APPENDIX C
System Administration Best Practices

In addition to the best practices outlined in Appendix B, the following should also be adopted by system administrators for servers under their control.

1. **Physical Security:** Servers must be housed in physically secure locations with restricted access. Best practice would be to control and monitor entry via the university's electronic card access system. These locations should have suitable HVAC, electrical and fire protection systems based upon server requirements.

2. **Backup:** A data backup/restoration process must be in place to protect against accidental loss of data. Best practice would call for daily backup with secure storage of backup media. Backups should be inherently off-site or carried off-site on a regular schedule to be determined by the requirements of the data housed.

3. **Disaster Recovery:** Depending upon the criticality of the system, a formal disaster recovery and business continuity plan may be required to protect the institution in the event of a catastrophic system failure.

4. **Logging:** Appropriate levels of system logging must be enabled and the output reviewed on a regular basis to facilitate the detection of unusual activity that might adversely impact system performance or security. Automated log analysis and exception reporting is recommended.

5. **Firewall Exceptions:** Firewall exceptions that expose system services to the outside world should only be done when necessary. Best practice is to open only the necessary ports required by the service(s) being provided. Servers and end-user workstations should reside in logically separate networks to limit exposure as much as possible.

6. **Vulnerability Scanning:** Vulnerability scans that look for exploitable weaknesses should be performed on a regular basis and action taken to remediate or mitigate exposed vulnerabilities.

7. **Secure Protocols:** Legacy protocols such as TELNET, FTP, POP and IMAP are inherently insecure because they transmit unencrypted passwords. Best practice replaces these protocols with their secure alternatives e.g. SSH, SFTP, POPS and IMAPS.

8. **Test Systems:** For servers that are critical to the business of the university, separate systems should be employed to allow staging and testing of changes before moving them to production servers.

9. **Least Privilege:** Systems and user roles should be configured on a "least privilege" basis so that the minimal required authority or access is granted. This

ensures that systems and users are less likely to cause harm, whether accidently or maliciously.

10. **Restricted Remote Access:** Best practice restricts certain services to campus network address ranges, thus limiting exposure of critical systems from the public Internet. ITS provides a Virtual Private Network (VPN) service to facilitate remote access to such restricted services. Examples of services that are restricted to the MSU network, thus requiring VPN access from off-campus, include remote desktop control and Administrative Banner.