LANCASTER COUNTY INFORMATION SECURITY POLICY

Approval Date: September 23, 2004

Effective Date: March 30, 2005

Last Approved Revision Date: June 3, 2021

Table of Contents

Page

Part I Security Policy

A. General Information

1. Introduction

Lancaster County is responsible for maintaining the confidentiality, integrity, and availability of information; protecting against reasonably anticipated threats or hazards to the security or integrity of its information and information systems; protecting against reasonably anticipated use or disclosures of such information that is not permitted by Lancaster County policies or state or federal laws; and for ensuring compliance with its security policies by members of the workforce.

Lancaster County is concerned with protecting its network and information systems, which include, but are not limited to county and non-county data, county and police mail servers, various file and application servers, firewalls and network operations.

This policy has been prepared to guide and inform Lancaster County employees, consultants, contractors and any users of the County's computing resources on the policies governing conduct within the County. The first, best, and most important line of defense starts with our people.

2. Terminology

This Information Security Policy and the policies and procedures referenced are a comprehensive guideline pertaining to all information system usage. This "policy" serves as the guideline for the acceptable use for all County resources, such as computers, documentation and facilities. Some policy directives are quite clear on their own, while others need to be more clearly defined through written procedures.

The term "Security Officer" is used throughout this document. The term signifies the individuals who are charged with responsibility for developing, implementing and ensuring compliance with security policies.

The term "Open-Records Officer" is the individual who is responsible to receive, track and respond to requests for public records, in compliance with the Pennsylvania Right-to-Know Law.

The term "sensitive information" shall include, but is not limited to, protected health information, personal information, police data and any other Lancaster County data that is not considered a public record. Personal information, is an individual's first name or first initial and last name, linked to any of the following: social security number, driver license number or financial account number.

The term "system" is defined as the data and communications infrastructure purchased and maintained by Lancaster County Government or its appointed representatives.

"Cloud Storage" is a cloud computing model in which data is stored on remote servers accessed from the Internet, or "cloud." It is maintained, operated and managed by a cloud storage service provider on a storage servers that are built on virtualization techniques

The use of the word "shall" throughout this document indicates that the condition must be met unconditionally. The use of the word "should" throughout this document indicates that the condition need not be met in all circumstances but is considered important and is not to be ignored.

The use of the word "user" throughout this document indicates any person using the County's computing resources. The term "employee" refers to any individual employed by Lancaster County on a full- time or part-time basis.

3. Purpose

It is the practice of Lancaster County's Information Technology (IT) Department, and the IT components of other County departments to maintain facilities, computer systems, and access to local, state and national networks to support County business activities and to meet any legal requirements the County is subject to, including but not limited to safeguarding criminal justice and protected health information from unauthorized access, modification, disclosure or destruction. All system users are responsible for using the facilities, and computers in ways that (a) do not interfere with or disrupt the normal operation of business, (b) respect the rights of others, and (c) adhere to the specific policies and procedures that have been established.

Lancaster County has the responsibility to set policies that are consistent with the mission of the organization, and to make known those policies to their employees. IT has the authority to limit or refuse access to anyone who violates these policies or threatens the rights of other employees, and is required to make reasonable efforts to notify employees affected by decisions they have made. These policies and procedures are important to Lancaster County as they help protect the County's employees, assets, and reputation.

4. General Principles

(a) All employees, consultants, contractors and any users of Lancaster County's computing resources shall adhere to the Information Security Policy.

(b) All employees of Lancaster County shall receive security awareness training as part of their initial hiring procedure and refresher training every year, and sign an acknowledgement that they received this training. Signed forms acknowledging receipt of security awareness training will be maintained by each department.

(c) The placement of any policy under an inappropriate title or section does not nullify or diminish the requirement in any fashion.

(d) All security controls shall be accepted and supported by the people who are charged with monitoring and working with controls.

(e) Violation of the Security Policy by any employee, consultant, contractor or user of Lancaster County's computing resources may lead to disciplinary action including, but not limited to, censure, loss of computer privileges, termination or legal action as deemed appropriate by Lancaster County.

(f) This Security Policy shall be made available to all users in either a printed (hardcopy) format or in an online format. The Security Policy will be made available in both formats whenever possible.

(g) All suspected security incidents (actual or attempted breaches of security policies/procedures) should be reported to a Security Officer.

(h) All IT employees, consultants and contractors who are granted privileged access shall adhere to the Information Technology Confidentiality Pledge.

5. Scope

(a) This policy shall apply to:

(i) All employees.

(ii) All contractors and consultants upon commencing work.

(iii) All equipment attached to the County network.

