Policy Cover	
Title: General Technology Policy	**Effective Date:** March 20, 2018
	Adoption/Revision Date: March 20, 2018
Custodian: Information Technology Services Director	**Approving Body:** Executive Committee

1. **Authority**
    a. Executive Committee
2. **References**
    a. Various IT Steering Committee minutes.
3. **Purpose**
    a. To establish guidelines for General Technology use.
4. **Scope**
    a. Applies to all Clark County Government employees.
5. **Policy Overview**
    a. This sets expectations and guidelines for all Clark County employees and agents who use and manage information technology resources and services including, but not limited to, computing, networking, communications and telecommunications systems, infrastructure, hardware, software, data, databases, personnel, procedures, physical facilities, and any related materials and services.
6. **Policy Performance**
    a. The quantifiable performance indicator for this policy is one-hundred percent (100%) compliance by Clark County personnel.
7. **Clark County Mission Statement**

    The mission of Clark County and its employees is to provide cost effective services, with equal access to all citizens; to continue and enhance partnerships; to responsibly manage our resources and prepare for the future.

TABLE OF CONTENTS

Policy Statement

Clark County Government ("County") provides employees with access to and the use of a variety of information technology resources. These resources are provided to employees in an effort to allow them to be more efficient, productive, and to have access to information that is necessary for them to carry out their responsibilities as an employee of the County. Employees are expected and required to use these information technology resources in a manner consistent with their position and work responsibilities with the County.

In addition, employees are expected to follow all appropriate security practices and procedures designed to maintain the confidentiality, integrity, and availability of information and the associated automated systems, workstations and other equipment that create, receive, maintain, or transmit it.

Inappropriate use of the County's information technology resources or failure to follow the appropriate policies and procedures for information security and technology use may result in discipline up to and including discharge of employment. In addition, some information is protected by law, for which misuse by employees may result in legal, criminal, or monetary penalties including fines and/or imprisonment.

Responsible for Implementation

A. Clark County Government

Clark County Government 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 affiliated agencies and business partners.

The County maintains the authority to take any of several steps to protect the confidentiality, integrity, and availability of Information Technology Resources, and protect legitimate users from the effects of unauthorized or improper use of these facilities. These steps include the authority to limit or restrict any employee's usage of Information Technology Resources and facilities where they are located; the authority to inspect, copy, remove or otherwise alter any data, file, or system resources that may undermine the proper use of that system; and any other steps deemed necessary to manage and protect the County's Information Technology Resources and facilities where they are located. This authority may be exercised with or without notice to the employee; however, whenever possible, the Information Technology Services Director will consult with the department head or designee prior to taking action. The County disclaims responsibility for any loss or damage to data that results from its efforts to enforce these rules or from any changes, upgrades, or maintenance of the County Technology Resources.

B. **Information Technology Services**

Information Technology Services Department roles and responsibilities include, but are not limited to the following:

1. Maintaining, administering, and operating all servers, infrastructure and security equipment for Clark County Government agencies.

2. Acting as the custodian of the County's Information Technology Resources and implementing the Policies regarding information security.

3. Acting on behalf of Clark County Government and Department Heads to secure information, applications, systems and networks; providing authorized access to approved personnel; and monitoring, detecting, investigating and reporting on actual or suspected security breaches or incidents.

4. Acting as the gatekeeper for access to all Information Technology Resources, including Internet access. The Information Technology Services Department establishes the procedures for access to all Information Technology Resources, including the internet and is responsible for informing the departments of these procedures.

5. Utilizing appropriate destruction methods for obsolete removable media as well as non-removable media, following the Clark County Records Retention Schedule.

C. Department Heads

Department Heads' roles and responsibilities include, but are not limited to the following:

1. Being responsible for all electronic information in their areas, as well as stored documents and data archives. They determine who will be allowed to access their information, consistent with their policies, applicable laws, and this policy. The Department Head may delegate this authority to one other person in their organization who may act or sign on their behalf. The final responsibility for establishing clear guidance for their data and enforcing security policy lies with department heads as well as the Information Technology Services Department.

2. Determining application access roles and requirements and enforcing, monitoring, and managing them along with the Information Technology Services Department.

3. Ensuring that employees with access to Protected Health Information receive appropriate required training before authorizing access to this information.

4. Monitoring all Information Technology Resource usage by their employees to ensure it complies with all applicable laws and policies. To assist in the responsibility, Department Heads may request reports detailing Internet and Technology Resource usage from the Information Technology Services Department.

5. Training interns, volunteers, contractors, and other business partners of the appropriate security and technology use for the county as outlined in this document.

6. Comply with the Clark County Retention Schedule.

D. **EMPLOYEES**

All employees who are provided with access to Clark County electronic information are responsible for all usage of these resources. Following is a list of general responsibility statements, which are more fully detailed in other sections of this policy. Employees are responsible for:

1. Password protection,
2. Proper logout from all open applications,
3. Powering off CPU (computer) and monitor at the end of the employee's workday, unless needed for offsite/remote work,
4. Store all information on the file server,
5. Understanding and complying with all Federal and State laws and regulations and County and Department policies and procedures as they apply to Information Technology use, data security, and use of protected health information (PHI), electronic protected health

information (ePHI) and other restricted as well as sensitive information, collectively "Confidential Information",
6. Utilizing appropriate workstation physical security solutions,
7. Identifying and reporting technology use and/or security related problems and issues,
8. Users are and will be held accountable for all activity that occurs under their passwords and/or account name,
9. Comply with the Clark County Retention Schedule.

Definitions

A. Employee

All regular full-time, regular part-time, limited benefit employees, seasonal employees, temporary employees, State of Wisconsin employees working within County government, volunteers, and appointed or elected officials who have been granted access and use of Clark County's Information Technology Resources.

NOTE: Throughout this policy, the use of the term "Employee" includes Employees as described above, and Affiliated or Tenant Agencies and Business Partners as described below.

B. Affiliated or Tenant Agency / Business Partner

Departments or agencies that are members of, or occupy space within Clark County buildings, but whose networking and/or computer support comes from an external entity. This definition also includes contractors and vendors.

C. Electronic Protected Health Information (ePHI)

Any individually identifiable health information protected by HIPAA that is transmitted by or maintained in electronic media.

D. Information Technology Resources

For the purposes of this policy, the County defines Information Technology Resources as any equipment, hardware, or software that is assigned and available for employees to use in the course of their employment. These resources include, but are not limited to the following:

Printers, software applications, Information Technology Services, Internet access, VOIP, e-mail, personal computers, laptops, tablets, digital cameras, USBs/flash drives, plotters, scanners, mobile devices, smart phones, mobile data terminals, squad laptops, copy machines, electronic data and databases, servers, and the various networks.

E. Minimum Necessary

Protected health information (PHI) and other restricted as well as sensitive information, collectively "Confidential Information" that is the minimum necessary to accomplish the intended purpose of the access, acquisition, use, disclosure, or request. The "minimum necessary" standard applies to all Confidential Information in any form.

F. Protected Health Information (PHI)

Protected health information means individually identifiable health information that is: transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium.

