Policy & Procedure: HL-4.0	**Teleworking**
Effective Date:	**4/3/2017**
Last Approval Date:	**1/10/2020**
Approval Authority:	**VP, Compliance and Accreditation**

Policy:

Company provides teleworking arrangements to staff when it is mutually beneficial to both parties. The policy defines teleworking, describes the requirements for teleworking agreements, and outlines the responsibilities of both parties.

Refer to Section D herein for procedures regarding teleworking during inclement weather and emergency disruptions.

Procedure:

Teleworking is defined as any work arrangement that allows staff to work outside of their primary on-site work location at an alternate location, on a regular basis, at least one (1) day per week, pursuant to an approved Teleworking Security Agreement (HL-4.0A).

Occasional, non-regularly occurring, out-of-office work arrangements may be allowed on a case-by-case basis if approved by the employee's Operations Manager. A prospective teleworker is required to have a secure workspace dedicated in their own residence or they will not be considered for an a teleworking assignment. Any exceptions to the teleworking requirements must be approved by the Vice President, Operational Development. In situations where an active employee has a shared residence with a former Company employee, senior management reserves the right to withhold a teleworking assignment to mitigate security risks to protected data, physical property, and/or intellectual property.

Recommendations for teleworking assignments from Corporate IT and Manager, Compliance and Quality are presented to the teleworker's Operations Manager, Senior Vice President of Operations, Chief Operating/Financial Officer, Vice President, Operational Development, and/or Human Capital Business Partner before final approval or denial is made. A formal Teleworking

Security Agreement may be required for occasional teleworking arrangements and an Operations Manager's approval on one occasion does not imply that future requests of a similar nature will be approved.

Current tenure and disciplinary status may be considerations when determining eligibility for a teleworking assignment, per management's discretion. All teleworkers must acknowledge and sign a Teleworking Security Agreement. In some cases, Company may establish new or open positions in which teleworking is an expected condition of employment. For those designated teleworking positions, the job announcement will describe the teleworking requirement and the ability to work effectively and efficiently from an alternative worksite location, and this will be a qualification for the position.

Exception for On-Site Staff:
Company employees generally perform their job duties at on-site facilities. However, given the nature of the work, it is an accepted practice for certain employees to conduct their work activities on varied schedules and in alternate locations as appropriate. In circumstances involving staff with on-site workstations, a formal Teleworking Security Agreement is not required. If there is a need for a teleworker to work on-site, the employee's Manager will attempt to make available on onsite workstation. The teleworker should give his or her Operations Manager at least twenty-four (24) hours' notice to determine if an onsite workstation will be available when needed. If a teleworker is on call, they are required to pick up and return any on-call materials or devices as required to the onsite facility.

Procedures:

This policy is governed and administered by the senior management of Company and the Human Capital Business Partner. The teleworking arrangement is coordinated through the department of the teleworking employee. Leads and Supervisors with an interest in exploring a teleworking arrangement should consult their Operations Manager, Vice President of Operations, Senior Vice President of Operations, Chief Operating/Financial Officer, and Vice President, Operational Development.

The Senior Vice President of Operations, Chief Operating/Financial Officer, and/or Vice President, Operational Development must approve all teleworking arrangements after consultation with Corporate IT and Manager, Compliance and Quality to ensure data security and other information technology requirements are satisfied prior to sending it to the Human Capital Business Partner for final verification and placement in the employee's personnel file. Note: All teleworkers and management that are issued laptops or other teleworking computer equipment to facilitate offsite work responsibilities will automatically be granted remote access upon assignment.

The completed and signed original copy of the Teleworking Security Agreement will be retained and maintained by Human Capital in the employee's personnel file.

Voluntary teleworking arrangements may be discontinued, without cause, at any time at the request of either the teleworker, Operations Manager, Vice President of Operations, Senior Vice President of Operations, Chief Operating/Financial Officer, or Vice President, Operational Development. When practicable, Company or teleworker should provide a two (2) week notice of termination of the Teleworking Security Agreement. However, when teleworking is an expected condition of employment, the Teleworking Security Agreement may be discontinued anytime at the option of Company.

General Conditions of Teleworking Agreements:

A. Conditions of Employment. The teleworker's conditions of employment shall remain the same as for non-teleworking employees. Wages, benefits, and leave accrual will remain unchanged unless there is a change in employment status or scheduled hours that impacts benefit eligibility. In addition, all Company policies, procedures, and rules will apply at the teleworking site, including those governing internal communication, facilities and equipment management, financial management, information resource management, security and privacy, and safety. Failure to follow Company policies, procedures, and rules may result in termination of the Teleworking Security Agreement and/or disciplinary action, up to and including termination.

