Board of Education Curriculum, Assessment, and Professional Practices Committee Meeting

Thursday, April 23, 2026 6:30 PM
Board of Education Conference Room E, Live Stream: http://devos2.bethel.k12.ct.us/show?video=763ff4de0370 Materials can be viewed at: https://meetings.boardbook.org/Public/Organization/2425 The opportunity for members of the public wishing to make comments can attend and comment in-person or may send public comments to the Board via email or letter and it will be included as part of the record of the meeting., 1 School Street, PO Box 253, Bethel, CT 06801

1.	**AP Cybersecurity Course and Curriculum**	**Speaker(s):** Dr. Doolan
2.	**Public Comment** **(Please note: The Board welcomes Public Comment and asks that speakers please limit their comments to 2 minutes. Speakers may offer objective comments of school operations and programs that concern them. The Board will not permit any expression of personal complaints or defamatory comments about Board of Education personnel and students, nor against any person connected with the Bethel Public School System.)**	
3.	**Adjourn**	

Bethel Public Schools
Course Proposal

1. **Title of Course**: AP Cybersecurity

2. **Department(s):** CTE

3. **Submitted by**: Doolan

4. **Length of Course (full year, semester):** Full Year

5. **Grade Level(s), if applicable**: 10-12

6. **Prerequisites, if any**: None

7. **Short Course Description, suitable for Program of Studies:**
AP Cybersecurity is a broad introduction to the field of cybersecurity that aligns closely with a standard first-year college introductory cybersecurity course course. Students learn about common threats and vulnerabilities and how those combine to create risk. Students study how individuals and organizations manage risk and how risk can be mitigated through a defense-in-depth strategy. Students explore specific vulnerabilities, attacks, and mitigations,
and detection measures across a variety of domains, including physical spaces, computer networks, devices, data, and applications. Throughout the course, students consider the impact of cybersecurity on individuals, organizations, societies, and governments.

8. **Statement of Need for this Course**: ***Give the rationale for the proposal, including its relationship to past, current, and future development in the school system.***
The proposed AP Cybersecurity course addresses a growing need to prepare students for an increasingly digital and interconnected world. Cybersecurity is one of the fastest-growing career fields, with a significant demand for skilled professionals across industries. Offering this course provides students with exposure to critical concepts such as network security, data protection, ethical hacking, and risk management, helping them develop both technical and analytical skills.

This course also expands access to rigorous, college-level STEM opportunities, supporting students' readiness for postsecondary education and careers. It aligns with workforce trends and district goals of promoting career pathways in high-demand fields. Additionally, it helps students become informed digital citizens, capable of understanding and addressing real-world security challenges that impact individuals, organizations, and society.

9. **Course Objectives*:*** ***The purpose of the new or modified course should be stated here. What is it that the course seeks to help students achieve? What are the student outcomes expected at the end of a given time? What additional outcomes are being sought that cannot be defined in behavioral terms? What are relevant long-term course targets, such as student participation rates and evaluation criteria?***

The purpose of the AP Cybersecurity course is to provide students with a rigorous, college-level introduction to the principles and practices of cybersecurity while developing critical thinking, problem-solving, and technical skills.

By the end of the course, students will be able to:

- Understand core cybersecurity concepts, including network security, cryptography, threat analysis, and risk management
- Analyze and identify vulnerabilities in systems and propose appropriate security measures
- Apply ethical hacking and defensive strategies in simulated, real-world scenarios
- Interpret and respond to cybersecurity incidents using logical and evidence-based reasoning
- Communicate technical information clearly through written reports and presentations
- Demonstrate responsible and ethical use of technology as digital citizens

10. **Scope and Substance of the Course*:***

1. Introduction to Security
2. Securing Spaces
3. Securing Networks
4. Securing Devices
5. Securing Applications and Data

11. **Class Size*:*** ***State minimum and maximum class size and pupil/teacher ratio.***
25 students

12. **What specific improvements will this proposal make to the school's academic program and the commitment to the implementation of the *Common Core***

***Standards*?**

The AP Cybersecurity course will strengthen the school's academic program by expanding advanced computer science offerings and preparing students with in-demand technical and problem-solving skills. It supports the Common Core Standards by emphasizing critical thinking, analytical reasoning, and real-world application of knowledge. Students will engage in reading complex informational texts, writing technical explanations, and applying mathematical and logical reasoning to solve authentic cybersecurity problems, reinforcing key literacy and college- and career-readiness skills.