G. Remote Access

Connection to County networks and/or systems from outside of a County building or campus location may be done only through secure methods approved by the Information Technology Services Department. This includes, but is not limited to, dial-up from home or other locations, client-based VPN, router-based VPN, VAPP, or access to an application through the Internet.

H. Role
The category or class of person or persons doing a type of job, defined by a set of similar or identical responsibilities.

I. Sensitive Information
Release of such information would cause "undesirable" effects to Clark County (i.e., would impact the reputation of Clark County or business relationship with a client, vendor, or other interested party, but would not materially impact Clark County financials) (e.g. information not generally in the public domain, internal Information Technology Services policies and procedures).

J. Privacy Officer which is designated as Clark County Corporation Counsel and is defined as:
The **Privacy Officer** oversees all ongoing activities related to the development, implementation, maintenance of, and adherence to the organization's policies and procedures covering the **privacy** of, and access to, patient health information in compliance with federal and state laws and the healthcare.

K. Security Officer which is designated as Clark County Information Technology Director and is defined as:
The **Security Officer** is responsible for the ongoing management of information **security** policies, procedures, and technical systems in order to maintain the confidentiality, integrity, and availability of all patient health information systems.

Business use only

The County's Information Technology Resources shall be used for Clark County Government business only.

Personal Use of Information Technology Resources

The County does not allow ANY personal use of Information Technology Resources unless there are unique circumstances and approved by the Department Head.

Unacceptable Use of Information Technology Resources

Unacceptable use of the County's Information Technology Resources unless such a action is required by official investigative duties include, but are not limited to the following:

A. Unauthorized use.
B. Illegal purposes.
C. Transmittal, creation, viewing, installing, downloading, and/or copying of threatening, abusive, obscene, lewd, profane or harassing material or material which suggests any lewd or lascivious act.
D. Transmittal, creation, viewing, installing, downloading, and/or copying of derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes, sexual preference, political affiliation, or health condition.
E. Intentionally preventing or attempting to prevent the disclosure of your identity with the intent to frighten, intimidate, threaten, abuse or harass another person.
F. Unauthorized or improper transmittal of material that is confidential to the County, or is otherwise protected by law.
G. Disruption of network services, such as knowingly distributing computer viruses, or actual or attempted intrusion, destruction or defacement of information (hacking or cracking).
H. Interception or alteration of network packets.

I. Use of someone else's identity (e.g. user name) and password for access to Information Technology Resources.
J. Attempt to evade, disable, or decipher passwords or other security provisions of systems on the network without proper authorization.
K. Reproduction and/or distribution of copyrighted materials without proper authorization.
L. Allowing non-authorized individuals to access or use Information Technology Resources.
M. Attaching personal networking devices to the County network.
N. Downloading or storing PHI on workstations, personal devices, personal workstations and devices, etc.
O. Connecting to unauthorized networks through the organization's systems or devices.
P. Disabling or interfering with the County-installed anti-virus systems.
Q. Accessing Social Media sites on the County network without express written consent from the Information Technology Services Director, unless access is work related.
R. Requesting to receive or sending of chain letters/emails.
S. Changing operating system configurations, upgrading existing operating systems, or installing new operating systems.

Ethics Conflicts

Information Technology Resources shall not be used for commercial ventures, personal gain, religious or political causes.

Authorization of Use

Employees are to be provided access to County Information Technology Resources only if authorized by the appropriate department head or designee. Employees shall only be granted the minimum level of access to networks, information, and technology required to perform their job responsibilities. All access that is not specifically permitted is denied.

County Access

The County reserves, and intends to exercise its right, as is reasonably necessary, to search, review, audit, monitor, suspend, intercept or access an employee's use of the Information Technology resources provided to him/her.

Work Product

All work products created through the use of Information Technology Resources are the property of Clark County Government. Any materials developed, composed, sent or received, using County provided Information Technology Resources are, and will, remain the property of the County.

External Devices

No County documents are to be allowed on any external, mobile, or removable drives without the express written permission from the Information Technology Services Director. All external devices will/should be encrypted and secured. Clark County has deemed using external, mobile, or removable drives purchased/provided devices purchased / provided by others an unacceptable risk to Confidential Information and the organization's Information Technology Services and, therefore, will not accept or use them.

Should Confidential Information be provided on a USB / flash drive or CD purchased by Clark County, provide a disclaimer with the USB / flash drive or CD that states:

- To the best of our knowledge, this USB / flash drive or CD does not contain a virus or anything harmful to your equipment. You agree by using this device that you are using it at your own risk and will not hold Clark County liable for any issues that may arise by using it.

Non-County Owned / Personally Owned Devices

Non-County owned / personally owned devices (peripheral devices) include but are not limited to: cellular phones, smart phones, iPads, Notebooks, printers, etc.

A. These devices may be used to conduct Clark County related business as long as the public's information is adequately secured.
B. These devices shall not be utilized to record, document, take pictures of, or transmit PHI in any way.

No Expectation of Privacy

Employees do not have an expectation of privacy or privilege regarding the use of Information Technology Resources regardless of the assignment or creation of passwords, ID numbers or access codes.

Employees shall have no expectation of privacy when using County email, electronic communication tools, County devices or accessing County services using any device. All County devices and non-County devices accessing County Information Technology Services may be reviewed and audited by the Information Technology Services Director; including full activity, internet usage, key, screen, click and tap logging.

All files, data, information, faxes, email and other electronic communications created, stored, transmitted or accessed on County Information Technology Services are County property, and are not private and fully accessible to Clark County. Further all County systems may be monitored automatically and/or monitored without notice. Direct Supervisor may request access to employee email, files, computers or systems.

All County information may be treated as open records or public records and may be subject to public disclosure in accordance with applicable law, including, but not limited to, Open Records laws (Wis. Stats Chapter 19) and Crimes Against Property Laws (Wis. Stats Chapter 943).

Documents for Public Use

Any documents that are allowed to be distributed for public use electronically must be saved and distributed as a PDF documents.

Administration and Enforcement of this Policy

Administration and enforcement of the provisions contained herein shall be the responsibility of the employee's immediate supervisor and/or Information Technology Services Director and in turn, the department head.

E-mail Use

The following items apply specifically to the use of E-mail on Clark County Government systems:

A. E-mail is not a secured media, except inside the County's E-mail system. Any E-mail that can be sent out of the County's E-mail system, is considered non-secure. A special encrypted E-Mail system exists which is used to pass protected information, including PHI, outside of the County (County encryption, County TLS, and other organizations' secure encryption solutions).

B. E-mail is subject to applicable privacy, security, and records retention laws and guidelines for the information that a particular message contains. As such, E-Mail records must be appropriately secured and retained.

C. No employee shall e-mail sensitive, personal or Confidential Information, including PHI, unless it is authorized and sent by approved, encrypted methods (unless allowed by HIPAA privacy policies).

   a. Do not include PHI, such as a patient name, account number, phone number, etc. in the subject line of the email.
   b. Before sending the email, verify:
      i. You are sending it to the correct individual(s)
      ii. The email is/will be encrypted.

