

## Windows 2003 Security Checklist

System ID \_\_\_\_\_ System Owner \_\_\_\_\_  
System Location \_\_\_\_\_  
System Type and Model \_\_\_\_\_  
Date \_\_\_\_\_ Certifying Official \_\_\_\_\_

### CHECKLIST

#### General

- Remove any shared passwords
- Ensure there are unique UID and passwords for all accounts
- Ensure there are approved passwords for all accounts
- Disable the Guest account
- Ensure the Administrator account has a password
- Remove any vendor supplied accounts or change passwords
- Limit privileged users
- Enable the screen saver for a 10 minute delay
- Ensure a pre-logon message is displayed
- Set the following policies

#### Account Policy:

- Maximum Password Age: Expires in 180 days
- Minimum Password Length: 6 characters
- Account lockout after: 5 bad logon attempts
- Reset count after: 30 minutes
- Lockout Duration: 60 min

#### User Rights Policy:

- Backup files and directories: Administrators, Backup Operators
- Change system time: limit to Administrators, Power Users
- Log on locally: limit to Administrators, Users
- Manage auditing and security log: limit to Administrators
- Restore files and directories: Administrators, Backup Operators
- Take ownership of files and other objects: limit to Administrators
- Act as part of the operating system: none
- Debug programs: limit to Administrators
- Generate security audits: limit to Administrators
- Log on as a service: limit to Administrators or none
- Replace a process level token: none

#### Audit Policy:

- Logon and Logoff - Success and Failure
- File and Object Access - Failure
- Use of User Rights - Failure

- User and Group Management - Success and Failure
- Security Policy Changes - Success and Failure
  
- Is the NTFS file system used (Admin Tools/Disk Admin)?

**I understand that:**

This system is certified and accredited for a three-year period beginning with the date of certification. Any change or modification that impacts the security of the as described in this Short Form require recertification of the system. I must assure that the Short Form is accurate at all times and that the Site Configuration Management Plan is followed.

**I certify that the information in this Short Form is true and accurate to the best of my knowledge**

**Print Name/Sign** \_\_\_\_\_ **Date** \_\_\_\_\_

CIO or Approved Representative Name: \_\_\_\_\_  
*(please print)*

CIO or Approved Representative Signature: \_\_\_\_\_  
Date Approved: \_\_\_\_\_

