers, and support personnel to ensure that systems are designed and implemented that do not compromise the security of user accounts or passwords, or inappropriately embed credentials and rights within stored procedures which may be readable.

6.7 Use of password management software is authorized with the approval of Sarpy County Information Systems Operations Manager and Security Analyst.

6.8 Users should not cache or save passwords when requested by various software or applications.

Section 7: Two-Factor or Multiple-Factor Authentication

The use of multiple authentication factors to prove one's identity is based on the premise that an unauthorized user is unlikely to be able to supply the factors required for access. Multi-factor authenticated use is encouraged when appropriate. Use of multi-factor authentication devices will be inventoried per Policy 2, Section 5.1.

7.1 The authentication factors of a multi-factor authentication scheme may include:

- Some physical object in the possession of the user, such as a USB stick with a secret token, a bank card, a key, etc.
- Some secret known to the user, such as a password, PIN, etc.
- Some physical characteristic of the user (biometrics), such as a fingerprint, eye iris, voice, typing speed, pattern in key press intervals, etc.

INFORMATION TECHNOLOGY SECURITY POLICY

Policy 7: Workstation Security	Revision Date 8/24/2018 10:25 AM
	Page **1** of **3**

Section 1: Purpose

This document provides policy, direction, procedures and guidance for the installation, positioning and security of workstation systems for Sarpy County.

Section 2: Scope

This policy applies to all County employees, appointed officials, elected officials, department heads, interns/externs, contractors, business partners and volunteers.

Section 3: Exceptions

Requests for exceptions will follow Policy 12: Exception Request Process.

Section 4: Workstation Security

4.1 It is the responsibility of each Elected Official / Department Head to adhere to this policy concerning access and security requirements for each location containing technology equipment.

4.2 Physical safeguards for technology equipment will be provided by using one or more of the following: counters and partitions, locked doors, card access or combination key access systems, camera monitoring, and/or alarmed entrances.

4.3 There will be some cases in which technology equipment will be accessible to the general public. In general, the following rules will apply:

4.3.1 Technology equipment will be in a location, which can be locked or secured after normal business hours.

4.3.2 Technology equipment will be monitored to ensure that it is not removed or intentionally damaged while accessible to the public. When practical, equipment should be positioned near a security camera.

4.3.3 Information Systems will implement security controls that will technologically lock down or harden technology equipment so that a member of the public cannot access internal secured networks.

4.3.4 Public access terminals will be secured on a case-by-case basis.

4.4 Monitors should be kept from the plain view of anyone who does not have the appropriate access or clearance to information that may be displayed. This may be addressed by turning the monitor away from counter areas, or by installing a special shade or polarizing monitor filter. Site surveys shall be conducted by each department or office to check for unauthorized viewing from the following sources:

- Through outside windows
- From public hallways
- From public reception areas
- Reflection off of other objects
- Cameras

4.5 Keyboard, mouse, and other components should be kept far enough away from the public, so that they cannot be tampered with or stolen.

4.6 Access to counter workstation connections; USB, Serial, Parallel, HDMI, Ethernet, etc. should be controlled from public and visitor access.

4.7 The County will use standards that support workstation security. These include, but are not limited to:

- The utilization of appropriately patched operating systems.
- That each user does not have local administrator rights on his or her workstation.
- Shall be configured appropriately and secured for the purpose of the workstation.
- The utilization of an automatic screen saver that is password protected. Screen savers will automatically activate after no more than 10 minutes of inactivity. Users or departments will take no action that disables the use or prolongs the time frame of lock out measures.
- A standard warning message will be displayed on each system at time of user login. This message will inform each user that they are subject to applicable security rules and may be monitored.

4.8 Workstations will be either locked or logged off when not in use, **not powered down**. This enables I.S. to apply security patches and updates when necessary.

4.9 The County considers workstations a security item that is subject to accountability controls and inventory tracking. Workstations will be asset tagged and accounted for when entering the inventory. The asset will be tracked throughout its lifecycle and appropriately removed from inventory when removed from County service.

4.10 Printers should be kept in protected areas to keep sensitive information from being disclosed inappropriately.

4.11 Printed materials from any source should be kept secure and away from viewing and out of public reach.

Section 5: Local Administrative Access

Information Systems (I.S.) will not provide local administrative access to any IT equipment without a submitted Exception to this policy. Administrative privileges on a computer system allows access to resources that are generally unavailable to most users and permit the execution of action that would otherwise be restricted. When such privileges are administered improperly, granted widely, and not closely audited, attackers are able to exploit them and jeopardize the confidentiality, integrity and availability of technology resources.

Section 6: End-Point/Anti-Malware Security

Workstations will require that end-point security software (e.g. Anti-virus and/or Anti-malware) be loaded and current, to prevent viruses, Trojans, Ransomware, and malware from being loaded.

INFORMATION TECHNOLOGY SECURITY POLICY

Policy 8: Security Training and Assessment	Revision Date 2/21/2018 8:45 AM
	Page **1** of **1**

Section 1: Purpose

All technology users are critical to the defense and protection of sensitive county information, equipment and data. The Information Security Awareness training will assist technology users to implement security by incorporating various objectives learned within the training.

Section 2: Scope

This policy applies to all County employees, appointed officials, elected officials, department heads, interns/externs, contractors, business partners and volunteers.

Section 3: Exceptions

3.1 There are no exceptions to this policy for users of Sarpy County technology resources.

3.2 In some circumstances, equivalent security training will be considered in lieu of the County's training at the discretion of the Information Security Analyst or their designee.

Section 4: Information Security Training

4.1 Information Security Awareness Training

4.1.1 Information Security Awareness Training is scheduled at least once every calendar year.

4.1.2 Mandatory training modules are selected by the Sarpy County Information Security advisory group.

4.1.3 Mandatory Information Security Awareness Training will not exceed four hours per calendar year.

4.1.4 Noncompliance with mandatory training will result in the removal of access to all Sarpy County IT systems and equipment.