(iv) All custodial data of the County.

(v) All persons with granted authorized access *

* Elected officials are responsible for their own actions. Judges will be reported to the President Judge if they fail to comply with the County Policy.

(b) If a County Agency or any entity that the County provides information related services for has an existing security policy, the most restrictive policy or clause takes precedent.

(c) Department Heads may expand upon the policies contained herein for their Department's own Internet Access guidelines as long as the county policies are not negated or compromised.

6. Policy Process and Review

(a) IT will review the Security Policy on an annual basis.

(b) The Security Policy shall be revised only on the authority of the Lancaster County Consolidated IT Committee. Any such revisions shall be communicated promptly to all employees, consultants, contractors and any users of Lancaster County's computing resources.

7. Security Structure

The Lancaster County Consolidated IT Committee shall evaluate proposed or required changes to the existing Security Policy and the effect on County and Court operations. In this context, the Committee has established a security structure in accordance with the requirements of the Health Information Portability and Accountability Act (HIPAA), Pennsylvania Right-to-Know Law, CLEAN/NCIC rules and other known local, state or federal mandates. This includes the creation and definition of the security committee as well as of the security officer roles and associated responsibilities. The County of Lancaster has adopted the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) as a guiding framework for reducing risks to critical infrastructure. To address the risk management and assessment needs, the County of Lancaster adopted the NIST Risk Management Framework (RMF).

The Chief Clerk will act as the Administrative Security Official to oversee policy development, maintenance and enforcement for non-Court employees, contractors and consultants. The Court Administrator will fulfill this same role for Court employees, contractors and consultants.

A Chief Information Security Officer (CISO) has been appointed by and reports to the Chief Information Officer. The CISO shall be responsible for developing and maintaining the overall Information Security Policy and keeping agencies that fall under this policy informed of changes through regular communications to Departmental Security Officers. The CISO is also responsible to ensure compliance of the policy on all shared information systems (networks, servers). The position will be responsible for:

(a) Managing the information security function in accordance with the established policies and guidelines;

(b) Establishing and maintaining information security standards and procedures in compliance with county information security and risk management policies, standards and guidelines;

(c) Functioning as an internal consulting resource on information security issues;

(d) Conducting the information security risk assessment program;

(e) Reviewing compliance with the information security policy and associated procedures;

(f) Coordinating information security efforts with the Facilities Management Office, Human Resources and the Controllers Office - Auditing Section;

(g) Reporting information security issues to the Chief Information Officer;

(h) Coordinating security orientation and security awareness programs;

(i) Reviewing security violations and follow reporting procedures.

Each department that falls under the jurisdiction of this policy shall appoint a departmental Information Security Officer who shall perform department specific policy enforcement, and establish additional policies as required by their operation. The position will be responsible to handle requests made within their agency and to assist the CISO as needed in the following areas:

(a) Maintaining information security standards and procedures for their agency in compliance with County information security and risk management policies, standards and guidelines;

(b) Functioning as an internal consulting resource on information security issues for their agency;

(c) Reviewing compliance with the information security policy and associated procedures for their agency;

(d) Ensuring that their agency's data has been classified, based on the data classification guidelines that are a part of this document;

(e) For agencies impacted by HIPAA, ensuring that Business Associate Agreements are established with any business associates that receive protected health information from the Agency;

(f) Reporting information security issues to the CISO and their department head;

(g) Coordinating security orientation and security awareness programs for their agency.

(h) Reporting lost or stolen equipment to the IT department.

(i) Reporting the unauthorized access and acquisition of computerized personal information to Commissioners' office. Court Administration shall also be notified if the unauthorized access involved equipment owned by Lancaster County Courts or personal information maintained by Lancaster County Courts.

The CISO and the departmental ISOs shall also be jointly responsible for promoting the security and uninterrupted operation of computer-based application

systems at Lancaster County, and will identify and address exposures to accidental or intentional destruction, disclosure, modification, or interruption of information that may cause serious financial and/or information loss to Lancaster County.

8. Security Violations/Disciplinary Action

IT will log, investigate and report security breaches and violations to the Chief Information Officer and the affected Department Head(s).

It is the responsibility of any employee who observes prohibited activity to report such conduct. No employee will be dismissed, reprimanded, retaliated against, or otherwise intimidated for complying with the reporting requirements of this policy. Activities in violation of this policy should immediately be reported to a supervisor or Information Security Officer.

