REMOTE INFORMATION TECHNOLOGY POLICY

Remote Information Technology Policy, version 1.0		
Status:	☐ Working Draft	☒ Approved
Document Owner:	Don Becchetti	
Last Review Date:	07/26/2024	

This information is available in an alternate format upon request.
Lifeworks is an Equal Opportunity Employer.

Table of Contents

REMOTE INFORMATION TECHNOLOGY POLICY

Purpose

This document defines policies, guidelines, and best practices for the use of Lifeworks **computing devices**, defined as computers, mobile devices, mobile phones, tablets, hotspots, and all other computer devices, and any Lifeworks owned **technology equipment** (printers, monitors, copiers, scanners, keyboards, mice, docking stations, hubs, cameras, storage drives and cards, and all other technology equipment) when used for working from home or any other remote physical location outside the Lifeworks offices or program sites. If you have any questions, please contact the Information Technology (IT) department (open a Dynamics 365 case or call the IT Service Desk at 651.365.3786).

Scope

All Lifeworks Personnel are responsible for being aware of and complying with this policy. **"Lifeworks Personnel"** means paid and unpaid staff (including employees, temporary and contractors), volunteers, student interns, or any other persons who work for or on behalf of Lifeworks.

All Lifeworks Personnel using Lifeworks computing device resources from home, or from any other remote location.

The Lifeworks Remote Information Technology Policy applies to any individual, entity, or process that interacts with any Lifeworks information resources, **including but not limited to** computing devices, equipment, hosted systems, internal systems, data, databases, digital documents, cameras, digital storage devices, USB flash drive, SD card, and paper-based documents. All Lifeworks Services Personnel must read and agree to follow these policies and guidelines.

This information is available in an alternate format upon request.
Lifeworks is an Equal Opportunity Employer.

Policy

Network and Information Access

While remote access can increase productivity and efficiency, it also exposes Lifeworks to greater risk. Lifeworks Personnel are required to abide by the following policies and guidelines. Exceptions to these policies must be coordinated with the Lifeworks IT department.

- Remote information technology access and use of computing devices must comply with all other Lifeworks information technology policies. (Acceptable Use Policy, Security Policy, Privacy Policy) and any other Lifeworks Policies.
- Permitted remote information technology access must be conducted using computing devices owned by and provided by Lifeworks.
- Confidential data and protected data, including personal identifiable information (PII) and electronic protected health information (ePHI), must not be stored on local computing devices.
- All remote information technology access of Lifeworks information resources must take place from Lifeworks owned devices using encrypted local storage devices. The Lifeworks IT department will enforce local storage encryption using enterprise mobility management tools.
- Non-Lifeworks Personnel are prohibited from the use of Lifeworks technology equipment.
- Lifeworks Personnel must report theft or loss of any computing device or technology equipment to the Lifeworks IT department **IMMEDIATELY (as soon as you have discovered the computing device or equipment is missing or stolen).** To report loss or theft, submit an IT case by emailing D365-Information Technology or calling the IT Service Desk at 651.365.3786.

Information Protection

- Lifeworks Personnel must use IT approved and provided systems for remote access of Lifeworks technology resources.

- Lifeworks Personnel must not circumvent established procedures or use any tools or methods that are not provided by the Lifeworks IT department to transfer or share Lifeworks information resources.

Clean Desk

- Employees must secure all confidential information, including PII and ePHI, in their workspace at the conclusion of the workday and when they are away from their workspace for an extended period. This policy applies to electronic and physical hardcopy information.
- Lifeworks computing devices must have the screen locked, logged out, or shut down when unattended and at the end of the workday. Portable devices that remain in the remote workspace overnight must be shut down and stored in a secure location. Lifeworks computing devices used at job sites must be securely stored in locked storage.
- Lock all paper records in Lifeworks provided lockable storage (may include file cabinet, locking drawers, locking bag, or locked document boxes) at night or anytime you leave your workspace.
- When out in community spaces, never leave Lifeworks computing devices unattended.
- Printed materials must be immediately removed from printers or fax machines. Printing physical copies should be reserved for moments of absolute necessity. All documents should be viewed, shared, and managed electronically whenever possible.
- Passwords must not be written down or physically stored anywhere in the remote workspace.

Document Destruction

- All paper related to Lifeworks, including documents, forms, and notes, which are no longer needed must be shredded according to Lifeworks guidelines (Lifeworks approved and provided shredder, or secure shredding services at a Lifeworks controlled facility), before being recycled. All Personnel working from home, or other remote information technology locations, must have direct access to a Lifeworks provided cross-cut shredder or return for proper disposal at a Lifeworks controlled facility. Please follow all Lifeworks retention schedule and policies for securely destroying documents.

- All external data storage media, including external hard drives, USB storage, flash drives, thumb drives, CDs, DVDs, SD cards, digital cameras and associated hard drives, should be returned to the Lifeworks IT department for end-of-use destruction. Lifeworks IT devices and storage must be sanitized and/or destroyed by the Lifeworks IT department in accordance with Lifeworks data security standards.

Device Handling, Transport, and Storage

Work Purposes Only: Lifeworks technology resources are for work purposes only. Personal use is limited to emergency phone calls on mobile phones.

- While in transit, laptops and tablets must be contained within a laptop bag or similar outer protection (Lifeworks provided bag). Laptops must be shut off when they are not in use or stored and when they are in transit.
- You must always carry your Lifeworks-owned computing devices (tablets, laptops, phones) with you. If Lifeworks-owned computing devices are not allowed in certain environments, they must be stored out of sight and locked (trunks of vehicles) or left at home or locked up in an office if the device is not needed. Locations which have secured lockers can be used to store Lifeworks owned computing devices.
- While traveling, Lifeworks computing devices should be in your carry-on luggage. You should never transport Lifeworks computing devices in check-in luggage.
- In those exceptional cases when you cannot carry your computing devices, unattended devices must be stored out of sight and secured to the greatest extent possible. Computing devices should not be stored in vehicles that do not have separate lockable trunks.
- Computing devices must be screen-locked when unattended and tablets and laptops must be shut off when not in use.
- Lifeworks Personnel must not tamper with or change remote access or security settings as implemented by the Lifeworks IT department.

Connecting to Wi-Fi

Unsecured wireless network traffic is easily recorded or monitored, giving potential attackers access to your activity and the information you are transmitting. It is important that you only use secure wireless connections when performing work for Lifeworks.

Below are requirements for using wireless connectivity.

- Only use wireless access from your Lifeworks mobile device, home networks, and/or a Lifeworks provided cellular hotspot. to ensure the security of the connection whenever possible.
- Only use fully encrypted HTTPS website connections to transmit confidential or personal information.
- Do not use Wi-Fi networks which are not password protected.
- Disconnect from the W-Fi connection when you are finished with your session.
- You should log out of all applications and accounts and shut down your laptop when you will not be using it for an extended period and at the end of each day. Unless you are performing a required update to your laptop, the laptop should always be shut down at the end of each day.

Return of Equipment

Lifeworks Personnel must promptly return all Lifeworks owned and provided equipment when requested or at employment separation.

Rights & Responsibilities

All Lifeworks Personnel are responsible for awareness and compliance with this policy.

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Resources

Resources FRSecure Security Risk Assessment Roadmap

HIPAA Privacy Policies

HIPAA Security Policies

Image and Recording Policies

Password Policy

Password Construction Guidelines

Version History

Version	Modified Date	Approved Date	Author	Reason/Comments
1.0	07/26/2024	07/26/2024	Don Becchetti	Collaboration with Information Privacy and Security Office (IPSO)