Supplier Cyber Security Questionnaire

Supplier name _____

Supplier address _____

_____

Please select the answer from the choices provided to each question below. You have the option to upload additional comments or supporting information.

1. **Unknown Devices**
   Do you automatically identify and/or block unknown devices on your network?
   - ☐ No
   - ☐ Yes, identify
   - ☐ Yes, identify and block

   Notes _____

   Attachments _____

2. **Authorized Software**
   Do you maintain a list of authorized software, and if so, do you restrict users ability to install other software?
   - ☐ No
   - ☐ Yes, maintain a list
   - ☐ Yes, maintain a list and restrict installs

   Notes _____

   Attachments _____

3. **Vulnerability Management**
   Do you maintain a vulnerability management program that scans for known vulnerabilities in your environment, and assigns ownership for resolution?
   - ☐ No
   - ☐ Yes, for work stations
   - ☐ Yes, for servers
   - ☐ Yes, for workstations and servers

   Notes _____

   Attachments _____

OTTO FUCHS KG, Postfach 1261, 58528 Meinerzhagen, Germany
T. +49 2354 73-0, info@otto-fuchs.com

4. **Vendor Security Patches**
What percentage of your workstations and servers run an operating system version for which you still receive security patches from the vendor?

- ☐ Less than 80%
- ☐ 81% - 90%
- ☐ 91% - 95%
- ☐ 96% - 100%

Notes _____

Attachments _____

5. **Patching Frequency**
How frequently do you apply security patches?

- ☐ Once a year or less
- ☐ Twice per year
- ☐ Quarterly
- ☐ Monthly or more

Notes _____

Attachments _____

6. **Password Policy**
Select the option which most closely aligns with enforced password policy.

- ☐ No password policy
- ☐ Length and complexity
- ☐ Length, complexity and expiration
- ☐ Length, complexity, expiration and reuse

Notes _____

Attachments _____

7. **Workstation Access Controls**
How is administrative access to workstations granted?

- ☐ To all users
- ☐ To any user, as needed, permanently
- ☐ To any user, as needed, temporarily
- ☐ To all IT users

Notes _____

Attachments _____

OTTO FUCHS KG, Postfach 1261, 58528 Meinerzhagen, Germany
T. +49 2354 73-0, info@otto-fuchs.com

8. Access Permissions

In general, how is access to systems, applications, or data granted?

- ☐ Access is granted directly by asset owners, or by other users
- ☐ Access is granted directly by IT
- ☐ Access is granted directly by IT, after designated approvals
- ☐ Access is granted directly by a security or access management group, after designated approvals

Notes _____

Attachments _____

9. Web Access / Content Filtering

How is access to the web from company systems controlled?

- ☐ Users have unrestricted access
- ☐ Access is restricted based on site category, restricted to business need
- ☐ Access is restricted to business need, and malicious sites are blocked automatically
- ☐ Access is restricted to a list of known needed/safe sites
- ☐ In general, users do not have access to the web

Notes _____

Attachments _____

10. Backup and Recovery

Select the option which best describes your backup & recovery environment.

- ☐ No backups are present
- ☐ Backups are made when needed; before upgrades, etc.
- ☐ Backups are made regularly
- ☐ Backups are made regularly. Restores are tested to ensure systems can be recovered

Notes _____

Attachments _____

11. Backup Storage

How are backups stored?

- ☐ No backups are present
- ☐ Backups are on network shares, connected to the same network as the devices being backed up
- ☐ Backups are on tape, virtual tape, etc.
- ☐ Backups are on separate disks which stay attached to live systems
- ☐ Backups are on removable media or disks which are otherwise detached from live systems

OTTO FUCHS KG, Postfach 1261, 58528 Meinerzhagen, Germany
T. +49 2354 73-0, info@otto-fuchs.com

Notes _____

Attachments _____

12. Hardware Inventory

Select the option which best describes your inventory of hardware, to include clients, servers, networks, devices, etc.

- ☐ No inventory is kept
- ☐ Inventory is manually kept
- ☐ Inventory is created automatically
- ☐ Inventory is created automatically, and new hosts discovered automatically

Notes _____

Attachments _____

13. Remote Access

Select the option which best describes how remote access works in your organization.

- ☐ There is no remote access
- ☐ Limited to email, calendar, etc.
- ☐ Remote access to network, authenticated with username and password
- ☐ Remote access to network, certificate based multifactor
- ☐ Remote access to network, SMS, token or app based multifactor

Notes _____

Attachments _____

14. Management of Removable Devices

Select the option which best describes your organisations approach to managing removable (USB) devices.

- ☐ Removable devices are allowed without restriction
- ☐ Removable devices are allowed on an exception basis
- ☐ Removable devices must be approved encrypted devices
- ☐ Removable devices must be approved encrypted devices, and may only be used on an exception basis
- ☐ Removable devices are completely forbidden

Notes _____

Attachments _____

15. Network Design

Select the option which best describes your organisations network design.

- ☐ In general, all systems (workstations, servers, machines) can talk to each other. A "flat" network
- ☐ Servers and workstations are isolated, facilities/factory/other systems can

generally interact with many servers and workstations

☐ Servers and workstations are isolated, facilities/factory/other systems are only able to interact with a small set of required systems

☐ Servers, workstations, and other systems are isolated with virtualized networking,
micro segmentation, etc

Notes _____

Attachments _____

16. Wireless Network

Select the option which best describes your organisations wireless network security.

☐ WEP

☐ WPA

☐ WPA2 PSK

☐ WPA2 RADIUS

☐ No WiFi

Notes _____

Attachments _____

17. Security Awareness

Select the option which best describes your organisations security awareness program.

☐ No awareness program

☐ Program trains on 1 of (Identifying social engineering attacks, sensitive data handling, causes of unintentional data exposure, phishing, identifying and reporting incidents)

☐ Program trains on 2 of (Identifying social engineering attacks, sensitive data handling, causes of unintentional data exposure, phishing, identifying and reporting incidents)

☐ Program trains on 3 of (Identifying social engineering attacks, sensitive data handling, causes of unintentional data exposure, phishing, identifying and reporting incidents)

☐ Program trains on all of (Identifying social engineering attacks, sensitive data handling, causes of unintentional data exposure, phishing, identifying and reporting incidents)

Notes _____

Attachments _____

18. Incident Response

Select the option which best describes your organisations security incident response program.

☐ No incident response program

☐ Documented incident response plan

☐ Documented incident response plan and dedicated incident response personnel

☐ Documented incident response plan, dedicated incident response personnel, and periodic drills/test scenarios which exercise the plan

Notes _____

Attachments _____

19. Testing

Select the option which best describes your organisations penetration testing program.

☐ No penetration testing program

☐ A penetration testing program is established

☐ A penetration testing program is established, and regular tests are performed

☐ A penetration testing program is established, regular tests are performed, and issues identified in tests are tracked to resolution

Notes _____

Attachments _____

Prepared by _____

Date _____ Signature _____

CEO/CIO/CISO _____

Date _____ Signature _____