Users who do not comply with the Security Policy agree to be subject to disciplinary actions as defined in the Lancaster County Progressive Disciplinary Policy or in the Lancaster County Court Progressive Disciplinary Policy for Court employees. Lancaster County reserves the right to revoke user privileges immediately and without prior notice in cases where it deemed necessary. This policy does not supersede the disciplinary action under HIPAAr, CJIS or other applicable regulations.

B. System Access Control

1. System Access Requests

(a) Unique Logon Identification: IT will assign unique logon identification codes to each user for Lancaster County computers and other specialized applications.

(b) Network and e-mail Access: Network and e-mail access requests shall be provided to the IT Department in writing. (E-mail requests are acceptable if sent by an individual with the authority to authorize access.) The request for access must include the signature of the Head of the Department or an individual delegated in writing by the Department Head as having such authority. No one is authorized to sign system access requests unless designated in writing by the Department Head to IT as having the authority to authorize access.

(c) Application Access: Access to an application shall be granted by the Department Head who owns the application the access is requested for, or an individual delegated in writing by the Department Head as having such authority. The Head of the Department who owns the application is required to authorize access to each associate or contractor for access to his or her application system. For distributed systems (systems used by more than one department) the Departments involved will establish in writing a procedure for authorizing IT to grant access to their application(s).

(d) Emergency Access: Access requests of an emergency nature are requests which require immediate action. Any emergency access request shall be coordinated directly with the CISO.

2. [redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted] case [redacted].
- [redacted]

3. Password Handling

(a) Passwords shall remain confidential.

(b) Passwords must not be displayed, printed, or otherwise recorded in an unsecured manner.

(c) If the password to an account becomes known to more than the user the account is assigned to, the password should be changed as soon as possible.

4. Access Control

(a) Users shall be strictly forbidden from using any element of the system that they are not authorized to use.

(b) Users shall be strictly forbidden to bypass any access control system.

(c) Generic user IDs set up for Public Access shall be restricted to be able to access public applications and to PCs designated for Public Access.

(d) Non-Public Generic user IDs can be used by departments only if the generic user-ID is restricted by IT to one or several machines specified by the department.

5. Security Tokens

A security token (also referred as a hardware token, authentication token, USB token, cryptographic token or key fob) is a physical device that is given to an authorized user to function as a part of the authentication process or to provide access that would otherwise be unavailable. Security tokens shall be safeguarded at all times.

(a) Security tokens will not be stored in an unsecure manor or remain connected to devices that are not in use. If a device requires a security token, the device and security token shall not be stored or transported together.

(b) Security tokens shall not remain connected to unattended devices in areas open to the public.

(c) Lost or stolen security tokens shall be immediately reported to the agency issuing the security tokens.

(d) Agencies issuing security tokens are required to track who they have issued security tokens to and collect them as part of the employment termination process.

6. Termination of Access/Login Identification

Individual department ISOs are required to notify IT when an individual is transferred or leaves Lancaster County employment. IT should be provided with information regarding personnel transfers and departures from the Departments involved. IT shall ensure that access to electronic protected information is terminated when employment of a workforce member is terminated for any reason.

C. System Use

1. Login / Logout Procedures

(a) Logon Identification:

All employees of Lancaster County or its associates are required to have a unique logon identification assigned to them to utilize a Lancaster County computer system, except for desktop or laptop computers operating in a stand-alone mode. (This does not apply to any generic user IDs.) The use of this logon identification and password provides the user access to the information and data within the Lancaster County computers to which they have been authorized.

Users are not permitted to allow another person to log-on to any computer utilizing their account information, nor are they permitted to utilize someone else's account information to log-on to a computer.

If a user notices or becomes aware of any unusual login activity on their account, the user will report it to the Security Officer.

(b) Logout Procedures:

Users shall log out of their workstations at the end of each day. If the user needs to remain logged onto the workstation while unattended, a screen lock that requires a password to deactivate will be employed.

When leaving a server, workstation, or other computer system unattended, workforce members must lock or log out of all applications and database systems containing confidential information. This does not apply to Servers, workstations, or other computer systems that are located in locked or secure environments.

(c) Automatic Logoff:

Servers, workstations, or other computer systems containing protected health information or other confidential data must employ screen locks or automatic logoff mechanisms. The aforementioned systems must lock the screen or terminate a user session after a maximum of 30 minutes of inactivity. Screen locks shall require a password to regain access.

Users are not permitted to leave their workstation logged onto the network while unattended, unless their workstation is in a secure location and/or the screen is locked.

Servers, workstations, or other computer systems that are located in locked or secure environments need not implement screen locks or automatic logoff mechanisms.

2. E-mail Usage

(a) Users shall not transmit via e-mail any material that is obscene, pornographic, or which constitutes hate literature as is defined by local, state or federal laws.

