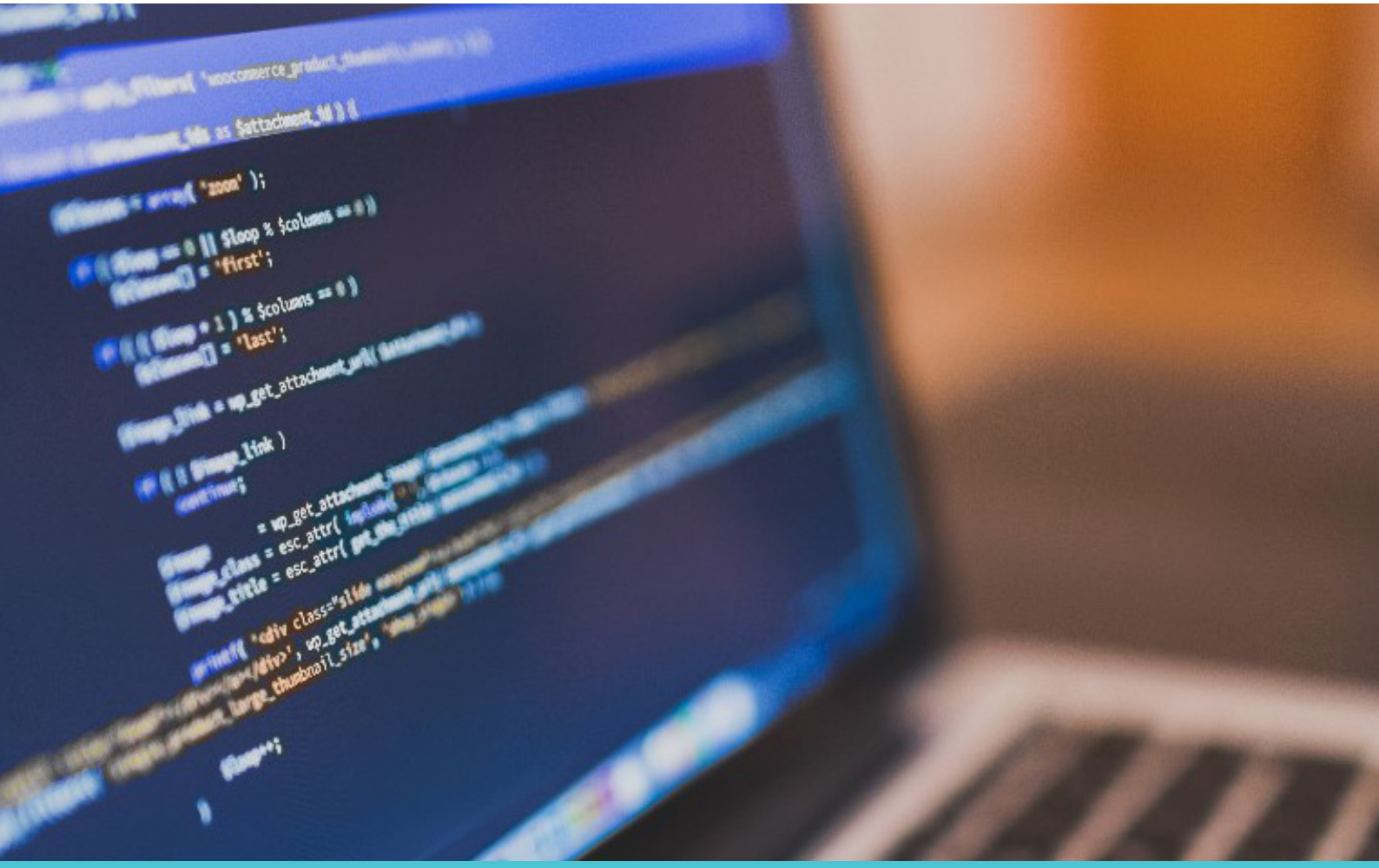
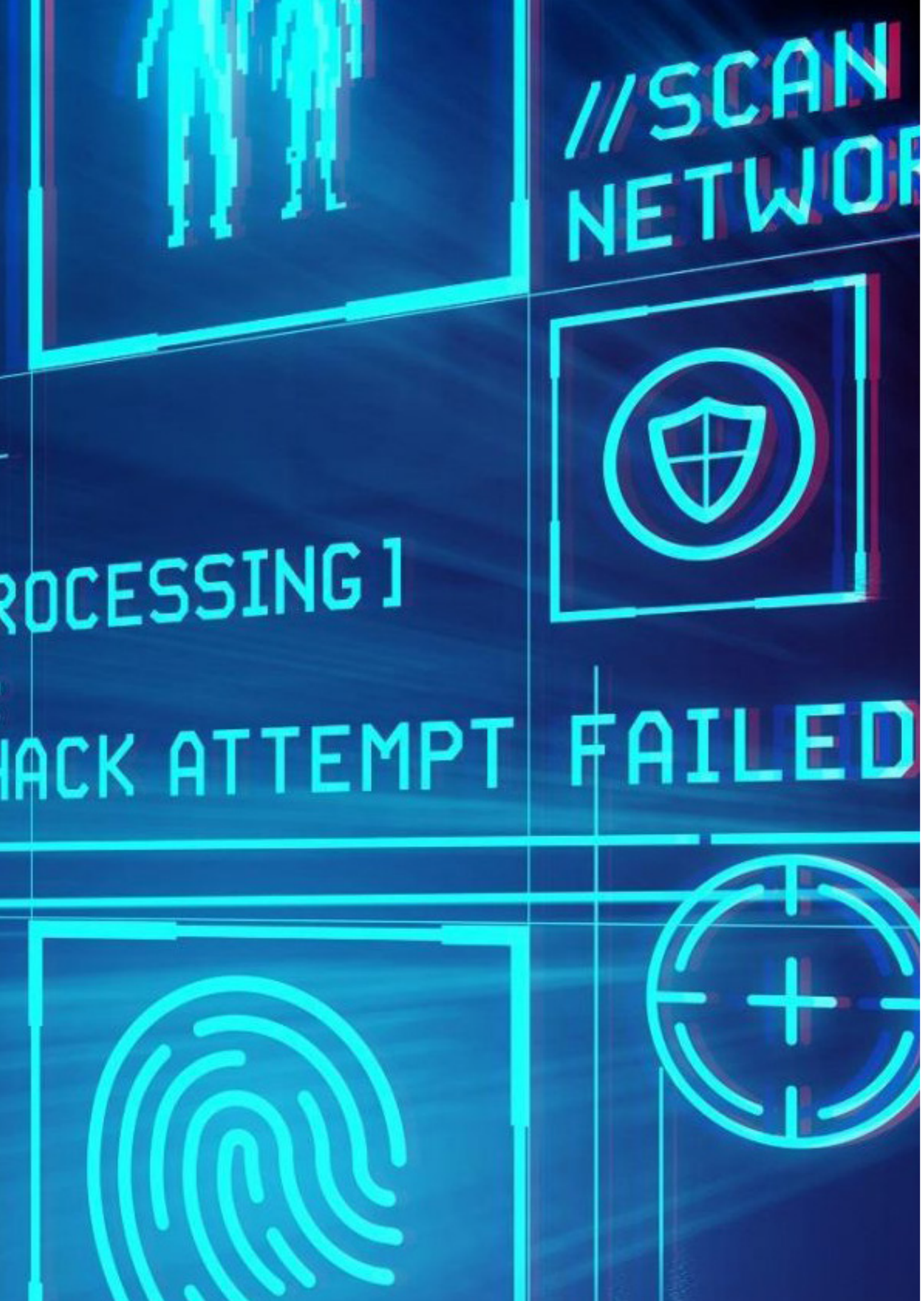


