CHAMPION PLASTICS, INC

INFORMATION SYSTEMS SECURITY POLICY

CHAMPION PLASTICS, INC.

Table of Contents

Revised: 1/2022

Introduction

Cyber-attacks are very real and present threats for Champion Plastics and the companies that we supply. It is vitally important to the future of our business that we improve our cyber readiness. Our goal is to protect Champion Plastics data, our customers' data, and your personal data from being compromised and used for malicious purposes.

The reality is that simply clicking on a suspicious email link can allow a malicious actor to access our network, thereby accessing our company's data, our customer's data, and your personal data. I am committed to making Champion Plastics more cyber resilient by preventing attacks and being prepared when one does occur.

Regards,

Mike McDermott

Roles and Responsibilities

The overall security and integrity of all computer based systems is the responsibility of the IT Department.

Security and Awareness Training

New and existing employees must go through security and awareness training conducted by the IT Department. This training to be documented on the Champion Plastics Training Matrix.

IT Asset Management

All company owned equipment is to be listed and maintained in the IT Asset Management Spreadsheet.

Onboarding/Offboarding

Champion Plastics will not engage, directly or indirectly, in human trafficking. Champion prohibits human trafficking abuses.

Phishing Scams

Phishing is one of the most widely used cyber-attacks against businesses. Phishing is a form of social engineering, which occurs when a cyber attacker uses human interactions (ex. befriending you on social media, sending you a fake invoice, and requesting bank account information) to obtain or compromise information about our company and computer network systems. Anyone with an email account or smartphone can receive a phishing email or text. It only takes one person responding to a phishing email to put our entire organization at risk. Learning what phishing looks like and following the guidelines in this policy will help us be less vulnerable to a breach from a phishing attack. Our phishing policy applies to all employees and contractors accessing systems, networks, and information, whether from the company or personal devices.

Employee Guidelines:

1) If an email is from an unknown sender, do not provide any personal information or take action by opening an attachment, clicking on a link, or entering information in a pop-up box.
2) If the email is from a known sender, check the identity of the sender before clicking on any attachment in the email. You can check the email of a sender by hovering over the name of the sender when you cannot see the email address to be sure the email address looks correct.
3) If any email contains a link or asks you to enter information, carefully check the identity of the sender before taking action.
4) If you open an email that looks suspicious, look at the full email address of the sender and check the email carefully for errors like grammar or spelling mistakes.
5) If any email doesn't look legitimate, do not open any attachments or follow any directions in the email.
6) Bring any suspicious emails to the attention of your Cyber Leader or IT staff. Take a screenshot of the suspicious email and send it in a new email message to your Cyber Leader or IT for review.
7) When receiving a document from an external source, always open it in read-only protected view.
8) Call the sender to verify information especially if a financial transaction is involved.
9) Pay attention to mobile phishing attempts.

Multi-Factor Authentication

1. Multi-factor authentication (MFA) for all network access. MFA requires users to present more than one piece of evidence (credential) whenever the user logs in to a company account (ex. company email, payroll, human resources, etc.). MFA usually falls into three categories: something the user knows, a password, something the user has (fingerprint), or something the user receives (a code sent to the user's phone).

2. All employees must use at least two different credentials when accessing company network systems. Approved credential types include mobile phones, email and personal questions.

Operating System and Software Updates

Prompt and complete patching of systems is critical to defending against attacks. All employee computers, personal devices connected to the network, and servers must be kept updated and patched against the latest security vulnerabilities to best protect our data, systems, and

networks. If updates are not installed, the door is left wide open to known security vulnerabilities and likely missing out on new features and benefits.

Employee Guidelines:

1) Enable auto-update on all your devices, including personal devices, such as cell phones and tablets that connect to our network. This action includes operating system auto-update (e.g.: Windows, OS X, iOS, Android, etc.). If you have questions on how to enable these features, please contact Jeff Ignatowski
2) Do not ignore the auto-update notifications. Once prompted, install the update within 24 hours. If you are unable to do so, please notify Jeff Ignatowski
3) When selecting software or cloud services, favor vendors that have robust and effective policies and procedures around patching.