(b) Users shall not re-transmit any warnings about viruses or malicious code to multiple users, with the exception of the Security Officer or other IT designated personnel.

(c) Users shall not use their e-mail to engage in any criminal activity as defined by relevant criminal legislation.

(d) Users shall use an IT approved DISCLAIMER on all business-related e-mail messages. Sample Disclaimer Language: *Note: The comments on and attachment to this e-mail are intended only for the use of the individual or entity to which it is addressed, and may contain information that is privileged, confidential and exempt from disclosure under applicable law. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you received this in error, please contact the sender and delete the original message, any attachment(s) and copies. Thank you for your cooperation.*

(e) Users should not use any e-mail account other than their Lancaster County issued account(s) for official business correspondence. Should any user use a personal e-mail account on a county owned device, they should be aware that they are still subject to network monitoring and there should be no expectation of privacy.

(f) Users shall not divulge their e-mail password to anyone.

(g) Users shall be aware that their e-mail, e-mail address and all correspondence are the property of Lancaster County.

(h) E-mail may be subject to monitoring without prior notice, including but not limited to network diagnostics, investigative purposes, etc. An elected official's e-mail may only be monitored upon approval by the Board of Commissioners.

(i) Users shall not use e-mail to distribute criminal history information gained from a query of the State Police CLEAN database.

(j) Any e-mail containing protected health information to be sent to someone outside of Lancaster County Government must be encrypted during transmission.

(k) E-mail sent or received by County employees in connection with official business is considered public records and must be treated appropriately.

(l) Users shall follow County established disposal and archival guidelines for e-mail.

(m) County e-mail and associated attachments stored on a mobile device must remain secured at all times, through device pass codes and encryption, as appropriate.

3. Internet Usage

All users of this service agree to hold Lancaster County harmless from any and all claims, losses, damages, obligations or liabilities, directly or indirectly relating to this service and or the networked information available via this service.

Lancaster County shall enforce the following Internet usage controls:

(a) All County employees are granted access to the Internet unless identified by their Department Head as prohibited from having such access.

(b) Each employee is responsible to use the Internet responsibly and respectfully. The predominant use of the Internet will be for the furtherance of County or Court business. Personal use of the Internet must be limited and will not take priority over work activities. If an employee is found spending excessive time on personal use of the Internet, the employee may be disciplined including access to Internet being revoked.

(c) The Department Head will determine the appropriateness of the material relative to the business requirements of each Department. While it is anticipated that employees may engage in some limited personal use of the Internet, under no circumstances may County or Court employees access or participate in inappropriate material or activities available on the Internet. Inappropriate materials and activities could include, but not be limited to, pornography, hate groups, online gambling, activities related to personal profit, and political activities. Engaging in inappropriate activities can result in termination of employment.

(d) Employees should be aware of the risks involved in downloading material from the Internet and executing programs originating as e-mail attachments. The Department Head reserves the right to establish specific policy regarding material downloaded from the Internet. All material downloaded or saved from the Internet, including e-mail attachments, should be business related and should be scanned by a reliable and updated virus detection utility.

(e) All Internet chat facilities and streaming media are strictly prohibited for all employees unless it is business related. The downloading of large non-business related files is prohibited. This includes music files such as MP3s, movies (MPEGs), "webcasts" or real time productions as well as non-streaming files such as most .wav, .avi, and .mov files. These media files and streaming media applications use a tremendous amount of bandwidth and severely degrade our overall Internet performance. The use of file sharing "peer-to-peer" web sites is prohibited from any County PC.

(f) Sensitive information should not be placed in Cloud Storage or on a website accessible from the Internet without security measures being implemented

and used and approved by the head of the department that is the custodian of the information.

4. No Expectation of Privacy

All network traffic, including, but not limited to e-mail, Internet, and LAN communications shall be subject to electronic monitoring, thus there should be no expectation of privacy by the system user.

5. Prohibited Activities

Users shall not use Lancaster County computing resources for any purposes that violate applicable laws, including but not limited to:

(a) libel or slander other users, individuals or institutions;

(b) posting or in anyway compromising the personal information of others;

(c) extortion;

(d) violation of copyright, (i.e. pirating software);

(e) gaining or attempting to gain unauthorized access to any kind of network, service, information, communications or computing facility or resources, inclusive of Lancaster County network;

(f) damaging or destroying the integrity of a computer system, or the data or programs stored on a computer system.

(g) displaying, receiving, or disseminating sexual or pornographic material, in any form, for personal or non-work-related use.

(h) activities focused on creating personal profit.

