

University of Maryland Baltimore (UMB) Workstation Security Standard

Effective Date: 04/14/03

Purpose

This standard establishes a framework for ensuring that local and networked workstations deployed within UMB's campus are managed in a secure and predictable fashion.

Scope

UMB is a distributed environment with corresponding local responsibilities for maintenance of workstation security. This security standard is recommended for all local and networked workstations and all users who access those resources. It pertains especially to those resources that support vital business functions and that maintain confidential, sensitive, or private personal or institutional information.

Standard(s)

To maximize the security of standalone workstations as well as workstations connected to the network, where feasible:

1. Maintain physical access controls
2. Require that network passwords are a minimum of 6 characters long
3. Prevent the reuse of passwords over a 12 month period
4. Promote the use of password expiration of local accounts at least every 6 months
5. Ensure that users have unique and separate network accounts
6. Use antivirus software to ensure that files saved to workstations are not infected
7. Promote the standard that primary and alternate administrator accounts are the only accounts with access to all files on the local workstation
8. Ensure that only approved and licensed software is installed on the workstation
9. Password protect all confidential files on individual workstations
10. Secure all transfers of confidential data between workstation and server
11. Back up critical data on a periodic basis