Organizational Guidelines:

4) Ensure that patches are installed, or installed for testing, within 72 hours of patch release for servers and infrastructure systems (such as routers).
5) Subscribe to all mailing list/notification systems of existing vendors to ensure you receive notifications of patches.
6) In the case of critical systems or software, test updates/patches before they are deployed.
7) On a quarterly basis, scan and monitor all devices to verify that all appropriate released patches have been installed.

Password Policy

The first line of defense against opportunistic hackers is a hard-to-crack password. Making a strong password takes just a few seconds and is a key part of good cyber hygiene. Every employee should commit to using strong passwords and authentication practices so that the data and work we collectively and individually access each day are best protected against attack. Our password policy applies to all employees and contractors accessing systems, networks, and information, whether from the company or personal devices.

This policy applies to all employees and contractors accessing systems, networks, and information,
whether from company devices or personal devices.

1) Office 365 Password must be changed every 90 Days

2) Use passwords or PINs on all devices, including your personal phone and tablet.
3) Create strong passwords using a passphrase. A passphrase is a string of words or characters without spaces.
4) Never use the same password for business or personal purposes.
5) Passwords must be changed if there has been a cyber incident. Never use or reuse the same password on two (or more) systems at the same time.
6) Never share accounts among multiple people.
7) Always enable multi-factor authentication if it is available for any applications used on company devices and with personal devices used for business.

Anti-malware/Anti-Virus

Champion Plastics' devices shall utilize the latest technology in Anti-Malware/Anti-Virus software. Updates are to be made regularly as available by the provider.

Physical Security

All private offices shall be locked during off-hours and weekends. The IT equipment closet shall remain locked at all times. Front office access shall be restricted during 2nd and 3rd shifts and weekends.

Backup/Cloud Strategy

Champion Plastics will utilize Cloud based services wherever possible. All user's data to be continuously backed up utilizing Carbonate. Additionally, a redundant backup of company servers to be backup utilizing WD Cloud continuously.

Once a year, a physical backup of all data is to be performed with the backup then being stored offsite.

WiFi Accounts/SSIDs

1. The use or personal computers attached to Champion Plastics' Wi-Fi and internal networks is prohibited.

2. Personal phones may be used but only attached to the "CHAMPVISITOR" Wi-Fi

network.

3. SSID password are to be changed yearly by the IT Department

Remote Access/VPNs

Remote Access to Champion Computers is prohibited except were deemed necessary by management. In such cases remote access will provided using a secure VPN only.

User Accounts

User access should be limited to the minimum job requirements for that role.

Business Continuity & Incident/Disaster Recovery Plan

Overview

A comprehensive, step-by-step Incident Response Plan (IRP) equips us to quickly respond, resolve, and learn from every incident. This IRP serves as a roadmap for what to do when responding to a cybersecurity incident, to ensure we have a strategic response rather than a reactive one.

1. Shut Down Computer/Device
2. Isolate device from Network/Internet
3. Evaluate Scope of the incident
4. Diagnose device offline
5. Remediate or replace device

USBs & Removable Media

While USBs and removable media are often used, they are a common carrier of viruses and malware among computers. Making good decisions about how we use (and do not use) USBs and removable media will help us keep our data secure and avoid unnecessary attacks from these devices. It also applies to the use of all types of removable media, including USBs. This policy applies to all employees and contractors accessing systems, networks, and information, whether from the company or a personal device that connects the network.

The use of removable media (e.g. USB external hard drives) which originate outside the premises of Champion Plastics is prohibited. Internal removable media clearly marked as "Champion Plastics" is allowable.

Employee Guidelines:

1) Champion Plastics prohibits the use of USBs and removable media devices by employees, except in rare circumstances and as defined below.