4.1.5 Human Resources and the Information Systems Security Analyst will work together to record and verify that training requirements are met annually.

4.1.6 Sarpy County Information Systems will utilize various methodologies and tests to assess the effectiveness of the Security Training.

Section 1: Purpose

The purpose of this document is to establish policies for responding to information and network security incidents in Sarpy County.

It is the intention of Sarpy County to adhere to a standardized procedure of responding to security incidents. The County shall create and maintain preventative measures to avoid any reasonably anticipated events that would compromise the confidentiality, integrity, or availability of data stored on the County network or County owned devices. It is also the intent of this policy that each investigation results in recommendations or courses of action that will lessen the likelihood of a recurrence whenever possible.

Section 2: Scope

This policy applies to all County employees, appointed officials, elected officials, department heads, interns/externs, contractors, business partners and volunteers.

Section 3: Exceptions

3.1 There are no exceptions for users of Sarpy County technology resources.

Section 4: Descriptions and Definitions of Incidents

4.1 **Denial of Service**
Denial of service attacks are those incidents which cause network or information resources to abnormally terminate operations, degrade operation, or be disrupted or interdicted to the point where they cannot efficiently perform their intended function. This can be caused by a targeted attack from one or more internal or external sources, a server crash or network failure either by intentional attack or a natural occurrence, or a denial of physical access to a facility or devices. Such an event could affect critical systems used throughout the County and would need to be addressed immediately and investigated.

4.2 **Malicious Code**
Any worms, Trojan horses, rootkits, ransomware, bots, or viruses brought into the County network intentionally or unintentionally have the potential to attack and destroy data quickly, or to compromise the confidentiality and integrity of our

information. Such an event will require immediate attention and shall be investigated.

4.3 **Unauthorized Access**

If anyone gains access without authorization to the County network or County owned media, devices, or servers, then that would be classified as a violation of policy and a security incident. This incident would require immediate attention and coordination between multiple departments or offices.

4.4 **Inappropriate Usage**

An individual who accesses systems, networks or data, without fully complying with all relevant policies, violates the Policies & Procedures Manual and/or Personnel Rules & Regulations. Examples include, but are not limited to the access of inappropriate websites, using the County e-mail system for inappropriate, non-work related materials; abusing systems or using them for unintended purposes; using workstations, servers or other devices to attempt to monitor, detect passwords, probe systems or networks, or other such hacking or cracking activities. This type of incident may be less critical, but does require prompt response.

4.5 **Unauthorized Release or Disclosure**

The accidental or intentional release, disclosure, loss or theft of data or information or any device containing data or information would be included under this category. This type of event may more commonly be known as a breach and includes, but is not limited to, restricted categories of information which may require protection under the law.

Section 5: Incident Response and Reporting Procedures Framework

Incident Response and Reporting Activities generally fall within these major categories.

5.1 **Preparation and Prevention**

This is the process of creating a policy severity index and reporting structure for incidents, and creating a security posture which may prevent incidents from occurring.

5.2 **Detection, Investigation and Analysis**

These are the steps involved in identifying an incident, providing immediate notification to appropriate parties, analyzing the available information, assembling the incident response team participants, creating an action plan, gathering data and/or evidence, and determining the extent of access or damage.

5.3 Containment, Eradication and Recovery

Once an incident is verified, this process is involved with stopping the spread of the incident or problem, cleaning affected systems, recovering data, involving law enforcement agencies (if appropriate), finalizing the collection of logs and data, and returning systems or networks to a fully operational condition.

5.4 Reporting

All users of Sarpy County systems are responsible for reporting known or suspected information technology security incidents. Any such incidents must be promptly reported to the Sarpy County Help Desk at 402-593-4357. Sarpy County I.S. will work with the reporting party and contact the appropriate authorities as necessary.

5.5 Release of Information

Control of information during the course of an incident or investigation of a possible incident is very important. Communication will be on a need to know basis and is considered restricted data during a security incident investigation. Employees with knowledge of the incident are not to share any details with anyone other than the incident response team and management. The public release of information will follow the Sarpy County Communications Policy.

5.6 Notification Activities

The law may require notification to affected individuals in some cases. Notable examples of such laws are Nebraska's Financial Data Protection & Consumer Notification of Data Security Breach Act of 2006 and the Payment Card Industry Standards.

5.7 Post-Incident Activities

Determining root causes, creating final reports, complying with all legal requirements, determining corrective actions, and ensuring that those corrective actions become a part of the preparation and prevention process are all requirements of the post-incident activities category.

INFORMATION TECHNOLOGY SECURITY POLICY

Policy 10: IT Procurement and Use	Revision Date 4/10/2018 3:15 PM
	Page **1** of **3**

Section 1: Purpose

The purpose of this policy is to provide guidance to departments and offices about the acquisition process of information technology products and cloud services. All departments and offices seeking to purchase, use, or obtain IT products, or cloud services, must utilize the I.S. Department for those purchases and follow this procedure as applicable.

Section 2: Scope

This policy applies to all County employees, appointed officials, elected officials, department heads, interns/externs, contractors, business partners, vendors, and volunteers.

Section 3: Exceptions

Requests for exceptions will follow Policy 12: Exception Request Process.

Section 4: Cloud Services

4.1 Use of cloud computing services (e.g. Amazon Web Services, Google Cloud Platform, Microsoft Azure, etc.) for work purposes must be formally authorized by the Sarpy County Information Systems Director, Operations Manager, and Information Security Analyst.

4.2 Use of Software as a Service (SaaS) must be formally authorized by the Sarpy County Information Systems Director, Operations Manager, and Information Security Analyst.

4.3 The Sarpy County Information Systems Security Analyst will certify that security, privacy and all other IT management requirements will be adequately addressed by the cloud services vendor.

Section 5: Information for Review

5.1 List of Preapproved Items for Purchase

5.1.1 The Sarpy County Information Systems Department will maintain a list of preapproved items for purchase by departments and offices. The list will identify equipment and technical items that are low cost and pose low risk to the procurement criteria. Departments and offices are approved to purchase items on this list.

