

Part 1: Preparedness

SECURITY BOOT CAMP

**An actionable test security
workbook for educators and
organizations delivering
online exams.**

WELCOME!

In the age of ubiquitous remote online testing, it is more essential than ever to ensure security, prevent cheating and theft, and lock down the validity and trustworthiness of your exams.

Even with the use of high-quality proctors, it's still possible for test takers to subvert the rules, steal test content, and gain an unfair advantage. The online testing environment provides an especially fertile breeding ground for such behavior.

That's where the **Security Boot Camp** comes in. This workbook series will highlight key test security concepts and provide actionable worksheets and resources to help you understand and apply these concepts to your program, so you can make sound decisions for your security.

On page 3, you'll find **eight steps for improving the security of online tests**. This list will serve as the outline for all three of the Security Boot Camp workbooks. In **Part 1** of the Security Boot Camp, you'll learn about the best way to achieve test security **Preparedness**. Creating a robust **test security plan** and **publicizing your security measures** are two key ways to ensure you're prepared for any threats that look your way.

So dust off that stylus or fire up that printer, give your trusted team members a call, and follow along. It's time to head to Security Boot Camp!

8 STEPS TO TAKE **RIGHT NOW** TO IMPROVE SECURITY FOR YOUR ONLINE TESTS

PART 1: PREPAREDNESS WORKBOOK

CREATE A SECURITY PLAN

1

PUBLICIZE YOUR SECURITY MEASURES

2

PART 2: TECHNOLOGY WORKBOOK

EVALUATE YOUR ONLINE TESTING SOLUTION

3

LEVERAGE SECURE ITEM TYPES

4

TURN YOUR ITEM POOL INTO AN ITEM OCEAN

5

PART 3: EVALUATION WORKBOOK

CONDUCT A QUALITY ASSURANCE CHECK

6

SEARCH THE WEB FOR TEST CONTENT

7

REVIEW YOUR TEST DATA

8



BACKGROUND

WELCOME.....	2
EIGHT STEPS FOR IMPROVING SECURITY.....	3
AN OPEN LETTER TO THE WORLD OF ONLINE TESTING.....	5

MODULE 1: CREATING A SECURITY PLAN

GLOSSARY.....	9
INTRODUCTION BY DR. JOHN FREMER.....	10
COURSE PRE-WORK.....	12
PART 1: WHY DEVELOP A TEST SECURITY PLAN.....	13
PART 2: 5 TOPICS TO COVER DURING PLANNING.....	14
PART 3: KEY ROLES TO FILL ON YOUR TEAM.....	15
PART 4: KEY COMPONENTS OF YOUR SECURITY INCIDENT RESPONSE PLAN.....	16
SAMPLE TEST SECURITY PLAN OUTLINE: CERTIFICATIONS...	18
SAMPLE TEST SECURITY PLAN OUTLINE: STATES.....	19
NOTES.....	20

MODULE 2: PUBLICIZE YOUR TEST SECURITY MEASURES

GLOSSARY.....	22
INTRODUCTION BY ALISON FOSTER GREEN.....	23
PART 1: EXAMPLES OF DETERRENCE.....	26
PART 2: THREE COMPONENTS OF DETERRENCE.....	27
PART 3: DETERRENCE TACTICS FOR YOUR PROGRAM.....	28
NOTES.....	30

An Open Letter to the World of Online Testing

from Dr. David Foster
CEO of Caveon Test Security



Hi there,

In just a few short weeks, the COVID-19 pandemic has upended nearly every aspect of our lives, including the way important testing is done. For those students, teachers, professors, candidates, testing organizations, and testing service vendors who have had their plans for taking or giving tests disrupted, I want to offer this message of optimism. Your exams can still be taken and administered securely, even during a pandemic.

Nationwide quarantines and social distancing measures have made it so we can no longer take tests in classrooms, at testing centers, or in other locations. To solve this problem, testing organizations are quickly introducing new solutions that will allow individuals to test online from their own homes. These methods often rely on the use of online proctors to keep those tests secure.

