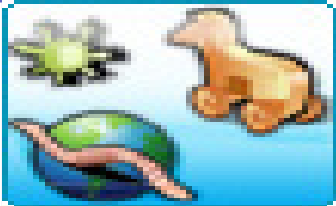


Control System Security

Anti Virus Guidelines



The information in this document is subject to change without notice, and should not be construed as a commitment by ABB. ABB provides no warranty, express or implied, for the information contained in this document, and assumes no responsibility for the information contained in this document or for any errors that may appear in this document.

Revised 01/15/06



Anti-Virus Overview

- Anti-Virus Software is designed to detect and protect against computer viruses:
 - Protects data and normal function of computer.
 - Minimizes time and effort spent dealing with infections.
- The use of Anti-Virus software is a critical element of any process control security strategy:
 - Anti-Virus software when used alone is insufficient
 - Successful Virus prevention begins at the IT network level
 - All organizations should develop a comprehensive prevention program that provides a high level of protection.



Anti-Virus Overview

- Anti-Virus software will not prevent all viruses:
 - If infections occur, AV software will alert you to the virus.
 - Reputable AV software programs can help “clean” (remove) the virus.
 - Important to have pro-active security measures in place (e.g., security patch management) as well as procedural and technical controls to prevent malware (worms, viruses) infections.
- Having Anti-Virus Software installed is not enough:
 - Can give a false sense of Security.
 - Once deployed, Anti-Virus software and definition files must be kept up to date to remain effective
 - Anti-Virus products fail because they are too difficult to use and manage.



Anti Virus Configuration Guidelines

- Automatic scheduling of full system scans may cause Severe Performance Degradation
 - Could impact operators ability to respond to an abnormal situation
 - Perform full system scans only 'on demand' when it will not interfere with operations or during periods of low activity
 - Exclude frequently accessed files and directories from on-access scanning
 - Limit the amount of CPU time used during on-access scanning
- Where On Access file scanning is enabled:
 - Provide feedback to users that an infection was found:
 - Allow users to clean infected files
 - Prompt for user intervention before moving files to quarantine directory
 - Scan boot sectors on removable media
- Review virus scan reports regularly



Anti Virus Signature File Deployment

- Update signature files regularly:
 - Subscribe to Anti-Virus vendor's notification and update services.
 - Leverage enterprise Anti-virus policies and procedures.
- Test Anti-Virus signature files off-line before deploying:
 - Where possible, signature files should be tested on a suitable non-production system to verify compatibility with installed applications.
 - Verify proper operation on a single node.
 - Deploy to production system only after signatures have been tested and verified.
- Automatic Deployment of Signature files:
 - Stage distribution from a central deployment host.
 - Follow recommendations of Anti-Virus software supplier.
 - Stagger automatic deployment to eliminate potential for common cause failure

