Manufacturing Sector TOP 10 Cybersecurity Essentials

01
Never Connect Unverified USB Devices
Treat USB drives as potential malware carriers; use only approved hardware.

02
Use Individual Logins; Do Not Share Credentials
Credentials are personal; sharing risks the entire network's security.

03
Lock Screens Before Leaving Your Workstation
Use Ctrl + Alt + Delete (Windows) or Control + Command + Q (Mac) to secure devices.

04
Report Any Unusual Computer or Equipment Alerts Immediately
Prompt reporting prevents possible cyber or operational threats.

05
Use Only Approved Software and Tools
Avoid installing unauthorized apps, websites, or personal devices on factory systems.

06
Double-Check Email Authenticity Before Clicking Links
Beware phishing emails impersonating management or IT. Verify before acting.

07
Keep Factory Equipment Software Updated
Regular updates protect against vulnerabilities and cyberattacks.

08
Prevent Unauthorized Entry to Facilities
Verify identities and coordinate with supervisors when maintenance personnel arrive.

09
Report Lost or Stolen Devices Without Delay
Missing devices pose critical risks; inform security or IT immediately.

10
When in Doubt, Consult Security or IT Teams
Early questioning can prevent breaches and operational disruptions.

vyings

Contact **VYINGS** for fractional cybersecurity leadership.

www.vyings.com
info@vyings.com

Need help securing your organization?