ARBONIA
IT SECURITY

Arbonia Services AG
Amriswilerstrasse 50
9320 Arbon
Switzerland

https://security. arbonia.com

IS-ISD-GROUP-007-LEGACY-SYSTEMS-IT-SECURITY-REQUIREMENTS

Contact
Thomas Zehnder

thomas. zehnder@arbonia.com
T +41 71 440 55 14

To	All Arbonia IT Teams
Fyi	-
From	IT Board
Date	13.05.2022

Instruction on the handling of legacy systems

This instruction applies to all legacy systems (e.g. Windows XP, Windows 7, Windows Server 2003/2008/2008R2 etc.) which are no longer supported by the manufacturer (end of support / end of life) and/or no longer receive current updates.

Measures valid for all legacy systems:

- Remove device from the domain
- Block Internet access
- Lock removable media
- Remove local admin permissions for daily work
- Enable and configure local Windows firewall (whitelisting - deny all / allow specific)
- Move system to its own network segment / VLAN
- Implement password policy (user / administrator / service)
- Do not use AutoLogons (If needed, only encrypted with Sysinternals)
- Define network communication and ports (source, destination, ports)
- Allow access to network resources (network shares, etc.) only via dedicated/special authorized users and permissions
- Restrict remote connections (internal/external) and do not allow uncontrolled external access via the Internet (use of Teamviewer only allowed in LAN)
- Protect all legacy systems with restrictively configured microfirewalls

Additional measures if Domain Membership is needed:

- Use dedicated accounts per device (daily work and admins)
- Use dedicated service accounts per device/service
- Secure local admins with LAPS
- Restrict LogonTo (authorize dedicated AD accounts only)
- Restrict registration times if possible
- Use Arbonia GPO's for OS hardening

Further measures (if possible / as soon as available)

- Use 2FA for login to legacy systems

All exceptions must be documented and agreed with the Arbonia Security Team.

Kind regards
Arbonia IT Board