2) Employees must use cloud applications and secure email encryption to share and store all files.

3) Any USBs and removable media devices currently in use must be discontinued immediately and first scanned before transferring the files to the cloud for storage.

Exception Case Guidelines:

4) All USBs and removable media devices (including new ones) must be scanned by Jeff Ignatowski on a computer not connected to the network to verify that no malicious code is present.

5) Only employees who will routinely find themselves in situations where information needs to be shared with a trusted party without access to a secure network can request to be approved to use USBs and removable media devices and must get a pre-scanned device from the IT Department
6) After an employee uses a USB to share information with a trusted party or receives a USB or removable media device from a trusted party, the USB or removable media device must be re-scanned on a computer not connected to the network for malware or malicious code by the IT Department

7) Employees must never accept or use a USB or removable media device received from an unverified party (i.e., at a trade show, given to them by a vendor, picked up in a parking lot,).

E-Mail And Other Equipment Usage

All electronic and telephonic communication systems and all communications and information transmitted by, received from, or stored in these systems, including any software, are the property of Champion Plastics and as such are to be used principally for job-related purposes. Likewise, use of business equipment, facsimiles, computers, telephones and copy machines is intended for business purposes only.

Employees using Champion Plastics equipment for personal purposes do so at their own risk. Further, employees are not permitted to use a code, access a file, copy, download, upload any software or retrieve any stored communication unless authorized to do so or unless they have received prior clearance from management. All pass codes are the property of Champion Plastics. No employee may use a pass code or voice-mail access code that has not been issued to that employee or that is unknown to Champion Plastics. Employees who violate this policy are subject to disciplinary action, up to and including discharge.

Champion Plastics' policy regarding internet, voice mail and e-mail resources is as follows:

1. Transmitting, viewing, retrieving, or storing any communications of a discriminatory or harassing nature, or materials that are considered obscene or X-rated, is strictly prohibited.

2. Accessing pornographic internet sites, displaying/printing any associated materials, pictures and cartoons is strictly prohibited.

3. Harassment of any kind is prohibited. No messages with derogatory or inflammatory remark about an individual=s race, sex, age, disability, religion, national origin, physical attributes or sexual preference shall be transmitted. No abusive, profane or offensive language is to be transmitted through the Firm=s e-mail or internet resources.

4. Personal or private use of Champion Plastics' internet, voice mail and e-mail resources should never interfere with business. This includes game playing and personal communication not associated with Champion Plastics business.

5. Uploading/Downloading of unapproved software, copyrighted materials, trade secrets, proprietary or financial information or similar materials is prohibited without prior written authorization from management.

6. Participating in an inappropriate news group, chat room or accessing an unbusinesslike Web site, could reflect unfavorably on the user=s professionalism and job and should not occur. Carefully consider the possible consequences of such actions.

7. Notwithstanding Champion Plastics' right to retrieve and read any voice or electronic mail messages, such messages should be treated as confidential by other employees and accessed only by the intended recipient. Employees are not authorized to retrieve or read any voice or e-mail messages that are not sent to them unless they receive prior written approval from management.

8. Each employee is responsible for the content of all text, audio or image files that they place or send over Champion Plastics' e-mail/internet system. No e-mail or other electronic communications may be sent which hides the identity of the sender or represents the sender as someone else. All messages communicated on Champion Plastics' e-mail/internet system should contain the employee's name.

9. Communications sent by employees via Champion Plastics' e-mail/internet system and voice mail system must not disclose any confidential or proprietary Champion Plastics or customer information.

10. Champion Plastics may monitor and record and/or listen to all internet, e-mail and voice mail usage, to assure compliance with our policies, for cost analysis/allocation and for legitimate business interests. Thus, Champion Plastics may listen to, access and/or disclose any information in the electronic communication and telephone systems, even that protected by your personal password, at any time, with or without notice to the employee. Employees have no expectation of privacy in connection with the use of these systems, or in the transmission, receipt, or storage of information in such systems.