5.1.2 The list described in this section is referred to as "Appendix A – List of Preapproved Items for Purchase". The I.S. Department may revise Appendix A as necessary.

5.2 Documentation

5.2.1 Departments and offices seeking to purchase IT equipment or software will submit the form titled "IT Procurement Request".

5.2.2 Types of documentation needed for review may include:

- A description of what is being considered for purchase
- A price quote from the vendor
- A list of technical requirements describing the hardware, software and network infrastructure needed to support the proposed system or software
- A diagram and explanation of the technical architecture (when available or requested)

5.3 Procurement Review Criteria

5.3.1 Criteria to be reviewed for the procurement:

5.3.1.1 Complies with Sarpy County standards and enterprise architecture

5.3.1.2 Avoids unnecessary duplication of expenditures

5.3.1.3 Addresses opportunities for collaboration or data sharing, if applicable

5.3.1.4 Represents the correct technology for the job

5.3.1.5 Complements the skills, resources and capabilities of the department or office

5.4 Approval Timelines

5.4.1 Routine purchases such as PCs, laptops, printers and low cost items not on "Appendix A – List of Preapproved Items for Purchase" will be reviewed and responded to within 2 business days.

5.4.2 More complex requests will be reviewed and acted upon within 3 business days. Requests for further clarification or additional information will require additional review time. The goal is to resolve all issues and provide a final action within 10 business days. Requests for further clarification or additional information will require additional review time.

5.4.3 Major requests (RFPs, RFI's) will be reviewed and acted upon within 7 business days. Requests for further clarification or additional information will require additional review time. The goal is to resolve all issues and provide a final action within 12 business days (excluding the time required of the agency responding to requests for additional information).

INFORMATION TECHNOLOGY SECURITY POLICY

Policy 11: Cloud Storage	Revision Date 4/10/2018 3:15 PM
	Page **1** of **1**

Section 1: Purpose

The purpose of this document is to establish policies and procedures for the use and procurement of cloud storage.

Section 2: Scope

This policy applies to all County employees, appointed officials, elected officials, department heads, interns/externs, contractors, business partners, vendors and volunteers.

Section 3: Exceptions

Requests for exceptions will follow Policy 12: Exception Request Process.

Section 4: Procurement, Authorization and Use

4.1 Employees will use Sarpy County provided and authorized cloud storage solutions. Enterprise adopted solutions allow the County to provide security, custody, and auditing where necessary.

4.2 Use of cloud storage for work purposes must be authorized per policy 10 “IT Procurement and Use". The Sarpy County Information Systems Security Analyst will certify that security, privacy and all other IT management requirements will be adequately addressed by the cloud vendor.

4.3 For any cloud storage not previously approved or county provided that require users to agree to terms of service, such agreements must be reviewed and approved by the Sarpy County Information Systems Director, County Attorney, and the Information Security Analyst.

4.4 The use of cloud storage must comply with all applicable laws, rules and regulations, including those governing the handling of personally identifiable information, Federal, State or County financial data or any other data owned or collected by Sarpy County.

4.5 The Data Steward and Sarpy County Information Systems Department will determine what restricted data is authorized for cloud storage.

4.6 Personal (non-enterprise or County authorized) cloud storage (e.g. OneDrive, Drop Box, Google Drive, etc.) accounts may not be used for the storage, manipulation or exchange of County related communications or County owned data.

INFORMATION TECHNOLOGY SECURITY POLICY

Policy 12: Exception Request Process	Revision Date 4/10/2018 08:00 AM
	Page **1** of **1**

Section 1: Purpose

The purpose of this document is to establish the process through which an exception to the Information Technology Security Policy be requested. If a requirement of the Information Technology Security Policy is not met, an exception is to be requested.

Section 2: Scope

This policy applies to all County employees, appointed officials, elected officials, department heads, interns/externs, contractors, business partners, affiliated agencies, vendors, and volunteers.

Section 3: Exceptions Process

3.1 Exceptions will be kept on file by the Information Systems Department and managed by the Information Security Analyst.

3.2 Exception requests must be submitted by the Elected Official, Department Head or designee using the "IT Security Policy Exception Request" form.

3.3 Exception requests are subject to review and approval from each of the following:

- Director of Sarpy County Information Systems or their designee
- Information Security Analyst or their designee

Section 4: Exception Request Details

4.1 Exceptions to policies may require implementation of alternate compensating security controls (compensating controls) to maintain security and reduce risk. Options for compensating controls may be recommended by the requesting party or the Information Systems Department. Compensating controls will be the responsibility of the requesting unit to implement and maintain through coordination and cooperation with the Information Systems Department.

4.2 The requestor may receive a request for additional information from the Information Security Analyst or designee.

4.3 The requestor will be notified of the decision to approve or deny.

4.4 All requests for exceptions will be retained by the Information Security Analyst.

4.5 Exceptions will be reevaluated after a period of 12 months

INFORMATION TECHNOLOGY SECURITY POLICY

Section 1: Purpose

This document describes the security policies governing access to the Information Systems Office area.

Section 2: Scope

This policy applies to all Sarpy County Information Systems staff and all other County employees with Information Technology roles.

Section 3: Exceptions

Requests for exceptions will follow Policy 12: Exception Request Process.

Section 4: Office/Suite Access

4.1 Information Systems employees will receive a key card with access allowing them 24/7 access to the Information Systems Office.

4.2 The Information Systems Office is considered a secure area. Non-employees who require access will be escorted at all times.

4.3 The West door of the Information Systems Office has key card security and shall remain locked at all hours.

4.4 All employees that have key cards will have access to the West door of the Information Systems Office during normal business days: 7:50 am – 4:45 pm.

4.5 Contractors, requiring consistent and continuous access, and anyone else authorized by the Information Systems Director will be provided access by the issuance of a key card. The doors and exits, as well as the access hours will be authorized based on business need only. Such key cards will be issued to the authorized individual, and remain in his or her possession during the period of employment or need.

