
 Curriculum Development
 Centers Program
Awardee of The Office of the National Coordinator for
 Health Information Technology

Component 9 – Networking and Health Information Exchange

Unit 9-2 Privacy, Confidentiality, and Security Issues and Standards

This material was developed by Duke University, funded by the Department of Health and Human Services, Office of the National Coordinator for Health Information Technology under Award Number H24CC000024.

Unit 9-2 Objectives

- Define access control methods
- Analyze access restrictions to data storage and retrieval (physical and software)

Component 9/Unit 9-2 Health IT Workforce Curriculum
Version 2.0/Spring 2011 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

Component 9/Unit 9-2 Health IT Workforce Curriculum
Version 2.0/Spring 2011 3

Access Control Best Practices

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

Component 9/Unit 9-2

Health IT Workforce Curriculum
Version 2.0/Spring 2011

4

Access Control Models

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

Component 9/Unit 9-2

Health IT Workforce Curriculum
Version 2.0/Spring 2011

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

Component 9/Unit 9-2

Health IT Workforce Curriculum
Version 2.0/Spring 2011

6

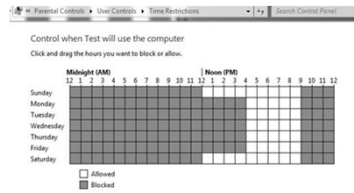
Access Control List (ACL)

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.



Account Restrictions

- Account expiration
- Time of day
- Login location



Passwords

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

Passwords Should Never

- Be default passwords
- Should never be written down
- Should never be a word in a dictionary, words spelled backwards, common misspellings, and abbreviations (English or other languages)

Component 9/Unit 9-2

Health IT Workforce Curriculum
Version 2.0/Spring 2011

10

Passwords Should Never (Continued)

- Substitute letters with numbers
- Be used for more than one account
- Contain personal information
 - Social engineering

Component 9/Unit 9-2

Health IT Workforce Curriculum
Version 2.0/Spring 2011

11

One-time Passwords (OTP)



Component 9/Unit 9-2

Health IT Workforce Curriculum
Version 2.0/Spring 2011

12

Physical Access Control

- Location
- Doors



Key-in-knob



Deadbolt



Cipher lock



RFID

Component 9/Unit 9-2Health IT Workforce Curriculum
Version 2.0/Spring 201113

Physical Access Continued

- Video surveillance
- Access log
- Mantrap

Component 9/Unit 9-2Health IT Workforce Curriculum
Version 2.0/Spring 201114

Biometrics

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

Component 9/Unit 9-2Health IT Workforce Curriculum
Version 2.0/Spring 201115

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.

Component 9/Unit 9-2 Health IT Workforce Curriculum
Version 2.0/Spring 2011 16

Virtual Private Networks (VPNs)

Component 9/Unit 9-2 Health IT Workforce Curriculum
Version 2.0/Spring 2011 17

Security Policies

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

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 legal, defensible, 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:

- Distribution of or damage to equipment, software, or data belonging to Durham Technical Community College or to other individuals or entities;
- Disclosure or unauthorized monitoring of electronic communications and electronically stored information;
- Disabling or overloading or attempting to disable or overload any system or network;
- Misappropriation of copyright or trademark laws or rights of others (e.g., downloading or distributing pirated software, videos, 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 access to Durham Technical Community College's information systems, intranet, or networked computers;
- Use of computer communications facilities in ways that compromise 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 pornography, obscenity, 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 "spam" 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 file sharing (e.g. music or video downloads);
- Violation of network usage policies and legislations;
- Posting, sending, or intentionally accessing material that is inconsistent with or inappropriate to the mission of the college;
- Violation of privacy;
- Harassment;
- Hate or racism;
- Fraud or misrepresentation; and
- Use of Durham Technical Community College's logo without prior approval.

Component 9/Unit 9-2 Health IT Workforce Curriculum
Version 2.0/Spring 2011 18
