SECTION 415: TELEWORK POLICY

PURPOSE: It is the policy of Black Hawk County to consider telework as a viable, flexible work option that represents a mutually beneficial arrangement between the employee and their employing department. **Telework is a privilege, not an employee right or entitlement.** Telework is defined as any work arrangement that allows an employee to work outside of the employee's primary worksite at an alternate location pursuant to an approved Telework Agreement.

Teleworking is a cooperative arrangement between employees, supervisors, and their departments. Employees must be able to carry out the same duties, assignments, and other work obligations at their alternate location as they do when working on the County's premises. Employees must be available to attend scheduled meetings and participate in other required office activities as needed.

The County recognizes that offering flexible work arrangements can benefit employees, departments, and the organization. This includes, but is not limited to:

- Ability to function during an emergency when the regular worksite is inaccessible
- Increased productivity
- Efficient use of County resources, including office space
- Recruitment and retention of highly qualified employees
- Greater flexibility for employees and departments
- Improved employee morale and job satisfaction
- Reduced employee absenteeism
- Reduced employee commute time and costs
- Decreased parking congestion.

The Teleworking Policy applies Countywide, and department heads are encouraged to make teleworking available to all eligible employees in their departments to the extent possible.

SCOPE: This policy applies to all Black Hawk County employees. Whenever the provisions of this policy are in conflict with federal or state laws or regulations, or with a current collective bargaining agreement between the County and a certified bargaining unit, the provisions of the collective bargaining agreement and/or the laws or regulations shall prevail.

ELIGIBILITY: Teleworking is a cooperative and mutually beneficial arrangement between an employee and the employee's department. Eligibility for teleworking is based on both the position and the employee. Not every job, or every employee, is well-suited for teleworking and eligibility is primarily based on a department's assessment of an employee's work and work habits.

Employees must have successfully completed their probationary period to be eligible for teleworking authorization. Employees whose work habits demonstrate that they can work independently and productively without direct supervision, are self-directed, reliable and trustworthy in carrying out all of their duties and responsibilities, meet timelines, proven

attendance record, and are responsive and communicate effectively are best suited for teleworking.

Position Eligibility
An employee's position may be suitable for teleworking when the job duties:

- Are independent in nature
- Lend themselves to measurable deliverables
- Do not require frequent interaction at the regular worksite with supervisors, colleagues, clients, or the public, in person
- Do not require the employee's immediate presence at the regular worksite to address unscheduled events, unless alternative arrangements for coverage are possible
- Are not essential to the management of on-site workflow.

Employee Eligibility
Employees may be suitable for telework arrangements under the following criteria as determined by their supervisor:

- Demonstrated dependability, motivation, and responsibility
- Effective communication with supervisors, coworkers, and clients
- The ability to work independently
- A consistently high rate of productivity
- A high level of skill and knowledge of the job
- The ability to prioritize work effectively
- Good organizational and time management skills.

Departmental Eligibility
A Department Head or Elected Official reserves the right to not implement telework arrangements for their entire department.

Employees who are not upholding County obligations, such as meeting performance or conduct expectations, are not eligible to telework.

TELEWORK ALTERNATIVES: Teleworking agreements may be authorized on a regular or temporary basis. Regular telework agreements may not exceed more than 40% of a 40-hour work week (16 hours for full-time employees, and pro-rated for part-time employees), unless approved by a Department Head, and must be renewed annually.

Regular means an employee works away from the regular worksite on an established day or days, and on a recurring schedule. Employees who telework on a regular basis must be available to work at the regular worksite on teleworking days if needed. Conversely, occasional requests by employees to change their regularly scheduled telework days may be accommodated by the supervisor, if possible. Employees must obtain prior authorization to change a regularly scheduled telework day.

Temporary means an employee works away from the office on an infrequent or one-time basis. This option provides an ideal arrangement for employees who generally need to be in the office, but who sometimes have projects, assignments, or other circumstances that meet the eligibility criteria as determined by the Department Head.

