CYBR-2100 Cyber Ethics & Cyber Law

Week 1 – Ethics, Law & Professional Responsibility

Welcome to Week 1.

You already know that cybersecurity professionals need technical skills. This course focuses on another part of the profession: deciding when, why, and under what authority those technical capabilities should be used.

Throughout this course, you will work with realistic cybersecurity situations involving ethics, law, privacy, organizational policy, governance, professional responsibility, and artificial intelligence.

This is not a course built around memorizing legal terminology. You will be expected to analyze situations, question assumptions, evaluate evidence, use emerging technologies, and defend professional decisions.

This Week's Big Question

Just because we can, should we—and who gets to decide?

Cybersecurity professionals may have access to networks, logs, accounts, communications, vulnerability information, security tools, administrative privileges, cloud systems, and increasingly powerful AI-enabled security technologies.

Having the technical ability to perform an action does not automatically mean you are:

- authorized to perform it;
- legally permitted to perform it;
- permitted by organizational policy to perform it;
- ethically justified in performing it.

This week, you will begin learning how to tell the difference.

What You Will Learn

By the end of Week 1, you should be able to:

- Distinguish legal requirements, regulations, organizational policies, professional ethics, and personal morality.
- Explain why technical access does not automatically establish authorization.
- Apply multiple ethical frameworks to cybersecurity situations.
- Identify stakeholders, competing interests, risks, and potential harms.
- Apply professional ethical principles to cybersecurity decisions.
- Identify missing information before making a professional decision.

- Identify missing information before making a professional decision.
- Examine ethical concerns created by AI-enabled cybersecurity technologies.
- Use AI to assist professional reasoning while independently evaluating its output.
- Develop and defend a professional cybersecurity recommendation.

Five Ideas You Need This Week

1. Law

Laws establish requirements that may be enforced through governmental authority.

Cybersecurity professionals may encounter laws involving issues such as:

- unauthorized computer access;
- privacy;
- data protection;
- intellectual property;
- cybercrime;
- electronic communications;
- breach response.

You are not expected to become an attorney.

You are expected to recognize when a cybersecurity decision raises a legal question that requires authoritative research or appropriate legal guidance.

2. Regulation

Regulations establish requirements under governmental or regulatory authority.

Which regulations apply depends on factors such as:

- industry;
- jurisdiction;
- type of organization;
- type of information;
- affected individuals;
- services being provided.

A regulation that applies to one organization may not apply to another.

3. Organizational Policy

Organizations establish their own internal requirements.

Examples include:

- acceptable-use policies;
- access-control policies;
- incident response procedures

- incident-response procedures;
- data-classification policies;
- employee-monitoring policies;
- privacy policies;
- AI acceptable-use policies;
- generative AI policies.

Something can violate organizational policy without necessarily violating criminal law.

4. Professional Ethics

Professional ethics addresses how professionals are expected to behave when exercising specialized knowledge, access, authority, or influence.

Cybersecurity professionals routinely make decisions that affect other people.

Professional responsibilities may include:

- avoiding harm;
- protecting privacy;
- maintaining confidentiality;
- acting honestly;
- maintaining competence;
- respecting authorization;
- protecting the public.

This week you will use the ACM Code of Ethics and Professional Conduct.

https://www.acm.org/code-of-ethics (https://www.acm.org/code-of-ethics)

5. Personal Morality

Personal morality concerns your individual beliefs about right and wrong.

Those beliefs may influence your thinking, but professional cybersecurity decisions cannot rely only on personal opinion.

You need to be able to explain why a decision is professionally defensible.

Two Distinctions to Remember

LEGAL ≠ ETHICAL ≠ AUTHORIZED ≠ GOOD POLICY

AI RECOMMENDED ≠ VERIFIED ≠ AUTHORIZED ≠ CORRECT

You will return to both ideas throughout the course.

Ethical Frameworks

Ethical frameworks provide different ways of examining difficult decisions.

You are not expected to memorize philosophy textbooks. You are expected to use these frameworks to analyze cybersecurity situations.

Consequentialism / Utilitarian Reasoning

Ask:

Which option is likely to produce the greatest overall benefit while minimizing harm?

Cybersecurity example:

An organization introduces aggressive monitoring that could detect attacks more quickly but also significantly increases surveillance of employees.

What are the benefits?

Who might be harmed?

Duty-Based Ethics / Deontology

Ask:

What duties, rules, or obligations must be respected even when breaking them could produce a desirable result?

Examples might include duties involving:

- confidentiality;
- authorization;
- honesty;
- professional responsibility.