Let me state that I am a wholehearted advocate for this type of online testing. In 2006, I proposed the concept of online proctoring—also referred to as remote proctoring—at the annual conference of the Association of Test Publishers. In 2013, I reviewed the services of several new online proctoring vendors, [comparing them on the security features](#). Two years later, Caveon published its security [Standards for Online Proctoring](#), providing a way to evaluate the professionalism of any remote proctoring service. For any program considering the move to online testing, and wishing to create or use an online proctoring solution, I would recommend those two publications and others available on the [Caveon website](#).

However, I need to add a word of caution. Online proctoring is far from a security panacea. Although well-designed proctoring systems—online or onsite—provide some useful security features, tests remain vulnerable to a number of significant security threats that will undermine the test's soundness and trustworthiness.

I repeat—when you put your exams online, even if you are using a competent method of remote proctoring, the two *most dangerous* test security threats remain: **proctors cannot detect when individuals are stealing your test content, and they cannot stop individuals who are cheating by using pre-knowledge.** If these threats cannot be detected by online proctors or proctors working at testing centers, then they are free to do extensive damage.

Let me explain these threats in more detail (without all the industry jargon).

#1: Theft of Test Content.

The first of these threats is the sure theft of test content (your test questions and answers) by individuals using hidden cameras. These are the kind of cameras that can be concealed in a button, the frame of eyeglasses, a lapel pin, or simply appear to be part of the fabric of a shirt. They are capable of recording an entire test session in high-resolution digital video. They are inexpensive, widely available, and easy to set up and use.

Even though a proctor might be closely monitoring an individual taking an exam, if that individual is motivated to steal test questions (to share with a friend or sell online), they will be able to easily steal the entire test—with no risk of being caught! That information can then be easily shared with someone in the neighboring room, apartment, or even on another continent.

#2: Cheating Using Pre-knowledge.

The second threat that cannot be detected by proctoring is cheating on the test using pre-knowledge of the test content. The term “pre-knowledge” is used to describe any information gained about the content of the exam prior to testing. For example, a test taker could purchase the answers to test questions online and memorize them before taking the exam. This form of cheating follows the theft of content described above.

A person with access to the stolen content can cheat confidently and effectively, knowing in advance all the questions and their answers. No proctor, however diligent, can tell the difference between an honest test taker and one who has gained an unfair advantage through pre-knowledge.

As a test security company, we have established practical and actionable solutions for all test security threats, including the two described above. We freely share and discuss test security solutions when we attend conferences, conduct webinars, and through other resources available on our website. Our mission at Caveon is to keep *every* exam safe and the test scores valid and trustworthy for important decisions. At this time, if you are curious about adopting online testing and want to safely navigate these dangerous waters, please visit the website and request a free consultation. We are here to help.

To be clear, I'm not advocating that you abandon your goal of online testing or proctoring your tests. **I believe online testing is the future of this industry and has tremendous potential, but only if it is done *securely*.** I simply want to help make this transition as painless as possible by making you aware of the very dangerous threats that jeopardize your exams *before* they arise and help you understand that viable solutions do in fact exist.

Sincerely,



David F. Foster
Chairman & CEO

[Caveon Test Security](#)

LOOKING AHEAD

- What are some things you can do to make your tests more secure right away? (Pages 3, 11)
- Where should you be looking to expand or enhance your program's security? (Pages 14, 15)
- How can you take stock of the security measures you have in place? (Page 16)

MODULE 1

CREATE A SECURITY PLAN

QUESTIONS YOU MAY HAVE

- How do you go about creating and implementing a comprehensive Test Security Plan? ([Page 11](#))
- What topics do you need to cover during the planning phase? ([Page 14](#))
- What should you consider when implementing a Test Security Incident Response Plan? ([Page 16](#))

SECURITY PLAN TERMS AND CONCEPTS

Detection

A set of systems put into place to uncover threats and test security breaches. Detection solutions can have a significant deterrent effect, but only if the scope and effectiveness of those solutions are broadly communicated.

Deterrence

A set of actions involving specific communications that are meant to inhibit and discourage individuals from committing test fraud, cheating on exams, or stealing test content. Deterrent methods aim to produce a psychological effect that presses would-be-cheaters to re-think and abandon unethical tendencies.

Prevention

An action meant to stop cheating or theft before it can take place. Preventative measures are implemented by testing programs before an exam is administered.

Reaction

An action a testing program takes in response to a test security breach. Reactive solutions can have a significant deterrent effect, but only if the scope and effectiveness of those solutions are broadly communicated.