D. Employees shall not open unusual looking or unexpected E-Mail. E-Mail is often used by others for illegal purposes and may contain computer viruses.

E. Employees shall not respond to E-Mail requesting personal or banking information, or requesting user ID's or passwords.

F. If an employee has any doubt about the authenticity of an E-Mail, website link within an E-Mail, suspicious E-mail attachments (e.g. from an unknown sender or from a known sender that you do not believe would have sent the E-mail), or about what the E-Mail is requesting, the employee shall:
   a. Not click on these website links or attachments;
   b. Delete the email if known to be SPAM or junk; and
   c. Notify their supervisor and Information Technology Services Department immediately when uncertain.

G. Except as provided in paragraph H. below, all employees shall have the following confidentiality notice in every email that is sent:

   a. CONFIDENTIALITY NOTICE: This e-mail, including any attachments, may contain confidential, privileged and/or proprietary information. Disclosure of this email, including any attachments, is strictly limited to the recipient intended by the sender of this message. Receipt by anyone other than the intended recipient does not constitute waiver or loss of the confidential or privileged nature of the communication. Any review, use, copying, disclosure, or retention by others is strictly prohibited. If you are not an intended recipient or you have received this e-mail message in error, please contact the sender and delete this e-mail, any attachments, and all copies.

H. Any employee providing legal advice (attorney) shall have the following Confidentiality Notice in every email that is sent:

a. CONFIDENTIALITY NOTICE: This e-mail message may contain information which is subject to the attorney-client privilege and/or attorney work-product doctrine and therefore confidential. Disclosure of this email, including any attachments, is strictly limited to the recipient intended by the sender of this message. Receipt by anyone other than the intended recipient does not constitute waiver or loss of the confidential or privileged nature of the communication. Any unauthorized review, disclosure, dissemination, duplication or use is prohibited. If you are not the intended recipient or you have received this e-mail message in error, please notify this office immediately and delete or destroy the original and all copies.

Texts

A. Texting is an unsecured method of communication and can, therefore, be intercepted by unauthorized individuals
B. As the County does not have a means to encrypt texts, Confidential Information/PHI may not be texted at any time from any device, whether or not the texting device is owned by the County (unless allowed by HIPAA privacy or confidentiality policies or the recipient provides written informed consent).

Internet use

Internet resources are provided to employees in an effort to allow them to be more efficient, productive, and to have access to information that is necessary for them to carry out their responsibilities as an employee of the County. Employees are expected and required to use the Internet in a manner consistent with their position and work responsibilities with the County. Approval of the employee's department head (designee) is required to get access to the Internet. Inappropriate use of the County's internet resources may result in discipline up to and including discharge of employment. In addition, the employee may be subject to civil and/or criminal penalties.

The following items apply specifically to the use of the Internet:

A. All Internet users are responsible to ensure they are in compliance with all applicable laws and County policies, including computer security, virus detection, and access to questionable sites and/or material.

B. Under no circumstances shall the Internet be used to access lewd, objectionable, pornographic sexually explicit, or illegal materials, or sites that are sponsored by or contain materials regarding discrimination, hate groups, or gambling. The only exception is when such access is used to perform official investigations, required in the course of one's work, and approved by the Department head.

C. Internet access requires authentication through the firewall to ensure that only authorized employees may access the Internet.

D. Streaming media should only be used for official or training purposes. The Internet shall not be used to listen to radio or TV broadcasts for entertainment. Using the CC-Guest wireless account on a personal phone is allowed.

E. Instant messaging is not allowed, except for that which is provided by the County's E-Mail system.
    a. Instant messaging is an unsecured method of communication and can, therefore, be intercepted by unauthorized individuals.

b. Workforce may utilize the County's messenger system to internally exchange communications that include Confidential Information.
c. PHI may not be sent through any other instant messaging systems at any time from any device, whether or not the instant messaging software and/or device is owned by the organization.

F. Employees shall not purchase any items on the Internet from any County workstation or network connection using a personal credit or debit card, unless that transaction is for County business (such as purchasing plane tickets or to guarantee a hotel room for a conference).

G. Employees shall exercise caution when prompted to enter information which will identify them or the networking architecture of the County. If there is any question regarding the legitimacy of the site or the information being requested, the employee must notify their supervisor or contact the Information Technology Services Department before proceeding. Employees accept all risk when entering personal, medical, or financial information of any kind on external websites.

H. Personal accounts. PHI and County related business may not be sent through personal email, text, instant message, blog, chat rooms, or other personal accounts, or posted or "discussed" on social media or any other websites or publically accessible Information Technology Services (e.g. Facebook, Instagram, Flickr, LinkedIn, Myspace, Snapchat, Tumblr, Twitter, YouTube, etc.). Refer to additional social media requirements in the Social Media Policy and Procedure.

I. Employees shall not download programs or plug-ins from the Internet unless authorized to do so by the Information Technology Services Department. Such actions could download viruses or other malicious code, or could violate licensing and copyright laws.

J. File downloads such as *.pdf files, word documents, research materials, etc. are permissible, as long as they are work related.

K. The Internet shall not be used to attack or test the security of other systems.

Remote Access

Clark County allows remote access for users using a client access software. Requests for remote access via the client access software must be submitted to the Department Head and IT department.

The following items apply specifically to Remote Access use:

A. Remote access service is provided to conduct County-related business only.
B. Remote access service shall only be used while employee is an authorized user and employed by the County. Authorization ends at termination of employment with the County.
C. Service may be limited, suspended or terminated is cases of suspected or known issues by employee, with or without notice to the user.
D. The County has the right to limit the duration and number of available remote access sessions.
E. All users shall abide by the Clark County Confidentiality Agreement (Attachment A) and the General Technology Policy when accessing and using any information that resides on Clark County information systems.
F. Users agree to apply safeguards to protect County information assets from unauthorized access, viewing, disclosure, alteration, loss damage or destruction. Appropriate safeguards include use of discretion in choosing when and where to use remote access services, prevention of inadvertent or

intentional viewing of displayed or printed information by unauthorized individuals, and use of antivirus software on remote computers.

Password Use

Information Technology Resource passwords shall be of sufficient strength so as not to be easily cracked or broken by unauthorized individuals, and to ensure the safety of the information and networks within Clark County Government. The Information Technology Services department will establish and communicate specific requirements for password content.

