Rangeview High School
Cybersecurity
Course Syllabus
2022-2023

Course Title: Cybersecurity
Instructor's Name: Randy Mills
Contact Numbers: Rangeview 303.695.6848
e-mail rdmills@aurorak12.org

Course Description: PLTW Cybersecurity gives students a broad exposure to the many aspects of digital and information security, while encouraging socially responsible choices and ethical behavior. It inspires algorithmic thinking, computational thinking, and especially, "outside-the-box" thinking. Students explore the many educational and career paths available to cybersecurity experts, as well as other careers that comprise the field of information security. The course contains the following units of study.

Unit 1 Personal Security (19%)
Unit 2 System Security (22%)
Unit 3 Network Security (31%)
Unit 4 Applied Cybersecurity (28%)

Course Concepts

Information Security

- Evaluate and define information security needs
- Authenticate and authorize access to information
- Organize and protect information stored in a file system

Security Algorithms

- Analyze and improve cryptography algorithms
- Apply various encryption measures to secure information

Data Abstraction

- Analyze network traffic at varying levels of abstraction
- Recognize patterns in traffic flow to identify cybersecurity events
- Recognize signatures and symptoms of malware to identify an attack

Computer Systems and Networks

- Manage operating system resources necessary for network configuration
- Implement protection measures to secure computers and devices on a network
- Monitor network activity and traffic flow

Threat Investigation

- Analyze the evidence of a cybersecurity event
- Identify system vulnerabilities that permitted an attack and the user actions that can secure the system
- Know and use investigative techniques of digital forensics

Industry Standard Tools

- Virtual machines with a variety of configurations
- Network visualization and topology tools
- Penetration testing software
- Packet analysis software

Professional Skills

- Ethical Hacking
- Collaboration in Cyber Teams

- Agile Project Development/Scrum
- Teamwork and Collaboration
- Presentation/Communication
- Public Speaking
- Ethics
- Cybersecurity Best Practices

Grading Scale:

GRADE	SCALE	PERCENTAGE RANGE
A	4.0	90-100
B	3.0	80 -89
C	2.0	70-79
D	1.0	60-69
F		0-69

Body of Evidence:
There are two types of assessment, formative and summative.
Formative (assessments for learning) provide direction for improvement for the student and adjustment of instruction for the teacher e.g. observation, quizzes, homework, discussion, drafts, etc.
Summative (assessment of learning) provide information to be used in making judgments about a student's achievement at the end of a sequence of instruction, e.g. final drafts, tests, assignments, projects, performances, etc.

Class Expectations
Make up work and Office Hours: It is the responsibility of the student to make up assignments as soon as you return to class after an absence. In some cases an alternative assignment may be given to the student. A student has two days for each day missed. **No credit will be given for work missed during unexcused absences. Please see Mr. Mills for times for appointment. Completing work in a timely manner is a component of proficiency.**

Student Handbook and Classroom Policies:

Bullying:
Definition: Any written, verbal or pictorial expression, physical or electronic act or gesture, or a pattern thereof by a student that is intended to coerce, intimidate or cause any physical, mental, or emotional harm to any student. This includes the creation of an intimidating, hostile, or significantly offensive environment that interferes with the learning or performance of school-sanctioned activities of any student.

Examples of Bullying:

- Derogatory written or pictorial communications in any media (e.g., letters, notes, cellphones, social networks, voice mail, text messages, pager messages, newspaper articles, invitations, posters, photos, cartoons);
- Derogatory verbal comments (e.g., name-calling, taunting, hostile teasing, spreading rumors, epithets, jokes or slurs);
- Threats of force or violence against a person's body, possessions or residence (e.g., obtaining food or money by threats of force); or

- Physical conduct (e.g., provocative gestures, overly rough horseplay, restricting freedom of action or movement, violence, defacing or destruction of property).

Any student engaged in bullying will face disciplinary action. All concerns of threats or rumors must be reported to a staff member as soon as possible.

Cyberbullying:
Definition: Being cruel to others by sending or posting harmful material using the Internet, cell phone, or any social media. Spreading or forwarding rumors or threats or photos via social media is a serious offense.

Any student engaged in cyberbullying will face disciplinary action. All concerns of threats or rumors must be reported to a staff member as soon as possible. Cyberbullying is a criminal offense and police will be notified.

Academic Dishonesty
Academic dishonesty as defined by our safe schools policy is: Untruthful or deceptive behavior in connection with academics, including plagiarism, cheating on tests or assignments or changing grades without authorization.

FIRST OFFENSE
A zero on the assignment, test, or quiz with no opportunity to make up the work for credit.

SUBSEQUENT OFFENSES
A zero on the assignment, test, or quiz with no opportunity to make up the work for credit AND referral by an RHS Faculty member to the Dean of Students and documentation into the Infinite Campus conference log.

Parent notification will be made in all circumstances. Multiple offenses of any of the above may result in failing a class.