Security Incident Response Plan

A plan that dictates what actions need to be taken when a testing irregularity occurs.

Security Plan/Handbook

A written, living document that discusses how you and your team will address test security.

The Test Security Process

A series of actions revolving around the prevention, deterrence, detection, and reaction to test security threats. All testing programs should implement the test security process in order to mitigate risk and provide the best form of protection for their tests.

THE IMPORTANCE OF PLANNING WITH SECURITY IN MIND



JOHN FREMER

Dr. John Fremer is a Founder of Caveon Test Security where he serves as President of Consulting Services. With more than 50 years of experience in the field, he has served as President of the Association of Test Publishers (ATP), The National Council on Measurement in Education (NCME), and the Association for Assessment in Counseling (AAC). John received the 2007 ATP Award for Contributions to Measurement. He served as editor for the NCME journal Educational Measurement: Issues and Practice and is the co-editor to the Handbook of Test Security (2013).

How do you protect and defend something that is important to you? If you're an educator, test administrator, proctor, or certification manager, you want to protect and defend the validity of your test scores against the efforts of wildly motivated, tenacious, creative, and skilled cheats and thieves.

Though many test programs have been surprised by test security threats they were ill-prepared to defend against, we have seen programs emerge as winners against these wily dangers with meticulous protective planning and execution.

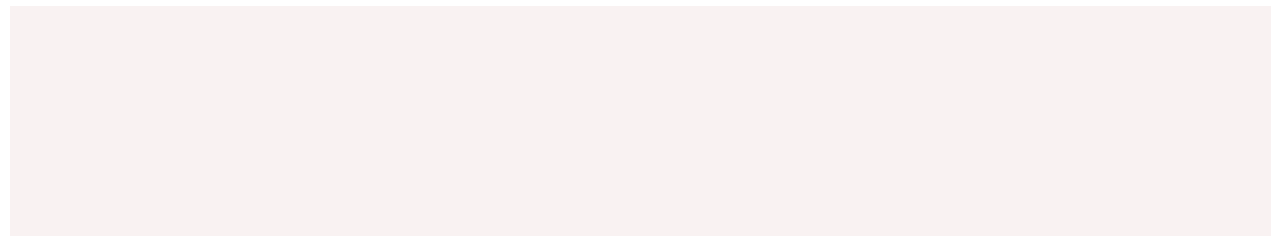
It all starts with a comprehensive game plan. Through security planning, testing program managers can come to understand the strengths, tendencies, and habits of those who exploit test security weaknesses. Then, they can thwart the efforts of their adversaries.

But how do you go about creating and implementing a comprehensive Test Security Plan that counters test security threats?

Identify the Key Roles: Which team members and assets will you require to maximize the protection of your tests? (**See page 15.**) These roles should leverage the strengths of various members of your team while also mitigating their weaknesses. During security planning, we define and identify test security roles and responsibilities in order to maximize the effectiveness of the protection plan.

Plan for the Worst: In the real world, rarely does everything go exactly according to plan. The opposition seeks to foil the best-laid strategies and tactics. Defensive strategists understand the importance of Incident Planning, incorporating contingencies, flexibility, and adaptation. When tactics prove less successful, new tactics must be employed. By crafting reactions for every contingency you could imagine, testing professionals can confound the other team no matter what transpires. Despite best efforts, cheats and thieves make advances, so test program managers must prepare and invoke contingency plans of their own.

CRITICAL THINKING: What is the worst possible scenario your program could face due to a security breach? What reaction would this breach currently prompt from your team?



For a high-stakes assessment program, the Test Security Plan serves as a compilation of:

- The security safeguards in place
- The policies that guide the implementation of those safeguards
- The procedures to be applied in realizing that implementation
- The provisions for responding to threats to the security of the assessments.

The Test Security Plan should be a **resource** for all program staff and a **demonstration** of the program's due diligence in preserving test validity and serving the interests of its stakeholders. While there are clear industry-wide standards for test security, each Test Security Plan is unique to the organization that creates it.

BIG PICTURE QUESTIONS

Does your program document test security measures and breaches?
If the answer is no, why not? If yes, how?

Do you keep track of the various ways you communicate with stakeholders? How?