4.6 Lost or stolen access cards must be reported immediately to Court Security during normal business hours (402-593-4365) or after business hours using the non-emergency number (402-593-4111). Those reporting lost or stolen access cards must ask the dispatcher to notify the Sheriff's Office Assigned Duty Commander (ADC). **This is very important as I.S. staff typically have building access rights after normal business hours.**

4.7 The Information Systems Director can have key card access changed for Information Systems employees at any time.

4.8 The Information Systems Director will request reports from Court Security, on a semi-annual basis, to review those who have access to the Information Systems Office(s).

INFORMATION TECHNOLOGY SECURITY POLICY

Policy 51: Data Center Access and Maintenance	Revision Date 4/10/2018 3:15 PM
	Page **1** of **4**

Section 1: Purpose

The purpose of this document is to establish policies and procedures for providing access and maintenance to the Sarpy County Courthouse and Sheriff's Office Data Centers.

Section 2: Scope

This policy applies to data centers managed and controlled by Sarpy County Information Systems Department.

Section 3: Exceptions

Requests for exceptions will follow Policy 12: Exception Request Process.

Section 4: Data Center Access and Maintenance

Only key card access should be used to access the Data Centers. In the event of an emergency situation where key card access is not available to access Data Centers, a physical key may be used. The key can be obtained by contacting Facilities Management at 402-593-2332 during working hours or 402-505-1849 after hours.

4.1 It shall be the policy of Sarpy County that all Data Centers are secured, restricted areas. Access shall be granted to only those individuals who have a mission-essential business need and who have been appropriately authorized. Data Centers are <u>not</u> common workspaces. Equipment and traffic in the Data Centers shall be kept to a minimum.

4.2 There are six types of access defined in this policy:

- NO Access (default)
- Accompanied Access (being escorted)
- Unaccompanied Access 8 to 5 (standard business hours)
- Unaccompanied Access 24/7
- Emergency Access
- Maintenance Access

4.3 Key card access to the Data Centers will not be provided to non-County employees.

4.4 Evaluation of individuals having access to Data Centers will be continuous. Individual access can be removed at any time.

4.5 The Information Systems Director or Operations Manager will request reports, on a semi-annual basis, to review those who have access to any Data Center. Court Security shall prepare these reports upon request to the Information Systems Director or Operations Manager or provide the Information Systems Director or Operations Manager access to the report.

4.6 By entering a Data Center, individuals accept responsibility to monitor activities and report things that may look wrong or out of place. It is everyone's responsibility to recognize others who are in the room and to try to verify the identities of unrecognized individuals.

Section 5: No Access

5.1 The default for all employees is NO Access.

Section 6: Accompanied Access (Escorted Access)

6.1 This level of access is for anyone that has a business need to be in a Data Center but does not have access.

6.2 Only the Director of Sarpy County Information Systems, Operations Manager, Infrastructure Administrator, Systems/Network Administrator, and Network and Telecommunications Specialist can assign or be an escort. This will generally be the I.T. Director and the Operations Staff (not including Technical Support Specialists).

6.2 Escorts must remain in the Data Center during the entire visit and be in a position to observe the individual(s). Escorts assume responsibility for the actions of those they escort into a Data Center and are responsible to clear them back out, ensuring that they have not removed any equipment, media, or data.

Section 7: Unaccompanied Access (24/7 and 8 to 5)

7.1 This level of access will be granted to the least possible number of employees. Employees in this category should be full-time and have completed an advanced background check. The employee shall have exhibited a level of trust and confidence, which would justify this level of access.

7.2 Key card access is obtained through written authorization by the Information Systems Director or Operations Manager and completion of a key card request form through Courthouse Security.

7.3 This level of access does NOT automatically have escort privileges unless permitted (see Section 6.2)

Section 8: Emergency Access

8.1 In the event of fire, natural disaster, chemical spill, or any other event which would render a Data Center hazardous or unsafe, the building will be evacuated immediately. Any personnel with access to Data Centers shall affect an Emergency Power Off (EPO), cutting electricity to all systems, if it is apparent that imminent damage could be caused to the systems.

Imminent damage could include, but not necessarily be limited to, the observation of:

- fire
- water leaking/pouring into electronic equipment or racks
- smoke
- arcing of electrical circuits/power.

8.2 Emergency personnel, such as fire, police, and/or the Sarpy County Sheriff's Department, will generally control access to the site during the entire course of the emergency. Only the site commander or senior emergency staff member on site may authorize access to the Data Center.

8.3 If the site can be accessed, but cannot be used for normal business operations, personnel may be called into a Data Center to begin a process of an orderly shutdown, and begin removing equipment, racks, etc. that are functional or may be repairable. Priority will be given to the safety of personnel, and to evacuating as much equipment as possible to a safe indoor location, or a safe and guarded outdoor location, until it can be moved to a better location. Precise procedures and instructions will depend on the nature and extent of the emergency. The senior I.T.

staff member on site will direct the effort, and work with other agencies to secure help to move and transport equipment.

8.4 Movement, repair and restoring of service will be prioritized in accordance with the continuity of operations plan. In the absence of a continuity of operations plan, I.S. personnel should work with a prioritized list of services considering public safety first, financial systems second, public services third, and then all other services.

Section 9: Maintenance Access

9.1 Facilities personnel have key cards and access codes for unaccompanied 24/7 access. This access should be used only in the case of a page, alarm or emergency. All such access should be reported to the Facilities Director, who should log the information and report this access to the I.S. Director or I.S. Operations Manager.

9.2 Facilities Management will notify the I.S. Director or I.S. Operations Manager whenever there is work being performed that may possibly affect the data center. This work may be in adjacent offices or on utilities for the building.

9.3 Any maintenance work done on the physical structure, walls, doors, utilities, or locks of the Data Centers will be approved by the I.S. Operations Manager or I.S. Director.

