Data Center Best Practices

Revised – February 3rd, 2020

Version 2.0.0

Table of Contents

1. Initial Document

Creation Date: February 7th, 2020

2. Revision

Revised By: 2020 IE Committee

Revision Date: 02-07-2020

Version Number: 1.0.0

3. Acknowledgments

The final release document is a collaborative work between the following committee members:

4. 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 maintenance can be found at university's policy repository, https://policy.kennesaw.edu. Other policies may be applicable to your server based on data usage, programs offered, or other criteria. Please regularly audit the available policies at the policy repository.

5. Physical Security and Disaster Recovery

5.1 Physical Security Practices

5.1.1 Walk Through

There is no substitute for physical examination of facilities. A periodic computer room inspection should be performed in person to assure a proper physical situation. Administrators should verify that there are no problems such as plumbing or cooling leaks, warning lights, doors ajar, unplugged power cables, etc.

5.1.2 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 the university's door access process. All data centers door access should be protected by a digital lock system with two-factor authentication enabled such as PIN+card. Access request is to be reviewed and approved by the respective leadership owner for each data center. Data center access should also be reviewed on a routine basis by the data center owner to verify the access list.

Physical access to a server opens many avenues of risk. Should an intruder gain access to a server console, it is possible that serious damage or data theft could occur, either through console manipulation, physical security overrides or physical theft.

Additionally, there are non-malicious events which can occur around server equipment when inexperienced personnel have access to sensitive areas. These include but are not limited to unintentionally leaving doors insecure, tripping power or other cabling, and spills of materials hazardous to personnel or hardware.

Whenever possible and appropriate, areas which hold mission critical infrastructure or highly sensitive data shall be monitored with a camera system. This system should have both live view and archival capabilities.

5.1.3 Redundant Power

All servers should be operated with some form of backup power system. This system will protect the hardware from power surges and fluctuations. In addition, it will power the system during power outages. All data centers are to be protected by a natural gas generator in the event of a power outage for the data center. Each data center should maintain a UPS to protect against power outages in short durations, provide clean consistent power to the data center infrastructure, and provide enough power to transfer the power from building to generator and back during power outages. It is recommended that the batteries in these UPS be maintained on a routine basis since they degrade over time. Each rack will contain A and B redundant power in case of a PDU or UPS failure.

How long the redundant power system can power servers in a power failure is a function of the criticality of the servers. In non-critical, academic settings, a few minutes of redundant power may be all that is needed to smooth over a brief outage. For mission critical servers, it may be necessary to provide the capability of 24 by 7 redundant power.

The system should be tested regularly during off-peak time periods, with technical personnel present.

5.1.4 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.

5.1.5 Climate Control

Server hardware requires a controlled environment to prevent damage and ensure efficient procession. The preferred temperature range is between 65 °F and 82 °F with the optimal temperature range between 68° and 71° with a relative humidity between 40% and 60%. This will normally require supplemental cooling equipment. If your server room is too warm, seek assistance from campus physical plant operations to determine how the room can be better cooled. Areas which hold critical systems should have fully redundant HVAC systems.

5.1.6 Clustering, Failover, Redundant Servers

If the operation of your servers is critical, you may want to consider server clustering and/or server failover. Active/Passive configurations are designed primarily for failure proofing your server. Active/Active clusters also answer this concern, but additionally provide improved performance through load sharing. Active/Active setups are therefore correspondingly more expensive and complex. Clustered server hardware should be as identical. For mission critical servers a redundant server(s) should be kept at geographically diverse location(s).

5.1.7 Redundant Storage

Storage used in servers will be redundant. Either of the following methods may be used in combination or alone.

5.1.7.1 Redundant Array of Independent Disks (RAID)

RAID is a system of combining multiple disks to enhance performance and/or redundancy of the individual disks. This is the preferred way of implementing redundancy. Without delving into proprietary methods, RAID has 7 different configurations. In depth discussion of RAID levels is beyond the scope of this document, but RAID levels 1, 5, 6, and 10 each fulfil the redundancy requirements.

5.1.7.2 Replication

Replication is when data is copied, at frequent intervals, to hardware at another physical location. Intervals can be as short as “on-write” to hourly. Any interval longer than that does not constitute “redundancy” but falls into the category of backups.

5.1.8 Labeling

All machines should have a correct label, both a physical label and in any menu on the associated KVM (Keyboard, Video, and Mouse) switch. Take care that any physical label does

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

5.2 Disaster Recovery Practices

5.2.1 Disaster Recovery Plan

Each server should follow a overarching disaster recovery plan. This plan should include a set of policies, tools, and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a disaster.

5.2.2 Data Protection

Servers and data should follow some type of consistent data protection plan. It is best practice to back up daily. These backups should be kept onsite for an easy and speedy recovery while maintaining an offline copy using either tape (sent to secure storage) or cloud storage.

5.2.2.a Off -Site Backup Storage

At least one full backup set of your data should be kept in a secure offsite location. This may be accomplished through physical or electronic means. Disaster recovery services such as Iron Mountain or cloud storage may be used to fulfil this requirement.

5.2.2.b Testing Backups

Backups should be tested via full restore on a routine and repeated basis.