The following items apply specifically to password use:

A. Each user shall have his/her own, unique login account and password. No default user ID or password will be permitted on any system.
B. Passwords shall not be stored on or near computer equipment, nor written down unless they are locked and accessible only to the owner.
C. Passwords shall not be stored in clear view or left in a place that someone else may see/find them.
D. If passwords are stored electronically they must be stored in an encrypted file / system that is approved by the Information Technology Services department and password protected.
E. Under no circumstances shall employees share, or be required to share, login credentials, normally Defined as the combination of both their user ID and password.
    a. Under rare circumstances a user may have a legitimate need to share a user ID and password with Information Technology Services to support and fix a system issue. When this is done, the user must:
        i. Observe all activities completed by Information Technology Services (if this is not feasible, Information Technology Services documents the dates and times the users' user ID and password were known by Information Technology Services).
        ii. Change the password immediately after this issue has been resolved.
F. Employees do not have expectation of privacy regarding the use of E-Mail on County systems regardless of the assignment of passwords, ID numbers or access codes.
G. Vendor supplied default passwords are changed before a system is attached to the organization's network.
H. Users that do not recall their user name and password need to contact the Help Desk. IT Help Desk will:
    a. Verifies the user's identity by:
        i. Calling the user back at their registered office phone, mobile phone, or home phone according to the organization's records.
        ii. Request and receive an email from the user's known email account.
        iii. If the first two options are not possible, obtain written approval by the Security Officer or Information Technology Services Director.
    b. Verbally provides the user with a temporary, one-time use user name and password.
G. Passwords are stored in an encrypted format and are encrypted when transmitted.
H. Passwords are not displayed at any time. Password characters are replaced with asterisks "*" or other symbol when typed.
I. Passwords are not included in any automatic logon script, macro or terminal function keys, etc. (i.e., passwords must be manually entered at logon time), whenever possible.
J. Organization leaders and System Administrators may not maintain a list of user passwords.

Users are responsible for all inquiries, entries, and changes made to any Information Technology Resource using their user names and passwords.

The following minimum password controls are put in place for all Information Technology Services and documented by the Security Officer (automated/programmed whenever possible):

A. Password strength:
    a. Minimum of eight (8) characters, and requires two of the following: number, upper case, lower case, and symbol/special character (e.g. #, $, *, /, etc.).
    b. Smart phones require a pass code or thumb print.
B. May not include anything personal or that are easy to guess (family member or pet names, user names, SSN, birth dates, dictionary words – unless a complex series of words, special characters and numbers are used, etc.). Users change passwords after first log-in.
C. Users change passwords every 180 days (this is automatically enforced by the system) and whenever there is reason to believe they have been compromised.
D. Users may not reuse a password for five or more password changes.
E. For Information Technology Services that do not have the above stated capabilities, the highest levels of password controls are utilized and documented. Password controls are improved when the ability to improve them becomes available.

Information Technology Services that create, receive, maintain or transmit, or otherwise provide access to PHI, whenever possible automatically lock accounts after three invalid login attempts within five minutes.

A. The user account locks for a period of 10 minutes. After this period, the bad password count is reset to zero and the user can attempt to log on.
B. IT System Administrators have the ability to unlock accounts at any time.

Electronic Signatures

A formal electronic signature can be captured using multiple tools and systems. The level of protection/encryption and verification for signatures depends on the materials being handled. There are numerous types of electronic signatures that may be used when conducting County business.

1. When you leave the area or stop using a device, press the windows key + the L key to lock your PC or log out of your PC or device, because an unattended logged in device allows others to use your electronic identity/signature.

2. Various other forms of approved electronic signatures in combination with appropriate security software include:
    a. A stylus for a handwritten signature on a tablet or other hand writing capture device
    b. A finger print as a signature
    c. Others – for more information contact the Information Technology Department.

3. Digital scans of hand written signatures.

Workstation Physical Security

Employees are responsible for maintaining the physical security of their desktop workstations, portable computing devices, and removable media (such as flash drives, external hard drives and CD's) by restricting and controlling physical access to these items. This is accomplished by utilizing the following physical security solutions:

A. Properly positioning and protecting systems such that the information cannot easily be read or obtained.
B. Monitors should generally be kept from the plain view of anyone who does not have the appropriate security access or clearance to information that may be displayed. Make sure that monitors cannot be viewed through outside windows, from public hallways, from public reception areas, or by reflection off other objects.
C. Utilize a special shade or polarizing monitor filter, when necessary.
D. When approached by an individual that may be able to view information to which they are not authorized, minimize the information system or otherwise secure it so that the individual is not able to view the information.
E. Do not allow any other individual to use any of the organization's Information Technology Resources that are not authorized by the organization to utilize them.
F. Keep keyboard, mouse, and other components far enough away from public so they cannot be tampered with or stolen.
G. Printers should be kept in protected areas to keep sensitive information from being disclosed inappropriately or use a program such as Follow me to sign on to the device to access printed information.
H. Printed materials from any source should be kept secure, away from viewing, and out of public reach.
I. Many workstations may utilize a locked down configuration where the user will not have local administrator rights on his or her own workstation to prevent the installation of unauthorized software.
J. Workstations and Information Technology Services shall utilize an automatic screensaver that is password protected and which activates after a set period of inactivity.
    a. Workstations are set to lock after 10 minutes of inactivity.
    b. VPN sessions are set to lock after 30 minutes of inactivity.
    c. Where this solution has been implemented or required, departments or employees shall take no action to disable or prolong the set time frame of this screensaver.
    d. Exceptions are approved by the Privacy Officer and Security Officer.
    e. Press the windows key + the L key to lock your PC or log out of your PC or device when not in use.
K. Removable media will have the same security requirements as the highest sensitivity of information on that device, and should be stored and secured as such.
L. Since most County information is network accessible, there should be minimal need to copy data to removable media. PHI may only be copied onto removable media that is encrypted and after being approved in writing by the Information Technology Services Department. Individuals that receive approval to download data are responsible for managing and protecting it from unauthorized access, disclosure, and theft.
M. All media storage devices shall be destroyed, following the Clark County Records Retention Schedule, by the Information Technology Services Department when it has been determined that they are no longer of use and must not be discarded in the trash.

Security and Confidentiality of Confidential Information

All employees are required to comply with state and federal laws and regulations, as well as County and Department procedures and policies regarding the use and security of electronic protected health information (ePHI), and other restricted as well as sensitive information, collectively "Confidential Information" (e.g. proprietary, sensitive, personal, or confidential information). Failure to comply will result in discipline up to and including termination of employment. In addition, the employee may be subject to civil and/or criminal penalties.

HIPAA Security Polices and Procedures

Employees who are involved with a covered function and have access to electronic protected health information (ePHI) per Federal and State laws have the responsibility to follow all documented HIPAA security and privacy practices, procedures and policies provided by Clark County. Employees must keep desktop computers, and all portable computers, physically secure and prevent them from being accessed by unauthorized users. Employees must keep ePHI data from being read by or distributed to unauthorized users.

Security of Confidential Information

Clark County Government is responsible for providing employees with the means to keep Confidential Information secure. Clark County Government is also responsible for providing secure access to Confidential Information.

Employees shall keep Confidential Information safe, private, and unavailable to employees and non-employees who have no business need to access Confidential Information. This is accomplished by:

A. Utilizing all appropriate workstation physical security measures as outlined in the workstation physical security section of this policy such as invoking the automatic screensaver, using monitor filters or enclosures, or positioning the monitor so it cannot be viewed by unauthorized individuals.
B. Logging out or locking the workstation before leaving it unattended.
C. By logging off and powering down all computer workstations at the end of workday, unless needed for work related business offsite.

Secure Computers When Not in Use

Employees shall secure workstations when not in use, by using technical solutions as stated elsewhere in this policy, that ensure only authorized users operate computers that have access to Confidential Information. Employees shall be provided with unique user IDs and shall be required to use network and application passwords to gain access to Confidential Information.