9.4 Large scale maintenance/construction projects should require that construction staff, that may have access to Data Center equipment, have criminal background checks performed to be reviewed by the County Sheriff and I.S. Director or their designees

9.5 All maintenance work done will be documented and kept by the Operations Manager. Information logged should be: Date, Time, Repair, Company / Contractor doing repair(s), Date and Time Completed.

9.6 Sheriff personnel have key cards and access codes for unaccompanied 24 / 7 access. This access should be used only in the case of an alert, alarm, training or emergency. All such access should be reported to the I.S. Director or I.S. Operations Manager.

INFORMATION TECHNOLOGY SECURITY POLICY

Policy 52: Application Development and Procurement	Revision Date 4/10/2018 3:15 PM
	Page **1** of **2**

Section 1: Purpose

The purpose of this document is to provide guidance to ensure that the development, configuration, and deployment of applications incorporates the best practices of information security and provides for the confidentiality, integrity, and availability of applications and information.

Section 2: Scope

This policy applies to all Sarpy County Information Systems staff and all other County employees with Information Technology roles, and it applies to all applications in use at the County, accessed by the County, or containing County information.

Section 3: Exceptions

Requests for exceptions will follow Policy 12: Exception Request Process.

Section 4: Application Development/Procurement Security Policy Summary

Every application development or procurement effort shall include the goal of ensuring that information is appropriately protected, to include the server resources on which the application will run. Each developer should become familiar with basic principles of secure application development in order to produce secure applications.

Section 5: Application Development/Procurement Security Procedures

5.1 Security shall be considered throughout all phases of an application's lifecycle – from consideration/inception all the way through decommissioning and disposal.

5.2 In addition to securing the information in the application, a system shall also protect the host operating system, hardware and end-user environment from malicious activity.

5.3 Vendors shall be asked to show documentation and/or certification of their systems' security during bid or procurement action as necessary. Certifications may be any common or accepted industry standard.

5.4 Development/procurement activities will generally adhere to guidelines and checklists published by the *National Institute of Standards and Technology (NIST) U.S. Department of Commerce - Security Considerations in the System Development Life Cycle 800-64 R2*.

5.5 Applications shall contain auditing/logging capabilities to provide appropriate controls for security compliance. The identity of those using the system will be carried through the various program components, such that each action taken on a system can be tracked to an individual user.

INFORMATION TECHNOLOGY SECURITY POLICY

Policy 53: Data Backup and Storage	Revision Date 4/10/2018 3:15 PM
	Page **1** of **3**

Section 1: Purpose

The purpose of this document is to establish policies and procedures for the consistent and correct backup of data in Sarpy County Data Centers. It is the policy of Sarpy County to perform daily backups of data.

Section 2: Scope

This policy applies to data managed and controlled by the Sarpy County Information Systems Department and other county employees with Information Technology roles. This does not include systems defined as end user devices, such as desktops, laptops, iPads, tablets or personally owned devices.

Section 3: Exceptions

Requests for exceptions will follow Policy 12: Exception Request Process.

Section 4: Data Backup and Storage Practices

4.1 Backups will be done on a daily basis but the schedule may be modified to accommodate a more relaxed schedule for systems where data does not often change. Offsite storage of backups will be utilized to provide resiliency and aid in contingency planning.

4.2 Backups are intended for restoring accidentally deleted files and to recover servers from a business continuity event. They are not designed as a record retention tool.

4.3 Responsibility for the backup and restore functions lie with the Systems and Operations Group of the Information Systems Department. Restores are requested through the Sarpy County Information Systems Help Desk.

4.4 A standardized backup architecture should be used within each technical family. Technology will prescribe how backups are to be conducted and the software and hardware that is required.

4.5 Scheduled backup media/device accountability and control shall be handled as follows:

4.5.1 All backup media/devices will be inventoried and signed for when custody is transferred.

4.5.2 Only County employees will handle backup media/devices.

4.5.3 When outside the Data Center backup media/devices will not be left unattended.

4.5.4 A verifiable chain of custody will be established with the handling and disposal of backup media/devices. Certification of destruction shall be obtained and forwarded in electronic form to the County Records Department.

4.6 All backup media/devices will be treated with the same level of security as the system that the information came from. The entire backup media/device shall have the classification of the highest sensitivity of information on any one of its files. If one file contains protected information the entire backup media/device requires that level of security.

4.7 The authorized locations for physical backup media and device storage will be at these locations, except while in transit.

4.7.1 Courthouse Data Center

4.7.2 Emergency Communications Data Center

4.7.3 Sheriff's Office Data Center

4.7.4 City of Bellevue, Wall Street, Data Center

4.7.5 Sarpy County Records Management Center

4.8 Backup media/devices will not simply be thrown away or placed in surplus. Backup media/devices will be disposed of in accordance with "Policy 4— Media Handling and Sanitization".

4.9 Backups should be verified and tested at least annually and should include the successful ability to:

4.9.1 Restore a server and all associated software/storage to be completely operational from a backup;

4.9.2 Selectively restore SQL database and/or table;

4.9.3 Selectively restore Exchange database; and,

4.9.4 Restore a file and/or directory.

4.10 Any Cloud based backup solution must adhere to “Policy #11— Cloud Storage”.

INFORMATION TECHNOLOGY SECURITY POLICY

Policy 54: Device Installation and Configuration	Revision Date 4/10/2018 3:20 PM
	Page **1** of **4**

Section 1: Purpose

The purpose of this policy is to establish policies and procedures for installation and configuration of technology devices.

Section 2: Scope

This policy applies to all Sarpy County Information Systems staff and all other County employees with Information Technology roles.

Section 3: Exceptions

Requests for exceptions will follow Policy 12: Exception Request Process.

Section 4: Network Device Installation and Configuration

When a known, high-risk vulnerability is discovered, a fix will be applied or patch installed as soon as feasible.

4.1 Switches and Routers

4.1.1 Switches, routers and other connectivity equipment will be based on the Information Technology infrastructure standards determined by the Information Systems Director and Operations Manager.

4.1.2 The Information Systems Department will specify, procure, configure, install and/or approve all network connectivity devices.

