Data Center Best Practices

Revised – 02/13/2023

Version 2.0.3

Table of Contents

1. Initial Document

Creation Date: February 7th, 2020

2. Revision

Revised By: 2020 IE Committee

Revision Date: 02/13/2023

Version Number: 2.0.3

3. Usage

This document contains a set of guidelines and best practices recommended by the Best Practices Committee at Kennesaw State University.

This document is intended to serve as a general guideline for setting minimum standards for data centers and how they should be maintained. Furthermore, the ever-changing nature of information technology prevents this document from being entirely inclusive but should serve as a general baseline for data centers. Please feel free to query the System Administrators Group and ListServ for additional guidance.

KSU policy regarding server set up and mainteua0.005 Tw 0.22 0 T.r46.1 (t)-4 (0.[g)6 (u):62.7005 Twrs)2

4.1.2 Limited Access

Servers should always be in a secured, locked area. Access to these areas will be granted only to persons when physical access is required for their job duties. Entries into these secure areas will be tracked and preferably with an electronic key card system. Door access is reviewed and granted through

4.1.4 Fire Control

Servers should be protected in the case of fire by a fire suppression system. The system will be designed to limit any damage it will cause to the server hardware. As traditional water based fire extinguishing systems will likely cause as much damage to the server as the fire, alternatives, such as inert or synthetic gas suppression systems, should be considered.

4.1.5 Climate Control

Server hardware requires a controlled environment to prevent damage and ensure

not occlude any ventilation ports. Many "security" issues relate to unknown machines, or the wrong machine being taken down at the wrong time.

4.2 Disaster Recovery Practices

4.2.1 Disaster Recovery Plan