Destruction of Obsolete Removable Media Containing Confidential Information

Subject to applicable record retention laws and schedules, employees shall contact the Information Technology Services department for destruction of removable media and all obsolete removable media containing Confidential Information or other information requiring protection.

Computer Hardware/Software Usage

The following items specifically apply to the use of Clark County Government computer hardware and software.

A. **Personal Use of County Computer Hardware and Software**
Employees shall not be granted permission to use County computer hardware/software for personal purposes. Copying and use of County-owned software is not permitted without proper authorization from the Information Technology Services Department and Department Head, in

compliance with all applicable laws, policies and procedures. Employees may use the CC Guest wireless connection for personal purposes on their personal devices (not County-owned).

B. **Alterations of Computer Hardware**

County-owned computer equipment must not be altered in any way, i.e. removing or adding CD-ROM drives, video cards, memory, etc.

C. **Disposal of Obsolete Hardware and Software**

Information Technology Services Department is solely responsibly for the proper disposal of all County-owned software and hardware. Departments shall contact the Information Technology Services Department for proper disposal.

1. Destruction/disposal/sanitization of Confidential Information is done according to the organization's record retention policy/schedule and as allowed by law.
    a. Client records are not destroyed/disposed/sanitized if they are known to be, or if there is a potential for them to be, involved in any open investigation, audit or litigation.
        i. Destruction/disposal/sanitization is suspended for these records until such time as the situation has been resolved.
        ii. If the records have been requested in the course of a judicial or administrative hearing, a qualified protective order is obtained to ensure that the records are returned to the organization or properly destroyed/disposed/sanitized by the requesting party.
    b. Media containing Confidential Information scheduled for destruction/disposal/sanitization is secured to prevent unauthorized or inappropriate access until the destruction/disposal is complete.
2. Refer to the Attachment D, Disposal of Confidential Information – Example Methods.
3. Servers are generally not be re-commissioned for other use until an evaluation is completed to determine that residual data requiring special security considerations have been deleted. Certificate of Disposal form (Attachment E) filled out and signed by the Information Technology Services Department is required.
4. No media shall be disposed of without being erased, degaussed and/or destroyed first, ensuring that Confidential Information cannot be recovered or reconstructed. The Information Technology Services Department shall prepare all decommissioned computer equipment for disposal. Certificate of Disposal form (Attachment E) filled out and signed by the Information Technology Services Department is required.
    a. All hard drives must be cleaned with software that is DoD 5220.22-M and Gutmann method compliant (The Gutmann method is an algorithm for securely erasing the contents of computer hard drives, such as files).
    b. All saleable PC equipment shall have the hard drives taken out and destroyed before they are sold or donated. Certificate of Disposal form (Attachment E) filled out and signed by the Information Technology Services Department is required. The person purchasing or receiving said equipment, must sign the Clark County Property Purchase Disclaimer(Attachment F) before receiving their equipment.
    c. Non-saleable equipment shall be disposed of in accordance with applicable statutes, and ordinances governing disposal and recycling of computer and computer related equipment. Certificate of Disposal form (Attachment E) filled out and signed by the Information Technology Services Department is required.
5. For additional disposal methods for other types of media, refer to the attached Disposal of Confidential Information – Example Methods (Attachment D).
6. The Information Technology Services Department updates the inventory asset list, as well as applicable hardware and software license documentation.

D. Reuse of Electronic Media Containing Confidential Information

1. Before the reuse of any recordable and erasable Media (e.g. hard disks, workstations, laptops, tapes, cartridges, USB drives, smart phones, SAN disks, SD and similar cards), the Information Technology Services Department facilitates removal of all PHI and/or makes it inaccessible, cleaned, or scrubbed through one of the following methods:
    a. Reused within the organization:
        i. Overwrite the data (for example, through software utilities);
        ii. Degauss the Media; or
        iii. Reformat it so that files are not accessible to the new user(s)
    b. Reused external to the organization: Dispose of it according to a method described above.
2. The Information Technology Services Department:
    a. Documents and/or obtains documentation when this is done, as well as the method used and date/time it was completed
    b. The Information Technology Services Department updates the inventory asset list, as well as applicable hardware and software license documentation.

E. **Software Installed on County Computers**

Only software purchased by the Information Technology Services Department and properly licensed to the County shall be installed on County computers. All installations shall be done by Information Technology Services staff or authorized department staff. The use of this software must be in compliance with the manufacturers license agreement and cannot be copied to multiple computers unless permitted by the license agreement. Unauthorized software(such as shareware, freeware, or employee-owned software) can only be installed on County computers by and with the approval of the Information Technology Services Department staff.

F. Compliance with Software Copyright Laws

Use of computer software is subject to Federal copyright laws. Copying and using software without explicit permission from the copyright owner constitutes copyright infringement. Employees who willfully and knowingly infringe a software copyright by making, acquiring, installing, downloading, or using unauthorized copies of computer software shall be subject to discipline up to and including termination of employment. In addition, criminal and/or civil penalties may apply.

G. Unauthorized Software/Hardware

Clark County prohibits the following types of computer software or hardware from being installed and/or used on County computers unless approved and installed by the Information Technology Services department or needed for work or investigative purposes:

1. Games – including Microsoft games that are included with the Microsoft operating System.
2. Demonstration or evaluation software
3. Interactive internet games
4. Employee-owned software
5. Freeware
6. Shareware
7. Instant messaging software – all external Instant Messaging Services are prohibited.
8. Chat room / Chat channels –acceptable only if used for verifiable business purposes.
9. Streaming Software, including but not limited to music sites, podcasts, webcast and videos.
10. Personal keyboards, mice, speakers or any other personal hardware devices.

11. Applications (unless used for County purposes) to include but not limited to: Weather Bug, Facebook, Twitter, RSS widgets, gambling/gaming sites, personal file sharing sites, such as DropBox, Box, etc.
12. Online shopping that is not directly related to job requirements.
13. Connection of any workstation to the organization's network or utilize Information Technology Services on workstations not owned by the organization.
14. Tools or techniques to break/exploit or disable security measures.

H. Software Audit

To ensure that Clark County Government is in compliance with the US Copyright law, Information Technology Services Department shall conduct a periodic electronic software audit of all workstations and Servers owned by the County. These audits shall be conducted with or without notice to employees. If unauthorized software is found, it shall be removed from computers and Department Heads or designees will be informed of the removal.

I. **Removal of Unauthorized Software**

Information Technology Services Department shall remove all unauthorized software that has been installed on any County computer or other Information Technology device following the steps outlined below:

1. The specific PC or device with the unauthorized software will be identified through the electronic software or by other means.
2. Information Technology Services will contact the user and/or Department Head (designee) to determine if there is a legitimate business reason why the unauthorized software has been installed on a County computer.
3. If the Department Head (designee) indicates that the unauthorized software is needed for the employee to do their job, the following process must be used.
   a) The Department head must request the software be purchased and installed by the Information Technology Services Department.
   b) If the software was installed by the department/employee, the unauthorized software will be automatically removed and a message will be sent to the Department Head (designee).