(i) activities related to on-line gambling;

(j) activities that overly tax network bandwidth without prior approval from IT.

6. Computer Viruses & Worms

(a) Unlicensed software shall not be run on any Lancaster County computer or computer system.

(b) No shareware games, utilities, or any other shareware file may be loaded onto any computer system without the approval of a Security officer.

(c) Users should be cautious about opening attachments to e-mail messages if the sender of the message is not known to the user.

(d) Users shall not disable or remove any antiviral program, without the permission of the Security Officer.

(e) Users bringing storage media from outside Lancaster County environment shall ensure that such media is scanned for viruses before being used. Users shall utilize automatic virus scanning to examine documents and executables stored on the file server.

(f) Each computer system must execute a virus protection program at boot-up that has been approved by Lancaster County IT. The virus definition file used by the virus protection software must be kept current. It is the responsibility of the departmental ISOs to periodically check that virus protection programs are running on computers in their department and are current.

(g) No employee shall copy, distribute, or introduce any software known or suspected of being infected with a virus onto a computer system.

(h) If the employee's computer system is operating in a manner that is not consistent with its typical operation, the employee should promptly notify IT or their Security Officer. The system may have a virus.

(i) If an employee's computer or storage media has been found to contain a virus, the employee must notify Lancaster County IT. The employee should supply Lancaster County IT with information which includes name or type of virus, software used to detect the virus, extent of infection, source of virus (if known), potential recipients of infected material, and steps taken to disinfect the virus, if any.

7. Dial up, Modem Use & VPN

To protect the data that resides on our computer systems it is imperative that we maintain a positive control over all of the communications entry points that could be utilized to access our computer systems. To achieve this objective, IT will establish controls and procedures to positively identify authorized remote users of Lancaster County computers and to preclude access by unauthorized users to all Lancaster County computers. The controls and procedures that are developed and installed should also be capable of identifying suspected attempts to breach the security measures in place.

(a) The installation, set-up and use of PC software which provides a remote user control of an in-house desktop computer (e.g. Carbon Copy, Close-up, PC Anywhere, Procomm Plus, Remote Desktop, VPN) requires the prior approval of the Application Owner(s) and IT for all application(s) which can be accessed. Such installation, set-up and use will be required to adhere to procedures specified by IT to restrict and control such access. Any machine that is set up to host a remote session must be locked when not in use.

(b) Dial-up numbers for non-public dial-in access shall be classified as sensitive data.

(c) Users shall use personal firewalls if connected to County networks through a dial up or Internet connection.

(d) Users shall not install modems on LAN-based workstations, without the express written permission of IT. Workstations with built-in modems shall not be connected to an analog telephone lines at any time, unless approved by IT.

(e) Any computer that has been authorized to have a modem must be shutdown at the end of each day, or the phone jack unplugged from the modem.

(f) A modem may be connected within the same computer that accesses CLEAN data if the Agency has received written permission from the Pennsylvania State Police CLEAN Administration.

8. Fax Modem Use for CLEAN Information

The use of a fax modem to transmit CLEAN/NCIC data to another criminal justice agency is allowed under the following conditions:

(a) There must be a firewall type device on the faxing computer.

(b) The person issuing the fax must make contact with the person who is to receive the fax prior to and immediately after the fax is transmitted to confirm receipt.

(c) Auto answer must be disabled.

(d) The Information Security Officer must approve the fax modem.

9. Encryption

(a) Protected health information that is transmitted electronically shall be kept confidential via encryption.

(b) Sensitive data shall not be stored on a laptop or portable storage media without supervisory approval. Sensitive data stored on a laptop or portable storage media must be encrypted before leaving the work place. The use of a County approved cloud based storage facility is preferred to storing data on a laptop or portable storage media.

10. Sale and/or Disposal or Re-use of Computer Hardware

Sale and/or disposal of computer hardware shall mean the sale or auction of said equipment to another party, loaning the equipment to an approved organization, or

the actual final disposal of said equipment. Prior to the sale or disposal of the system, or re-use of a system, the hard disk shall be 'cleaned' by utilizing media degaussing, so that no data can be recovered.

11. Lost or Stolen Computer Equipment

An employee that has had Lancaster County-issued computer equipment stolen or lost shall report the next workday:

1. to their supervisor, Department Head or Elected Official, or a Security Officer.

2. to local law enforcement where the loss or theft occurred

The department supervisor, Department Head or Elected Official, or Security Officer shall then inform the IT Department via the IT Help Desk.