Do you have any deterrence measures already in place? If so, what else would you do, in an ideal world, to deter potential cheaters?

WHY DEVELOP A TEST SECURITY PLAN



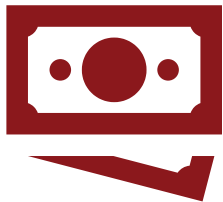
DEFENSIBILITY

A Test Security Plan is scientifically and legally defensible, which also makes it one of the most important tasks you can carry out for your program.



SECURITY

Another tool in your test security toolbox, a Test Security Plan allows you to calmly and confidently move forward when a security breach occurs.



INVESTMENT

A test security plan is a small incremental cost that protects your investment in your program's most important asset—the validity of your assessments.



TRAINING

Beyond helping prevent headaches in the event of a test security breach, a Test Security Plan helps guide staff training and overall efficiency throughout all the stages of your exam's life.



PREVENTION

Proven to decrease suspicious test taking, developing a Test Security Plan is one of the strongest preventative measures an assessment program can take.

5 TOPICS TO COVER DURING PLANNING

1

IMPLEMENT A FORMAL SECURITY PLAN OR HANDBOOK

While you may already have some or many of your security elements in place, it is important to develop a formal, living document that outlines your team's approach to test security. Make it available to stakeholders.

2

SECURE THE TEST DEVELOPMENT PROCESS

Research and establish best practices for test development as part of your test security plan. Include details about the security of the environment in which you develop your items, who you'll use as SMEs to write and review items, and the process you'll use to securely manage everything.

3

SECURE THE TEST ADMINISTRATION PROCESS

Research and establish best practices for test administration, including test taker identification processes; proctoring policies, training, and certification; and any monitoring that will take place before, during, or after testing.

4

APPOINT A SECURITY DIRECTOR

Appoint a Security Director who will be a resource and conduit for test security activities, from planning to execution and evaluation. Consider selecting your candidate from a pool of Certified Exam Security Professionals (CESPs).

5

CREATE A SECURITY INCIDENT RESPONSE PLAN

Your incident response plan dictates what to do when a testing irregularity occurs. It should create a consistent methodology for handling infractions and breaches, and establish protocols for penalties upon infraction.

KEY ROLES TO FILL ON YOUR TEAM

MANAGEMENT

Oversees overall test security efforts

WHO COULD PERFORM THIS ROLE ON YOUR TEAM?

BUDGETING

Takes care of budgeting and funding for security activities

WHO COULD PERFORM THIS ROLE ON YOUR TEAM?

ANALYSIS

Conducts or oversees statistical analyses for detecting irregularities

WHO COULD PERFORM THIS ROLE ON YOUR TEAM?

WEB PATROLLING

Monitors internet and social media for stolen test content

WHO COULD PERFORM THIS ROLE ON YOUR TEAM?

TRAINING

Responsible for staff training and awareness

WHO COULD PERFORM THIS ROLE ON YOUR TEAM?

INVESTIGATIONS

On the front lines of any irregularity investigation

WHO COULD PERFORM THIS ROLE ON YOUR TEAM?

SECURITY INCIDENT RESPONSE PLANNING

What steps need to be taken in order to implement the below components into your Test Security Plan?

COMPONENT	EXAMPLES	IMPLEMENTATION
Agreements	<ul style="list-style-type: none"> • Examinee/Candidate/Student agreements • Vendor agreements • Contractor agreements 	
Policies	<ul style="list-style-type: none"> • How will you handle a breach of those agreements? • What will be the response if examinees are caught with unauthorized technology? 	
Practices for analysis and monitoring	<ul style="list-style-type: none"> • Will you monitor remote test administrations? Will you monitor in-person testing? How? 	
Incident Response Matrix	<ul style="list-style-type: none"> • Match all types of incidents to the appropriate response (e.g., caught cheating = invalidation of the test, and examinee cannot retest for 6 months). 	

MODULE 1 • PART 4
SECURITY INCIDENT RESPONSE PLANNING

COMPONENT	EXAMPLES	IMPLEMENTATION
Investigative strategies	<ul style="list-style-type: none">• How will you conduct investigations? How will you know if and when they are necessary?	
Communications plan	<ul style="list-style-type: none">• What will be communicated? To whom? How soon?	
Training Plan	<ul style="list-style-type: none">• Who should receive training? What should the training entail?	