13. **What impact – positive or negative – will this proposal have upon other courses or programs offered within the subject area in <u>your building</u>?** ***For example, will the addition of this course reduce the number of pupils in other courses in the department?***

The addition of the AP Cybersecurity course will have a largely positive impact on other courses and programs across buildings, with minimal disruption. This course is designed to complement existing computer science pathways rather than replace them. It may increase student interest and enrollment in foundational courses such as introductory programming, networking, or digital literacy, as students build the prerequisite skills needed for success in AP Cybersecurity.
While a small number of students may shift from other elective offerings into this course, the overall effect is expected to be an expansion of opportunities rather than a reduction in participation in other elective offerings.

14. **What impact – positive or negative – will this proposal have on other courses/programs offered in the <u>other buildings</u>?** ***For example, would this proposal cause adjustments to be necessary in feeder programs or follow-up programs? Would it be necessary to reduce the number of pupils in other departments (in teacher assignments, etc.) be necessary?***

The addition of the AP Cybersecurity course will have a largely positive impact on other courses and programs across buildings, with minimal disruption. This course is designed to complement existing computer science pathways rather than replace them. It may increase student interest and enrollment in foundational courses such as introductory programming, networking, or digital literacy, as students build the prerequisite skills needed for success in AP Cybersecurity.
While a small number of students may shift from other elective offerings into this course, the overall effect is expected to be an expansion of opportunities rather than a reduction in participation in other elective offerings.

15. **Would adoption of this proposal require staff adjustments, e.g., employing new staff, retraining veteran staff?** ***If yes, show the number of positions involved the first year, compared to the past, and project the figure for each of the three successive years?***

No adjustments needed

Resources & Development Needs:

1. **Will a writing team be necessary to prepare a curriculum guide?** ***If so, submit a proposal for curriculum work along with this course proposal.***
   No
2. **What research has been conducted in the area addressed by this course?** ***Summarize that research and indicate the relationships of the research to this proposed course. Indicate any trends or practices in other schools.***

   Research in cybersecurity education shows that students often have limited knowledge and inconsistent safe practices, leaving them vulnerable to threats such as phishing and malware. (SRJIS)

   Studies also demonstrate a strong positive relationship between cybersecurity education and student awareness/behavior, confirming that structured instruction significantly improves students' ability to recognize and respond to cyber risks. (RSIS International)

   At the same time, there is a documented global workforce shortage in cybersecurity, partly due to a lack of early educational pathways at the high school level. (OUP Academic)

   Research further identifies key characteristics of effective cybersecurity education:

- Hands-on, experiential learning (e.g., simulations, games, competitions) improves engagement and understanding (NSF Public Access Repository)
- Structured curriculum integration is necessary to build long-term digital safety and resilience (NCERT Journals)
- Programs should align with skills-based frameworks to address workforce gaps (MDPI)

   Overall, research strongly supports introducing cybersecurity education in high school through applied, interdisciplinary, and skills-focused instruction.

   The AP Cybersecurity course aligns closely with this research:

- It provides broad access with no prerequisites, addressing the documented lack of early exposure
- It emphasizes real-world, hands-on learning, consistent with research supporting simulations and applied experiences
- It focuses on core practices such as risk analysis, mitigation, and threat detection, aligning with workforce frameworks

- It integrates technical, human, and ethical dimensions, reflecting interdisciplinary research recommendations

  Because of this alignment, the course directly responds to research-identified needs: improving student awareness, building practical skills, and creating pathways into cybersecurity careers.

