Server Administration Policies

Based on my observation all three-university policies state their IT policies and procedures that must be adhered by all IT professionals utilizing their services. UITS Arizona places strong emphasis on data center policies while UITS Miami gives a brief description of secure back up storage/data center procedures. While Boise State does acknowledge the appropriate storage back up procedures there are no further details on data center personnel access, access logs, or unauthorized access. All three entities place considerable focus on areas they believe to be most important. For example, the policies administered by the University of Miami seems to be a general overview explaining the medical information technology services that are available and provided. Boise State places focus on securing their data and avoiding any potential hazards or risk. Again, UITS Arizona places strong emphasis on their data centers access policies and procedures.

Based on Miami UITS there are no policies and or procedures in regards to equipment installation, and change management methods. However, UITS Miami does mention server specific procedures such as site licenses for both anti-virus and anti-spyware software as well as off-site storage backup procedures. UITS Miami also explains that physical access to data centers are controlled by security systems. Intruder alarms are monitored by the Department of Security. Uninterruptible power supply and emergency generators are available to maintain power without interruption. FM200 and Inergen fire suppression systems will be at hand to extinguish fires without damaging equipment or backup tape systems.

Boise State seems to deviate from specific equipment procedures, safety rules, security/personnel access, and change management policies. Boise State does acknowledge that proper server virus software be equipped as well as security and operating system patches or hot fixes be applied. In addition appropriate back up of the OS, applications, data, and configuration documentation must be maintained.

Examining UITS Arizona emphasis is placed on upholding UITS data centers environments, enhanced security, fire suppression equipment, alarms, uninterrupted power (UPS and generators), high-speed network connectivity and 24x7 operator coverage. Significant emphasis is placed on data center access and etiquette. CatCard swipe access will only be given to approved individuals. Individuals requiring infrequent access will be granted escorted access as needed. Access logs at each data center must be maintained at all times, unauthorized access must also be logged and maintained. The data center etiquette appendix highlights equipment installation polies such as all working areas being clean and free of debris as well as having rack enclosures neat and free of unused equipment. Floor tiles should also never be raised without prior consent.

In conclusion, placing more emphasis on equipment installation policies as well as safety procedures in the case of an emergency and change management methods during prolonged downtime hours could strengthen UITS Miami. Boise State could also beef up their equipment policies, safety rules, data center access privileges, and lastly their change management procedures. UITS Arizona mentioned most of the specific areas but should probably be much more detailed they also excluded all change management actions.