**Number:** HR**-**316

**Policy Number (if applicable):**

**Office of Primary Responsibility:** Human Resources

**Effective Date: 01/23/2024**

**Review Date: 01/23/2024**

**Title of Procedure:** Remote Use of Hocking College Resources

**Purpose:**

The purpose of the Remote Site Security Standards is to provide the data protection security necessary to comply with the College’s Telework Policy. These standards are mandatory requirements and establish an effective baseline of appropriate system, administrative, and physical controls to safely an effectively secure a remote working environment.

These standards apply to all College employees, or contractors with the College who have been provided with College owned equipment or utilizing personally-owned computer, or other equipment to connect to College network from a remote location.

1. **Protecting Critical Information:**

One of the most important aspects of information security is protecting critical information. Confidentiality, integrity and availability are the three predominant principles of information protection. Compromising these principles leaves systems and critical information in jeopardy. Establishing remote site access creates the potential for security risks and threats that could result in damage to the integrity of the College, cause financial loss to the College, and /or personal hardship to individuals. Threats are the accidental or adversarial attacks against the College, while risks are the realization of the threat based on its potential loss. Below are some of the security threats that should be considered when determining whether remote site access is feasible in your department.

* 1. The networks utilized are not controlled by the College and may be more open. Physical loss of data residing on equipment used for remote site access.
  2. Access to data by those unaffiliated with the College, including family members, on shared devices in a household
  3. Disgruntled users or employees who abuse the privilege of remote site access to acquire or steal College data
  4. Intercepted or stolen data transmitted over an insecure network
  5. Home devices may be subject to E-Discovery requests

1. **Standards for Operating from a Remote Work Environment:**
2. Operating Environment
   1. All employee computers connected to the College’s network via remote site access technologies must use current/up to date anti-virus software to ensure that their computer is protected from hackers and malware. All employee computers connected to the College network via remote site access technologies should employ a software or hardware-based firewall.
   2. All equipment should utilize operating systems and software that are currently supported by a legitimate vendor (i.e. Microsoft, Apple, Adobe, etc.).
   3. All employee computers connected to the College network must automatically or manually apply all necessary Operating System (OS) and application security updates or “patches” and keep the equipment up to date.
   4. As a rule, users may not store any College restricted data on their personally owned devices. Restricted data includes data that the College is required to protect under regulatory or legal requirements. Examples include student or employee identifiable information (i.e., name, SSN, birth date, home address, etc.), medical records, legal records, student records, police records, and credit card information. Restricted data needs to be protected at the same level as required on campus.
   5. The wireless (wi-fi) preferences/settings for your computer and portable devices must not be set up to auto-connect to any wireless network they detect. Auto-connecting to unknown networks could put your computer and data at risk.
   6. The employee is responsible for ensuring that family members do not violate any College policies, do not perform illegal activities, and do not use the access for outside business interest. The employee bears responsibility for the consequences should the access be misused.
   7. A minimum internet bandwidth requirement minimum for remote access is 20MB. The equipment and service required to achieve this recommendation are the responsibility of the employee.
   8. Secure remote access must be strictly controlled. Control will be enforced via multi factor authentication or public/private keys with strong pass-phrases.
   9. Employees and contractors with remote access privileges must ensure that their College owned or personal computer, which is remotely connected to Hocking College’s network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
   10. Reconfiguration of a home user’s equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
   11. Organizations or individuals who wish to implement non-standard remote access solutions to the College’s network must have approval from the Hocking College’s IT department.
3. Physical Security
   1. Hardware, software, and data destruction of restricted materials must be done securely and disposed of at the termination of business need, and in conjunction with the College records retention policy. Remote working arrangements should be equipped to facilitate this activity (shredder).
   2. Employees and units are responsible for security breaches involving NPPI (non-public personal information). The measures described will help reduce the number of security breaches and limit the cost, time, and negative publicity associated with such breaches.