Rights Approach

Ask:

Whose rights are involved?

Consider issues such as:

- privacy;
- autonomy;
- property;
- confidentiality;
- due process;
- informed consent.

Justice / Fairness

Ask:

Who receives the benefits, and who carries the risks or burdens?

This becomes particularly important when automated systems classify, rank, monitor, flag, or restrict people.

Virtue Ethics

Ask:

What would an honest, competent, responsible, and trustworthy cybersecurity professional do?

This shifts the question from simply following rules to considering what professional character requires.

AI Is Part of Cybersecurity Practice

Artificial intelligence will not be treated as a separate topic that appears once during this course.

AI is already changing cybersecurity practice, organizational decision-making, privacy, governance, intellectual property, monitoring, risk management, and professional responsibility.

You will therefore use and evaluate AI throughout CYBR-2100 where it applies to the material.

That includes actually working with AI tools, not simply discussing them.

During Week 1, you will use ChatGPT Edu to assist with ethical analysis and then evaluate the quality of its reasoning.

You may discover that AI:

- identifies something your team missed;
- makes an unsupported assumption;
- overlooks a stakeholder;
- oversimplifies an ethical conflict;
- produces an incorrect or questionable legal claim;
- generates a convincing answer that still requires verification.

Your job is not simply to ask what the AI said.

Your job is to determine whether you should trust it and how you know.

Class Meeting 1
Technical Capability, Authorization & Ethical Judgment

During the first class meeting, you will:

- examine a cybersecurity investigation scenario;

- distinguish law, regulation, policy, ethics, and morality;
- classify realistic cybersecurity situations;
- apply ethical frameworks;
- identify missing facts and assumptions;
- use ChatGPT Edu to analyze a cybersecurity ethics problem;
- compare AI-generated reasoning with human professional judgment.

AI Reasoning Lab

Your team will provide ChatGPT Edu with a fictional cybersecurity scenario and ask it to analyze the situation using multiple ethical frameworks.

You will then evaluate its response.

Look for:

- unsupported assumptions;
- missing stakeholders;
- questionable legal claims;
- authorization issues;
- incomplete ethical reasoning;
- conclusions requiring verification.

You will ultimately make your own professional recommendation.

Between the Two Class Meetings

Read selected portions of the ACM Code of Ethics and Professional Conduct:

https://www.acm.org/code-of-ethics (https://www.acm.org/code-of-ethics)

Come to the second class prepared with:

1. Two ACM principles you believe directly apply to cybersecurity professionals.
2. One realistic cybersecurity example for each principle.
3. One principle that becomes more complicated when AI or automation is involved.
4. An explanation of why AI makes that responsibility more complicated.

Be prepared to explain and defend your choices.

Class Meeting 2

Professional Judgment, Stakeholders & AI-Enabled Cybersecurity

During the second meeting, you will apply what you learned to increasingly complex cybersecurity decisions.

Topics and activities include:

- professional codes of ethics;
- competing professional responsibilities;
- stakeholder analysis;
- privacy and authorization;
- AI-assisted threat detection;
- false positives;
- bias and assumptions;
- human oversight;
- AI risk management;
- professional accountability.

Applied Case: AI Flags an Insider Threat

You will work as part of a cybersecurity team responding to an AI-generated insider-threat alert.

The system has flagged a cybersecurity student based on activities such as:

- unusual login times;
- privacy-tool use;
- virtual machines;
- network scanning;
- downloading cybersecurity resources.

Your team will determine whether those behaviors indicate malicious activity—or whether legitimate cybersecurity education could look suspicious to an automated system.

Consider:

- What evidence actually exists?
- What assumptions is the system making?
- What information is missing?
- Who could be affected?
- What authorization is required?
- What privacy concerns exist?
- What happens if the system produces a false positive?
- What happens if the organization ignores a legitimate threat?
- Should automated detection lead directly to automated action?
- Who is accountable for the final decision?

Introducing the NIST AI Risk Management Framework

You will begin working with the NIST Artificial Intelligence Risk Management Framework.

NIST AI Risk Management Framework:

https://www.nist.gov/itl/ai-risk-management-framework (https://www.nist.gov/itl/ai-risk-management-framework)

The framework introduces four core functions:

GOVERN – MAP – MEASURE – MANAGE

For this week's work, think about them this way:

GOVERN

Who is responsible, and what policies and oversight should exist?

MAP

What is happening, who could be affected, and what could go wrong?

MEASURE

How do we know whether the system performs appropriately?

MANAGE

What should the organization do about the risks it identifies?