4.1.3 Whenever possible and/or monetarily feasible, physical access to switches and routers will be secured in a locked closet, cabinet, or room to protect from intrusion and tampering. These areas shall be limited to individuals that require access. Whenever remodeling (or new construction) occurs that is in the vicinity or served by an I.T. device, the access to the device shall be considered to align with this policy.

4.1.4 Administrative (configuration) access will be provided to the least number of personnel and only those having a direct need for this access.

4.2 Perimeter Defense and Security Appliances

4.2.1 These shall be deployed with the approval of the Sarpy County Information Systems Director, Operations Manager and Information Security Analyst.

4.2.2 Log file data requires additional protection to ensure that results of security investigations, issues, or incidents are not released inappropriately.

4.2.3 Details of firewall, security devices type, software versions, and configuration data will not be disclosed without the permission of the Information Security Analyst.

4.2.4 Administrative (configuration) access to security devices will be provided to the least number of personnel, and only those having a direct need for access at this level.

4.2.5 All changes will be evaluated and tested both before and after moving them into production. Unanticipated consequences, which may weaken security, will be sufficient cause to return the device to the last known good configuration.

4.2.6 Firewall and router rule sets and access control lists will be reviewed by Operations and Information Security Analyst on a quarterly basis. All scheduling and audit documentation will be done by the Information Security Analyst.

4.2.7 Firmware and/or software versions will be kept current to within 90 days or on a known stable and secure version.

4.3 Servers and Appliances

4.3.1 All servers and appliances will be installed and secured in an authorized data center or data closet.

4.3.2 Servers or appliances being configured or “setup” outside a data center will be secured and placed in a safe working environment. Servers and appliances should never be placed on the floor or a box while powered on.

4.3.3 Administrative (configuration) access will be provided to the least number of personnel, and only those having a direct need for access at this level.

4.3.4 Access to the hosts will be the minimum necessary for an individual to perform their assigned tasks or duties.

4.3.5 Appropriate security management practices and controls will be used for servers and appliances and will generally adhere to guidelines and checklists found in NIST 800-123 Guide to General Server Security.

4.3.6 Servers will have the standard county end-point security (anti-virus, malware detection) software installed and configured for frequent and periodic updates.

4.3.7 For availability requirements, backups will be conducted in accordance with "Policy #53— Data Backup and Storage".

4.3.8 Servers and appliances will be monitored for unauthorized activity.

4.3.9 Incidents will be reported in accordance to "Policy #9— Incident Response and Reporting".

4.4 Wireless Networking Devices

By its very nature, wireless networking is less secure than traditionally cabled networks. Technology has provided simple and inexpensive ways to clandestinely connect to or monitor the functions of wireless networks or devices. In some cases, wrongdoers may be able to illegally capture information and data, utilize networked resources for their own unauthorized purposes, or disrupt the operation of wireless networks or devices. Sarpy County will take additional steps in the deployment and security of wireless networks and equipment.

4.4.1 Wireless equipment will only be installed with authorization of the Information Systems Department.

4.4.2 Wireless access points will only be connected to internal networks with physical and logical security.

4.4.3 Public wireless shall be implemented in such a manner as that no part of the public wireless traffic touches or rides on any of the same equipment as the county's Network.

4.5 Remote Administration of Internal Devices

4.5.1 Use of strong authentication mechanisms (e.g., strong passwords, public/private key pair, two factor authentication, etc.)

4.5.2 When possible, utilize device host access (by IP address) lists to restrict remote access

4.5.3 Use of secure protocols that provide encryption of both passwords and data (e.g., SSL, HTTPS) when reasonable and appropriate, rather than insecure protocols (e.g., Telnet, FTP).

4.5.4 Grant permissions to only those with a job related need.

4.5.5 Implement the 'Principle of Least Privilege' to those who are granted permissions.

4.5.6 Reset factory default passwords and regularly change any default accounts or passwords for remote administration utilities or applications to follow password policy.

4.5.7 Disable remote capabilities of devices or device accounts if remote access is not employed by the agency.

4.6 Peripheral Devices

4.6.1 Firmware on printers, scanners, faxes, copiers, cameras, multi-function devices, etc. will be kept current to within 90 days or on the most current known stable and secure firmware version.

4.6.2 Default settings and passwords will be changed and all unused network protocols shall be disabled. **Note:** Password complexity should be followed from "Policy 6 – Passwords" whenever possible.

4.7 Backup of Configuration

4.7.1 All devices, wherever possible, will have the configuration settings (file) backed up and retained in a secure location. A minimum of three (3) backup versions should be saved. The secure location should be part of the nightly backup processes.

Policy 55: Server Patching	Revision Date 4/10/2018 3:15 PM
	Page **1** of **2**

Section 1: Purpose

The purpose of this policy is to establish a baseline of procedures to be used in patching server systems. These procedures will have a direct and immediate impact on Sarpy County vulnerability management practices.

Section 2: Scope

This policy applies to all Sarpy County Information Systems staff and all other county employees with Information Technology roles.

Section 3: Exceptions

Requests for exceptions will follow Policy 12: Exception Request Process.

Section 4: Server Operating Systems

4.1 The Operations Team and/or its designee will manage and patch the Operating Systems.

4. 2 Standard Patches and Upgrades

4.2.1 Sarpy County will continually upgrade Operating Systems in order to stay on manufacturer supported versions.

4.2.2 Sarpy County will generally wait 30 – 60 days from the release of a service pack or major upgrade before scheduling installation and testing. These will be processed through the change control process.

4. 3 Security Patches and Critical Updates

4.3.1 All attempts should be made to install security patches and critical updates on all systems within two (2) weeks, or as soon as feasible, following the release of the patch or update.

5.1 Application and Database Servers

5.1.1 All application server and database server patching will follow “Policy 56 – Change Control”.

5.1.2 Final approval for patching applications, including databases used by the application, lies with the application owner or steward.