Once the IT Department receives the report of lost or stolen equipment, the CISO shall then notify the Commissioners' office, Department Head or Elected Official, and the District Attorney's office (if the theft or concern appears to be severe in nature). Court Administration shall also be notified if the equipment is under the responsibility of the Lancaster County Courts.

Once the Commissioners' office has received notification of lost or stolen equipment, the appropriate Commissioners' office representative shall contact the insurance agency for next steps.

D. Data Classification Process / Responsibility

1. Data Classification

To ensure the proper handling and disposal of data and information within Lancaster County it is necessary to establish a data classification scheme for Lancaster County data. Computer output regardless of the media used, which is classified in accordance with this classification scheme will comply with the local, state and federal laws that apply to its access and distribution. It is the responsibility of the Department Heads or their designees that are serving as custodians of various types of County data to properly classify the information under their jurisdiction and adhere to all applicable laws and policies. For the purposes of this document any information that is not a public record should be considered sensitive information.

(a) Originators of data shall be responsible for assigning a classification to the information and adhering to applicable laws and policies.

(b) Users shall not release information to the public unless it is a Public Record or they are authorized to do so either by job function, direct supervisor or

Open-Records Officer. For Court maintained information, authorization must come from the direct supervisor or Rule 509 Officer.

Notwithstanding the categories and definitions below, access to and disposal of information pursuant to this policy shall be in compliance with all applicable Federal, state, and local laws, rules and regulations.

2. Data shall be classified as:

(a) **Public Record** –Information, regardless of physical form or characteristics, that (1) documents a transaction or activity of an agency or department, (2) is created, received, or retained pursuant to law or in connection with a transaction, business, or activity of the agency or department, and (3) is not exempt from disclosure pursuant to any Federal, state, or local law, rule, regulation, or judicial order.

(b) **Proprietary -** This classification includes all information that may normally be considered general information, however, for business reasons management has determined that its use and dissemination need to be controlled. This includes any records that are identified as exceptions to the **Pennsylvania Right-to-Know Law.**

(c) **Protected Health Information –** Individually identifiable health information that is maintained or transmitted in any form or medium. **Access to and disposal of this information shall be in compliance with the Lancaster County HIPAA Policy and applicable provisions of FERPA**

(d) **Criminal History Information –** Information collected by criminal justice agencies concerning individuals, and arising from the initiation of a criminal proceeding, consisting of identifiable descriptions, dates and notations of arrests, indictments, information or other formal criminal charges and any dispositions arising therefrom. The term does not include intelligence information, investigative information or treatment information. **Access to and disposal of this information shall be in compliance with the provisions of 18 Pa C.S.A. Chapter 91 et al regarding automated Criminal Justice Information Systems and protected information and the Rules and Regulations of the Pennsylvania Attorney General's Office.**

(e) **Intelligence Information –** Information concerning the habits, practices, characteristics, possessions, associations or financial status of any individual compiled in an effort to anticipate, prevent, monitor, investigate or prosecute criminal activity. **Access to and disposal of this information shall be in compliance with the provisions of 18 Pa C.S.A. Chapter 91 et al regarding automated Criminal Justice Information Systems and**

protected information and the Rules and Regulations of the Pennsylvania Attorney General's Office.

(f) **Investigative Information –** Information assembled as a result of the performance of any inquiry, formal or informal, into a criminal incident or an allegation of criminal wrongdoing and may include modus operandi information. **Access to and disposal of this information shall be in compliance with the provisions of 18 Pa C.S.A. Chapter 91 et al regarding automated Criminal Justice Information Systems and protected information and the Rules and Regulations of the Pennsylvania Attorney General's Office.**

(g) **Treatment Information –** Information concerning medical, psychiatric, psychological or other rehabilitative treatment provided, suggested or prescribed for any individual. **Access to and disposal of this information shall be in compliance with the provisions of 18 Pa C.S.A. Chapter 91 et al regarding automated Criminal Justice Information Systems and protected information and the Rules and Regulations of the Pennsylvania Attorney General's Office and the Lancaster County HIPAA Policy.**

(h) **Personal Information** - is an individual's first name or first initial and last name, linked to any of the following: social security number, driver's license number, financial account number, birth year or unique identifier assigned to an individual. The unauthorized access and acquisition of computerized personal information that materially compromises the security or confidentiality of person information maintained by the county is considered a breach of security and requires notification of the affected individuals.

(i) **Information and Technology Management Information** - information regarding the IT resources and systems required to support departmental operations, even when all mission-related information processed by the system is intended to be available to the general public.

3. Handling Sensitive Data

Sensitive data is considered any data that is not a public record and for the purposes of this security policy it can be considered data that falls into one of the following previously defined classifications: proprietary information, protected health information, criminal history information, intelligence information, investigative information and treatment information.