B. Hours of Work. The Teleworking Security Agreement will specify the regularly scheduled work hours agreed upon by the teleworker and his or her Operations Manager. The amount of time the teleworker is expected to work will be based on specified performance goals established by the Senior Vice President of Operations and Chief Operating/Financial Officer before assignment to a teleworking arrangement, and in compliance with the Fair Labor Standards Act (FLSA), Company policies and procedures, and the Teleworking Security Agreement. A teleworker must be available during regularly scheduled work hours by telephone, email, or other specified methods of communication with his or her Operations Manager, co-workers, or other staff with whom job-related communication is necessary.

A teleworker may need to attend on-site job-related meetings, training sessions, and conferences if the employee's Operations Manager provides at least twenty-four (24) hours prior notice, per the Teleworking Security Agreement. In addition, the teleworker may be requested to attend on-site meetings called with less than twenty-four (24) hour prior notice. Operations Managers will use electronic means of communication whenever possible as an alternative to requesting attendance at "short notice" meetings, but there may be times when the teleworker's physical presence is deemed essential. In such cases, the Operations Manager must provide enough prior notice to allow the employee a reasonable time to travel to the onsite location to participate in the meeting.

If a teleworker has technical issues during initial teleworking set up, he or she will have up to two (2) hours to get the issue resolved. If the time exceeds two (2) hours, the teleworker will be charged PTO hours in excess of two (2) hours or they can choose to come into the onsite location and save the PTO if an onsite workstation is available.

If there are technical issues outside the initial teleworking setup, the teleworker will attempt to resolve the issue with the assistance of the Corporate IT within one (1) hour of becoming aware of the issue without being required to use PTO. If the issue takes longer than one (1) hour to resolve, the teleworker will need to either return to the onsite location, take PTO, or at the Operations Manager's discretion allow the teleworker the opportunity to make up the time.

C. Fair Labor Standards Act (FLSA): Teleworking employees will be non-exempt from the overtime requirements of the FLSA unless special circumstance apply and approved by the Human Capital Business Partner. Employees are responsible for the accuracy of their time cards.

D. Inclement Weather and Emergency Disruptions: If the primary onsite location is closed due to inclement weather or an emergency disruption, the Operations Manager will contact the teleworker and provide instructions about the continuation of work at the teleworking site. If there is an emergency at the alternate worksite, such as a power outage, the teleworker will notify his or her Operations Manager as soon as possible. The teleworker may be reassigned to the primary onsite location, other alternate worksite, or be required to take PTO.

E. Alternate Worksite: A Safety and Security Checklist (HL-4.0B) must be completed prior to a teleworking arrangement commencing. Corporate Security and Compliance will schedule a virtual teleworking assessment and complete the checklist at that time. The Safety and Security Checklist may be completed virtually using a webcam, FaceTime, RingCentral™ application, or other means.

The teleworker must establish and maintain a dedicated workspace that is quiet, clean, secure and safe, with adequate lighting and ventilation. The teleworker must confirm that the work location is free of recognized hazards. If the teleworker does not have their equipment in a room with a locked door, they must purchase computer privacy screens to ensure the security and privacy of Protected Health Information (PHI). The computer privacy screens must be purchased by the teleworker. The cost of the computer privacy screens will not be reimbursed by Company. If the teleworker is out of the office, the workspace (including equipment) must be secured. The teleworker will not hold business visits or meetings with professional colleagues, customers, or the public at the alternate worksite. Meeting with the other staff will not be permitted at the alternate work location unless approved in advanced by the employee's Operations Manager. Company reserves the right to visit the alternate worksite as long as twenty-four (24) hour prior notice is provided, unless an unannounced on-site visit is required by law, regulation, or Company policy. Unannounced, onsite compliance visits may be completed annually or more frequently if needed. In lieu of an unannounced, onsite visit, ongoing compliance may be assessed virtually using a webcam, FaceTime, RingCentral™ application, or other means.

The teleworker also agrees to adhere to any zoning regulations applicable to the designated alternate worksite. Company is not responsible for any zoning violations resulting from establishment of the alternate worksite.

F. **Investigations/Inspections:** In case of injury, theft, loss, or tort liability related to teleworking at the alternate worksite, the teleworker must allow Company to investigate and/or inspect the teleworking site. Random, annual onsite audits may be performed by Corporate Security and Compliance to confirm compliance with all teleworking requirements. In lieu of an onsite visit, investigations/and or inspections may be completed virtually using a webcam, FaceTime, RingCentral™ application, or other means. If it is found that teleworkers are notifying each other of the random audits, those employees will automatically lose their teleworking privilege.

G. **Equipment:** All equipment, including computer workstations, will be provided by Corporate IT. Company will provide the following equipment at the teleworking worksite:

- Network access device
- Soft or hard telephone
- Headset, mouse, and keyboard
- Two (2) x 24" monitors
- Ergonomic assistive devices that are already in place at a primary worksite location and prescribed by a physician, as evidence by a prescription in the personnel file.

