Memo

To: Oshkosh Corporation Suppliers

From: Oshkosh Corporation Purchasing and IT Information Security

Date: November 11, 2019

Subject: Cyber Hygiene

What is Cyber Hygiene?

You want to think of cyber hygiene much as your personal hygiene, maintaining good health and well-being by engaging in good practices. The point is to maintain the good health of your computer environment so that it is protected from threats and remains useful. Much like your immune system protects you, good practices can ensure your computer environment is resilient to attacks. Maintaining a good working computer environment can be difficult, however there are some basic practices that regularly followed will go a long way to protect you.

Cyber Hygiene Best Practices

The following list is not all-inclusive but straightforward practices that will go a long way to secure your computer environment:

1. Inventory all devices and software in your organization – Knowing what you have in your computer environment is the primary pillar on which all other practices rest.
2. Protect all pages on your public-facing websites, not just those that collect information.
3. Secure your network by using firewalls and password protected wireless access.
4. Patch software and hardware – Patching will ensure that you minimize the number of vulnerabilities in your environment.
5. Test for vulnerabilities – Testing needs to go beyond just the software but making sure that the cyber hygiene practices are being followed.
6. Limit administrative privileges – By making sure only select individuals can make major changes, you can limit the ability for damage to your computer environment whether by malicious intent or otherwise.
7. Backup your data – Keep your data secure not only from malicious actors but equipment failure as well. An extra security measure is to encrypt all data and devices.
8. Use strong passwords – Passwords are the easiest way to secure your computer environment so long as you make sure that strong passwords are used. Biometrics and other ways of verifying your identity are available but reliable technology today is expensive and complicated to implement.
9. Educate your employees about cyberthreats and hold them accountable.
10. Control physical access to computers and network components.

These best practices are a good starting point for establishing good cyber hygiene. Additional steps beyond these listed would be needed to further harden your security practices. Further information visit the following sites:

Wisconsin Manufacturing Extension Partnership (WMEP) Cybersecurity - https://www.wmep.org/services/cybersecurity/

National Institute of Standards and Technology (NIST) Cybersecurity Framework - https://www.nist.gov/mep/cybersecurity-resources-manufacturers/nist-cybersecurity-framework