5.1.3 SQL server patching will require approval from the administering Database Administrator and/or designee and all Application Stewards prior to patching.

5.1.4 Application and database patches will be retrieved directly from the vendor or a recognized vendor authorized download location.

INFORMATION TECHNOLOGY SECURITY POLICY

Section 1: Purpose

The purpose of this policy is to establish a consistent approach to technical change control. Information Technology (IT) must manage system change in a rational and predictable manner. Change requires planning, monitoring, testing and follow-up evaluation to ensure that Sarpy County operations run smoothly.

Section 2: Scope

This policy applies to all Sarpy County Information Systems staff and all other County employees with Information Technology roles.

Section 3: Exceptions

Requests for exceptions will follow Policy 12: Exception Request Process.

Section 4: Operational Procedures

The change control process shall be formally defined and documented. A change control process shall be in place to control changes to all critical county information resources (such as hardware, software, system documentation and operating procedures). This documented process shall include management responsibilities and procedures. Wherever practicable, operational and application change control procedures should be integrated.

4.1 Change Control Process

The change control process may include, but not be limited to, the following items:

- Logged Change Requests;
- Identification, prioritization and initiation of change;
- Proper authorization of change;
- Requirements analysis;
- Inter-dependency and compliance analysis;
- Impact Assessment;
- Change approach;
- Change testing;
- User acceptance testing and approval;
- Implementation and release planning;
- Documentation;

- Change monitoring;
- Defined responsibilities and authorities of all users and IT personnel; and/or
- Emergency change classification parameters.

Section 5: Documented Change

All change requests shall be logged whether approved or rejected on a standardized and central system. The approval of all change requests, and the results thereof, shall be documented.

A documented audit trail containing relevant information shall be maintained at all times. This should include change request documentation, change authorization and the outcome of the change.

Section 6: Changes affecting Service Level Agreements ("SLA")

The impact of change on existing SLA's shall be considered. When applicable, changes to the SLA shall be controlled through a formal change process, which may include contractual amendments when necessary.

Section 7: Risk Management and Impact Assessment

A risk assessment shall be performed for all changes and dependant on the outcome, an impact assessment should be performed.

The impact assessment shall include the potential effect on other information resources and potential cost implications. The impact assessment should, where applicable consider compliance with legislative requirements and standards.

7.1 Impact Assessment Considerations

7.1.1 Approval

All changes shall be approved prior to implementation. Approval of changes shall be based on formal acceptance criteria i.e. the change request was done by an authorized user, the impact assessment was performed and proposed changes were tested. Approval levels may be dependent on scoring the impact assessment.

7.1.2 Communicating changes

All users, significantly affected by a change, shall be notified of the change. Communication levels may be dependent on scoring the impact assessment.

7.1.3 Implementation

Implementation will only be undertaken after appropriate testing and approval by stakeholders. All major changes shall be treated as new system implementation and shall be established as a project. Major changes will be classified according to effort required to develop and implement said changes.

7.1.4 Fall back

Procedures for aborting and recovering from unsuccessful changes shall be documented. Should the outcome of a change be different to the expected result (as identified in the testing of the change), procedures and responsibilities shall be noted for the recovery and continuity of the affected areas. Fall back procedures will be in place to ensure systems can revert back to what they were prior to implementation of changes.

7.1.5 Documentation

Information resources documentation shall be updated on the completion of each change and old documentation shall be archived or disposed of as per the documentation and data retention policies.
Information resources documentation is used for reference purposes in various scenarios i.e. further development of existing information resources as well as ensuring adequate knowledge transfer in the event of the original developer and/or development house being unavailable. It is therefore imperative that information resources documentation is complete, accurate and kept up to date with the latest changes. Policies and procedures, affected by software changes, shall be updated on completion of each change.

7.1.6 Business Continuity Plans (BCP)

Business continuity plans, if they exist, shall be updated with relevant changes, managed through the change control process. Business continuity plans rely on the completeness, accuracy and availability of BCP documentation. BCP documentation is the road map used to minimize disruption to critical business processes where possible, and to facilitate their rapid recovery in the event of disasters.

7.1.7 Emergency Changes

Specific procedures to ensure the proper control, authorization, and documentation of emergency changes shall be in place.

7.1.8 Change Monitoring

All changes will be monitored once they have been rolled-out to the production environment. Deviations from design specifications and test results will be documented and escalated to the change owner for resolution.

Policy 57: Specialized Accounts	Revision Date 4/10/2018 3:15 PM
	Page **1** of **3**

Section 1: Purpose

This policy establishes rules and procedures for the use and administration of specialized accounts used for Sarpy County Systems and Networks.

Section 2: Scope

This policy applies to all Sarpy County Information Systems staff and all other county employees with Information Technology roles.

Section 3: Exceptions

Requests for exceptions will follow Policy 12: Exception Request Process.

Section 4: Specialized Accounts

There are unique requirements governing the use of specialized accounts within county information systems. Specialized accounts are those accounts that 1) are required for the proper functioning of systems, utilities or applications; **and** 2) that have rights which exceed those of a standard user account. This definition includes, but is not limited to such account types as Administrator, Admin-equivalent, root, SA accounts, service accounts and super-users. While these account types are known by various names and aliases, the concept of higher-than-normal access is the distinguishing factor.

Such accounts provide extraordinarily high levels of access to varieties of systems. If used correctly, such access is vital to the correct operation of our applications and systems. At the same time, such accounts also add significant vulnerabilities and risk to the county. They must be carefully configured, managed and administered to effectively balance both risk and benefit. The following policies will be strictly adhered to:

4.1 Specialized accounts will be approved only when absolutely necessary, and the number of them will be kept to a minimum. They will only be provided to meet certain specific business needs or application requirements and not because of being assigned to a particular organization or position.

4.2 Specialized accounts will be approved only by the Operations Manager and will be appropriately documented by utilizing a User Request Form.

4.3 Generic or shared accounts will not be used for a specialized account.

4.4 System and Elevated Privilege Accounts

4.4.1 Users that have access or privileges to create or change accounts are prohibited from modifying or creating accounts to add specialized access without the proper authorization.