SAMPLE TEST SECURITY PLAN OUTLINE:

CERTIFICATION AND ADMISSIONS TESTING GROUPS

TEST SECURITY PROTECTIONS

GENERAL PROGRAM SECURITY MEASURES

TEST DEVELOPMENT SECURITY

SERVICE PROVIDER SECURITY

DATA SECURITY

THREAT DETECTION ACTIVITIES

DATA FORENSICS

WEB MONITORING

TEST ADMINISTRATION SECURITY ARRANGEMENTS

TEST ADMINISTRATION SECURITY ARRANGEMENTS

CANDIDATE TRAINING

TEST DELIVERY VENDOR SECURITY PROVISIONS

SECURITY INCIDENT RESPONSE PLAN (SIRP)

INCIDENT REPORTING

INCIDENT EVALUATION

MAKING THE RESPONSE DECISION

FORMAL INVESTIGATION OPTION

IMPOSITION OF SANCTIONS

ROOT CAUSE ANALYSIS

SAMPLE TEST SECURITY PLAN OUTLINE: STATES

INTRODUCTION AND OVERVIEW OF TEST SECURITY HANDBOOK

IMPORTANCE OF TEST SECURITY FOR STATES

OVERVIEW OF TEST SECURITY HANDBOOK

TEST SECURITY GOALS

BEST PRACTICES FOR TESTING SECURITY

SECURITY PLAN OVERVIEW

PREVENTION

TEST SECURITY MANAGEMENT

BUDGET AND FINANCE

TEST DEVELOPMENT AND MAINTENANCE

MAINTENANCE OF INTELLECTUAL PROPERTY
AND TEST-TAKER PRIVACY

USING EXISTING TRAINING OPPORTUNITIES

SECURE ITEM AND TEST DESIGN

CODES OF ETHICS

DETECTION

ASSESSMENT ADMINISTRATION TECHNOLOGY THREATS

WEB MONITORING

ASSESSMENT MONITORING PROCEDURES

TESTING IRREGULARITIES DETECTION ACTIVITIES:
STATISTICAL ANALYSIS

GUIDELINES FOR TEST SECURITY DETECTION ACTIVITIES

NOTES / BRAINSTORMING PAGE

TO-DO LIST

TASKS	PRIORITY	DUE DATE	
<hr/>	<hr/>	<hr/>	<input type="checkbox"/>
<hr/>	<hr/>	<hr/>	<input type="checkbox"/>
<hr/>	<hr/>	<hr/>	<input type="checkbox"/>
<hr/>	<hr/>	<hr/>	<input type="checkbox"/>
<hr/>	<hr/>	<hr/>	<input type="checkbox"/>

MODULE 2

PUBLICIZE YOUR SECURITY MEASURES

QUESTIONS YOU MAY HAVE

- How can you publicize your test security measures to protect your intellectual property? (Pages 25–28)
- How can you implement the key components of severity, certainty, and celerity into your Incident Response Matrix? (Page 29)
- What methods can you implement to discourage cheating and item theft before, during, and after your exam? (Page 30)

SECURITY PLAN TERMS AND CONCEPTS

Celerity

The swiftness of the response from a testing program to an offender when a test security breach occurs.

Certainty

The act of ensuring that a form of punishment takes place whenever a breach in test security has occurred.

Crisis Communication

The strategies a testing program has in place for responding to a test security breach, stopping the spread of inaccurate information, and next steps for keeping the program running smoothly.

Honor Code

A set of rules that examinees must agree to adhere to when taking a test. The rules represent the integrity that the institution expects its examinees to stand up to.

Non-disclosure Agreements

A legally-binding agreement that examinees sign promising they will not disclose any material seen on the exam.

Severity

The act of making a punishment harsh enough so that an examinee is fearful of receiving it.

PUBLICIZING YOUR TEST SECURITY MEASURES



ALISON FOSTER GREEN

As the Director of Marketing at Caveon Test Security, Alison utilizes tools such as digital marketing, public relations, and cutting-edge testing technology to promote the importance and value of test security. Having committed the last five years improving fairness in testing by ensuring that the validity of exams are not undermined by cheating and theft, Alison aims to enable people and institutions to understand the nuances of test security and empower them to act on their knowledge. She is a graduate of Middlebury College with an advanced degree from the London School of Economics.

