Revision History

Version	Date
Using an External IT Vendor Procedures and Guidelines, 1.0	2 August 2021

USING AN EXTERNAL IT VENDOR PROCEDURES AND GUIDELINES

Requirements

When using a non-USEIC IT technician or service, it is your responsibility to ensure in advance that related resources will be available. Please use the information below to make sure that any technician will have the necessary resources ready. In many cases you will need to request access or register information for the network well in advance. It is the responsibility of the Data Protection Officer (DPO) to ensure that any non-USEIC IT technician has access to all resources that will be needed for any troubleshooting or work they must perform. If requirements are not met in advance, you risk owing the vendor for an appointment where they were not able to complete support work.

1. Vendors Accessing Personally Identifiable Information (PII)

Each vendor or service provider that may receive, view, access, use, disclose or create PII from USEIC must be part of a contractual agreement.

2. Preparing for Computer Access

a. Verify whether the technician will require Administrative Rights on the computer. If so (and the computer is connected to the USEIC IT-managed Organizational Network) review the Administrative Rights required procedures.
b. Verify whether the work will require connecting any unregistered computer(s) to the wired Organizational Network. If so, submit an IP (network) address request to connect.
c. If the technician will be connecting to an organizational computer or resource remotely, verify whether VPN access will be required for the technician. If so, notify the DPO. The DPO will be able to grant access.

3. Computer, Printer, or other network-connected device installation

a. Any computers or other devices that connect to the Organizational Network must register for an IP (network) address and have the registration completed before they will be able to connect.
b. You must verify that the data port that the device will be plugging in to is active; if not request that it be activated.
c. Make sure that you have any/all required network cables to plug the system into the network.

4. Removal of Computer and Network Access

a. Verify that all contractual work has been completed by the vendor
b. If any, verify that all vendor computers or other devices that connect to the Organizational Network are disconnected
c. Verify that all Administrative Rights to computer, database, or Network accounts accessed by the vendor are disabled and archived.
d. Verify that all temporary user accounts are archived or deleted.
e. If applicable, change passwords of all accounts accessed by the vendor.
f. Verify the return of all keys and access cards.