POLICY: Telework is a privilege, not an employee right or entitlement. All County employees who telework must have an approved teleworking agreement under this policy. A department may have additional teleworking requirements, guidelines, or procedures, provided they are consistent with the intent of this program. Teleworking does not change the duties, obligations, responsibilities, or terms and conditions of County employment. Teleworking employees must comply with all County rules, policies, practices, and instructions.

A supervisor or a department may deny, end, or modify a teleworking agreement for any business reason that is not arbitrary or capricious. Similarly, a teleworking employee may end or request to change a teleworking agreement at any time. Employees may be removed from telework if they do not comply with the terms of their teleworking agreements.

Telework Authorization Guidelines

A. All essential position responsibilities must be achievable with no reduction of service provided to the public or fellow employees via remote access (phone, email, videoconferencing, etc.) and/or established work hours.
B. All telework arrangements must be approved by an employee's supervisor or Department Head prior to any work being conducted remotely.
C. Employees must work during their regular scheduled hours, any deviations from their regular schedule must be approved by their supervisor or Department Head in advance.
D. Employees must be reachable and responsive throughout their regular work hours by phone, email or messaging while teleworking, similar to when they are working onsite during normal hours of operation.
E. Employees authorized to telework may still be expected to report to work onsite at times and attend onsite meetings, trainings or other work events. Employees are subject to recall, if necessary, at their supervisor's discretion if their services are needed onsite or within a standard work schedule. This may occur with minimal notice. For some positions, alternative work arrangements may be better suited to and authorized for certain times of the year and not others.
F. Employees experiencing Internet connectivity issues while working remotely are expected to return to the traditional worksite for productivity purposes.
G. Employees in a supervisory role must be available to provide adequate supervision and assistance when needed to their direct reports. Supervisors should also consider a variety of scenarios when considering teleworking requests/recommendations to ensure that schedules do not become unreasonable to manage and that operations do not suffer.
H. Communication channels between employees, supervisors, and co-workers may function differently when teleworking and may require adaptation to be successful. During the development of the teleworking arrangement, the employee and immediate supervisor must establish both expectations for the work to be completed remotely and for ongoing communication regarding work assignments, progress, plans and problems are required. The Department Head reserves the right to require additional documentation or reporting as they deem necessary to verify the employee's time and/or work accomplished.
I. Teleworking is not intended to serve as substitute for dependent care, sick leave or other employee leave. Children or other members of the household in need of care or supervision shall not be under the employee's direct care during established work

time. Although limited modifications to an employee's schedule may be approved upon request to accommodate such needs, the focus of teleworking time must remain on the performance of job duties and meeting operational needs of the County.

J. Employees must perform work during their regular work hours while teleworking. Employees may take care of personal business during their breaks and unpaid lunch periods, as they would at the regular worksite.
K. While teleworking is authorized, the Employee shall maintain their remote workspace in a safe condition, free from hazards and other dangers.
L. While teleworking, employees must refrain from using streaming video and internet access except for official business.
M. Employees must read the Telework Policy and Telework Technology Usage Procedures and submit an agreement through the departmental approval process before teleworking. Employees approved to telework will be asked to complete a survey to track the number of telework employees and evaluate the program.
N. These guidelines recognize temporary telework may be granted to an employee whose position is generally not eligible for a regular telework arrangement. Temporary authorizations may be approved on a case-by-case basis by the Department Head without a signed Teleworking Agreement under the following conditions:
    a. Actual time performing work must be accurately tracked and reported by employees and appropriate accruals used for any portion of the scheduled hours not worked or when the employee was engaged in personal matters.
    b. The supervisor and employee establish a mutual understanding of the work to be performed. Monitoring email and answering phone calls is generally not considered sufficient work to warrant teleworking authorization, however completing online continuing education or mandatory trainings would be considered sufficient work.
    c. The employee meets the equipment and security requirements/technical guidelines for telework to complete established work assignments.

