

CYBR C093N: SECURE COMMUNICATION AND CLOUD SAFETY

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), • Letter Non-Credit (L)

Course Description

Students will learn secure communication and collaboration practices using email, messaging, and cloud-based tools. Topics include multifactor authentication, password managers, secure file-sharing, phishing awareness, and safe use of cloud storage. This course will emphasize privacy protection, data classification, and responsible information handling in team environments. Transfer Credit: Not Transferable.

Course Level Student Learning Outcome(s)

1. Apply secure authentication and password management tools in professional contexts.
2. Demonstrate safe communication and file-sharing practices using cloud and collaboration tools.
3. Identify risks related to phishing and data exposure in cloud environments.

Course Objectives

- 1. Explain the role of authentication and password management in workplace security.
- 2. Configure multi-factor authentication and use a password manager effectively.
- 3. Safely store, share, and back up files using cloud services.
- 4. Identify phishing and social-engineering tactics targeting cloud users.
- 5. Apply privacy and data-handling best practices in shared digital environments.
- 6. Evaluate the security features of common workplace collaboration tools.

Lecture Content

- Introduction to Workplace Cyber Hygiene
- Authentication and Password Managers
- Multifactor Authentication (MFA)
- Cloud Storage and File-Sharing Security
- Email and Messaging Threats
- Phishing and Social Engineering in the Workplace
- Data Classification and Privacy Settings
- Secure Collaboration Tools (Teams, Google Workspace, etc.)
- Backups and Recovery in Cloud Systems
- Everyday Habits for Secure Communication

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 compose short analyses describing how secure communication tools, MFA, or cloud-sharing settings prevent workplace data exposure.

Out-of-class Assignments

Students practice configuring password managers or MFA on personal accounts, explore cloud-sharing tools, and evaluate potential risks in real-world collaboration platforms.

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 assessing cloud-based communication or file-sharing situations to identify risks and select appropriate secure-handling strategies.

Required Writing, Problem Solving, Skills Demonstration

Students write concise analyses of secure-communication practices, apply problem-solving to workplace cloud-safety situations, and demonstrate skills such as enabling MFA and managing cloud-sharing settings.

Resources Subscreen

- **Open Education Resource:** Charles Sturt University Library. *Digital skills: Professional identity and skills.* (2024).

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

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.