# CYBR C094N: WORKPLACE DATA PROTECTION AND INCIDENT AWARENESS

| Item | Value |
|---|---|
| Eff Term | Fall 2026 |
| Curriculum Committee Approval Date | 12/05/2025 |
| Top Code | 070800 - Computer Infrastructure and Support (CTE) |
| Units | 0 Total Units (Lecture Units 0) |
| Hours | 27 Total Hours (Lecture Hours 27) |
| Total Outside of Class Hours | 0 |
| Total Student Learning Hours | 27 |
| Course Credit Status | Noncredit (N) |
| Material Fee | No |
| Basic Skills | Not Basic Skills (N) |
| Repeatable | Yes; Repeat Limit 99 |
| Open Entry/Open Exit | No |
| Grading Policy | P/NP/SP Non-Credit (D),<br>• Letter Non-Credit (L) |

## Course Description

This course introduces essential practices for protecting organizational data and responding to common security incidents. Students learn how to recognize suspicious activity, follow reporting procedures, maintain device and network security, and understand the basics of privacy regulations. This course will emphasize building awareness, accountability, and communication within professional security culture. Transfer Credit: Not Transferable.

## Course Level Student Learning Outcome(s)

1. Identify potential security incidents and follow basic reporting procedures.
2. Apply data protection practices that comply with organizational and privacy requirements.
3. Describe how employee actions contribute to cybersecurity culture and risk reduction.

## Course Objectives

- 1. Identify types of data and their protection requirements (public, confidential, restricted).
- 2. Recognize signs of malware, unauthorized access, or data misuse.
- 3. Demonstrate how to secure devices, removable media, and shared drives.
- 4. Explain incident reporting steps and escalation protocols.
- 5. Discuss the role of employees in maintaining cybersecurity culture.
- 6. Summarize basic privacy and compliance concepts (e.g., HIPAA, FERPA, GDPR awareness).

## Lecture Content

- Understanding Workplace Data and Risk
- Device Security and Safe Network Use
- Malware and Ransomware Awareness
- Recognizing and Reporting Security Incidents
- Data Classification and Handling Procedures
- Privacy and Compliance Basics
- Safe Use of Portable Media and Devices
- Security Policies and Employee Responsibility
- Building a Security-Minded Workplace Culture
- Continuous Learning and Awareness Resources

## Method(s) of Instruction

- Enhanced NC Lect (NC1)
- Live Online Enhanced NC Lect (NC9)
- Online Enhanced NC Lect (NC5)

## Instructional Techniques

This course will utilize a combination of lecture, hands-on lab assignments, system simulators, classroom discussion with student interactions, problem-solving techniques, quizzes, exams, and troubleshooting assignments to achieve the goals and objectives of this course. All instructional methods are consistent across all modalities.

## Reading Assignments

Read open educational resource materials, journal articles and corporate reports, news articles, and interactive career websites.

## Writing Assignments

Students prepare brief reflections or scenario responses explaining how employee actions influence data protection and incident reporting.

## Out-of-class Assignments

Students review sample workplace policies, classify example data types, or practice recognizing suspicious activity in simulated everyday situations.

## Methods of Student Evaluation

- Short Quizzes
- Written Assignments
- Projects (Individual/Group)
- Problem Solving Exercises
- Skills Demonstration

## Demonstration of Critical Thinking

Students demonstrate critical thinking by interpreting indicators of potential security incidents and deciding when and how to escalate concerns according to policy.

## Required Writing, Problem Solving, Skills Demonstration

Students prepare short written responses to workplace data-protection cases, solve incident-recognition and reporting challenges, and demonstrate skills such as applying data-handling rules and identifying risky behaviors.

## Resources Subscreen

- **Open Education Resource:** Raisinghani, M.. *Foundations of Information Systems*. (2025).

- **Open Education Resource:** Tolboom, R.. *Computer Systems Security: Planning for Success*. (2022).

## Eligible Discipline(s)

- Computer information systems (computer network installation, microcomputer technology, computer applications): Any bachelor's degree and two years of professional experience, or any associate degree and six years of professional experience.
- Computer service technology: Any bachelor's degree and two years of professional experience, or any associate degree and six years of professional experience.
- Computer science: Master's degree in computer science or computer engineering OR bachelor's degree in either of the above AND master's degree in mathematics, cybernetics, business administration, accounting or engineering OR bachelor's degree in engineering AND master's degree in cybernetics, engineering mathematics, or business administration OR bachelor's degree in mathematics AND master's degree in cybernetics, engineering mathematics, or business administration OR bachelor's degree in any of the above AND a master's degree in information science, computer information systems, or information systems OR the equivalent. Note: Courses in the use of computer programs for application to a particular discipline may be classified, for the minimum qualification purposes, under the discipline of the application. Master's degree required.