MANUFACTURERS: PRE-PURCHASE GUIDE FOR EQUIPMENT*

Before you purchase or otherwise acquire a piece of equipment, whether it be a CNC machine or a cell phone, answer the questions below. These questions are intended to help you make a well-informed decision about your purchase and understand what safety, cybersecurity and other risks might impact the long-term cost-effectiveness of your purchase.

The sequence of the questions are in terms of equipment lifecycle covering financing, installation, use, maintenance and disposal of the equipment. There may be additional questions specific to your circumstances that you will want to include in your decision-making.

Some of the questions you might not be able to answer - be mindful of those. In this instance, what you don't know CAN hurt. Your local MEP Center may be able to help.

1. Will you lease or buy?

Leasing is becoming increasingly popular for high-tech equipment as it provides protection against obsolescence, but it can be more expensive in the long run, and customers may lose control over updates and upgrades. Whichever option you choose, check contracts for provisions that protect customers from security, quality and compatibility problems that may develop and how those problems will be addressed (see question 7).

2. Where will it be located?

Documentation for the equipment may provide much of this information, but other information is dependent on the business (e.g., protection from nuts in a food processing plant).

- Where is the most efficient location?
- What are the safety requirements?
- What are the security requirements?
- What are the utility requirements?

3. Does it require ancillary equipment?

Sometimes one purchase can lead to several others. Many add-ons are included to either protect people from the equipment or to protect the equipment from the environment.

- Does it require special safety equipment to install, operate or maintain? (e.g., safety sensors, light screens, fire suppression, personal protective equipment (PPE), or static electricity protections.)
- Does it require protection from the environment? (e.g., power fluctuation protection, or protection from moisture or humidity operating limits.)

4. What connections does it have?

Any time a piece of equipment electronically "talks" to something else, be it a sensor or the internet, that communication channel typically has an IP address and represents a cybersecurity risk that should be protected. The more connected a piece of equipment is, the higher the cybersecurity risk.

- Does it have a USB port, disk drive, network adaptor or other connection point (whether used or not)?
    - » How will the connection points (and associated communication channels if used) be secured?
- If the equipment will need data (e.g., a design file or updates) to operate, how does it receive, store, verify and protect that data?

5. Who will use it?

People often represent the most significant safety and security risk.

- Will training/retraining be necessary to be able to use the equipment safely?
    - » Who will provide the training?
- What kind of safeguards will be included so that only those who are permitted to use the equipment have access to it (for regular use and for maintenance or for changing settings)? [Note: Ensure any login/ authentication processes follow best practices (e.g., dual-authentication) while not putting undue strain on employees (e.g., single sign-on).]

6. How often will it be used?

If the equipment is used less often than anticipated in usual maintenance schedules or less often than regular security updates are made available, this can result in both increased cybersecurity risk and decreased reliability.

7. What are the maintenance expectations?

Maintenance can be an expensive endeavor, making or breaking the usefulness of a piece of equipment. It is also a time when unexpected problems can surface such as compatibility issues and cybersecurity concerns leading to long-term unanticipated expenses.

- How often is the equipment expected to need maintenance?
    - » What is the expected mean-time-to-failure?
    - » What is the anticipated down-time?
- How will someone know the equipment is not working properly? [For example, are there indicator lights? Will there be quality control checks?]
- Is there a backup option in case the equipment fails unexpectedly?
- What is covered by warranty and/or a service contract?
- If it breaks in such a way as to cause a safety or security issue, how will that be handled?
    - » Who will be held liable?
- What kinds of maintenance can be done in-house vs. externally?
- Can it be replaced or upgraded piece-by-piece over time? [A modular repair model can cause compatibility problems, but is less of an immediate financial burden than replacing all at once.]
- How will maintenance solutions be verified as effective? [For example, did a change result in reduced quality? When possible, test maintenance solutions or review others' experiences with a solution prior to implementing.]
- If it needs much more maintenance than expected or maintenance is ineffective, what are the options? [e.g., Replacement? Refund?]

8. What does the equipment's end-of-life look like?

Some equipment is designed to last decades, while other equipment lasts a few years at most. Understanding and planning for what will happen when the equipment dies will prevent production interruptions and some cybersecurity concerns.

- If the expected life span of the equipment is less than the expected use period, there will be increased cybersecurity and reliability risk when the equipment becomes obsolete.

- Are there hazardous materials or sensitive data storage that need to be considered when disposing of any part of the equipment?

Next Steps

Once you have answered these questions, it's time to make a decision to purchase the equipment or not. If you purchase the equipment, use the information you gathered to make sure it is installed and configured in a way that meets your efficiency, safety and security requirements.

Your local MEP Center will have resources to help you make the best decisions possible for your business and can help you understand the safety, security, quality and efficiency of the equipment you either purchase or lease.

THE MEP NATIONAL NETWORK

The MEP National Network is a unique public-private partnership that delivers comprehensive, proven solutions to U.S. manufacturers, fueling growth and advancing U.S. manufacturing.

CONTACT US

100 Bureau Drive
Gaithersburg, MD

(800) MEP-4MFG
(Celia Paulsen)

mfg@nist.gov

The content in this document is intended to be used to help inform equipment assessment and selection. However, any resulting equipment decisions on the part of the reader are the sole responsibility of the reader, and NIST MEP is not liable for any results or ramifications of such decisions.