CYBER SECURITY

Information Technology Cyber Security Policy

CONTENT



WITH PURPOSE
TO PROTECT YOU
AND THE COMPANY!

With our growing use of technology to collect, store, & manage information - we become more and more vulnerable to severe security breaches. Errors, hacker attacks and tricks, and system malfunctions could cause significant financial damage and can jeopardize company data.

For this reason, we have implemented a number of security measures and prepared instructions to help mitigate security risks with tips for best use practices for company safety.

Both provisions for preserving the security of our data and technology and our company cyber security policy are outlined in this document.

PARAMETER REMINDERS

TOP SECURITY

As the landscape continues to change in technology and in data sharing, the following policy rules have been initated to increase security protocols:

NO Personal or outside supplied USB drives without approval

One of the easiest ways for hackers to attack and breach company security is through USB drives. Hackers will pose as and mis-represent partner suppliers and companies claiming to send USB drives with information or presentations, but instead has malware intended to attack the company network. If a supplier or vendor provides a USB, this MUST be tested and checked with IT before using. If needed for work use, the company will provide a pre-approved USB drive for work use only.

NO personal online storage unless approved for business

(i.e. - Dropbox, Personal OneDrive); File sharing and cloud storage platforms are great ways to transfer and share data, however use of these MUST be approved by IT to ensure security.

NO personal devices used for company use

Please refrain from using personal devices for work related content, your personal device could unknowingly transfer contaminated data or harmful viruses to the network!

NO social media networks

Please refrain from browsing social media platforms on your company devices.

NO browsing or surfing the internet for personal use

Please be mindful and use the internet to only search for company or work related content or platforms.

