	Pol No. 1028
	Department: IT **Title:** Teleworking Policy
	Author: Megan Sroka
Effective Date: 6/1/2021	**Revision Date:** 5/15/2024
Approver Name; Title Chad Davis; Chief Information Officer	**Signature & Date** Chad Davis (May 15, 2024 17:49 EDT)

1. PURPOSE

This policy establishes ECHO's Teleworking requirements, for managing risks from employees working at alternate work locations. The Teleworking Policy helps ECHO implement security best practices with regard to logical and physical security, and remote access. The policy defines Telework, indicates the requirements for Teleworking and outlines the responsibilities of Teleworkers. When the information in this policy is not sufficient for a given security topic, this policy may indicate a separate Policy or Procedure (SOP) that contains more details.

2. SCOPE

This policy applies to employees, contractors, consultants, and temporary workers who access network, computer, or other electronic devices associated with ECHO business. Any information or systems not specifically identified as the property of other parties, that is transmitted or stored on ECHO IT business systems or IT resources is the property of ECHO.

This policy is directed toward the employee's Telework environment, which includes any place where an employee regularly conducts work, such as the employee's home. If temporarily working remotely from a location other than the usual telework environment, employees are required to comply with ECHO's ***Remote Access Policy***, and use their best judgement to ensure the environment is appropriate to conduct business.

Violations of this policy may result in corrective action, as described in the Employee Handbook.

3. POLICY

Teleworking, or telecommuting, is the concept of working from home or another location on a full- or part-time basis. Teleworking is not a formal, universal employee benefit. Rather, it is an alternative method of meeting the needs of the company. The company has the right to refuse to make teleworking available to an employee and to terminate a teleworking arrangement at any time. Employees are not required to telework.

ECHO ensures that suitable protections are in place to protect against the theft of equipment and information, the unauthorized disclosure of information, and unauthorized remote access to the organization's internal systems or misuse of facilities. (HITRUST 0415.01y1Organizational.10) ECHO offsets the risk of telecommuting through the purchase of insurance. (HITRUST 0409.01y3Organizational.3)

Teleworking employees are responsible for understanding these requirements and signing an attestation of abiding by ECHO Teleworking requirements.

1. Teleworking activities are only authorized if security arrangements and controls are in place, as determined by the *Teleworking Attestation*. ECHO's security team may ask additional questions or request additional evidence before Teleworking is approved. (HITRUST 0405.01y1Organizational.12345678)
2. Teleworking employees will meet reasonable physical security requirements and protections of ECHO assets and documents, including meeting reasonable protections from family and visitors.
    a. Prior to authorizing teleworking, the physical security of the teleworking site is evaluated by means of the Teleworking Attestation, interviews, and any other means deemed appropriate by the IT Security department. Any threats/issues identified are addressed. This will be done as part of the employee IT onboarding process. (HITRUST 0407.01y2Organizational.1)
    b. Results of the evaluation are considered confidential and are not shared externally.
3. Teleworking employees will complete all required security awareness and privacy training, including the risks of teleworking, the controls implemented, and their responsibilities as a teleworker, prior to being authorized for telework. (HITRUST 0408.01y3Organizational.12)
4. Teleworkers are responsible for communicating with information security personnel in case of security incidents.
5. Teleworkers are forbidden to use privately owned computers to access ECHO Information Systems or Data unless they are using VDI, as authorized by ECHO.
6. Teleworkers are subject to ECHO's ***Acceptable Use & Monitoring*** Policy

Conditions of Employment: All ECHO Standards of Conduct and policies apply to individuals who are teleworking. Failure to follow policies, rules, and procedures may result in termination of the telework arrangement and/or disciplinary action.

Hours of Work: The amount of time the teleworking employee is expected to work shall remain the same as for on-site work, unless specified otherwise in writing. A teleworking employee must be available during scheduled work hours by phone, e-mail or other specified methods of communication with their supervisor.

Equipment: ECHO will provide suitable equipment to perform all permitted work and secure remote access. ECHO will also provide all required hardware & software support and maintenance including all normal IT auditing and security monitoring. The teleworker is responsible for safe transportation and set-up of equipment and providing a suitable internet connection.

Data Security & Confidentiality: ECHO instructs all personnel working from home to implement fundamental security controls and practices. (HITRUST 0416.01y3Organizational.4) Security and confidentiality shall be maintained by the teleworker at the same level as expected on-site.

Confidential and sensitive data should not be saved on the local computer. The teleworker is responsible to ensure that non-employees do not access ECHO data in any format.

4. REVISION HISTORY

DATE	DESCRIPTION
5/19/2021	Original Policy
5/18/2022	• Scope changed to reflect only ECHO Employees, Contractors, Consultants and Temporary workers (not vendor contractors). • §3 added "ECHO offsets the risk of telecommuting through the purchase of insurance. (HITRUST 0409.01y3Organizational.3)" • §3.6 added "Teleworkers are subject to ECHO's Acceptable Use & Monitoring Policy" • Under "Equipment" removed "the use of personally owned computers is forbidden" as this was addressed in §3.5 • Removed Compliance Manager as a signer
5/17/2023	§3.5.2 added (in bold) "Teleworkers are forbidden to use privately owned computers **to access ECHO Information Systems or Data**."
5/15/2024	Added "…unless they are using VDI, as authorized by ECHO" to #5.

5. APPROVALS

TITLE	APPROVED BY	SIGNATURE
VP of Systems Architecture	Jamie Kosempa	Jamie Kosempa
Director, GRC	Charlie McVan	Charlie McVan Charlie McVan (May 15, 2024 15:51 EDT)
Human Resources Manager	Stephanie Szabo	Stephanie Szabo Stephanie Szabo (May 15, 2024 15:52 EDT)

6. REFERENCES

N/A

7. ATTACHMENTS

N/A