# FIRST Principles of Cybersecurity

TOPIC: FOUNDATIONAL PRINCIPLES

GRADES: 6-8, 9-12

LESSON DURATION: N/A

SOFT SKILLS: CRITICAL THINKING, COLLABORATION, CREATIVITY, PRESENTATION

CREDIT: NSA GENCYBER CAMPS

---

## Introduction:

- In the summer of 2014, the NSA began a summer outreach program entitled, GenCyber. The summer camps have three goals: to increase interest in cybersecurity careers and diversity in the cybersecurity workforce of the nation, to help all students understand correct and safe online behavior and how they can be good digital citizens, and to improve teaching methods for delivery of cybersecurity content in K-12 curricula (GenCyber, 2017). At the core of the camp curriculum are ten foundational principles called the First principles. This lesson plan allows students to explore each principle and apply it to real world scenarios through an unplugged activity.
- This activity requires a basic level of computing terminology and can be further enhanced by basic knowledge of the CIA triad and cybersecurity concepts.

---

## Materials:

- A copy of the First principles
- Teacher version of the principles
- Teacher background information on cybersecurity concepts (CIA triad)
- Presentation tool-PowerPoint or large pieces of paper

---

## Activities:

1. Divide students into small groups. Be sure to attempt to put one creative student in each group.
2. Explain to the class that today students will look at some core security and computer science concepts. Each group will be supplied the term and a brief definition. The group then must come up with a real-world example of the term. Students may need help with this part so be sure to have read the teacher version above.
3. The group must draw a picture of the example and also explain it in words.
4. Each group should be assigned one of the principles. The teacher should walk around and ensure that each group has an understanding of the concept before they begin developing the poster/visual.
5. Students should be asked to present their work to the whole class. A discussion should occur on each principle. Other groups can also supply examples as the discussion occurs. The focus should be on the core definition of the principle as well as its application to information

security. For example, layering could be defined as the practice of setting up multiple layers of network security. The goal is that the layers are pre-determined to strategically work together to protect the confidentiality, integrity, and availability of information on the network. If an adversary penetrates one layer, it is hoped that the next layer of security will thwart the attack. Adversaries operate on a cost/benefit analysis scheme, just like the rest of us. If the network protection is good enough that the adversary sees no benefit in further pursuing an attack, they will move onto the next victim. On the flip side, layering cannot be so overly complicated that the system professionals do not know how it works.

6. After all groups have presented, the teacher may choose to complete a follow-up enrichment activity. Assigning each group a different principle, each group must now develop a skit portraying the concept. Allow the groups time to develop ideas and be creative. Allow the use of props. Do not allow groups to work together or share their principles.
7. When each group is done, play a game of First Principle Charades. Each group should perform the short skit and all others in the room should guess which principle is being displayed. After each skit, take a few moments to review the principle.