You will work with AI governance in greater depth later in the course.

Optional Video

NIST – Introduction to the NIST AI Risk Management Framework (AI RMF 1.0): An Explainer Video

https://www.nist.gov/video/introduction-nist-ai-risk-management-framework-ai-rmf-10-explainer-video (https://www.nist.gov/video/introduction-nist-ai-risk-management-framework-ai-rmf-10-explainer-video)

Cybersecurity Governance Connection

You will also begin connecting ethical decisions to cybersecurity governance through the NIST Cybersecurity Framework 2.0.

NIST Cybersecurity Framework 2.0:

https://www.nist.gov/cyberframework (https://www.nist.gov/cyberframework)

You do not need to master CSF 2.0 this week.

For now, recognize that cybersecurity decisions exist within an organization, not just inside the security team.

Your Week 1 Graded Work

Ethics Framework Application

Ethics Framework Application

Points: 40

Category: Case Studies, Simulations & Interactive Activities

You will analyze a cybersecurity ethics scenario and develop a defensible professional recommendation.

Your analysis will require you to:

- identify the decision;
- separate facts from assumptions;
- identify missing information;
- identify stakeholders;
- distinguish legal, policy, authorization, and ethical concerns;
- apply two ethical frameworks;
- apply professional ethical principles;
- evaluate the role of AI;
- develop a recommendation;
- support significant claims with authoritative evidence;
- critically evaluate AI assistance.

You are graded on the quality of your reasoning, evidence, application, and professional judgment.

Portfolio Setup/Update

Points: 10

Category: Cyber Law, Ethics & Governance Portfolio

You will establish or update the professional portfolio where you will showcase CYBR-2100 work.

If you already have a cybersecurity portfolio, continue building it.

Students already using GitHub are encouraged to continue developing their GitHub portfolio.

Your portfolio will grow throughout the course with work involving areas such as:

- cyber ethics;
- law and privacy;
- governance and policy;
- AI ethics and governance;
- professional communication;
- cybersecurity decision-making.

Professional Decision Exercise: Trust the Alert?

Points: 15

Category: Professional Decision Exercises

Instead of a traditional weekly quiz, you will make a professional decision using the concepts from this week.

You will respond to a scenario in which an AI-enabled security platform gives a CFO's account a 92% likelihood of compromise and recommends immediately disabling it.

You will need to:

- make an immediate decision;
- distinguish facts from assumptions;
- identify evidence you need;
- evaluate your authority;
- apply an ethical or professional principle;
- evaluate the AI recommendation;
- defend your decision;
- use ChatGPT Edu to challenge your initial reasoning;
- decide whether that challenge should change your final recommendation.

There is not necessarily one correct action.

You will be evaluated on whether your decision is professionally defensible.

Preparation & Professional Engagement

Points: 10

Category: Professionalism & Engagement

This includes:

- ACM Code preparation;
- applied class activities;
- team analysis;
- professional discussion;
- responsible use of AI;
- meaningful contribution to cybersecurity decision-making exercises.

Meaningful participation matters more than simply talking frequently.

Week 1 Checklist

Before completing Week 1:

- Participate in Class Meeting 1.
- Complete the cybersecurity classification activity.
- Participate in the AI Reasoning Lab.
- Review the ACM Code of Ethics and Professional Conduct.
- Prepare your ACM principles for Class Meeting 2.
- Participate in the AI insider-threat case.
- Work with the introductory NIST AI RMF concepts.

- Work with the introductory NIST AI RMF concepts.
- Participate in the security-team briefing.
- Submit the Ethics Framework Application.
- Complete or update your professional portfolio structure.
- Submit Professional Decision Exercise: Trust the Alert?
- Complete the required preparation and professional engagement activities.

Before You Leave Week 1

You should now be able to explain why these statements are important:

Technical capability does not equal authorization.

Legal does not automatically mean ethical.

AI-generated does not automatically mean accurate.

Professional judgment cannot simply be outsourced to a tool.

What to Expect Next Week

Next week, we move from foundational ethical decision-making into cyber law and legal authority.

You will begin examining how laws and legal concepts affect cybersecurity activities such as:

- accessing computer systems;
- conducting security testing;
- investigating incidents;
- handling digital information;
- monitoring activity;
- responding to cybercrime.

We will continue using realistic scenarios rather than treating law as a list of statutes to memorize.

AI will remain part of the work as we examine authorization, AI-assisted investigations, automated actions, evidence, and legal responsibility.

Come prepared to tackle the next professional question:

Who actually gave you permission to do that?