Brieser CONSTRUCTION

Section 50
Safety Health and Environmental Manual

2024

Cyber Security

PURPOSE

The purpose of the policy is to describe the physical safeguards applicable for each server, desktop computer system and wireless computer system used to access, transmit, receive and store PII and sensitive company data to ensure that appropriate security is maintained, and that access is restricted to authorized employees. The purpose of the policy is also to assure that systems containing PII and/or sensitive company data are accessed only by those persons or software programs that have been granted appropriate access rights. It is also to develop the response to and reporting of security incidents, including the identification of and response to suspected or known security incidents, the mitigation of the harmful effects of known security incidents, to the extent possible, and the documentation of security incidents and their outcomes.

NETWORK SECURITY

The Company will take reasonable and appropriate steps to prevent unauthorized access to workstations, servers and portable devices including laptops, smartphones, CD-ROMs, DVDs, USB Drives, etc. that store or access PII and sensitive company data. However, it is up to you the employee to be proactive in doing your best to prevent cyber breaches with your assigned equipment.

- Workstations and laptops that are in common areas that store or access PII and/or sensitive company data should be physically placed with the monitor so that it prohibits unauthorized people from viewing confidential information such as logins, passwords, PII and/or sensitive company data.

- Workstations and laptops that are in common areas that store or access PII and sensitive company data should utilize privacy screens to prevent unauthorized access to the data.

- Workstations and laptops that are in common areas that store or access PII and sensitive company data should be secured by restraints such as locking cables.

- To the extent technically feasible all portable devices that contain PII and/or sensitive company data should be encrypted to protect the contents. In addition, encryption should be used when sending any PII and/or sensitive company data across public networks and wireless networks. Public networks include email and Internet access.

- Portable devices and media should be concealed from view when offsite to prevent theft.

NETWORK SECURITY continued

- All network servers, application servers, routers, database systems, device management system hardware, and other servers should be located in a room or an area that can be physically secured by lock and key or any other appropriate security mechanism to limit access to only authorized personnel.

- All workstations, servers and portable devices will run anti-virus / anti-malware software that protect against malicious software. The software must be current and up to date with virus / malware definitions. Employees must use and keep active current versions of approved anti-virus / anti-malware software scanning tools to detect and remove malicious software from workstations and files. Employees must not disable these tools unless specifically directed by computer support personnel to do so to resolve a particular problem.

- A network firewall should be in place to protect PII and/or sensitive company data. The firewall protection should be up to date. Firewalls should be monitored, and alerts should be triggered in the event of unauthorized intrusion or suspected intrusion.

- Log files from network equipment should be stored and retained. Log files from network equipment include firewalls, network servers, desktops, laptops, and other devices. The required length of retention of log files may vary depending on federal, state or industry regulations.

- All workstations, servers, and portable devices, where feasible, must implement a security patch and update procedure to ensure that all relevant security patches and updates are promptly applied based on the severity of the vulnerability corrected.

- Periodic network vulnerability scans should be performed on all internal as well as external (Internet facing servers, websites, etc.) systems. Results of the vulnerability scans should be analyzed and known vulnerabilities should be remediated and/or patched. After all vulnerabilities are remediated, an external network penetration test should be performed to ensure that unauthorized external access into the network is prevented.

NETWORK SECURITY continued

- Reasonable and appropriate steps will be taken to prevent unauthorized access to workstations, servers and portable devices from misuse and physical damage, vandalism, power surges, electrostatic discharge, magnetic fields, water, overheating and other physical threats.

    - Workstations must not be located where they will be directly affected by extremes of temperature or electromagnetic interference. Precautions should also be taken to ensure that workstations cannot be affected by problems caused by utilities, such as water, sewer and/or steam lines that pass through the facility.

    - All facilities that store systems that contain PII and/or sensitive company data, should have appropriate smoke and/or fire detection devices, sprinklers, or other approved fire suppression systems, and working fire extinguishers in easily accessible locations throughout the facility.

    - All servers that contain PII and/or sensitive company data, should be connected to an Uninterrupted Power Supply (UPS) to prevent server crashes during power outages or spikes. Servers should be configured to shut down in a controlled manner if the power outage is for an extended period.

    - All systems should be connected to surge protectors, where feasible, to protect against power spikes and surges.

- A user identification and password authentication mechanism shall be implemented to control user access to the system.