J. **Copying Software Disks and Manuals**

The copying of software disks and manuals is strictly prohibited unless it is authorized by the Information Technology Services Department as well as by the associated software license agreement, or received through written correspondence with the software owners.

K. **Use of State-Provided Computers and Software**

Employees who are assigned to use a State-provided PC or who utilize software provided by the State are required to comply with all State policies and procedures.

Incident Reporting

Employees have a responsibility to report any actual or suspected information or network security incidents to their direct supervisor or Department Head (designee) and in turn shall report the incident to the Information Technology Services Director.

A. **Types of Incidents Which Must Be Reported**

The following types of incidents are examples of situations that must be reported as a possible security incident:

1. Unauthorized release of information through any means, such as in an E-Mail, verbal conversation, text, etc., whether intentional or accidental
2. Unauthorized receipt of any information that is protected from disclosure (such as health care information through an email or fax).
3. Posting, transmitting, storing, or communication of Confidential Information to unauthorized applications, on social media websites, on personal devices, etc.
4. Receipt of E-Mail that looks to be illegal or contains sexually explicit, hate-group related, or otherwise illegal material.
5. Suspicion that a password has been disclosed or that someone may have been using one of your login credentials or accounts.
6. Any individual asks you for your or another individual's password
7. Any individual requests to use your or another individual's account to review Confidential Information.
8. Receipt of any E-Mail that triggers anti-virus software.
9. Alerts from the anti-virus software or other systems/applications.
10. Computer attacks coming from outside the County, or any suspected virus, worm, or other malicious code.
11. Theft, loss, or unauthorized removal of media, data, storage devices, disks, or CDs.
12. Unauthorized access to the County's computer system(s) by a third party.
13. Denial of Service: An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.
14. Inappropriate Usage: A person violates unacceptable use policies.
15. Unplanned Downtime: The network, system, and/or applications are not accessible due to any unexplainable circumstance causing downtime (due to system failure, utility failure, disaster situation, etc.).
16. Installation of unauthorized software.
17. Inappropriate disposal of Confidential Information.
18. Noncompliance with the County's security policies and procedures.
19. Inappropriate use of the County's Information Technology Resources. Examples include, but are not limited to , access of inappropriate web sites; using County systems for inappropriate, non-work related materials; abusing County 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/cracking activities.

B. **Incident Reporting Procedures**

Employees shall use one of the following options to report an actual or suspected security incident:

1. Report the incident to your Supervisor or Department Head.
2. Send an e-mail to the County Information Technology Services Director, describing the incident.
3. Call the County Information Technology Services Director to report an incident.

Incidents shall be investigated by the Personnel Director as well as the County's Information Technology Services Director. In addition, if the security incident involves ePHI, the Security Officer, Privacy Officer shall be notified so that an investigation can be conducted. Investigation assistance may be requested from workforce members and other system users. All individuals are required to cooperate with the investigation process and provide factual information. Workforce may not interfere with investigations or disciplinary proceedings by willful misrepresentation or omission of facts or by the use of threats or harassment against any person. Whether it was intentional or non-intentional, individuals suspected of non-compliance of the Privacy Rule, Security Rule, and/or the organization's privacy and security policies and procedures are provided

the opportunity to explain their actions. Clark County reserves the right to notify law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity.

Procedure when users change or leave a position

The Information Technology Services User Access Authorization form(Attachment B) needs to be filled out when a new user starts or a user retires, resigns, transfers, or is terminated, etc. in regards to Information Technology Resources:

A. **Requirements for New and/or Departing Users(J:\Everyone\Policies\IT Policies)**:

1. **New and/or Transferred User Access** –
    a. Each department is required to notify the Information Technology Services Department at least 1 week in advance of new/transferring employees hire/transfer date. Information Technology Services User Access Authorization form (Attachment B) must be completed, signed by Department Head, and submitted to IT by this time, when possible. The Information Technology Services Access Authorization form defines the user's permission to access the County's Information Technology resources. Access levels/roles selected are based on the approved role based access levels, as defined in the above Roles section.
    b. All new employees are required to sign the Clark County Confidentiality Agreement (Attachment A).
    c. When access changes are made, Department Heads utilize the "Change in Responsibilities / Termination Checklist" (Attachment C) to make all necessary changes.

2. **Information Technology Services Department Responsibilities** –
    a. Sets up access based on the Information Technology Services User Access authorization Form(Attachement B).
    b. Maintains the following documentation:
        i. A copy of the request
        ii. Name of the individual who requested the access
        iii. Name of the person who set up the access
3. **Departing Users** -
    a. Each department is required to give the Information Technology Services Department at least one week notice, unless an emergent situation arises, of employees departing employment and other departing users. An Information Technology Services User Access Authorization form(AttachmentB) must be completed and signed by the department head by this time. The Information Technology Services User Authorization form defines to the IT department when the user profiles shall be disabled and/or deleted and how the user's data files and old email should be handled, as well as how they want to handle all the other Technology resources that the user had access to.
    b. Also request access be terminated if there is evidence or reason to believe the following:
        i. The user has been using their access rights inappropriately;
        ii. A user's password has been compromised (a new password may be provided to the user if the user is not identified as the individual compromising the original password); or
        iii. An unauthorized individual is utilizing a user's User Login ID and password (a new password may be provided to the user if the user is not identified as providing the unauthorized individual with the User Login ID and password).
    c. Notify the IT department as soon as practical of unscheduled terminations.

4. **Information Technology Services Department Responsibilities** –
    a. Disable accounts immediately or as soon as practical after receiving requests, whether received verbally or in writing.
    b. Maintains the following documentation:
        i. A copy of the Information Technology Services Employee Access Authorization form(Attachment B) (or documentation of the termination request received)
        ii. Reason for the termination (e.g. termination of relationship with the organization, compromised password, inactive account, etc.)
        iii. The date and time access was terminated
        iv. Name of the person who terminated the access.

5. **Securing equipment** - When a user leaves a position for any reason, the Information Technology Services Director and/or Department Head may deem it necessary to remove their Technology Resources that were assigned to them (like a computer) and put said equipment in a secure locked room within the Information Technology Services Department until such time that the equipment is cleared of any issues there may be. Facilitate completing an Information Technology Services User Access Authorization form(AttachmentB) and Change in Responsibilities / Termination Checklist forms (Attachment C).

B. **Departments may have "generic" profiles** for temporary positions such as an LTE or intern. However, this profile can only be assigned to one person at a time and the password shall be changed prior to a new person using the profile. When the profile is not used, the Information Technology Services Department will disable it.

Violation of the terms and conditions contained in this policy may result in disciplinary actions, up to and including discharge, and termination or limitations of access for the violator to any one or all Information Technology Resources.

Policy Attachments

Attachment A

CLARK COUNTY

CONFIDENTIALITY AGREEMENT

I understand that Clark County Government has a legal and ethical responsibility to safeguard the privacy of all clients and to protect the confidentiality of their health information. The Clark County Government must assure the confidentiality of its human resources, payroll, fiscal, research, computer systems, and management information (collectively "Confidential Information") and may disclose such confidential information only as expressly authorized by law.

