Revision History

Version	Date
Network Protection Policy, 1.0	30 July 2021

NETWORK PROTECTION POLICY

I. Introduction

The secure management of the Organizational Network (as such term is defined in the USEIC Data Protection Charter (the "Charter")), which may span organizational boundaries, requires the careful consideration of the flow of information and the regulatory requirements regarding monitoring and protection of Networks. The Organization requires that all Network, communications, and telecommunications related equipment and devices, including cabling, be installed, and maintained by the Data Protection Officer (DPO).

Capitalized terms used in this Policy without definition are defined in the Charter.

II. Policy

A. Standard Requirements

1. The following equipment must be installed and maintained by the DPO and IT staff:
   - Communications cabling, including any permanent cabling and/or cabling between workspaces and rooms intended to be used for voice and data networking or other communications;
   - Routers on the Organizational Network that serve to segment the Network;
   - Communications switches and hubs (e.g., Ethernet switches) on the Organizational Network;
   - Wireless Access Point (WAPs) and other wireless devices that provide access to, or bridge, the Organizational Network;
   - Telecommunications equipment (e.g., PBXes, VOIP systems, etc.);
   - Cellular telephone (voice and data) communications infrastructure cabling, antennas, and equipment; and
   - Cable and satellite television infrastructure cabling, antennas, and equipment.
2. All Network enabled devices connected to the Organizational Network must use (a) the DHCP to configure Network IP addresses and (b) the DNS protocol for Server information. Network enabled devices connected to the Organizational Network must adhere to USEIC's Network and security procedures.
3. The DPO implements the appropriate logging and monitoring of Networks in accordance with the USEIC Information Resource Access Control and Log Management Policy.
4. Standard protections are established by the DPO and implemented by IT staff to safeguard the confidentiality and integrity of organizational information passing over public and wireless Networks.

B. Waivers and Exceptions

Any Executive Manager may request that a Network or communications infrastructure that is not maintained by the DPO or IT staff be granted a waiver of the provisions of this Policy by the DPO. Such a waiver may only be

granted if the DPO determines that there are compensating controls in place to address all major information security risks.