(a) When users are printing reports on printers other than those located in secure facilities, they are responsible for ensuring adequate protection for the information contained in the report.

(b) Users are responsible for ensuring that the printout of sensitive information is sent to an appropriate printer and picked up immediately. If sensitive information is inadvertently sent to the wrong printer, the person responsible shall report the incident at once to the departmental Security Officer.

(c) Sensitive information should not be faxed unless no other alternative exists.

(d) All sensitive material that is copied or printed shall be disposed of in the manner defined by the applicable law or policy.

(e) When photocopying sensitive material, employees shall take every precaution to ensure that unauthorized persons do not see the material.

(f) When photocopying sensitive material, employees shall make only as many copies as are necessary. If excess copies are made, the employee responsible shall destroy any unused copies.

(g) When photocopying sensitive material in an unsecure facility, the employee responsible shall remain at the photocopier while the document is printing, wait for the document to print out, and retrieve it immediately.

(h) When photocopying sensitive material, the employee responsible shall ensure that no copies or partial copies are left unaccounted for.

(i) Documents containing sensitive data shall not be left unattended.

(j) Employees who have desks in an open area shall secure any sensitive material before leaving their desk.

(k) County maintained sensitive information is not allowed to leave the County owned or leased facility unless approved by a Senior Staff member responsible for the information in question. A County approved cloud-based storage facility is considered a County leased facility.

(l) The unauthorized access and acquisition of computerized personal information that materially compromises the security or confidentiality of person information maintained by the county is considered a breach of security and requires notification the affected individuals.

(m) Employees who access sensitive data from a device not owned by the county need to ensure that the device is secured and that a copy of the sensitive data does not remain on the non-county device. One way this can occur is when an employee accesses e-mail from a home computer or their personal cellphone.

(n) The use of Cloud Storage for sensitive data requires authorization by the head of the custodial department.

4. Use of Cloud Storage

Lancaster County has acquired a cloud-based solution that will provide users with cloud storage for their exclusive use, to replace their current 'home' drive, as well as cloud storage in a shared environment, to replace the current shared drives. Users should store work documents and data on cloud-based storage, rather than on device hard drives or USB storage devices, as cloud based storage provides better security than the alternatives.

(a) Use of cloud computing services for work purposes, other than the solution acquired by the County, must be formally authorized by the Chief Information Officer. The Chief Information Officer will certify that security, privacy and all other IT management requirements will be adequately addressed by the cloud computing vendor.

(b) For any cloud services that require users to agree to terms of service, such agreements must be reviewed and approved by the Legal Department.

(c) The use of such services must comply with County Information Security Policy.

(d) The use of such services must comply with all laws and regulations governing the handling of personally identifiable information and protected health information.

(e) Cloud storage of sensitive data must be approved by the director of the department who is the custodian of that data.

(f) Unapproved cloud storage accounts may not be used for the storage, manipulation or exchange of county-related communications or county data.

(g) Users may not self-provision cloud storage and processing services to store, process, share, or manage county data.

(h) Upon termination, IT will make the contents of the former employee's cloud storage available to a designated individual in the department.

E. Physical Security

1. Physical Security - General

(a) Users who have desks in an area open to the public are to secure any sensitive material before leaving.

(b) All sensitive material (including hard copy code) must be disposed of in accordance with the applicable county procedure. In many cases hard copy materials must first be shredded before being placed in the trash for disposal.

(c) All data storage media must be bulk erased prior to being placed in the trash or transferred to another department / agency.

(d) Copiers that are equipped with internal storage that retains the images of documents must be erased before being disposed. Copier leases shall include language that ensures the internal storage device is erased or removed before County returns the copier.

(e) Users working in secure facilities are to keep all perimeter doors secured or otherwise maintain physical security at all times.

(f) Users are required to report anything they believe is a security weakness or security breach to an Information Security Officer.

(g) Users may not loan an access card to anyone for any reason.

(h) Users are not to allow unauthorized person(s) to enter a secure facility along with the employee.

2. Physical Security - Clear Desk Policy

The Clear Desk Policy is intended to define what is expected from an employee, consultant, or consultant in regard to protecting the contents of their work area.

(a) Any employee of the organization shall ensure that any sensitive data be secured at all times.

(b) In the event an employee must leave his or her work area leaving any documents or other media containing sensitive data unattended, the user must lock their office door.