  Trends and Practices in Other Schools

  Research and case studies show that high schools are increasingly adopting cybersecurity programs due to workforce demand and national priorities. (ScholarSpace)

  Common practices include:

- Embedding cybersecurity into STEM and CTE pathways

- Using hands-on labs, simulations, and gamified environments (e.g., Capture-the-Flag competitions) to enhance learning (Wikipedia)
- Expanding access through clubs, camps, and competitions
- Emphasizing equity and access, ensuring broader student participation (ERIC)

  These trends reflect research recommendations for experiential, accessible, and career-connected cybersecurity education.

  Overall Conclusion: The research supports the need for cybersecurity education at the secondary level. Studies show that structured, hands-on instruction improves student awareness and skills, while also helping address a significant workforce gap.

  The AP Cybersecurity course aligns with these findings by combining:

- Experiential learning
- Interdisciplinary content
- Workforce-relevant skills

3. **Textbook (if applicable):**
   None
4. **Other Resources Recommended:**
   Learning platform (Perkins)
5. **Names of Staff Who May Teach the Course:**
   Casey Ragan
6. **Training of Staff Required:**
   AP Cybersecurity teacher training
7. **Department Approval**: ***Please have at least 50% of the department members or***

grade level teachers indicate their approval with their signature and date.

_____ Date _____

_____ Date _____

_____ Date _____

Signature of School Administration:

_____ Date _____

Signature of District Administration:

_____ Date _____

Please submit this form electronically to Dr. Brooks and also submit a hard copy with signatures via inter-office mail. Thank you!

AP Cybersecurity

M. Doolan

AP Cybersecurity

Yearlong Advanced Placement course developed by the College Board as part of its "Career Kickstart" initiative. Designed for a national launch in the 2026–27 school year, this course offers a comprehensive, entry-level introduction to the field of cybersecurity, focusing on defending systems, analyzing threats, and managing risk.

About AP Career Kickstart

AP Career Kickstart courses provide high schools with a new set of AP offerings that prepare students for high-skill, high-growth careers through:

- Instruction in both technical and professional skills
- Emphasis on hands-on learning grounded in authentic scenarios
- Alignment to career and technical education (CTE) and industry standards
- Opportunity to earn an employer-endorsed credential upon achieving a qualifying exam score

How AP Career Kickstart Courses Are Developed

Every AP course is designed—and regularly updated—to include current data, evidence, and findings in each discipline. AP courses include the content and skills most frequently taught in introductory college courses, so that students who earn qualifying scores on AP Exams can be placed into upper-division college courses with a strong foundation for success.

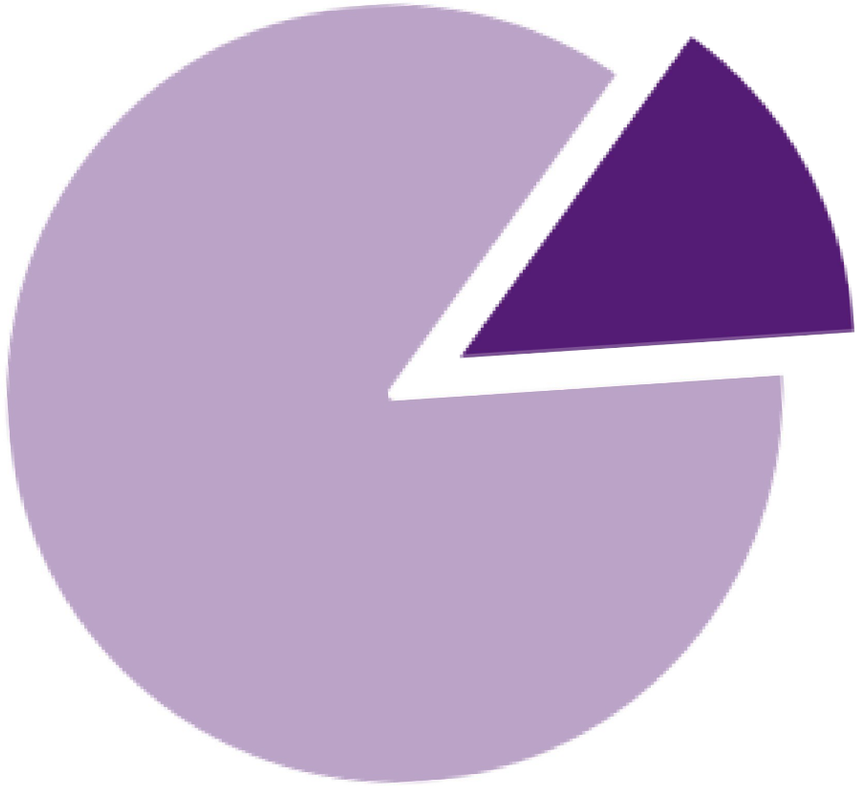
AP Career Kickstart courses are built in partnership with industry advisors, higher education faculty, high school educators, and career and technical education (CTE) leaders. These advisors are engaged to evaluate research; recommend course skills, scope, and sequence; and review the course framework and the AP Exam.

