

Available Training ^[1]

The Office of Information Security provides awareness and training to departments across the CU system. Check out these training courses and other learning opportunities.

CU: Information Security Awareness

Duration: 30 minutes

Overview: This course provides an overview of information security principles, as they apply to information at the University of Colorado. Upon completion, you will be able to:

- Identify sensitive information that requires special handling
- Recognize and report phishing scams
- Choose strong credentials for logging into your accounts
- Protect information on portable devices
- Recognize signs of an insider threat

The course is updated annually.

Audience: **All CU employees must complete the training within the first 60 days of employment and every two years thereafter.**

Access to the course ^[2]

CU: Information Security for IT Service Providers

Duration: 40 minutes

Overview:

- Provides an overview of security practices and policies for IT services providers.
- Has a target audience that includes employees, students, contractors, and POIs who serve as programmers, server/workstation support, account administrators, webmasters, and others.
- Covers policy, security management, access management, physical and environmental security, and incident detection and reporting.
- Includes a 10-question quiz that learners must pass with 100% to receive credit.
- Requires learners to acknowledge they will uphold confidentiality and agree to access information only as required for authorized tasks.

OIS recommends that departments establish this training as a required course for those within

the targeted audience. (The course is updated annually.)

Audience: An IT Service Provider (ITSP) is any person that designs, builds, implements, supports, or provides an IT service to university departments or individuals. ITSPs include website administrators, workstation support staff, server administrators, software programmers, application developers, data network technicians, user account administrators, computer center personnel, and more.

Access to the course [3]

CU: Controlled Unclassified Information (CUI)

Duration: 40 minutes

Overview: Controlled Unclassified Information (CUI) is unclassified but sensitive information relating to the interests of the U.S. government. Upon completion, you will be able to:

- Identify security risks to CUI
- Prevent improper access to or use of CUI
- Mark CUI according to regulations
- Report incidents that put CUI at risk
- Find resources for additional information on CUI

Audience: As a member of a research team working with CUI, you are responsible for keeping it safe from unauthorized access and release. This course is **required for all who generate or use data that has been designated as CUI**, including:

- Principal Investigators (PIs)
- Faculty, staff, or students
- External contractors

Access to the course [4]

CU: IT Security PCI DSS v3

Duration: 45 minutes

Overview: This course identifies the major changes from version 2 to version 3 of the Payment Card Industry Data Security Standard (PCI DSS). Four important guidelines are covered:

- Version 3 changes to the PCI Data Security Standard
- Building a security-minded culture
- Scoping the cardholder data environment
- Completing a Self-Assessment Questionnaire

Audience: The target audience is current Campus Merchants and their IT staff; general PCI system users such as: accountants, ticket sellers, and cashiers who work with PCI security compliance.

Access to the course [5]

CU: HIPAA Regulations - CU System

Duration: 30 minutes

Overview: This course covers the basics of HIPAA privacy and security for CU System Administration.

Audience: All CU System Administration employees who use HIPAA-protected information are **required** to take this course.

Access to the course [6]

CU: Accessibility for Digital Communicators

Duration: 45 minutes

Overview: This course is for anyone who is responsible for creating or managing digital communications for the University. It provides information and techniques to address Information and Communication Technology (ICT) and accessibility compliance with the American Disabilities Act (ADA) as it applies to digital communications.

Audience: The target audience is all Digital Communicators at CU campuses.

Access to the course [7]

In-Person and Customized Learning

The Office of Information Security provides in-person and customized learning experiences for your team or department, such as communications, presentations, and simulated phishing exercises. This service is available to any department within CU, regardless of campus. Please contact OIS at security@cu.edu [8] to learn more.

LinkedIn Learning

- **Cybersecurity at Work** by Carolina Wong, released February 2020, total time is 55 minutes
- **Security Tips** by Scott Simpson, updated September 2019, total time 3 hours 43 minutes

Groups audience:

Office of Information Security

Source URL: <https://www.cu.edu/security/awareness/available-training>

Links

[1] <https://www.cu.edu/security/awareness/available-training>

[2]

<https://universityofcolorado.skillport.com/skillportfe/custom/login/saml/login.action?courseaction=summary&ass>

[3]

<https://universityofcolorado.skillport.com/skillportfe/custom/login/saml/login.action?courseaction=summary&ass>
[4]
<https://universityofcolorado.skillport.com/skillportfe/custom/login/saml/login.action?courseaction=summary&ass>
[5]
<https://universityofcolorado.skillport.com/skillportfe/custom/login/saml/login.action?courseaction=summary&ass>
[6]
<https://universityofcolorado.skillport.com/skillportfe/custom/login/saml/login.action?courseaction=summary&ass>
[7]
<https://universityofcolorado.skillport.com/skillportfe/custom/login/saml/login.action?courseaction=summary&ass>
[8] <mailto:security@cu.edu>