Fort Stockton ISD Cybersecurity Policy

HB 3834

Policy Brief & Purpose

Fort Stockton ISD cybersecurity policy outlines our guidelines and provisions for preserving the data security and technology infrastructure.

The more we rely on technology to collect, store and manage information, the more vulnerable we become too severe security breaches. Human errors, hacker attacks, and system malfunctions could cause great financial damage and may jeopardize Fort Stockton ISD's reputation.

For this reason, we have implemented a number of security measures. We have also prepared instructions that may help mitigate security risks. We have outlined both provisions in this policy.

Scope

This policy applies to all our employees, contractors, volunteers and anyone who has permanent or temporary access to our systems and hardware.

Policy elements

A. **Confidential data**

Confidential data or **PII***, Personally Identifiable Information*, is secret and valuable. Common examples are:

- Unpublished financial information
- Data of customers/partners/vendors
- Patents, formulas or new technologies
- Customer lists (existing and prospective)

All employees are obliged to protect this data. In this policy, we will give our employees instructions on how to avoid security breaches.

B. **Protect personal and district devices**

When employees use their digital devices to access district emails or accounts, they introduce security risk to our data. We advise our employees to keep both their personal and district-issued computer, tablet and cell phone secure. They can do this if they:

- Keep all designated devices password protected.

- Keep antivirus software and OS (patches) up-to-date.
- Ensure they do not leave their devices exposed or unattended.

- Install security & Operating System updates of browsers and systems monthly or as soon as updates are available.

- Log into district accounts and systems through secure and private networks only. Avoid public networks when logging into distinct email or Google File Stream. You are opening up your account to hackers on Public Network.

- We also advise our employees to avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.

- When new hires receive district-issued equipment they will receive instructions for:

- Acceptable Use & Security Workshops
- Device Administrative Password
- Installation of updates

Employees should follow all instructions to protect their assigned devices and refer to FSISD IT Department if they have any questions.

C. **Keep emails safe**

Emails often host scams and malicious software (e.g. worms.) To avoid virus infection or data theft, we instruct employees to:

- Avoid opening attachments and clicking on links when the content is not adequately explained (e.g. "watch this video, it's amazing.")

- Be suspicious of clickbait titles (e.g. offering prizes, advice.)

- Check email and names of people they received a message from to ensure they are legitimate.

- Look for inconsistencies or giveaways' (e.g. grammar mistakes, capital letters, an excessive number of exclamation marks.)

  If an employee isn't sure that an email they received is safe, they can refer to our IT Director.

D. Manage passwords properly

Password leaks are dangerous since they can compromise our entire infrastructure. Not only should passwords be secure so they won't be easily hacked, but they should also remain secret. For this reason, we advise our employees to:

- Don't use words that can be found in any dictionary of any language and use a combination of upper and lowercase letters, numbers, and symbols.

- Don't use passwords that are based on personal information or that can be easily accessed or guessed including birthdays, names of pets, or favorite movies and books that can be found by a quick search on social networking sites.

- Use passphrases like "Thispasswdis4myemail!" to help you remember complex passwords.

- Exchange credentials only when absolutely necessary. When exchanging them in-person isn't possible, employees should prefer the, and only if they personally recognize the person they are talking to.

- Never exchange usernames and passwords in the same digital communication if that is your only option. Break up credentials and send them in separate digital means. For example: send username in email and text message only the password.

- Use different passwords for different accounts and change them regularly.
- Make sure account login pages use encryption including a URL that begins with "https:" instead of "http:". Look for the padlock icon in the browser bar, too. If the padlock icon appears on the webpage, but not in the browser bar, it might just be a graphic that a cybercriminal embedded to trick you into feeling secure.

Remembering a large number of passwords can be daunting. Reparable password management tools such as Dashlane and LastPass can help manage your passwords.

E. Transfer data securely

Transferring data introduces a security risk. Employees must:

- Avoid transferring sensitive data (e.g. student information, employee records) to other devices or accounts unless absolutely necessary. When a mass transfer of such data is needed, we request employees to ask our IT Department for help.

- Share confidential data over the district network/ system and not over public Wi-Fi or private connection.

- Ensure that the recipients of the data are properly authorized people or organizations and have adequate security policies.

- Report scams, privacy breaches, and hacking attempts

Fort Stockton ISD Technology Department needs to know about scams, breaches, and malware so they can better protect our infrastructure. For this reason, we advise our employees to report perceived attacks, suspicious emails or phishing attempts as soon as possible to our specialists. Our IT Department must investigate promptly, resolve the issue and send a districtwide alert when necessary.

Security Specialists are responsible for advising employees on how to detect scam emails. We encourage our employees to reach out to them with any questions or concerns.

F. Additional measures

To reduce the likelihood of security breaches, we also instruct our employees to:

- Lock their devices when leaving their desks.

- Report stolen or damaged equipment as soon as possible to IT Department.

- Change all account passwords at once when a device is stolen.

- Report a perceived threat or possible security weakness in the district-owned systems.

- Refrain from downloading suspicious, unauthorized or illegal software on district equipment.

- Avoid accessing suspicious websites.
- Employees are expected to comply with the FSISD Acceptable Use Policy

FSISD Technology will be responsible for the following:

- Install firewalls, anti-malware software, and access authentication systems.
- Arrange for security training to all employees.
- Inform employees regularly about new scam emails or viruses and ways to combat them.
- Investigate security breaches thoroughly.
- Follow these policies provisions as other employees do.

G. Remote employees

Remote students and employees must follow this policy's instructions too. Since they will be accessing Fort Stockton ISD's accounts and systems from a distance, they are obliged to follow all data encryption, protection standards, and settings, and ensure their private network is secure.

We encourage them to seek advice from our IT Administrators.

H. Disciplinary Action

We expect all our employees to always follow this policy and those who cause security breaches may face disciplinary action:

- First-time, unintentional, small-scale security breach: We may issue a verbal warning and further train the employee on security.
- Intentional, repeated or large-scale breaches (which cause severe financial or other damage): We will invoke more severe disciplinary action up to and including termination and possible criminal charges.
- The District Administration will examine each incident on a case-by-case basis.

Additionally, employees who are observed to disregard our security instructions will face discipline, even if their behavior has not resulted in a security breach.

I. Take security seriously

Everyone, from our students, employees, contractors, and partners to our district, should feel that their data is safe. The only way to gain trust is to proactively protect our systems and databases. We can all contribute to this by being vigilant and keeping cybersecurity top of mind.

References

Homeland Security. (2013, May 8). *Protecting your Personal Information with Secure Passwords*. Retrieved from Homeland Security.