NO personal e-mail on company computers

Phishing through E-mail is one of the most common ways hackers attack networks. Opening an email in your personal or company inbox that is suspicious could infect the entire network! Limiting and prohibiting the use of personal email use helps to eliminate security risks.

All Software MUST be approved & installed by IT

Software downloads are another way outside sources often use to spread harmful viruses, always be sure to check with IT before downloading anything to your company device!

NO personal file sharing via Skype

Skype is a great way to share company documents, data, and information - but it does present a security risk if sharing any personal data that is not company approved.

NO cellphones connected to business computers

Plugging in personal devices is one of the easiest ways unknowingly transfer potential viruses and cause harmful data breaches! Always charge your device in the wall socket!

GUIDELINE FOR

PASSWORDS

80% OF HACKING ATTACKS ARE PASSWORD RELATED

Passwords are the EASIEST way for hackers to breech and access personal and company data.

For employees your E-mail and O365 / Office Applications need to ensure a secure password. If you ever think your password was stolen or hacked, contact IT!

For any company-used plaforms & for personal use it is highly recommended to keep the following in mind:

ALWAYS A GOOD IDEA TO ENABLE 2-FACTOR AUTHENTICATION

If an option, ALWAYS enable 2-factor authentication. This adds an additional layer of protection in ensuring that you are the correct user. This is strongly recommended for any critical information and for personal financial related password!

STRONG PASSWORD GUIDELINES

For a Strong Password:

- **Use 16+ Characters**
- **Use capital letters**
- **Use lowercase letters**
- **Use numbers**
- **Use symbols**

UPDATE REGULARLY & NEVER USE THE SAME PASSWORD

For best security, it is recommended to update your password *every 60 days!*

NEVER use the same password twice! Every personal and company accout should have a unique and random password!

Hackers work to steal information through “one-click” that gives access to the entire network.

E-MAIL PHISHING & MALWARE ATTACKS

E-MAIL PHISHING

Emails are the most frequent host to scams and malicious software. Tricks from hackers will appear to come from executive leadership or other familiar sources. To avoid virus infection and data theft we instruct employees to:

- Avoid opening attachements and clicking links when the content is not adequately explained.
- Be suspicious of click-bait titles (ex. offering prizes, advice, lucky winner)
- Check e-mail & names of people that you received the message from to ensure they are legitimate and contain the standard company e-mail signature.
- Look for inconsistencies or give-aways (ex. doesn’t sound like the tone of the person, odd grammer or punctuation)
- ANYTHING that has to do with Microsoft, Email, or account related - ALWAYS contact IT to report and ensure that it is a real request!

If you are not sure if an email is safe, **ALWAYS contact IT support.**

MALWARE ATTACKS

Malware = Software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system or network.

DON’T CLICK ON A LINK OR OPEN AN ATTACHMENT UNLESS YOU KNOW IT’S 100% SAFE!

SECURITY MEASURES

DISCIPLINARY ACTION, TRANSFER OF DATA, & ADDITIONAL TIPS

WE TAKE SECURITY SERIOUSLY

Everyone, from our customers and partners to our employees and contractors, should feel that their data is safe. The only way to gain & keep trust is to proactively protect our systems and databases.

DISCIPLINARY ACTION

We expect all our employees to always follow Top Security Parameters and heed the outlined security guidelines. Those that cause security breaches may face action:

- First-time, unintentional breach: We may issue a verbal warning & train employee on security.
- Intentional, repeated breach: We will invoke more severe disciplinary action. Employees who are observed to disregard security policy will face progressive discipline. Each incident will be examined on case-by-case basis.

ADDITIONAL TIPS

When connecting or working remote out of the office network - ALWAYS use a trusted VPN to ensure your information and data is protected!

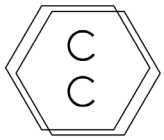
TRANSFER DATA SECURELY

- When working remote outside the office, use a secure VPN to protect your data!
- Avoid transferring sensitive data to other devices or accounts unless absolutely necessary. When data transfer is needed, we request you contact IT.
- ONLY share confidential company information over the company network, NOT over public Wi-Fi or private connection.
- Ensure that the recipients of data are properly authorized people or organizations.
- Report scams, privacy breaches, and hacking attempts!

ADDITIONAL TIPS

- Turn off screens and lock devices when leaving your desk for the day.
- Report stolen or damaged equipment ASAP to IT.
- Change all account passwords at once when a device is stolen or lost.
- Report a perceived threat or possible security weakness in company systems.

REMINDER: If you are ever concerned, unsure, or hesitant about a potential security threat, ALWAYS reach out to IT Support! *If for any reason you are concerned you opened suspicious content - pull the plug on your computer immediately!* **Suspcious activity, emails, or any communication should be reported right away!**



CAMERON CONSULTANTS

INFO@CAMERONCONSULTANTS.COM | LOS ANGELES, CA