(c) At no time should an employee leave any sensitive data on his or her desk unattended without any means of securing said data. This information should always be secured in a locked cabinet, safe, secured office or locked desk draw

(d) In the event the user must leave their work area and their workstation is left unattended, it is the responsibility of that user to ensure that their workstation is locked or that the password protected screensaver is manually invoked to protect access to the screen.

(e) At no time should an employee leave any type of County documents containing sensitive or county data on their desk in plain view.

3. Physical Security - Handling Visitors

(a) All visitors entering non-public areas of County or Court facilities should be required to sign in and be escorted at all times; only authorized

employees shall escort visitors. If a visitor needs to be left unattended to use a private office, the escort shall ensure that the office is clear of non-public material prior to the visitor entering.

(b) All visitors must sign in at the reception desk and then be accompanied to the person they are visiting. The receptionist shall keep a visitors log.

(c) All maintenance personnel IDs should be checked and may only be allowed on the premises after verification.

F. Background Investigations

Anyone with access to sensitive data or administrator privileges may be required to undergo a background check (criminal history), at the discretion of the applicable Department Head. In order to implement such a policy, Lancaster County must adhere to the following requirements:

(a) All IT employees and any employees with access to sensitive data or administrative privileges to the network, domain or an application that contains sensitive data will be required to undergo a background check.

(b) Background checks shall be initiated before an offer letter is signed, or upon such time that consent has been obtained.

(c) The Pennsylvania State Police require a background check for anyone with access to CLEAN/NCIC, JNET - Criminal History or who may be responsible for providing technical support to machines that provide this access. The Pennsylvania State Police will not grant CLEAN access to anyone that has been convicted of a Felony or Misdemeanor I charge.

(d) All IT employees will be added to a JNET 'watch list' to provide continuous monitoring by the Pennsylvania Justice Network.

(e) All applicable IT employees will be fingerprinted.

Each department shall be responsible for submitting a completed "Request for Employee Background Check" form for every employee with access to sensitive data or administrative privileges to the network, domain or an application that contains sensitive data. Failure to complete the form shall disqualify the individual from potential employment. Failure to provide truthful, correct and complete information on the form may result in disqualification

G. Contractor and Outsourcing Policy

1. Password Management for External Consultants

(a) All external consultants shall adhere to the applicable sections of the Lancaster County Information Security Policy. Any external consultant

who will have access to sensitive data during their engagement with the County shall be required to sign an acknowledgment that they will abide by the Lancaster County Information Security Policy.

2. Background Checks for External Consultants

(a) Prior to being allowed access to the Lancaster County network, all external consultants that could receive access to sensitive data should be subject to a criminal history background check.

(b) These background checks are necessary to protect the permanent employees of Lancaster County as well as any sensitive intellectual data that this individual may be working with.

3. Use of the Systems

(a) Users shall be strictly forbidden to use any element of the system that they are not authorized to use.

(b) Unauthorized users shall be strictly forbidden to use any element of the system.

4. [redacted]

[redacted]

H. [redacted]

[redacted]

[redacted]

[redacted]

A. [redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

B. [redacted]

1. [redacted]

[redacted]

[redacted] staff.

2. [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

3. [redacted]

[redacted]

[redacted]

[redacted]

4. [redacted]

- [redacted]

[redacted]

[redacted]

[redacted]

5. [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

6. [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted] [redacted].

7. [redacted]

[redacted]

[redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted] [redacted]

[redacted]

8. [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]

[redacted]

[redacted]

9. [redacted]

- [redacted]
- [redacted]

10. [redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]

11. [redacted]

- [redacted]
- [redacted]
- [redacted]

12. [redacted]

[redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

[redacted]

13. [redacted]

[redacted]

C. [redacted]

[redacted] [redacted]

[redacted]

[redacted] [redacted]

[redacted]

[redacted]. [redacted]

[redacted] [redacted]

[redacted]

[redacted] [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted].

[redacted]

(c) [redacted]

[redacted].

2. [redacted]

- [redacted]
- [redacted]
- [redacted]

3. [redacted]

[redacted]

[redacted]

4. [redacted]

[redacted]

5. [redacted]

[redacted]

D. [redacted]

1. [redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]

[redacted]

[redacted]

2. [redacted]

[redacted]

[redacted]

3. [redacted]

[redacted]

4. [redacted]

[redacted]

[redacted]

[redacted]

5. [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted].

E. [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted].

1. [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

- [redacted]

[redacted]

F. [redacted]

[redacted]

[redacted]

- [redacted]

[redacted]

- [redacted]

[redacted]

- [redacted]

[redacted]

G. [redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted].

2. [redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

[redacted]

[redacted].

H. [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted].

I. [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted].

J. [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]