TTM Technologies

Shop Floor IT Equipment Requirement for Suppliers

Roles and Responsibility:

- Suppliers delivering IT and OT equipment to TTM for use on the shop floor must meet the security requirements contained in this document
    - IT and OT equipment can include, but is not limited to, servers, computers, networking equipment, etc.
        - Collectively referred to as equipment in this document
- TTM must approve the manufacturer, models, and technical configuration of this equipment prior to delivery
- Suppliers must be able to demonstrate a robust cybersecurity posture
    - Supplier should submit a copy of any industry standard accreditation applicable to the products or services it is providing (e.g. ISO27001, NIST Cybersecurity Framework, CIS)
- Any deviation from the requirements of these standards must be approved in writing by TTM

General requirements:

- Equipment must be delivered to TTM with a licensed, and currently supported operating system (OS)
    - Operating systems must be current, installed OS should be no closer than 6 months prior to the end of life date
    - Supplier roadmaps should make provisions for OS end of life (EOL):
        - Equipment should be able to accept an upgrade to a current and supportable version if the provided OS becomes EOL
          or
        - Supplier should make a new equipment with a current and supportable version available to TTM
- Equipment should be delivered to TTM up to date, with the latest security patches applied
- Equipment and software must be capable of accepting regular updates and patches
- Equipment and software will be subject to vulnerability scanning; as a result of that, equipment should be resilient and not sensitive to scanning performed by TTM tools
- Antivirus – Computers and servers must be able to run TTM approved EDR or Anti-Virus solutions
    - All AV solutions must be approved by IT Security
- Computers and Servers must be capable of joining Microsoft Active Directory to perform their intended function using Active Directory accounts
- Software must be installed in a way as to not require administrative privileges for it to function properly
- Supplier must provide adequate documentation of use, understanding and maintenance of their software and systems where applicable
- Supplier must provide copies of all software and license keys for disaster recovery purposes
- If supplier will be providing maintenance remotely, connections must utilize BeyondTrust (TTM approved remote access solution for 3rd. parties)
    - Any other method of remote connectivity must be reviewed and approved by IT Security
- All back-door hooks and alternate remote access software must be removed from the system and software before shipping to TTM
- Equipment and software that handle sensitive data must have the capability to log system and file access

- All non-essential software, ports, protocols, and services on operating systems must be disabled
    - Only necessary services shall be enabled unless necessary for the equipment to function properly
    - All un-utilized software must be disabled or removed
- Equipment must be capable of industry standard data encryption in transit and at rest
    - At rest: Windows Servers and Desktops must be capable of FIPS validated Bitlocker or other TTM approved FIPS encryption methods
        - Virtualized Servers or Desktops do not need to be Bitlocker capable
    - Linux: LUX or other TTM approved encryption methods
    - In transit: IPSEC or other TTM approved encryption

Servers:

- Cannot be older than 2 hardware generations for new purchase
- Must support VMWare 8 or above (if virtualized – OVA, etc)
- Support industry standard data encryption methods
- All generic, guest, maintenance, and default accounts (where applicable) should be disabled

Software and Database:

- Interfaces for user login and user data input must be secure and utilize certificates signed by a trusted Certificate Authority (CA) only. Examples: HTTPS / TLS / SSH
- Vendor should restrict systems to individuals who require access, confirming principle of least privilege access
- Licenses should be transferrable between TTM locations and companies
- If supplier is providing customized applications to TTM, source code should be made available to TTM
- Any SaaS based systems, or systems requiring cloud access, require review and approval from IT Security
- Supplier must fix all vulnerabilities discovered in applications

Network Equipment:

- Firmware of network equipment supplied to TTM should be delivered with the latest stable version applied
- Network equipment must be purchased from an authorized dealer of manufacturer

Manufacturing and Test Equipment:

- Manufacturing and Test Equipment must be capable of connecting to TTMs Industry 4.0 platform, prior to leaving the supplier, utilizing one of the following protocols:
    - MODBUS
    - OPC-UA
    - MQTT
    - SECS/GEM – Supplier may be required to cover the cost of SECS/GEM if used

- Web API
- Direct Communication through the following PLC drivers:
  - Allen Bradley
  - Omron FINS TCP/UDP Must provide csv export of tag addresses in English
  - Omron NJ Driver Must provide csv export of tag addresses
  - Siemens S7-1500, S7-1200, S7-400, S7-300 Must provide tag addresses in English Others as approved by 4.0 team as long as they meet the data stream requirements.
- Other protocols may be approved by TTM site IT

Note: When shop floor equipment is PC controlled it will connect to TTM's Industry 4.0 systems using one of the protocols above

DOCUMENT REVISION HISTORY

Revision Number	Revision Date	Revised By	Comments
A	12.19.2024	BD	Convert from legacy format
B			