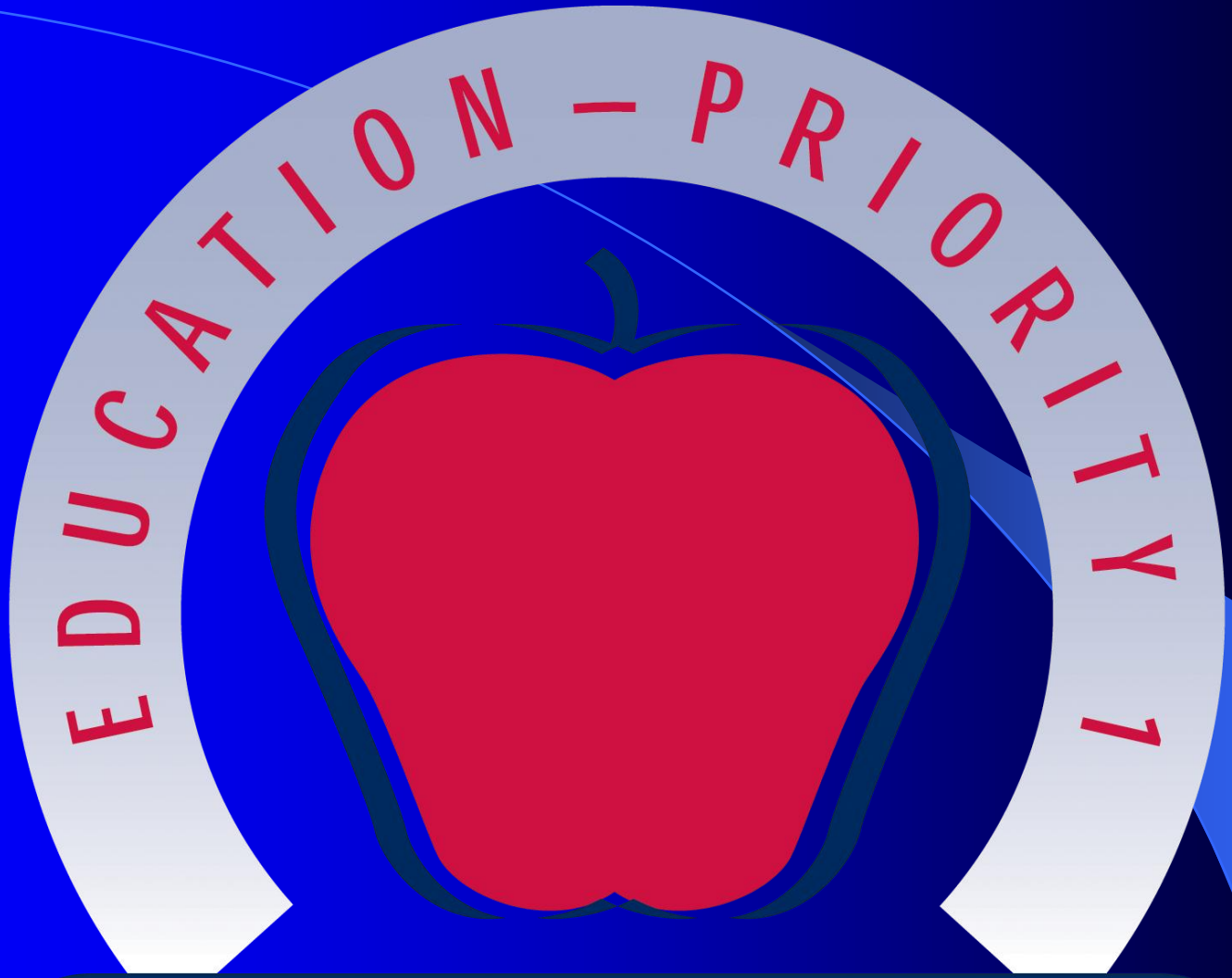

Taylor County School District

MIS Department

Information Technology Security Awareness Training

MIS Department

Introduction

Who am I?

Why are we here?

- Ensure confidentiality of data
- Protect stability of IT infrastructure
- Shield District from legal liability
- Satisfy state audit requirements

Network Acceptable Use Policy

- Signed annually by all employees and students who use district IT

- Not intended to be an exhaustive list of what IT *cannot* be used for

Network Acceptable Use Policy

Acceptable uses:

- "In support of education"

Any other use is a violation of policy

Network Acceptable Use Policy

Unacceptable uses include (but are not limited to:

- Sharing passwords
- Violating student privacy
- Using profane/offensive language
- Violating copyright law
- Personal financial gain or commercial activity
- Activities that do not adhere to the District's mission
- Partisan political activity, religious advocacy, activities on behalf of organizations having no affiliation with District

Network Acceptable Use Policy

Unacceptable uses include (but are not limited to:

- Unauthorized fundraising or similar activities
- Offensive or obscene material such as pornography, hate literature, sexually offensive or other inappropriate information
- Annoying or harassing another person
- Statements which demean a person because of his/her race, sex, sexual orientation, national origin, age, disability, color, or religion
- Any other usage that may create a potential legal liability for the District or compromise it in any way

Network Acceptable Use Policy

Possible consequences of violating policy:

- Revocation of access rights
- Suspension or expulsion
- Disciplinary action
- Criminal charges

Password Protection

Sharing of passwords under <u>any</u> circumstances is a violation of Board policy and a security risk!

- **You are responsible for anything that happens under your username**
- If you need to share what's on your computer with someone else (e.g., a sub), MIS can help
- Even MIS should not know passwords

Password Protection

- Do not write down passwords and store near computers
- Do not select obvious passwords
  - Do not underestimate what's obvious
    - Dog's name
    - Child's name
    - Favorite team
- Consider use of pass*phrase* instead of pass*word*
  - Longer than password, but easier to remember
  - Extremely hard to guess

Password Protection

- Passwords must be changed every 60 days
- Passwords can't be reused within a one-year period
- If you've given your password to someone else or think they've guessed it, change it immediately
- Accounts lock automatically after 5 failed login attempts within a 30-minute period
- Register with myPassword system
  - Can only be accessed from district computers
  - Select 3 secret questions
  - Can use to change password or unlock account

Confidentiality

- Lock computer if stepping away
- Don’t allow anyone to use your computer while logged in as you
- Orient screen so that privacy is maintained
- Do not e-mail confidential data outside of the district network without encryption
- Do not store confidential data on removable media (CDs, flash drives, etc.) without encryption

Protection of IT Assets

- Do not connect any unauthorized equipment to the network
- Do not install any software – Contact MIS
- Do not unplug or move IT equipment – Contact MIS
- If a security problem is identified, do not share – Contact MIS

Activity Logging

- All web traffic is filtered and logged
  - Site administrators and superintendent can request usage reports
  - Could be public record
- All e-mail is archived for ten years
  - Deleting a message from a mailbox does not remove it from the archive
  - Mail cannot be removed from the archive, even by MIS
  - Could be public record

Conclusion

- Adherence to policies and procedures protects students, district, and employees
- Biggest points to come away with:
  - Always protect your password
  - Use IT only for official purposes
  - Remember what is monitored and may be public record