PROCEDURE: Teleworking arrangements, whether employer or employee initiated, will be subject to the approval of the Department Head and will require a Teleworking Agreement form, signed by the employee, direct supervisor, and Department Head. A copy of the signed agreement must be submitted to Human Resources to be maintained in the employee's personnel file. Temporary telework authorization does not require a signed agreement, but informal documentation (i.e. email) of approval, duration, work to be performed and other relevant conditions is recommended. Department Heads have the authority to approve, modify or reject a request for a telework arrangement, and determine when the telework arrangement will go into effect.

The following steps must be completed before an employee is authorized to telework:

1. Employee reviews the position and employee eligibility criteria in this policy
2. Employee discusses position eligibility with their manager or Department Head
3. Employee completes the telework agreement online
4. Department Head reviews agreement, then signs off to approve, deny or modify agreement
5. Department Head notifies employee and the employee's supervisor of their decision

6. Approved, denied or modified Telework Agreement is placed on file with Human Resources
7. Employee authorized to telework must read and agree to the Telework Policy and Technology Usage Procedures
8. Employee authorized to telework may be required to complete the Telework Survey

Employees authorized to telework may end or request to change a telework arrangement at any time. Any requests to change a telework arrangement must be approved by the above procedure.

Teleworking authorization may be revoked at any time for any legitimate reason, as determined by the Department Head, including if the employee is not responsive during established work hours, the supervisor determines there is insufficient work available on a remote basis, the employee's performance or productivity suffers, the arrangement adversely affects other staff or department operations, or it is otherwise determined that there is insufficient benefit to the department to continue remote work.

The decision to approve, deny or modify and/or revoke teleworking authorization as determined by the Department Head is considered final and not subject to appeal or grievance procedures.

WORK HOURS, PAY AND TIMEKEEPING REQUIREMENTS: All the rules applicable at the regular worksite are applicable while teleworking. That is:

- Employees must perform designated work during regular scheduled work hours.
- Employees must account for, and report, time spent teleworking the same way they would at the regular worksite, or according to the terms of the teleworking agreement.
- Employees may work overtime only when directed to do so and approved in advance by the Department Head, or their designee.
- Employees must use and report all approved vacation, holiday, casual, and comp time taken for hours not worked in a regularly scheduled workday. Employees on vacation, paid time off, comp time or casual should not be teleworking.
- Employees who become ill must report the hours actually worked and use sick leave for hours not worked. Employees that are sick or using sick leave for appointments or care for family members, are not to be teleworking.
- Employees must obtain approval to use vacation, sick, or other leave in the same manner as employees who do not telework.
- Employees must obtain approval to telework on holidays in accordance with County policy and collective bargaining agreements.

Non-exempt employees must accurately record all hours worked on their timesheet in accordance with regular timekeeping practices. Non-exempt employees shall not work overtime, or alter their established work schedule, unless they have received prior approval from their Department Head. Accordingly, non-exempt employees must refrain from performing any work outside of their established, authorized work schedule without prior approval, including reading or replying to email or similar work tasks, including administrative tasks. In the event a non-exempt employee performs any work outside of their regularly scheduled hours, the non-exempt employee must report such time on their timesheet. The County will pay non-exempt employees for all hours/time worked, including

overtime. However, failure to obtain prior approval for overtime may result in discontinuation of teleworking arrangements and/or other disciplinary action.

WORKSITE: A teleworking employee must designate a work area suitable for performing official business. The employee must perform work in the designated area when teleworking. Requirements for the designated work area will vary depending on the nature of the work and the equipment needed and may be determined by the department.

Teleworking employees must work in an environment that allows them to perform their duties safely and efficiently. Employees are responsible for ensuring their work areas comply with the health and safety requirements in accordance with the County's Safety Program. The County and/or department may request photographs of the employee's designated work area to determine compliance with health and safety rules.

