Slide 1

Networking and Health Information Exchange

Unit 9b

Privacy, Confidentiality, and Security Issues and Standards

Slide 2

Access Control

- Who or what is allowed access to a particular resource and what level of access are they allowed
- Terminology
  - Identification
  - Authentication
  - Authorization

Slide 3

Access Control Best Practices

- Separation of duties
  - Require more than 1 person to perform an action
- Least privilege
  - Only give user the access they need

Slide 4

Access Control Models

- Discretionary Access Control (DAC)
- Mandatory Access Control (MAC)
- Role Based Access Control (RBAC)

Slide 5

Access Control Types

- Logical
  - Access to data files, programs and networks
    - Access Control Lists (ACLs)
    - Account Restrictions
    - Passwords
- Physical
  - Access to physical locations
    - Locks
    - Badges
    - Mantraps

Slide 6

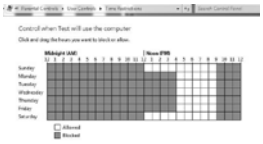
ACLs

An ACL is a list that is associated with file, directory or object that lists who has access to it and what access they have.

Slide 7

Account Restrictions

- Account expiration
- Time of day
- Login location



Slide 8

Passwords

- Combination of letters, numbers and special characters
- Recommend upper and lower case characters
- The more characters the better
- Should be changed frequently

Slide 9

Password Should Never

- Should never be written down
- Should never be a word in a dictionary, words spelled backwards, common misspellings, and abbreviations (English or other languages)
- Should never substitute letters with numbers
- Should never contain personal information
  - Social engineering

Slide 10

One-time Passwords (OTP)

Slide 11

Physical Access Control

- Location
- Doors

Key in knob

Deadbolt

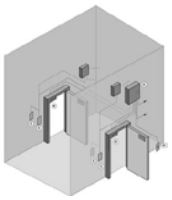
Cipher lock

RFID

Slide 12

Physical Access Continued

- Video surveillance
- Access log
- Mantrap



Slide 13

Biometrics

- Fingerprints
- Faces
- Hands
- Irises/Retinas
- Behavioral
  - Keystroke
  - Voice
- Cognitive

Slide 14

Authentication Practices

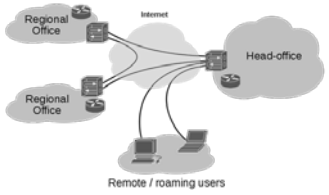
- Layering
- Multi-factor
- Single Sign-On (SSO)

Don't have a Windows Live ID? Sign up

One Windows Live ID gets you into **Hotmail**, **Messenger**, **Xbox LIVE** — and other Microsoft services.

Slide 15

Virtual Private Networks (VPNs)



Slide 16

Security Policies

A collection of policies that lay out specific rules and requirements that must be followed in order to provide a secure environment.

1. **Use computer resources in an acceptable manner.** Durham Technical Community College computing resources must not be used for any purpose which is not consistent with the mission of the college, which is illegal, dishonest, or potentially damaging to the reputation of the college, or which may subject the college to liability. Unacceptable uses of college computing resources include, but are not limited to, the following:
   - Destruction of or damage to equipment, software, or data belonging to Durham Technical Community College or to other individuals or entities;
   - Disclosure or trafficking in confidential or private information, including student information;
   - Disabling or overloading (or attempting to disable or overload) any system or network;
   - Infringement of copyright or trademark laws or rights of others (e.g. downloading or distributing pirated software, video, music, or data);
   - Violation of computer system security, including but not limited to the unauthorized use of computer accounts, access codes, or network identification numbers and email addresses assigned to others;
   - Unauthorized use of Durham Technical Community College's information systems, Intranet, or networked computers;
   - Use of computer communications facilities in ways that unnecessarily impede or disrupt the computing activities of other college users;
   - Intentional downloading or propagating the distribution of computer viruses, trojan horses, timebombs, worms, or other forms of destructive rogue programs;
   - Posting, sending, storing, or intentionally accessing pornographic, obscene, or sexually explicit material or images;
   - Posting personal messages or sending mass electronic messages for such purposes as selling, making solicitations to sell, communicating about partisan political activities, or distributing "junk" email such as chain letters or spam;
   - Academic or intellectual dishonesty;
   - Violation of software license agreements or copyright laws;
   - Recreational use such as peer-to-peer, mug file sharing (e.g. music or video downloads);
   - Violation of network usage policies and regulations;
   - Posting, sending, or intentionally accessing material that is inconsistent with or inappropriate to the mission of the college;
   - Violation of privacy;
   - Harassment;
   - Libel or slander;
   - Fraud or misrepresentation; and
   - Use of Durham Technical Community College's logo without prior approval.