Credentials and Industry Recognition

The AP Program partners with industry leaders to ensure the course skills align with employer demand for core requirements in high-growth, high-demand jobs. Along with the potential to earn college credit, students with qualifying scores on the AP Exam will earn the AP Career Kickstart Employer-Endorsed Credential. Created in partnership with industry experts, AP Career Kickstart Credentials accelerate students' progress toward in-demand careers and align with the needs of employers, college-level coursework, and secondary CTE programs.

Cybersecurity education is needed.

Employers lack trained professionals.



14%

Only 14% of organizations are confident that they have the people and skills required.

Source
“Global Cybersecurity Outlook 2025”
World Economic Forum

Employers are actively posting job openings.

514,359

Total Online Job Openings (February 2026)

Job postings for cybersecurity-related positions

Source: Cyber Seek

Course Content

Students develop the skills they'll need for success.

	Skill Category 1	Skill Category 2	Skill Category 3	Skill Category 4
	Analyze Risk *Evaluate risk to organizational assets.*	**Mitigate Risk** *Implement protective and deterrent security controls.*	**Detect Attacks** *Implement detection methods, monitor systems, and analyze evidence.*	**Collaborate** *Work with others and AI to accomplish a task.*
Communicating concepts *Explain key cybersecurity concepts.*	1.A Identify, with and without the support of AI, vulnerabilities, threats, and attack methods, and explain how they generate risk.	2.A Identify security controls and explain how they mitigate risks.	3.A Identify methods for monitoring systems and explain how they detect attacks.	4.A Develop clear, shared team objectives related to a cybersecurity task.
Investigating problems *Explain the parameters of a problem to plan for solutions.*	1.B Determine ways adversaries exploit vulnerabilities to compromise an asset.	2.B Determine layered security controls that address vulnerabilities.	3.B Determine strategies and methods to detect attacks.	4.B Determine clear roles and responsibilities for members of a team working to accomplish a cybersecurity task.
Assessing impacts *Evaluate impact on systems.*	1.C Evaluate, with and without the support of AI, the likelihood and impact of risks.	2.C Evaluate, with and without the support of AI, the impact of protective risk-management strategies.	3.C Evaluate the impact of threat detection methods.	4.C Implement AI as a collaboration tool individually and as a group.
Enacting solutions *Apply and communicate solutions.*	1.D Document, with and without the support of AI, the likelihood and impact of risks.	2.D Implement and log mitigations with and without the support of AI.	3.D Detect and classify cyberattacks by analyzing digital evidence with and without the support of AI.	4.D Complete assigned work to accomplish a collaborative cybersecurity task.

Plan

The Course at a Glance provides a useful visual organization of the AP Cybersecurity components, including:

- Sequence of units, along with suggested pacing. Please note, pacing is based on 45-minute class periods, meeting five days each week for a full academic year.
- Progression of topics within each unit.