The Human Capital Business Partner and Vice President, Operational Development will make any determinations in cases not addressed elsewhere in this policy. Equipment must be used exclusively by the teleworker and only for the purposes of conducting Company business.

The teleworker is responsible for safe transportation and set-up of all computer equipment and ergonomic assistive devices being directly delivered to the teleworking site. In addition, before removing any equipment from Company's primary worksite location. Corporate IT and Human Capital must check it out and record it for security and inventory purposes.

Limitations and Liabilities: Teleworker understands and agrees he or she is liable for property damages and injuries to themselves and third persons at or while transitioning from Corporation's main campus to the teleworking site. Teleworker agrees to defend, indemnify and hold harmless Corporation, its affiliates, employees, contractors and agents, from and against any and all claims, demands or liability (including any related losses, costs, expenses, and attorney fees) resulting from, or arising in connection with, any injury to persons (including death) or damage to property caused, directly or indirectly, by the services provided herein by teleworker or his or her willful misconduct, negligent acts or omissions in the performance of his or her duties and obligations under the Teleworking Security Agreement, except where such claims, demands, or liability arise solely from the gross negligence or willful misconduct of Corporation.

Equipment Liability: Company will repair and maintain any equipment owned by Company. The teleworker is responsible for safely transporting such equipment to

Company's primary on-site location for repair or maintenance unless movement of the equipment is likely to result in damage. Surge protectors, or other protective devices must be used with any computer made available to the teleworker, and all current virus protections and security measures must be implemented as recommended by Corporate IT.

Company may pursue recovery from the teleworker for Company property that is deliberately, or through negligence, damaged, destroyed, lost or stolen while in the teleworker's care, custody, or control. Company does not assume liability for loss, damage, or wear of privately-owned equipment.

Failure to Return Equipment: Teleworkers who transition back to primary on-site location or whose employment ends and fail to return Company-owned equipment will have the cost deducted from their paycheck.

H. Data Security & Confidentiality: Security and confidentiality shall be maintained by the teleworker at the same level as expected at all onsite locations. Confidential and sensitive data must not be saved on any local computer. Restricted, confidential, and proprietary information shall not be taken out of the teleworking site or accessed through an employee's personal system, including print or electronic form.

Exceptions to the printing rule may be made based on individual staff job requirements with senior management approval. The worker must be compliant with HIPAA privacy and security guidelines for storage and disposal of Protected Health Information (PHI), electronic Protected Health Information (ePHI), and Individually Identifiable Health Information (IIHI).

I. Data Property: Products, documents, patents, copyrights, inventions, and records developed while teleworking is the property of Company and are subject to Company control. The teleworker must have a method to safeguard the security of all Company data, including, but not limited to, intellectual property, proprietary information, confidential information, PHI, ePHI, and IIHI, and attorney-client privilege communication. All data property will be adequately secured by teleworker.

J. Record Retention: Products, documents, and records that are used, developed or revised while teleworking shall be copied or restored to Corporate IT's computerized record system. Maintenance of Company records must be consistent with Company's record retention policies and procedures (refer to HL-5.0 Record Composition, Retention, and Storage).

K. Work Audits: Management may perform unannounced audits of teleworker's performance annually or more frequently if necessary, to determine if the teleworker is meeting the minimum necessary performance goals of the teleworker's job description. In lieu of an onsite visit, audits may be completed virtually using a webcam, FaceTime, RingCentral™ application, conference call, or other means.

Telework Expenses:

- **Office Supplies:** Company will provide all necessary office supplies. Supplies normally available onsite will not be reimbursed unless pre-approved by the teleworker's Operations Manager. All supplies should be secured at the teleworking site and must not be used by the teleworker or others for personal use.

- **Phone Service and Network Internet Access:** Network internet access is the responsibility of the teleworker.

- **Travel and Incidental Costs:** The teleworker will not be paid for time or mileage involved in travel between the teleworking site and the primary onsite location, to include travel to and from related on-call transfer of duty. Unless otherwise outlined in the Teleworking Security Agreement, all incidental costs such as residential utility costs, homeowner or rental insurance, and cleaning services, are the financial responsibility of the teleworker.

- **Taxes:** Teleworkers should consult with at tax expert to determine the tax implications of a teleworking site. Neither Company or its representatives will provide guidance or claim responsibility for any local, state, and/or federal tax liability.

Authentication Requirements: Teleworking connections to Company's system network must meet all minimum-security requirements. To help achieve this goal, all teleworker connections will be authenticated with a Company-approved, enterprise grade dual factor authentication system. This ensures that only approved personnel have access to Company's system network.

Personal Cell Phone Use: Use of personal cell phones is against Company policy. Personal cell phones are not secure (e.g., employee's personal cell phone number would be listed on caller ID, etc.).

Attachments:

HL-4.0A – Teleworking Security Agreement
HL-4.0B – Teleworking Safety and Security Checklist