Employees are covered by workers' compensation laws when performing work duties at their designated alternate locations during regular work hours. Employees who suffer a work-related injury or illness while teleworking must notify their supervisor and complete any required forms immediately. The County assumes no liability for injuries occurring at the remote site outside of the teleworking employees established work hours or when conducting non-work-related tasks. The County is not liable for loss, destruction, or injury that may occur in or to the alternative worksite, this includes family members, visitors, or others that may become injured within or around the employee's alternative worksite. The County is not liable for damages to an employee's personal or real property while the employee is working at an alternate worksite.

Authorized County personnel may make on-site visits to the telework work site for the purpose of retrieving County-provided equipment, software, hardware, data, and/or supplies or for a work site safety/ergonomics check. Unless otherwise agreed to by the employee, the County will give a minimum notice of 24 hours before the visit.

EQUIPMENT AND SECURITY REQUIREMENTS: The Telework Policy and Program is intended to be cost-neutral. The County is not required to provide telework employees with materials or supplies needed to establish an alternate worksite (desk, chair, computer, software, cell phone, fax, copier, etc.), and assumes no responsibility for set-up or operating costs at an alternate worksite (telephone or internet services, etc.). Teleworking employees are required to read and acknowledge the Telework Technology Usage Procedures as established by the IT Department.

A teleworking employee must identify the equipment, software, supplies, and support required to successfully work at an alternate location and must specify those items in the telework application and agreement form. If the department does not provide the needed equipment, software, supplies, or support, and the employee does not have them, the employee will not be eligible to telework.

The IT Department and employee's department has the sole discretion to provide equipment, software, or supplies, or allow employees to use their personal equipment while teleworking. Departments providing equipment, software, or other supplies to teleworking

employees must reasonably allocate those resources based on operational and workload needs.

Under all teleworking alternatives, employees are responsible to protect County equipment, software, and supplies from possible theft, loss, and damage. If damage, loss or theft occurs, an employee must report it in a timely manner. The teleworking employee may be liable for replacement or repair of the equipment, software, or supplies in compliance with applicable laws on negligence or intentional conduct in the event of theft, loss, or damage.

All County rules regarding the use of computers and the internet apply while an employee is teleworking, regardless of whether the employee is using County-provided or personal equipment. In addition, teleworking employees must:

A. Provide high speed internet access that is password protected while teleworking
B. Abide by the County's IT policies or procedures related to VPN/remote access
C. Abide by the County's HIPAA policies and procedures related to accessing PHI/PII
D. Store equipment in a safe and clean space when not in use, for example, laptops unattended in a vehicle should be stored in trunk or out of visible sight.
E. Contact their supervisors if equipment, connectivity, or other supply problems prevent them from working while teleworking.

County and Personal Equipment

Equipment, software, or supplies provided by the County are for County business only. A teleworking employee does not obtain any rights to County equipment, software, or supplies provided in connection with teleworking. The employee must immediately return all County equipment, software, and supplies at the conclusion of the teleworking arrangement or at the department's request.

Any equipment, software, files, and databases provided by the County shall remain the property of the County. A teleworking employee must adhere to all software copyright laws and may not make unauthorized copies of any County-owned software. Employees may not add hardware or software to County equipment without prior written approval.

Employees who use their personal computer-related peripheral equipment (keyboard, mouse, USB hub, monitors, etc.) for teleworking are responsible for the installation, repair, and maintenance of the equipment. Personal laptops, computers, printers and scanners are prohibited from being used while teleworking.

Smart Technology and Listening Devices

Smart devices in an employee's home or remote worksite, such as voice-enabled devices, enhanced remotes, smart thermostats, security cameras, smart speakers, smart televisions, doorbell cameras, etc. are part of what is known as the Internet of Things (IoT). The "things" within the IoT rely on a connection to the cloud, sometimes using another device as a relay, to analyze and act on the data they gather. IoT devices can be compromised within minutes of connecting to the Internet, and default passwords are a major security weakness of these devices. If a teleworking employee is using a home network or internet connection, an unsecured IoT device could become an attack vector to any attached county equipment. To secure IoT devices:

A. Examine the default security options available and enable any security features.

B. Remove or turn off voice-enabled listening and recording devices in the telework environment.
C. Disable voice to text functions residing on any of mobile or networked devices when teleworking.