In the course of my employment/assignment/relationship at the Clark County Government, I understand that I may come into the possession of Confidential Information.

I further understand that I must sign and comply with this agreement in order to get authorization for access to any of the Clark County Government's Confidential Information

1. I will not disclose or discuss any Confidential Information with others, including friends or family, who do not have a need to know it.
2. I will not access or view any Confidential Information, or utilize equipment, other than what is required to do my job / authorized work for or with Clark County Government.
3. I will not discuss Confidential Information where others can overhear the conversation (for example, in hallways, on elevators, in break rooms, at restaurants, and at social events). It is not acceptable to discuss Confidential Information in public areas even if a client's name is not used. Such a discussion may raise doubts among clients and visitors about our respect for their privacy.
4. I will not make inquiries about Confidential Information for other personnel who do not have proper authorization to access such Confidential Information.
5. I will not willingly inform another person of my computer systems' user name(s), password(s) or access codes. Or, knowingly use another person's computer user name(s), password(s) or access codes instead of my own for any reason. If requested by Information Technology Services support for my password, I understand my password will need to be reset.
6. I will not make any unauthorized transmissions, inquiries, modifications, or purging of Confidential Information in the Clark County Government's computer systems.
7. I will password protect any computer prior to leaving it unattended.
8. I will comply with any security or privacy policy promulgated by the Clark County Government to protect the security and privacy of Confidential Information.
9. I will immediately report to my supervisor (if not a Clark County Government employee, to a Clark County Government supervisor) any activity, by any person, including myself, that is a violation of this Agreement or of any Clark County Government's General Technology policy and procedures.
10. Upon cessation of my employment / relationship with Clark County Government, I will immediately return any documents or other media containing Confidential Information to Clark County Government IT Department or appropriate Department Head or Supervisor.
11. I agree that my obligations under this Agreement will continue after the cessation of my employment / relationship with Clark County Government.
12. I further understand that all computer access activity is subject to audit.

I have read and understand the above statements, and I understand that failure to adhere to the above statements may result in fines and discipline up to and including discharge / termination of relationship with Clark County Government. I have read and will adhere to Clark County Governments General Technology Policy and Procedures.

Signature of employee/consultant/vendor/student/volunteer/other _____

Print Name _____ Date _____

Relationship to the Organization (employee, vendor, affiliated agency, etc.) _____

Signature of supervisor _____

Print Name _____ Date _____

Received by Information Technology Services Department

Authorized signature _____

Print Name _____ Date _____

TO BE FILED IN EMPLOYEE'S PERSONNEL RECORD

INFORMATION TECHNOLOGY SERVICES USER ACCESS AUTHORIZATION FORM

Supervisors and/or Department head: Please fill out and sign the following form.
To comply with security requirements, form should be completed and submitted to IT ONE (1) week prior to start date, position change, or termination (unless an emergent situation arises).

Reason (check one):*

☐ New Hire ☐ Rehire ☐ Termination/Retire ☐ Department Change
☐ Access Change ☐ Position Change(in same department) ☐ Name Change

*Required fields

Employee Number:* If not a county employee enter N/A		**Starting/Departing/Change Date:***	
Employee Name:*			
Department:*			
Position Title:*			
Supervisor: *			
Employee to Mirror access: (same access as?)			
External email address: (State, contracted employees)			
Check all that Apply:	☐ Keycard Access ☐ Agency Nurse ☐ State Employee ☐ Contracted Employee		

EXISTING HARDWARE

If NEW hardware is needed please go to NEW hardware section

Computer Name	What is the name of the device the employee will be using/used?		
Phone	New phone number needed? Existing phone number? Internal only line? Existing or new line added/moved to shared phone(multi lines on one physical phone)		
Jabber	Jabber iPhone or Android access? Do not need the cell phone number.	☐ iPhone Add ☐ Android Add	☐ Remove iPhone ☐ Remove Android

EMAIL & CALENDAR Access

Email Distribution Groups/Directories	Add/Remove name from department email groups/directories (which department). If transferring, which department group will their email be in?	
Shared Calendar	Anything other than a Department Shared Calendar. Example: **Wellness Calendar**. Specify Name of calendar	
Email on Printer for scanning to email	Specify the Name of Copier(s) where the email address needs to be entered for scanning to email	

SOFTWARE & Additional Access

Website update access	Training will need to be completed before access is given	☐ Training Needed ☐ Remove Access

MUNIS ACCESS ☐ Add ☐ Change ☐ Remove	
Username to copy for Access if Adding or Changing: (current or past Employee's name)	
Munis applications access: add or remove?	☐ Munis Production * ☐ Munis Train ☐ Munis TCM Production Workflow Approver Access ☐ **No** ☐ **Yes**
Finance Personnel Signoff – will be completed by Finance personnel when access has been added/changed/removed	Finance Initials _____Date _____

NEW HARDWARE **Quotes will be given by IT**		
Workstation	Specify exactly what you need. • Laptop or Desktop or another type of computer 14 in laptop – does not have 10 key ~ 15 in laptop – has 10 key • Dock - is a new dock needed? • Keyboard, Mouse, speakers, headset, webcam, desktop scanner	
Monitors	Do new monitors need to be ordered? How many? IT provides 1 monitor, additional needs to be purchased by Department	
Printer - **Personal Printer Not Network**	Specify needs: • Ability to print double sided? • Color printer? • Scanning? • How many drawers are needed? • Envelope or other paper sizes needed other than 8 ½ x 11?	
Phone	Regular desk phone, Reception phone (extra side cars) – how many?	

Any Other Comments or Instructions Please specify

Terminations only–

Does someone need access to terminated Employee's?

Email****: ☐ **No** ☐ **Yes - Who:** _____

** Email access will be given for 30 days after term unless IT is told otherwise

**** Please inform IT when access is no longer needed so they can finish disabling the account.

Home Directory/Local Laptop Files: ☐ **No** ☐ **Yes – Who:** _____

**** Files will be copied to the above named home directory ****

Voicemail: **Listen to, forward or delete all voicemails before sending IT this form.**

Email on their personal devices: C**heck that they have logged out - OWA or the OUTLOOK App**

Department Head / Supervisor Signoff

Requested completion date?* _____

Department head or (designee) name (please print):* _____

Date: * _____ Office phone: * _____

Department head or designee signature: * _____

Click to Submit Form (helpdesk@co.clark.wi.us)

IT Copy received: Ticket# _____ Date: _____
Personnel Copy Received: _____
Finance Copy Received: _____

Completed by Information Technology Services Department

Completed by: _____ Date: _____

IT Submit to CH Finance & Personnel IT Submit to RLC Finance & Personnel

IT Checklist - For IT use only:

