CTPAT Job Aid

Cybersecurity Checklist Sample

Last Updated: October 19, 2021

Cybersecurity Checklist

ABC Company

User access must be restricted based on job description or assigned duties. Authorized access must be reviewed on a regular basis to ensure access to sensitive systems is based on job requirements. Computer and network access must be removed upon employee separation.

A system must be in place to identify unauthorized access of IT systems/data or abuse of policies and procedures including improper access of internal systems or external websites and tampering or altering of business data by employees or contractors. All violators must be subject to appropriate disciplinary actions.

CTPAT Members should use a checklist to ensure proper access is granted and Information Technology (IT) security procedures are followed, and properly conveyed through training and awareness.

Employee: _____ Position: _____

Does the employee have access to the company's IT system? Yes: ☐ No: ☐

Date of Access: _____
Date of Termination: _____

Does the company have comprehensive written cybersecurity policies and/or procedures to protect Information Technology (IT) systems? Yes: ☐ No: ☐

Laptops/Desktops:

Is the user assigned a desktop/laptop? Yes: ☐ No: ☐

If so, has the equipment been verified against the IT inventory? Yes: ☐ No: ☐

Does the equipment have the most current versions/patches of anti-virus and firewall software?
Yes: ☐ No: ☐

CTPAT Job Aid

Cybersecurity Checklist Sample

Last Updated: October 19, 2021

Access Levels:

Is the employee's access restricted based on job description or assigned duties? Yes: ☐ No: ☐

If the access is restricted, what areas can the employee access?

Shipping/Receiving: _____
Accounting: _____
Payroll: _____
Purchasing: _____
Human Resources: _____
Other (Please Indicate): _____

Does the user have access to the internet? Yes: ☐ No: ☐

If so, is access restricted to certain sites? Yes: ☐ No: ☐

Comments: _____

Passwords:

Does the user have an individually assigned account? Yes: ☐ No: ☐

Is a password required to access the company's IT system? Yes: ☐ No: ☐

Is the user required to periodically change the password? Yes: ☐ No: ☐

If so, how often?

30 Days: _____
60 Days: _____
90 Days: _____
Other (Please Indicate): _____

Does the employee use a strong/complex password? Yes: ☐ No: ☐

Does the employee have a multi-factor authentication (MFA) process to access the IT system?
Yes: ☐ No: ☐

If so, what type?

Passphrases: _____
Biometric Technologies: _____
Electronic ID Cards: _____
Other (Please Indicate): _____

Comments: _____

CTPAT Job Aid

Cybersecurity Checklist Sample

Last Updated: October 19, 2021

Training:

Was the employee trained on the company's cybersecurity policies and procedures? Yes: ☐ No: ☐

If so, how often:

Upon Hire: _____
Semi-Annually: _____
Annually: _____
Only on Cause: _____
Other (Please Indicate): _____

Is the employee aware that they may be subject to appropriate disciplinary actions for violating IT security procedures? Yes: ☐ No: ☐

Comments: _____

Reminders:

Individuals with access to Information Technology (IT) systems must use individually assigned accounts.

Access to IT systems must be protected from infiltration via the use of strong passwords, passphrases, or other forms of authentication, and user access to IT systems must be safeguarded.

Passwords and/or passphrases must be changed as soon as possible if there is evidence of compromise or reasonable suspicion of a compromise exists.

As applicable, based on their functions and/or positions, personnel must be trained on the company's cybersecurity policies and procedures. This must include the need for employees to protect passwords/passphrases and computer access.

CTPAT Program

CBP.GOV/CTPAT
1300 Pennsylvania Avenue, NW Washington, DC 20229