Public Records and Security of Confidential Information

Under all teleworking alternatives, work completed remotely is regarded as official County business and therefore all files, records, papers, or other materials created while teleworking is considered County property.

The State of Iowa and County rules regarding public information and public records apply to teleworking employees. Public records include any writing containing information relating to the conduct of the public's business prepared, owned, used, or retained by the County regardless of physical form or characteristic. Public information means the contents of a public record. Upon receipt of an appropriate request, and subject to authorized exemptions, a teleworking employee must permit inspection and examination of any public record or public information in the employee's custody, or any segregable portion of a public record, within required time limits. This requirement exists regardless of where the public record is located.

Any employee approved for telework that has access to confidential information or HIPAA protected information shall set forth in the telework agreement what arrangements are taking place at the remote worksite to address protection of said information. Employees will also be required to acknowledge applicable sections of the county's HIPAA Policies and Procedures and complete additional training prior to receiving authorization to work remotely. Protected Health Information (PHI) is defined as confidential information, including demographic information, in a medical record or designated record set that can be used to identify an individual and that:

A. is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
B. relates to the past, present, or future physical or mental health or condition of an Individual; the provision of health care to an Individual; or the past, present, or future payment for the provision of health care to an Individual; and that either identifies the Individual or with respect to which there is a reasonable basis to believe the information can be used to identify the Individual.

Teleworking employees that handle PHI, confidential or sensitive material or process payments may be denied telework arrangements. To avoid breaches of confidentiality, employees are prohibited from:

A. Transporting physical confidential records from the worksite to use or reference in telework locations.
B. Printing or scanning confidential records in a telework location.
C. Communicating or accessing confidential records or information on personal electronic equipment, an unsecured or unauthorized network or internet connection (including public Wifi connection or not using VPN Connection), or in the presence of smart technology or listening devices.
D. Discussing or confidential information or records in the presence of unauthorized individuals.

E. Accessing confidential information or records that is visible to unauthorized individuals, such as monitors, or computer displays.
F. Storing confidential files on a thumb drive or external hard drive.

Teleworking employees that communicate PHI over the phone, virtually or electronically must safeguard the information by:

A. Being conscientious and aware of surroundings, and not communicating PHI while unauthorized individuals are present in the remote worksite that may be able to hear discussions.
B. Keeping their voice down when discussing PHI and limit discussions to the minimum necessary to conduct business.
C. Utilizing a 'private' space when discussing PHI and refraining from discussing PHI in open and public areas within the remote worksite.
D. When communicating PHI over the phone, confirm who is on the other end of the phone. Do not relay or discuss PHI over the phone unless confirmed that the identity of the person to whom you are speaking and their authority to discuss PHI involved.
E. Verifying home or remote security system cameras or not positioned behind workstation monitors or laptop where displayed PHI can be viewed or recorded.
F. Verifying home or remote smart technology or listening devices are positioned to not 'hear' or record PHI conversations or information.

Employees may not disclose confidential or private files, records, materials, or information, and may not allow access to County networks or databases to anyone who is not authorized to have access. Failure to comply with county policies or regulations regarding confidential information may result in disciplinary action up to and including termination.

COMPLIANCE AND ENFORCEMENT: The Human Resources Department administers this policy on behalf of the Board of Supervisors. Department heads, supervisors and employees who do not comply with the expectations and procedures set forth in this policy may be subject to disciplinary action.

Telework Technology Usage Procedures

Purpose
To establish guidelines for the proper use of technology by employees engaged in telework, ensuring the security, efficiency, and productivity of remote work environments.