Teach

COURSE SKILLS

1 Analyze Risk
2 Mitigate Risk
3 Detect Attacks
4 Collaborate

UNIT 1

Introduction to Security

~10 class periods

Skill	Topic
1 1.1	Understanding Social Engineering
1 2	1.2 Suspicious Website Logins
1 2	1.3 Best Practices for Public Networks
1 2	1.4 AI-Based Cybersecurity Attacks
2 3	1.5 Leveraging AI in Cyber Defense

UNIT 2

Securing Spaces

~21 class periods

Skill	Topic
1 2	2.1 Cyber Foundations
	2.2 Physical Vulnerabilities and Attacks
2	2.3 Protecting Physical Spaces
3	2.4 Detecting Physical Attacks

UNIT 3

Securing Networks

~26 class periods

Skill	Topic
1 3.1	Network Vulnerabilities and Attacks
2	3.2 Protecting Networks: Managerial Controls and Wireless Security
2	3.3 Protecting Networks: Segmentation
2	3.4 Protecting Networks: Firewalls
3	3.5 Detecting Network Attacks

UNIT 4

Securing Devices

~23 class periods

Skill	Topic
1	4.1 Device Vulnerabilities and Attacks
2	4.2 Authentication
2	4.3 Protecting Devices
3	4.4 Detecting Attacks on Devices

UNIT 5

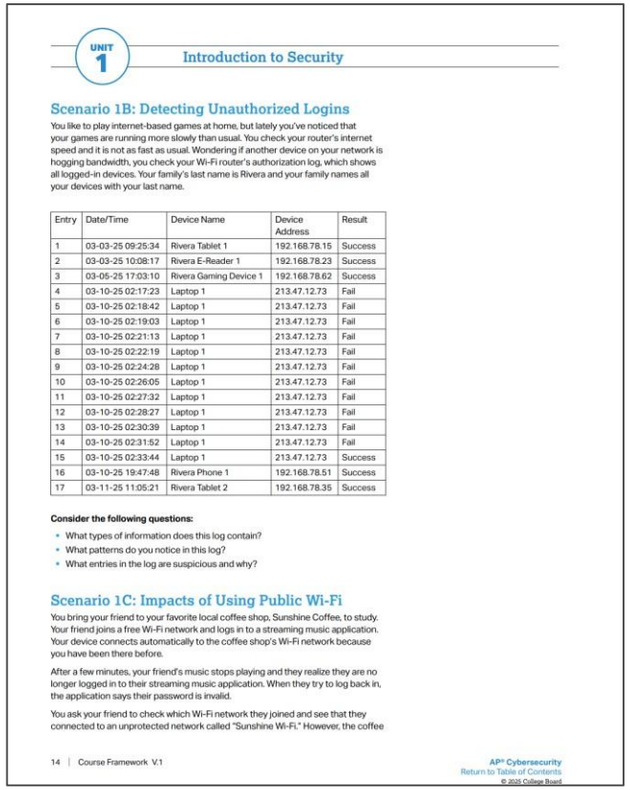
Securing Applications and Data

~30 class periods

Skill	Topic
1 5.1	Application and Data Vulnerabilities and Attacks
2	5.2 Protecting Applications and Data: Managerial Controls and Access Controls
2	5.3 Protecting Stored Data with Cryptography
2	5.4 Asymmetric Cryptography
2	5.5 Protecting Applications
3	5.6 Detecting Attacks on Data and Applications

Applied Learning

Students get real-world, everyday experiences with authentic cybersecurity scenarios.



UNIT 1 Introduction to Security

Scenario 1B: Detecting Unauthorized Logins

You like to play internet-based games at home, but lately you've noticed that your games are running more slowly than usual. You check your router's internet speed and it is not as fast as usual. Wondering if another device on your network is hogging bandwidth, you check your Wi-Fi router's authorization log, which shows all logged-in devices. Your family's last name is Rivera and your family names all your devices with your last name.