New/Change:		Termination:	
User Created in AD:	☐	User Disabled in AD:	☐
Emp # added in AD:	☐	Moved to Disabled user folder in AD:	☐
Exchange:	☐	Email disabled/or access for manager and ticket created for future disabling:	☐
Papercut (imported account):^	☐	Papercut (removed disabled accounts):	☐
Printer (add email):*	☐	Printer (remove email):	☐
Munis (Production/Train):*	☐		
CUCM (Phone/Jabber):*	☐	Update CUCM(Phone/Jabber):	☐
CUCA (Voicemail):*	☐	Update CUCA(check to make sure VM is empty or ask when they want VM deleted):	☐
Imagicle(Recording/Fax):*	☐	Folder/File access moved or access gave(pc & home directory):	☐
PC updated & Profile setup:**	☐	Move Home directory to Disabled user folder:	☐
New user email sent:	☐		
Supervisor email (ID/Password) sent:	☐		

*Not RLC ~ ^ Not Patrol or Jail ~ ** RLC office staff Not Nurses

Revised Date: 10/12/2023
Revision #: 13
Revised by: Rakovec, Bridget

Attachment C

CLARK COUNTY
Change in Responsibilities / Termination Checklist

The following checklist is to be used by Supervisors and/or Department Heads to safeguard access to confidential information when job responsibilities change and / or individuals are terminated.

Individual's Name:	
Title:	
Department:	

Supervisor / Department Head Task	Received / Completed
☐ Complete the Information Technology Services User Access Authorization Form and forward it to Information Technology Services	☐ Information Technology Services Department
☐ Return company issued cell phones and pagers, if applicable	☐ Information Technology Services Department
☐ Return keys (e.g., building, department, desk, file cabinets, etc.)	☐ Maintenance Director
☐ Make necessary changes to the ID badge/access card to reflect changes in title or role – forward to the Maintenance Director	☐ Maintenance Director
☐ Return parking pass, if applicable	☐ Maintenance Director
☐ Return file or cabinet keys	☐ Supervisor or Department Head
☐ Return uniforms/work clothes, if applicable	☐ Supervisor or Department Head
☐ Notify key contacts (insurance companies, business associates, vendors, etc.) regarding the change, as applicable	☐ Supervisor or Department Head
☐ Return credit card, if applicable	☐ County Clerk
☐ Phone and voicemail changes	☐ Information Technology Services Department

Supervisor / Dept. Head Completed By:	Please print name here:
Title:	
Signature:	
Date:	
Person Completing Task:	Please print name here:
Title:	
Signature:	
Date:	

Forward this completed form to Personnel Department. Personnel files this form in the employee's personnel file.

Attachment D

Disposal of Confidential Information – Example Methods

Confidential Information destroyed/disposed/Sanitized using a method that this information cannot be recovered or reconstructed. Methods used may include the following (and those previously described in this policy):

Medium	Method Used
Audiotapes	• Recycle (tape over), Degauss or pulverize.
Electronic Data/ Hard Disk Drives including drives found in servers, workstations, printers, and copiers	• Destroy data permanently and irreversibly through a DoD wipe, physical destruction (pulverize, shred, disintegrate, incinerate), Degaussing of it, or hard drive erasure software. • Methods of reuse: overwrite data with a series of characters or reformatting the disk (destroying everything on it). Deleting a file on a disk does not destroy the data, but merely deletes the filename from the directory, preventing easy access of the file and making the sector available on the disk so it may be overwritten.
Electronic Data/ Removable Media or devices including USB drives, SD cards, CDs, tapes, and cartridges	• Overwrite data with a series of characters or reformat it (destroying everything on it). Total data destruction does not occur until the data has been overwritten. • Magnetic Degaussing that leaves the sectors in random patterns with no preference to orientation, rendering previous data unrecoverable. Magnetic Degaussing will leave the sectors in random patterns with no preference to orientation, rendering previous data unrecoverable. • Shredding or pulverization is done for the final disposition of any removable Media when it is no longer usable.
Handheld devices including cell phones, smart phones, PDAs, tablets and similar devices.	• Activate the Software on these devices that remotely wipes ("bit-wipe") data from them. • When a handheld device is no longer reusable it is then totally destroyed by recycling or by trash compacting.
Optical Media	• Optical disks cannot be altered or reused, making pulverization an appropriate means of destruction/disposal.
PHI Labeled Devices, Containers, Equipment, etc.	• Shred or destroy so that the Confidential Information cannot be read or otherwise cannot be reconstructed; redaction is specifically excluded as a means of data destruction. Note: this is based on the Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals • Reasonable steps should be taken to destroy or de-identify any Confidential Information prior to disposal of this medium. Remove labels or incinerate the medium; or • Ribbons used to print labels may contain Confidential Information and are shredded or incinerated.
Paper Records	• Shred or destroy so that the Confidential Information cannot be read or otherwise cannot be reconstructed; redaction is specifically excluded as a means of data destruction. Note: this is based on the Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals. An example is to finely shred papers with a cross-cut shredder. Note: this example is from the CMS Information Security ARS.
Videotapes	• Recycle (tape over) or pulverize.

Attachment E

Certificate of Disposal
Information Technology Resources
Information Technology Department

Date:		
Department:		Employee:
Equipment model/name:		Equipment Serial number:
Hard drive model/name:		Hard Drive serial number:
Software name/version:		Other equipment name/version:
Method of disposal:		
Further notes and comments:		
IT employee Disposing of equipment:		IT Employee signature:
IT Director name:		IT Director signature:

Information Technology Department certifies that the above equipment has been properly disposed of and/or destroyed in accordance to all applicable Federal, State and Local Rules and Regulations.

Information Technology Department acknowledges, all electronic data on functional storage devices have been or will be overwritten by means of a destructive write process using a program that performs an overwrite of data on the hard drive. IT further acknowledges that all storage devices deemed to be non-functional have been or will be shredded or otherwise destroyed after removal of all data. All storage devices will be removed and destroyed before the equipment it was stored in is sold/donated. Non-saleable equipment will be disposed of in accordance with applicable statutes, and ordinances governing disposal and recycling of computer and computer related equipment

Attachment F

Policy Review Form

Completed by Policy Custodian

Policy Title	IT Services Director
Overview of Adoption/Revision	03 08 2018
Policy Submitted By	Cindy Currier
Policy Submitted To	IT Steering Committee and Executive Committee
Anticipated Date of Policy Final Approval	March 8, 2018

Completed by IT Steering Committee

Policy Received On	February 27, 2018
Policy Approved/Denied On w/ Reason	Approved
Policy Approved/Denied By	IT Steering Committee
Policy Storage Location	J:\Everyone\Policies\IT Policies
Policy Forwarded to Corporation Counsel	03 07 2018

Completed by Corporation Counsel

Policy Received On	03 07 2018
Policy Approved/Denied On w/Reason	Approved with changes
Policy Approved/Denied By	Jacob Brunette
Policy Forwarded to Executive Committee	03 08 2018

Completed by Executive Committee

Policy Received On	03 08 2018
Policy Approved/Denied On w/Reason	Approved
Policy Approved/Denied By	Executive Committee

Revision History		
Adoption/Revision Date	**Overview of Adoption/Revision**	**Adoption/Revision Reference**
March 20, 2018	Original	Resolution 13-3-18