Indiana State University Data Security Plan for Controlled/Regulated Data Sets

A data security plan for controlled/regulated data at ISU documents the following security technology and process requirements. These can vary depending on additional requirements mandated by the data set provider\*.

# Data Storage and Use

* **Data Repository**
  + an assigned location will be documented for the data storage.
    - This can be a data center storage system or a workstation hard-drive.
* **Data Terminal(s)**
  + ISU OIT managed workstation system(s) or server(s) that can connect to the Data Repository.
* **Duration/Renewal**
  + Period of time that ISU will hold the data with a defined renewal date.

# Systems and Network Security

* **Centralized Logging** 
  + Authentication logging
  + System logging
  + Network logging
* **Server/Workstation Physical Controls**
  + Secure location
  + Network isolation\*
  + USB port-disabled\*
* **Network Technical Controls**
  + Hardware Firewalls (Cisco Firepower)
  + Intrusion Detection (Cisco Firepower)
  + Intrusion Prevention (Cisco Firepower)
  + Secure network segmentation of workstations and/or data storage systems.
* **Server/Workstation Technical Controls**
  + Anti-Virus (McAfee Event Detection and Response)
  + Administrative privilege management/restriction (CyberArk)
  + Software Firewall (McAfee)
  + Data Loss Prevention (McAfee)
  + Full Disk Encryption (McAfee)
* **Change Management** 
  + Ticketed Tracking of User Provisioning (TeamDynamix ITSM)
  + Ticketed Tracking of System configurations (TeamDynamix ITSM)

# Employee Training and Management

* **Research Data/System Role Definition**
  + Security Administrators
  + System Administrators
  + Data Users
  + Data User Supervisors
* **Employee Training**
  + United Educators Cyber Security Awareness
  + New Employee Orientation Training
  + Phishing Simulation - KnowBe4 Email
  + Specific Departmental Training
* **Management**
  + Policy and OIT Standards
  + Internal Departmental Processes and Procedures

# Incident Response

**Incident Response** - Data, networks, and systems in scope of a Data Security Plan will follow the Indiana State University Computer Security Incident Response Plan in the event of a security incident. (ISU Stakeholder) and (DATA PROVIDER) will be included as the stakeholders in the event of a declared incident.