4.4.2 Administrator level accounts are to be used only for system or application administration. Users will **not** remain logged on or perform day-to-day functions with administrator level accounts. Access should be temporary and designed to perform a specific function. When complete, the user should log out, and log back in with their normal user account.

4.4.3 Windows Administrator accounts will be placed in a separate Organizational Unit of the Microsoft Active Directory.

4.5 Database Accounts

4.5.1 Database accounts shall be approved by the I.S. Database Administrator or designated I.S. Application steward.

4.6 Service Accounts

4.6.1 A service account is a specific type of specialized access account. It is designed as an account which is specifically used to run applications or services on a host machine. Users should never log in through a service account to perform non-maintenance activities.

4.6.2 Windows Service accounts will be placed in a separate Organizational Unit of the Microsoft Active Directory.

4.6.3 Applications, scheduled tasks, and services should never run under a standard user account. This will cause the application or service not to function when normal maintenance is performed or passwords are changed.

4.6.4 If a service account is created, and not logged into, the password must be changed every twelve (12) months or upon the departure of the dedicated system administrator. If a specialized account is or has ever been used for login purposes, the password will be changed per our normal policy for all user accounts.

4.7 Vendor / Vendor Support Account

4.7.1 Vendor / Vendor Support accounts are used by a hardware or software vendor that needs to have periodic access to systems.

4.7.2 Vendor accounts will be “locked” when not being actively used.

4.7.3 Windows Vendor accounts will be placed in a separate Organizational Unit of the Microsoft Active Directory.

4.7.4 Vendor accounts generally will not have password expiration dates.

Sarpy County Information Systems
List of Preapproved Items for Purchase

For the purpose of IT Procurement the following items are preapproved for purchase through Information Systems without the need to complete the IT Procurement Request Form:

1. Dell systems such as PC's and laptops per annual computer recommendations
2. Functionally equivalent parts needed to repair existing equipment
3. Cables for connecting computer components
4. Power cords / adapters
5. Extender cables for keyboards / mice
6. KVM (Keyboard - Video - Mouse) switches
7. USB / PS2 connectors
8. Memory chips
9. Laptop batteries
10. Laptop docking stations
11. UPS (Uninterruptible Power Supply) units, and replacement batteries
12. Keyboards, including those for tablet computers
13. Mice
14. Microphones
15. Speakers
16. Monitors that are ordered without a system
17. Hard drives
18. CD/DVD/Blu-ray drives and players
19. Video cards
20. Network cards
21. Barcode pens and readers
22. Card readers
23. Projectors and projector lamps
24. Desktop printers, scanners, and multifunction devices (combining some or all of the following: printer, copier, scanner, and fax machine)
25. Printer toner and ink
26. Small label printers
27. Blank CDs, DVDs, Blu-ray discs, or tapes
28. Digital voice recorders
29. Flash drives
30. Software books

31. Training CDs, DVDs or Blu-ray discs
32. Logic boards and computers that are integral parts of equipment that serves a primary purpose other than information management, including digital cameras, lab equipment, and motor vehicles.
33. The I.S. Department may provide documented preapproval for the purchase of certain other items for a Department.

IT Security Policy Glossary

Term	Definition
Air Gapped System	An air gapped computer is one that is physically segregated and incapable of connecting wirelessly or physically with other computers or network devices.
Biometrics	biometrics refers to authentication techniques that rely on measurable physical characteristics that can be automatically checked. There are several types of biometric identification schemes: face: the analysis of facial characteristics.
Brute Force Dictionary	Brute force means to systematically try all the combinations for a password. The brute force dictionary is the list of words to used in the combinations.
Cache	To store data locally in order to speed up subsequent retrieval.
Cloud Computing	the practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer.
End-point Device	An endpoint device is an Internet-capable computer hardware device on a network. The term can refer to desktop computers, laptops, smart phones, tablets, thin clients, printers or other specialized hardware such POS terminals and smart meters.
Exchange (Server)	The name of Microsoft's eMail Server Software product.
ISAG	Information Security Advisory Group
Jail Break or Jail Broken	Many smartphone, tablet, and game console makers include a layer of Digital Rights Management (DRM) software on their products. This DRM exists either to limit the software you can run on it, or is there for security reasons. Jailbreaking is the process of hacking these devices to bypass DRM restrictions, allowing you to run "unauthorized" software and to make other tweaks to your operating system.
Least Priveledge	Every program and every user of the system should operate using the least set of privileges necessary to complete the job. Primarily, this principle limits the damage that can result from an accident or error.
Magnetic Media	Media in various formats that use magnetic particles to store information. When particles are read by magnetic heads, the information/data that have been previously recorded will be reproduced. Examples of magenetic media are magenetic tape, floppy discs, and hard-drives.
Media	Physical devices or writing surfaces including but not limited to magnetic tapes, optical disks, magnetic disks, Large Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.
Optical Media	Storage media that hold content in digital form and that are written and read by a laser; these media include all the various CD and DVD variations, as well as optical jukeboxes and autochangers.
PII	Personal Identifiable Information - any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.
Role Based	Role-based access control (RBAC) is a method of regulating access to computer or network resources based on the roles of individual users within an enterprise. In this context, access is the ability of an individual user to perform a specific task, such as view, create, delete, or modify a file.

IT Security Policy Glossary

SaaS	Software as a Service is a software distribution model in which a third-party provider hosts applications and makes them available to customers over the Internet.
SQL	SQL is an abbreviation for structured query language, and pronounced either see-kwell or as separate letters. SQL is a standardized query language for requesting information from a database. When used in conjunction with Microsoft it refers to a database software product (Microsoft SQL Server).
Token	Something that the user possesses and controls (typically a key or password) that is used to authenticate the user's identity
Triad of Information Security	Confidentiality, integrity and availability, also known as the CIA **triad**, is a model designed to guide policies for **information security** within an organization.
VPN	A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the internet.