- Employees who suspect any inappropriate or unauthorized use of workstations should immediately report such incident or misuse to the Security Officer.

UNIQUE USER IDENTIFICATION

Employees will be assigned a unique user identification (i.e., user-ID) to access any system or application that transmits, receives or stores PII and/or sensitive company data.

- Each employee must ensure that their assigned user identification is appropriately protected and only used for legitimate access to systems or applications.
- If an employee believes their user identification has been comprised, they must report the security incident.
- Employees should be aware of the following password procedures to create and use strong passwords to protect PII and sensitive company data:
    - Should be a minimum of eight characters in length.
    - Should incorporate both upper- and lower-case letters (e.g., a-z and A-Z)
    - Should incorporate digits and punctuation characters as well as letters e.g., 0-9, (! @ # $ % ^ & * ( ) _ - + = { } [ ] : ; “ ‘ | \ / ? < > , . ~ `)
    - Should not be words found in a Dictionary.
    - Should not include easily guessed information such as personal information, names, pets, birth dates, etc.
- Employees should be aware of the following procedures to protect passwords:
    - Passwords should not be written down.
    - Passwords should not be shared with other employees.
    - If an employee suspects that their password has been compromised, they should report the incident immediately.
- Passwords should be changed at least every 90 days.
- After several failed password attempts, the employee’s account should be disabled (e.g., 3 or 5 failed attempts)

Automatic Logoff

- Systems that access or store PII and/or sensitive company data should implement an automatic logoff after a determined period of inactivity (i.e., 10 minutes of inactivity). Employees would need to login again to regain access and continue the session.

- When leaving a server, workstation, or other computer system unattended, employees must lock or activate the system's automatic logoff mechanism (e.g., CTRL, ALT, DELETE and Lock Computer) or logout of all applications and database systems containing or accessing PII and/or sensitive company data.

Encryption and Decryption

- To the extent technically feasible all portable devices that contain PII and/or sensitive company data should be encrypted to protect the contents. In addition, encryption should be used when sending any PII or sensitive company data across public networks and wireless networks. Public networks include email and Internet access.

- Employees should be trained on the use of encryption to protect PII and sensitive company data.

- All backup tapes and media that contain PII and/or sensitive company data should utilize encryption to protect the data.

- Secure encrypted remote access procedures should be implemented to protect systems that access or store PII and/or sensitive company data.

    - Authentication and encryption mechanisms should be required for all remote access sessions to networks containing PII and/or sensitive company data. Examples of such mechanisms include VPN clients, authenticated SSL web sessions, and encrypted Citrix/RDP client access.

    - Two-factor authentication (i.e., SMS pin notification) should be implemented where technically feasible.

- All wireless access to networks should utilize encryption mechanisms.

    - Employees should not utilize open public Wi-Fi networks.

Email and Phone Scam Safety

Scammers use email or text messages to trick you into giving them your personal and financial information. But there are several ways to protect yourself.

Phishing – The fraudulent practice of *sending emails* or other messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

Smishing – The fraudulent practice of *sending text messages* or other messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

Scammers use email or text messages to try to steal your passwords, account numbers, or Social Security numbers. If they get that information, they could get access to your email, bank, or other accounts. Or they could sell your information to other scammers. Scammers launch thousands of phishing attacks like these every day — and they are often successful. Many times, these messages are embedded with links that if clicked on can automatically download code to your device that will then send the scammers all of your personal or company information. This will open the door for the scammers to manipulate that information to their advantage.

Scammers often update their tactics to keep up with the latest news or trends, but here are some common tactics used in phishing emails or text messages:

Phishing emails and text messages often tell a story to trick you into clicking on a link or opening an attachment. You might get an unexpected email or text message that looks like it is from a company you know or trust, like a bank or a credit card or utility company. Or maybe it is from an online payment website or app. The message could be from a scammer, who for example:

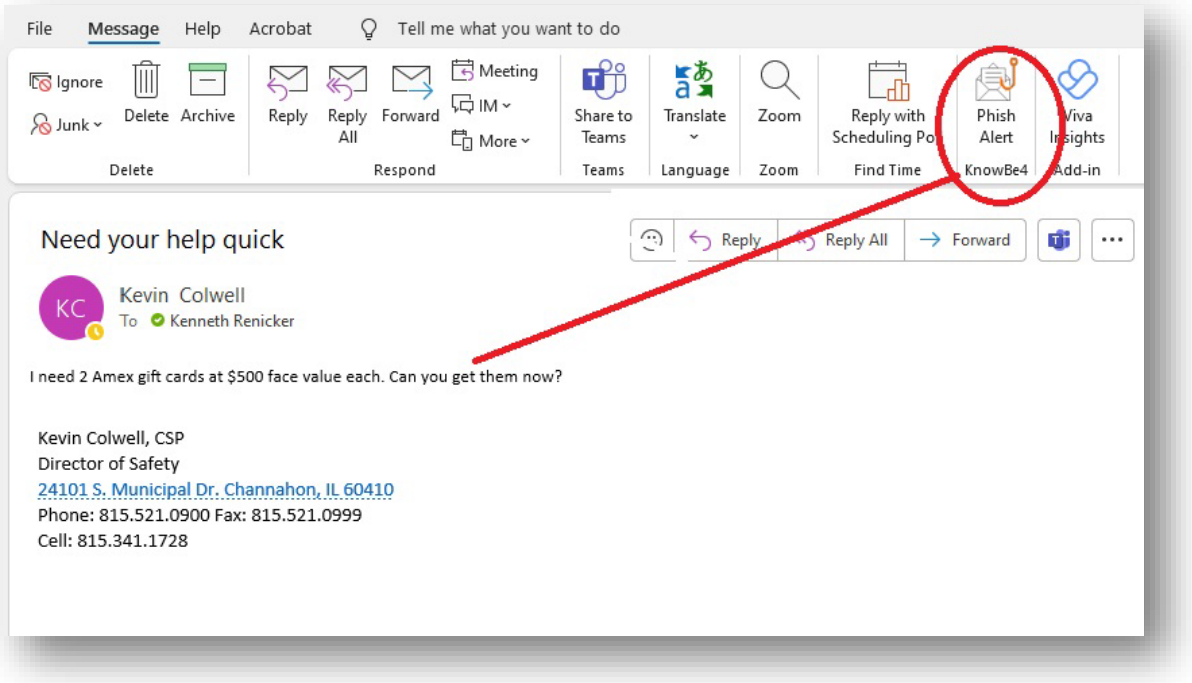
- Say they have noticed some suspicious activity or log-in attempts — they have not!
- Claim there is a problem with your account or your payment information — there is not!
- Say you need to confirm some personal or financial information — you do not!
- Include an invoice you do not recognize — it is fake!
- Want you to click on a link to make a payment — but the link has malware!
- Say you are eligible to register for a government refund — it is a scam!
- Offer a coupon for free stuff — it is not real!
- Disguise themselves as a coworker's email asking for a gift card or the release of company funds— it is a scam.

Email and Phone Scam Safety continued

If any of these types of examples occur or if you just get that feeling it is not right, do not touch anything and alert your supervisor or IT department immediately.

