

What is Security Awareness?

Security Awareness is the knowledge and attitude employees possess regarding the protection of the District's technology resources and the data stored in the information system.

Our primary focus is to achieve a long term shift in the attitude of our employees towards security. We want to enhance awareness and sense of protectiveness for the districts confidential information.



Sensitive Data

Student Information ...

Vendor Information ...

Employee Information ...

Examples Include:

- Social Security Numbers
- Address and contact information
- Date of Birth
- Identification Numbers

All of this information is considered sensitive data. The loss, misuse, modification or unauthorized access to this information will definitely affect the privacy of the individual.

Be responsive to Sensitive Data ...

Keep It Secure !!!



It's Everyone's Responsibility !!

Security Awareness is everyone's responsibility. Human error, not system weakness, is the leading cause of security incidents.

Our overall goal is to communicate District policies and encourage compliance, enhance awareness of information security, and educate you about information security techniques you can apply not only in the workplace, but for your personal protection as well.

The NEED TO KNOW's ...

1. What is Security Awareness
2. What are we protecting?
 - Sensitive Data
3. Who's Responsible? Everyone !!!
4. How do we protect this information?
 - District Policies & Procedures
 - Confidentiality Agreement
 - Electronic Communication Use Policy
 - Passwords
 - Secret, Multiple, Change, Memorize
 - Email/Internet Use
 - Not private, Beware, Business Only
 - PC Security
 - Lock, Log Off, Shut Down
 - Office Security
 - Secure, destruct, escort, private
5. Incident Reporting
 - Immediately report all incidents !!!



Remember ...
**We're Counting
on YOU !!!**

1. Create good cryptic passwords that can't be easily guessed, and protect your passwords
 - Don't share your passwords or private account information, and avoid writing them down.
 - Characteristics of good, cryptic passwords:
 - At least 8 characters in length.
 - Contain a mixture of upper and lower case letters, numbers, and symbols.
 - Difficult to guess (e.g. don't include real words or personal information like username, names of family members, places, pets, birthdays, address, hobbies, etc.).
 - Easy to remember (so you don't have to write them down).
2. Be cautious when using the internet:
 - Also, just opening a malicious web page can infect your computer. Be aware of where you are going before clicking on a web link.
 - Don't provide sensitive information to internet sites, surveys, or forms unless you are using a trusted, secure web page.
 - Be certain you don't put sensitive information in locations that are accessible from the Internet.
3. Practice Safe Emailing:
 - Never assume that email/attachments are private or confidential.
 - Don't open email attachments or click on links in emails unless you really know what you're opening.
 - Delete suspicious emails. Do not open, forward, or reply to them. Immediately delete the email or move it to your "junk mail" folder to prevent more messages. Once you have deleted the email, make sure to empty your recycling bin.
 - District email is for business use only.
4. Office Security:
 - Secure your area, files, and equipment before leaving it unattended.
 - Lock up sensitive materials.
 - Dispose of data sensitive/confidential document properly.
 - Be aware of visitors. Always escort visitors to their destination or to the security desk if you cannot assist them.
 - Practice proper telephone and email security to ensure non-discussion of confidential or sensitive information in private areas. Never share or discuss confidential data with unauthorized individuals.
5. Practice PC Security:
 - Protect and secure laptop computers and portable devices at all times.
 - Always shut your computer down properly before leaving.
 - Log off of, lock, or put your computer to sleep before leaving it unattended.