Entry	Date/Time	Device Name	Device Address	Result
1	03-03-25 09:25:34	Rivera Tablet 1	192.168.78.15	Success
2	03-03-25 10:08:17	Rivera E-Reader 1	192.168.78.23	Success
3	03-05-25 17:03:10	Rivera Gaming Device 1	192.168.78.62	Success
4	03-10-25 02:17:23	Laptop 1	213.47.12.73	Fail
5	03-10-25 02:18:42	Laptop 1	213.47.12.73	Fail
6	03-10-25 02:19:03	Laptop 1	213.47.12.73	Fail
7	03-10-25 02:21:13	Laptop 1	213.47.12.73	Fail
8	03-10-25 02:22:19	Laptop 1	213.47.12.73	Fail
9	03-10-25 02:24:28	Laptop 1	213.47.12.73	Fail
10	03-10-25 02:26:05	Laptop 1	213.47.12.73	Fail
11	03-10-25 02:27:32	Laptop 1	213.47.12.73	Fail
12	03-10-25 02:28:27	Laptop 1	213.47.12.73	Fail
13	03-10-25 02:30:39	Laptop 1	213.47.12.73	Fail
14	03-10-25 02:31:52	Laptop 1	213.47.12.73	Fail
15	03-10-25 02:33:44	Laptop 1	213.47.12.73	Success
16	03-10-25 19:47:48	Rivera Phone 1	192.168.78.51	Success
17	03-11-25 11:05:21	Rivera Tablet 2	192.168.78.35	Success

Consider the following questions:

- What types of information does this log contain?
- What patterns do you notice in this log?
- What entries in the log are suspicious and why?

Scenario 1C: Impacts of Using Public Wi-Fi

You bring your friend to your favorite local coffee shop, Sunshine Coffee, to study. Your friend joins a free Wi-Fi network and logs in to a streaming music application. Your device connects automatically to the coffee shop's Wi-Fi network because you have been there before.

After a few minutes, your friend's music stops playing and they realize they are no longer logged in to their streaming music application. When they try to log back in, the application says their password is invalid.

You ask your friend to check which Wi-Fi network they joined and see that they connected to an unprotected network called "Sunshine Wi-Fi." However, the coffee

Each unit includes between one and five scenarios that highlight professional career situations and require students to practice the use of the skills and course content within that unit.

- Work-based scenarios include:
- Conduct a physical vulnerability assessment of a new lab.
- Recommend and diagram a set of security features for three LANs on a naval submarine.
- Assess the risk from possible vulnerabilities of internet-connected farm equipment.
- Set access to proprietary research and development on an air-gapped computer.

Scenario 1A: Detecting Phishing Messages

To: ljones@school.edu
From: do-no-reply@g00gle.com
Subject [Urgent!] Access Restricted

One of your students has requested access to make a copy of a document. Click this link to authorize your student to copy your document.

If you don't click the link, **your student won't be able to copy the document and complete their assignment.**

Research shows that the faster teachers respond to students' document-sharing requests, the more likely students are to submit their assignments on-time.

The Google Drive Team

Question:

What evidence could you use to convince your teachers that this email is not legitimate?

Scenario 1A: Detecting Phishing Messages

To: ljones@school.edu
From: do-no-reply@g00gle.com
Subject [Urgent!] Access Restricted

One of your students has requested access to make a copy of a document. Click this link to authorize your student to copy your document.

If you don't click the link, **your student won't be able to copy the document and complete their assignment.**

Research shows that the faster teachers respond to students' document-sharing requests, the more likely students are to submit their assignments on-time.

The Google Drive Team

Question:

What elements of the email might cause someone to act impulsively?

Scenario 1A: Detecting Phishing Messages

To: ljones@school.edu
From: do-no-reply@g00gle.com
Subject [Urgent!] Access Restricted

One of your students has requested access to make a copy of a document. Click this link to authorize your student to copy your document.

If you don't click the link, **your student won't be able to copy the document and complete their assignment.**

Research shows that the faster teachers respond to students' document-sharing requests, the more likely students are to submit their assignments on-time.