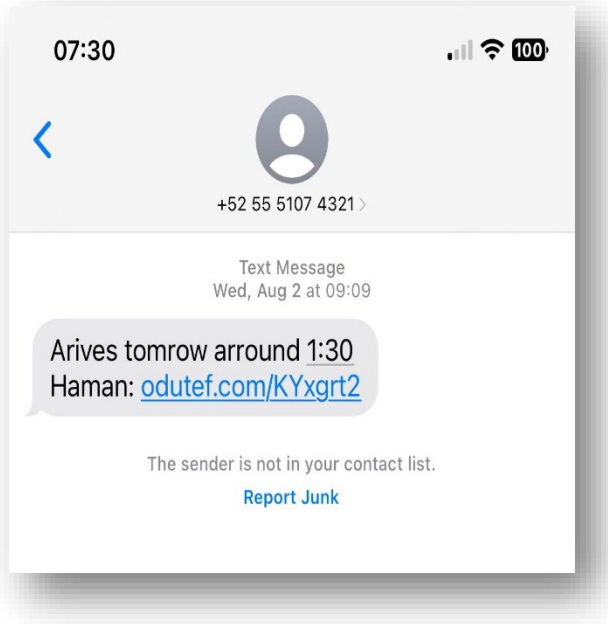
Phishing Example

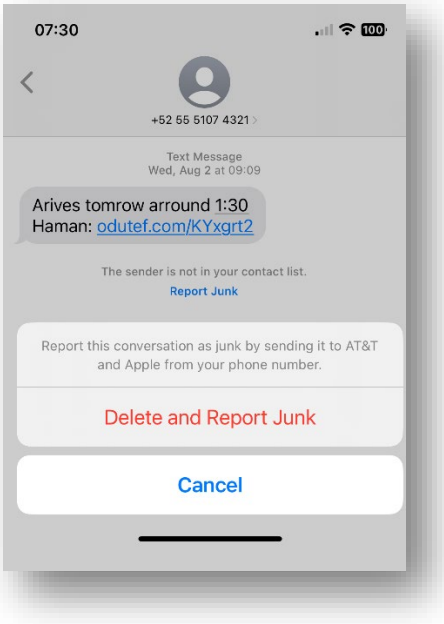
If you received an email that looks to be a scam of some sort you can quickly click the PHISH ALERT button on the far right of the open window. This will send this email to our IT department and automatically block that sender.



Smishing Example

If you received a text that looks to be a scam, or some sort of junk DON'T CLICK THE LINK! Click the *REPORT JUNK* link on the text. You will then click the *Delete and Report Junk* and this will be reported to your phone provider, and it will also block that sender.





If you have any questions or concerns about any email or text, stop and call the person attempting to contact you for verification or call our contracted IT department. EXCAL-TECH at 847-842-9570

REPORTING AND RESPONSE

- The Company will ensure that all incidents, threats, or violations that affect or may affect the privacy, confidentiality, integrity, or availability of PII and sensitive company data will be reported and responded to.

- The Company shall have a Security Incident Response Team (SIRT) charged with the responsibility of identifying, evaluating, and responding to security incidents. The Privacy Security Officer shall oversee the activities of the SIRT.

    - The SIRT will be responsible for investigating all known or suspected privacy and security incidents.

    - The SIRT will document a procedure for all employees to follow to report privacy and security incidents.

    - The Company will ensure that all employees receive training on how to identify and report security incidents.

    - All employees must follow the documented procedure to report security incidents. In addition, employees must report all known or suspected security incidents.

    - All employees must assist the SIRT with any security incident investigations.

Breach Determination

The Security Incident Response Team (SIRT) will investigate all reported and suspected security breaches. The SIRT will refer to federal or state regulations to help with breach determination. Breach determination varies between federal regulations such as HIPAA and GLBA. In addition, breach determination varies significantly between state regulations (for example, what may be considered a breach in one state may not be a breach in another state).

Breach Notification

If the SIRT determines that a breach of unsecured PII has occurred, breach notification of affected individuals may be required. The SIRT will refer to federal or state regulations to help with breach notification requirements. Breach notification requirements varies between federal regulations such as HIPAA and GLBA. In addition, breach notification requirements vary significantly between state regulations (for example, one state may have breach notification requirements that varies significantly from breach notification requirements in another state).

Key elements of a breach notification include:

- **Date of discovery**
  - Usually, a breach will be treated as discovered as of the first day the breach is known or by exercising reasonable diligence would have been known.

- **Timeliness of notification**
  - The Company will provide the required notifications without unreasonable delay after discovery of a breach. The amount of time The Company must notify affected individuals varies between federal and state regulations.

- **Content of notification**
  - If required, a notification will be provided to everyone affected by the discovered breach. The notification should include the following:
    - A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
    - A description of the types of unsecured PII that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number or other types of information were involved).
    - Any steps individuals should take to protect themselves from potential harm resulting from the breach.
    - A brief description of what The Company is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and
    - Contact procedures for individuals to ask questions or learn additional information, which should include a telephone number, an e-mail address, Web site, or postal address.
    - The notification should be written in plain language.

Methods of notification

The following methods are usually used to notify individuals affected by the discovered breach:

- **Written notice**
  - Written notification by first-class mail to the individual at the last known address of the individual or, via e-mail if the individual agrees to e-mail notice. The notification may be provided in one or more mailings as information is available.
  - If the individual is deceased notifications are usually sent to next of kin or personal representative

- **Substitute notice.**
  - If contact information is out of date and written notification cannot be made, a substitute notification may be used.
  - A substitute notification usually in the form of either a conspicuous posting on The Company's home page of its Web site, or conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach reside. The notice should include a contact phone number.

