

University of Maryland Baltimore (UMB) Server Security Standard

Effective Date: 04/14/03

Purpose

This standard establishes a framework for ensuring that servers deployed within UMB's campus are managed in a secure and predictable fashion. It is the responsibility of UMB network managers to protect and maintain the security of the networks they are charged with managing. System administrators are obliged to prevent trespassers from corrupting or misusing any segment of the enterprise network. Listed below are recommended standards to be followed by System Administrators where technically feasible.

Scope

UMB is a distributed environment with corresponding local responsibilities. Support for campus enterprise applications is managed centrally. This security standard is recommended for all server resources within the physical area of the UMB campus and all users who access those resources. It pertains especially to those resources that support vital business functions and that maintain confidential, personal, or protected information.

Standard(s)

To maximize the security of the network server environment, the System Administrator, where feasible:

1. Maintains physical access controls
2. Requires that administrator level passwords are a minimum of 8 characters long
3. Prevents the reuse of passwords over a 12 month period
4. Enforces password expiration at least every six months
5. Ensures that users have unique and separate server accounts
6. Uses antivirus software to ensure that files saved to servers are not infected
7. Recommends the use of antivirus software if the system supports email
8. Ensures that the primary administrator account is the only account with access to all files
9. Ensures that any new data copied onto a server is done in a fashion that logs the transaction/transfer
10. Ensures that only approved and licensed software is installed on the server
11. Provides the capability to log all confidential file access
12. Reviews activity logs for suspicious activity
13. Uses authentication between servers, as well as client and server, when transferring confidential data
14. Performs incremental backup on a daily basis
15. Performs full server backups at least weekly
16. Produces archival backup copies at least monthly
17. Stores backup copies of critical enterprise systems in a protected, off-site facility