The Google Drive Team

Question:

What are some potential consequences for someone who clicked the link in the email?

Scenario 1A: Detecting Phishing Messages

If someone clicks a link in a phishing email, several negative consequences could happen:

Malware infection	Link could install malware, spyware, or ransomware on the device.
Stolen credentials	Link may lead to a fake login page that steals usernames and passwords.
Identity theft	Personal information could be collected and used for fraud.
Account compromise	Email, banking, or social media accounts could be taken over.
Data loss	Files could be deleted, encrypted, or accessed without permission.
Financial loss	Attackers could make unauthorized purchases or transfers.

Scenario 3C: Configuring a Secure Wireless Network

As a Network Technician in the National Guard, you have been called to active duty in the aftermath of a natural disaster. You have been tasked with setting up a secure wireless network at a local high school gymnasium, which has been converted to an emergency shelter for people who lost their homes in the disaster. The secure wireless network should provide access to the internet.

There is a satellite link that will provide internet access. Your task is to determine the security features necessary to ensure that the network is safe to use. The security features you determine should be able to detect and log possible malicious activity on the network that would compromise security on performance. You will:

- Describe configurations to secure the wireless network
- Recommend a collection of detective controls to monitor the network and raise an alert for any potential malicious activity.
- Describe the impact of the detective-control recommendations.

Scenario 3C: Configuring a Secure Wireless Network

Student Response A

I would add security to the WiFi so hackers can't get in. Logs would be turned on to watch the network.

Scenario 3C: Configuring a Secure Wireless Network

Student Response B

For an emergency shelter, the wireless network should be secure but easy to use.

- **Configurations**: WPA3 encryption would protect wireless traffic, and network segmentation would separate staff and public users to limit the impact of a compromised device.
- **Configurations**: Access points would use WPA3-Personal for public access and WPA3-Enterprise for staff, with VLANs separating traffic.
- **Detective Controls**: Logging on the wireless controller and firewall would monitor failed logins, unusual traffic, and IDS alerts.
- **Impact**: These detective controls allow administrators to detect potential security issues with minimal performance impact while protecting user privacy.

Exam Design

Students sit for a fully digital exam in Bluebook.

The exam is **2 hours and 10 minutes** long and includes **60 multiple-choice questions** and **one free-response question**.

Section	Question Type	Number of Questions	Timing	Percent of Exam Score
I	**Multiple Choice** Students analyze scenarios and digital evidence to identify vulnerabilities, recommend mitigations, and detect potential threats.	60	80 minutes	70%
II	**Free Response** Students will use sources to determine security issues, attacks, and how a system is configured. Using evidence from the sources, students will also suggest ways to make the device more secure and show how they could fix or harden the device.	1	50 minutes	30%

Designed with job-relevant problem-solving

Review the following firewall for a server:

```
1.  Allow Inbound TCP  port 22 from ALL;
2.  Allow Inbound TCP  port 80 from ALL;
3.  DENY  Inbound TCP  port 443 from 192.168.0.0/16;
4.  Allow Inbound ICMP from ALL;
5.  Allow Inbound TCP  port 3306 from ALL;
6.  Deny  Inbound TCP  port 3389 from ALL;
7.  Allow Inbound TCP  port 443 from ALL;
8.  Allow Inbound TCP  port 587 from ALL;
9.  Deny  Inbound TCP  port 8140 from 192.168.45.0/24;
10. Deny  Inbound ALL  inbound traffic;
```

1 Mark for Review

A network technician is trying to access the server using port 443 from a machine with an IP address of 192.168.45.37. However, they are unable to access the server.

Which of the following changes could be made to the firewall in order for the network technician to access the server?

(A) Swap firewall rule 1 with firewall rule 10.

(B) Swap firewall rule 3 with firewall rule 4.

(C) Swap firewall rule 3 with firewall rule 7.

(D) Swap firewall rule 7 with firewall rule 10.