

## **Physical and Security Controls**

### **Appendix F**

The following physical and security controls must be adhered to:

1. Network systems must be installed in an access-controlled area. The area in and around the computer facility must afford protection against fire, water damage, and other environmental hazards such as power outages and extreme temperature situations.
2. File servers and/or storage containing PII, Confidential and/or Internal Information must be installed in a secure area to prevent theft, destruction, or access by unauthorized individuals.
3. Computers and other systems must be secured against use by unauthorized individuals. It is the responsibility of the user to not leave these devices logged in, unattended, and open to unauthorized use.
4. Ensure network systems and network equipment are properly secured to prevent unauthorized physical access and data is properly safeguarded to protect from loss. A record shall be maintained of all personnel who have authorized access.
5. Maintain a log of all visitors granted entry into secured areas or areas containing sensitive or confidential data (e.g., data storage facilities). Record the visitor's name, organization, and the name of the person granting access. Retain visitor logs for no less than 6 months. Ensure visitors are escorted by a person with authorized access to the secured area.
6. Monitor and maintain data centers' temperature and humidity levels. The American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE) recommends an inlet temperature range of 68 to 77 degrees and relative humidity of 40% to 55%.
7. Monitor and control the delivery and removal of all asset-tagged and/or data-storing IT equipment. Maintain a record of all such items entering or exiting their assigned location using the district approved technology inventory program. No technology equipment regardless of how purchased or funded should be moved without the explicit approval of the technology department.
8. Ensure that equipment being removed for transfer to another organization or being designated as surplus property is appropriately sanitized in accordance with applicable policies and procedures.