Cyber Security Training and Awareness Policy

Responsible Office	Information Technology Services
Responsible Party	Vice President for Information Technology Services / CIO
Last Revision	January 2024
Approved by	The Cabinet
Approval Date	
Effective Date	
Last Review	

Scope

All financial and administrative policies involving community members across campus, including volunteers, are within the scope of this policy. If there is a variance between departmental expectations and the common approach described through college policy, the college will look to the campus community, including volunteers, to support the spirit and the objectives of college policy. Unless specifically mentioned in a college policy, the college's Board of Trustees are governed by their Bylaws.

This policy applies to all CC employees, volunteers and contractors with access to CC systems, networks, CC information, nonpublic personal information, personally identifiable information, or client data.

All in-scope persons will collectively be referred to as employees for this policy.

Policy

- New employees must complete an assigned awareness training program within 30 days of hire.
- All employees must complete an assigned awareness training program annually. CC will test the efficacy of the security awareness training program through periodic social engineering exercises.
- Specialized Training: some departments, like HR, Finance, Leadership, Security Management, and IT, may have unique security needs. You might need additional training if you're in one of these teams. The Administration will specify these needs, and the training should be completed in the same timeline as the general Security Awareness Training.

- Supplemental training may be required in certain situations:
  - Security breaches that are tied to an individual's CC account.
  - Failure of a simulated security challenge as defined by taking one or more of the following activities on a simulated phishing test:

- Clicking on the link in the phishing test
- Opening an attachment from the phishing
- Replying to a phishing test email
- Entering data on a phishing email landing page
- Transmitting any information as part of a vishing (Phone Phishing) test

- A significant shift in job responsibilities which demands heightened security knowledge.

Procedures

Consequences for failing to complete training.

- If an employee misses the security training deadline, ITS will ask the employee’s direct supervisor/Student Conduct Office to enforce that person taking the training and will provide a 2-week extension of the deadline before account suspension is initiated.
    - If the end-user does not complete the training within the 2-week extension, the supervisor will submit an ITS service ticket to suspend the end-user’s account.
    - If the supervisor fails to submit the service ticket, ITS will still suspend the end-user’s account and notify the supervisor.
- To restore access, end-users must contact the ITS Solutions Center and explain they need access to complete the training.
- Once access is re-established, there is a 48-hour window to complete the training. Failure to do so will lead to another suspension.
    - Subsequent reactivation requires approval from HR/Student Conduct Office or the immediate supervisor.

Security Testing Through Simulated Exercises

From time to time, we'll simulate potential threats. These could be deceptive emails (phishing), misleading phone calls (vishing), or on-site assessments. Consider it a "practice drill" to see how well we can spot the fakes.

- **Timing of Tests**: The exact timing remains unpredictable. Like real-world security threats pop up when we least expect them, our tests will too. It keeps us on our toes!
- **Subjects of Testing**: While everyone will get tested, sometimes we zoom in on specific departments or folks, especially if we've noticed a specific risk.
- **Purpose**: After our "drills," we look at how we did. Any hiccups? We'll provide more training. It's all about ensuring everyone knows how to dodge those real-life curveballs.

Inadequate Performance in Security Exercises

- Any failure will mandate additional training or coaching
- Repeated inadequacies will lead to supervisor notification and intensified coaching measures

- Accruing three consecutive "Pass" evaluations will initiate a de-escalation in coaching intensity

What Counts as a "Failure"?

Generally, interacting with an actual phishing message in any way damages CC (other than opening it, which is unavoidable in many cases). We need you to be able to tell a phishing message from a legitimate one, so our tests are based on real phishing messages that have been turned into tests. Accordingly, a failure on our test is any of the following circumstances.

- Not finishing required training on time
- Not passing a security test (those fake “drill” emails or calls)
- Examples of failing a security test:
    - Clicking on a link in a test email.
    - Responding with any details to that email.
    - Opening a fake attachment.
    - Turning on macros in a test attachment.
    - Filling in details on a fake webpage from the test.
    - Sharing any information during a fake phone call (vishing).
- Even if there are many missteps in one test, we'll only count it as one "failure."

Sometimes, we might decide that a recorded "failure" was a mistake. If that happens, it won't count against you.

The following table outlines the penalty for failures. The CC ITS team may take steps not listed here to reduce an individual's risk to Colorado College.

Failure Count	**Resulting Level of Remediation Action**
First Failure	Mandatory completion of supplemental training to be assigned based on the employee role, policy violation, or at the reasonable discretion of the policy owner.
Second Failure	Supervisor notified. Employee attends secondary remedial training.
Third Failure	Employee AND supervisor attend in-person training and security counseling with CC ITS. HR begins Corrective action for policy violation.
Fourth Failure	Face-to-face meeting with employee, supervisor, CIO, and Director of HR. Additional training/technical controls at the discretion of the Administration. HR progresses corrective action for policy.
Fifth and Subsequent Failures	Formal disciplinary action initiated by HR, including but not limited to suspension and/or termination.

Erasing Previous Failures

The overarching objective of this policy is to educate, not punish. Recognizing that errors can be transformative learning opportunities, there are provisions for employees to rectify past missteps:

- Achieve three consecutive "Pass" evaluations in our security tests.
- Proactively report a simulated or genuine phishing attempt that could jeopardize college security.
- Complete a specified training module to the satisfaction of either the COO or CIO.

What counts as a "Pass"

At CC, when our team members take the right steps, it's noted as a "Pass." Here's what you can do to earn one:

- **Training**: Finish the security awareness training within the time given.
- **Spotting Fake Attacks**: If you identify a phishing email, report it by forwarding it to its@coloradocollege.edu with the phrase “scam report”
- **Avoiding Mistakes:** Not slipping up during a security test (like not falling for our test emails) counts as a Pass.

Evaluating Employee Risk Profiles

This section outlines various scenarios that might increase the risk profile of a CC employee. Those with a high risk profile may be subjected to more advanced social engineering tests and might receive more frequent or specialized training and testing.

- The employee's email appears in a recent Email Exposure Check report.
- The employee holds an executive or VP role, making them a high-value target.
- The employee has access to substantial CC confidential data.
- The employee utilizes their personal mobile phone for work tasks.
- The employee can access considerable Protected Health Information (PHI).
- Publicly available personal information about the employee is accessible on the Internet.
- The employee has previously fallen prey to information security breaches.
- The employee has had repeated violations of CC policies.

Responsibilities and Accountabilities

A structured approach to information security is critical for the organization. Here's a breakdown of the roles and responsibilities associated with this policy:

Chief Information Officer (CIO):

- Holds accountability for orchestrating an effective security awareness and training program.
- Ensures all employees are informed and equipped to safeguard both the organization's and our community members' digital assets.

Information Technology Services (ITS):

- Crafting and sustaining an extensive collection of information security guidelines, which encompasses this policy.
- Collaborates with other departments to facilitate proper awareness and training sessions. These sessions are aimed at enlightening staff about their duties, as outlined in various policies, regulations, contracts, and more.

Managers:

- Ensure teams under their purview actively participate in security training and awareness initiatives.
- Ensure that all employees under their charge are up-to-date with their required training.

All employees, contractors and volunteers:

- Personally responsible for completing all mandated security awareness training modules.