Scope
This policy applies to all employees approved for telework arrangements, including full-time, part-time, and temporary staff. Approval is at the discretion of the respective department head or manager.

Technology Equipment

1. **Provision of Equipment**:
    - Black Hawk County will provide the eligible employee with the necessary equipment for telework, including laptop, charger and bag. This equipment remains the property of Black Hawk County.
    - Docking stations will not be provided. An additional monitor may be provided if justification is approved by the Information Technology department.
    - Employees may not use personal equipment without prior approval. The county will not be responsible for maintenance or support of personal devices.

2. **Equipment Maintenance**:
    - The county will maintain and service all company-owned equipment. Employees are responsible for safeguarding this equipment and must report any issues immediately to IT support.

3. **Use of Equipment**:
    - Equipment provided by the organization is to be used for business purposes only. Personal use is not permitted.
    - Employees must ensure that unauthorized persons do not use company-owned equipment.
    - Employees must safely guard equipment from damage and liquids.

Security Measures

1. **Network Security**:
    - Employees must use a secure and reliable internet connection. The use of a VPN (Virtual Private Network) provided by the organization is required when accessing the company network remotely, particularly when accessing county network resources not based in the cloud.
    - Personal Wi-Fi networks must be secured with strong passwords to prevent unauthorized access.

2. **Data Security**:
    - Employees must comply with all organizational policies regarding the protection of sensitive information.

- All data should be stored on the organization's network or approved cloud storage solutions. Local storage on personal devices is prohibited. Local storage of PHI or PII on county issued devices must be on an approved network or cloud storage.

3. **Access Control**:
   - Passwords must be strong, changed regularly, and kept confidential. Multi-factor authentication (MFA) is required for access to sensitive systems.
   - Employees must log off and secure their devices when not in use.

4. **Software Use**:
   - Only approved software may be installed on company-owned devices. Unauthorized software installations are prohibited.
   - Regular updates and patches must be applied to all software to ensure security.

Communication and Collaboration Tools

1. **Email and Messaging**:
   - Employees must use the organization's email and messaging systems for all work-related communications.
   - Personal email accounts must not be used for business communications.

2. **Video Conferencing**:
   - Approved video conferencing tools should be used for virtual meetings. Employees must ensure their environments are professional and free from distractions during meetings.
   - Meeting links should not be shared with unauthorized individuals.

IT Support

1. **Technical Support**:
   - IT support will be available during regular business hours to assist with technical issues. Employees should report issues promptly to minimize downtime.
   - IT support will only provide remote assistance.
   - In case of equipment failure, employees must inform their supervisor and IT support immediately and report to their regular worksite. Alternative work arrangements may be made temporarily.

2. **Training**:
   - Employees will receive training on the proper use of remote work technology and cybersecurity best practices.
   - Additional training sessions will be conducted periodically to update employees on new tools, software, and security protocols.

Connectivity

1. **Internet**:
   - Employee must have their own reliable internet at their place of residence or approved satellite location and must adhere to County security best practices.

- Internet service must provide adequate speeds to support telework. Black Hawk County does not provide or cover the cost of internet services at the employee's residence or approved satellite location.

2. **Hotspots**:
    - Hotspots may be used when an internet service provider is inaccessible but is not recommended for extended/permanent use.
    - Hotspots access must be secured with a password that meets the county password complexity requirements (minimum 14 characters)
    - Dedicated cellular internet services are allowed as long bandwidth speeds are adequate.

Return of Equipment

1. **Upon Termination or End of Telework Arrangement**:
    - All company-owned equipment must be returned in good working condition.
    - Employees will be responsible for any damage beyond normal wear and tear.

2. **Data Return and Deletion**:
    - All company data must be transferred back to the organization's network. Employees must not retain any copies of company data after the termination of employment or telework arrangement.

By adhering to these guidelines, employees and the organization can ensure a secure, efficient, and productive telework environment.