Appendix A
Central Michigan University
Internet-Facing Server Registration Requirements

The following are the minimum requirements to operate a public-facing server (i.e. one whose content is available off-campus on the CMU Network.

1. All servers must be registered with CMU's Security Incident Response Team (CMU-SIRT) through the form provided at: https://ssl.cmich.edu/ServerRegistration.
2. At least one full-time employee (not a student employee) must be identified that is tasked with providing technical support for the server. Their contact information must be kept updated with SIRT for emergencies.
3. Systems housing information subject to one or more legal requirements (i.e. HIPAA, FERPA, etc) must be so identified.
4. A formal build procedure must be documented for the server (i.e. all steps to configure and secure the system). If assistance is required, CMU-SIRT has a recommended build checklist.
5. All systems must be patched and maintained according to operating system vendor recommendations. Patches should be applied in a timely fashion.
6. Credentials for the administrative account (i.e. "Administrator" on Windows and "root" on UNIX-type boxes) must be vaulted with the department head or director for emergencies.
7. All systems must use Central Domain authentication.
8. All systems must have an anti-virus agent loaded, running, and regularly updated. Such signature updates should be not more than one week old.
9. The server just be kept in a secure location with a documented list of individuals that have physical access to the system.
10. An appropriate backup and/or disaster recovery plan for the server and its data must be in place.
11. Event logging must be enabled and at least two weeks of events maintained. At a minimum (as allowed by the operating system and application), the following events must be logged:

a.	Audit Account Logon Events	Success and Failure
b.	Audit Account Management	Success and Failure
c.	Audit Logon Events	Success and Failure
d.	Audit Policy change	Success and Failure
e.	Audit Systems Events	Success and Failure

The following additional items are strongly recommended by CMU-SIRT.

1. The system should be regularly scanned for vulnerabilities. CMU-SIRT is available to perform this service if appropriate software is not available.
2. The mix of services on a single physical or virtual server should be limited as much as possible. For example, it is unwise to run both Microsoft SQL Server and Internet Information Server on the same server.
3. Programming best practices should be observed. Database access from web servers should be encapsulated in stored procedures with the minimum necessary rights granted to a SQL user to allow the transaction.