- **Notification to media**
  - In addition to notifying individuals of a known breach, a notification to the media may be required as well.

- **Notification to federal or state regulatory agencies**
  - The Company may need to report breaches of unsecured information to federal or state regulatory agencies.

- **Notification by Third Party Service Providers**
  - Third Party Service Provider responsible for a breach of The Company's PII or sensitive company data should be required to notify The Company within a pre-determined reasonable timeframe. The timeframe should be defined in a Service Provider Agreement.
  - Third Party Service Provider breaches may result in The Company having to notify The Company's affected individuals (such as customers & employee).

Cyber Security Policy Learning Exercise

Score: **%**

Employees Name: **Date:**

Answer each of the following questions by circling the appropriate letter.

1. The purpose of the policy is to describe the physical safeguards applicable for each server, desktop computer and wireless computer system used to access, transmit, receive, and store sensitive company data to ensure that appropriate security is maintained, and that access is restricted to authorized employees.
    a. True
    b. False

2. The Company will take reasonable and appropriate steps to prevent unauthorized access to workstations, servers etc. However, it is up to _____ to be proactive to prevent cyber breaches with your assigned equipment.
    a. Company President
    b. Safety Director
    c. Foreman
    d. You the employee

3. All workstations and portable devices will run anti-virus / anti-malware software. The software must be current and up to date Employees must not disable these tools unless specifically directed by computer support personnel to do so to resolve a particular problem.
    a. True
    b. False

4. Workstations and portable devices must not be located where they will be directly affected by_____.
    a. Time & space.
    b. Facebook and Apple TV.
    c. Emails and Text Messages
    d. Extremes of temperature or electromagnetic interference.

5. (Circle all that apply) Employees should follow the following password procedures:
    a. Should be a minimum of eight characters in length.
    b. Should incorporate both upper- and lower-case letters (e.g., a-z and A-Z)
    c. Should incorporate digits and punctuation characters as well as letters e.g., 0-9, (! @ # $ % ^ & * ( ) _ - + = { } [ ] : ; “ ‘ | \ / ? < > , . ~ `)
    d. Should be written down and saved somewhere easily found.
    e. Should not be shared with other employees.

6. If you receive an email or text message with a link you should always click on it to see what the sender is talking about?
    a. True
    b. False

7. If you believe you are being sent phishing or smishing scams you must alert the IT department immediately by clicking the phish alert button in an email or calling the IT Department phone number.
    a. True
    b. False

Cyber Security Policy Learning Exercise

Answer Sheet

1. The purpose of the policy is to describe the physical safeguards applicable for each server, desktop computer and wireless computer system used to access, transmit, receive, and store sensitive company data to ensure that appropriate security is maintained, and that access is restricted to authorized employees.
   - **a. True**
   - b. False

2. The Company will take reasonable and appropriate steps to prevent unauthorized access to workstations, servers etc. However, it is up to _____ to be proactive to prevent cyber breaches with your assigned equipment.
   - a. Company President
   - b. Safety Director
   - c. Foreman
   - **d. You the employee**

3. All workstations and portable devices will run anti-virus / anti-malware software. The software must be current and up to date Employees must not disable these tools unless specifically directed by computer support personnel to do so to resolve a particular problem.
   - **a. True**
   - b. False

4. Workstations and portable devices must not be located where they will be directly affected by_____.
   - a. Time & space.
   - b. Facebook and Apple TV.
   - c. Emails and Text Messages
   - **d. Extremes of temperature or electromagnetic interference.**

5. (Circle all that apply) Employees should follow the following password procedures:
   - **a. Should be a minimum of eight characters in length.**
   - **b. Should incorporate both upper- and lower-case letters (e.g., a-z and A-Z)**
   - **c. Should incorporate digits and punctuation characters as well as letters e.g., 0-9, (! @ # $ % ^ & * ( ) _ - + = { } [ ] : ; “ ‘ | \ / ? < > , . ~ `)**
   - d. Should be written down and saved somewhere easily found.
   - **e. Should not be shared with other employees.**

6. If you receive an email or text message with a link you should always click on it to see what the sender is talking about?
   - a. True
   - **b. False**

7. If you believe you are being sent phishing or smishing scams you must alert the IT department immediately by clicking the phish alert button in an email or calling the IT Department phone number.
   - **a. True**
   - b. False