Picture this: You're a business school candidate. You're about to take an exam that is built to predict your success in graduate school.

You know how important getting into business school is for your future, and you decide that the stakes are indeed high enough that you'd do anything within your power to ensure that you do well. You heard from a friend (who heard from a friend who heard from their cousin) that there's a website that hosts study materials for the exam. If you pay a small fee, you can even get your eyes on some live exam questions! It's risky, you know that. But you weren't the one who copied the exam questions. You're not the one selling them on the internet. And who really gets hurt here, anyway? It's possible that what you're doing is a crime, but even then, it's a victimless crime....

Right?

So you go to the site.

There, on the home page, you find a message. It appears the owner of the exam found this website before you did—they've taken the site down and posted a warning to all who may enter:

“We’re actively protecting our intellectual property. Move along.”

By now, you’re probably feeling sheepish. You weren’t trying to cheat! You didn’t realize that viewing stolen intellectual property might put your exam scores at risk. But it’s spelled out for you right on the home page—the people who’d stolen and used this content were punished. That could have been you!

What you’ve just witnessed was an example of deterrence. You’ve been reminded that cheating is wrong. You’ve been educated on the policies that the test owner has in place for punishing rule-breakers. Most importantly, you’ve been warned that if you attempted something similar, you’d likely not get away with it.

Okay, you can assume your own identity again. You may be wondering, what are some ways that I can introduce fraud deterrents into my own program?

Dictionary.com defines deterrence as “the act of discouraging an action or event through instilling doubt or fear of the consequences.” For the purpose of test security, the primary actions we seek to discourage are cheating and item theft. We do this by **instilling doubt** (“Can I really get away with this?”) and **establishing fear of the consequences** (“Is this really worth it if I get caught?”). Here are three methods you can use to deter wrongdoing:



Appeal to Moral Integrity

An example of a straightforward deterrent solution could be a sign at the front of the testing room that says “You know cheating is wrong. Don’t do it.” Simple. It reminds your test takers of the moral implications of cheating.

2

Educate About the Consequences

Educate your examinees about the sanctions your program has in place for fraudsters and violators of non-disclosure agreements. You can compound this strategy by requiring examinees to sign security oaths before taking the exam, simultaneously reminding test takers of your commitment to security and the potential consequences of violating that security.

3

Establish Doubt Through Publicity

Perhaps the most compelling way to deter potential wrongdoers is to establish doubt in the minds of would-be wrongdoers on whether they'd even benefit from attempting to cheat, let alone get away with it afterward.

Consider the previous example. The aspiring business student knew from reading the messages displayed on the formerly-fraudulent website that searching for live exam questions on this website was wrong (a moral appeal) and that you'd be punished and have your scores canceled if you broke the rules (an education-about-consequences deterrent). What truly stopped them from wrongdoing was the knowledge that the owner of this exam actively patrols the web. They learned that they wouldn't be able to get away with using exam-prep sources like this one. Even if they found a different source to buy your illicit test questions from, who's to say that website wouldn't be the next one on the security radar?

Don't be shy about the fact that you've implemented security features into your exams. Deter potential test fraudsters from stealing your intellectual property by telling them just how you detect and prevent fraud, and showing them that the likelihood of getting caught is high. By showing just how seriously you take your test security, you establish doubt that cheating efforts could be successful.

You should certainly appeal to your test takers' morality. You should also explain what consequences lie ahead for those who break the rules. But you should also make sure to maximize the security measures you already have in place by broadcasting them. Stop potential fraudsters in their tracks by making them doubt **a)** the relative benefit of attempting to cheat, and **b)** their own ability to get away with it. Send a message to all who need to hear it:

"We're actively protecting our intellectual property. **Move along.**"

WHAT DOES DETERRENCE LOOK LIKE?



Warning Labels



Fines and Sanctions



Supervision



Punishment for
Extreme Wrongdoing



Policies Posted to
Admonish Behavior



Security Screening to
Detect and Deter

3 COMPONENTS OF DETERRENCE

According to references on deterrence theory, effective deterrence involves three key components: Severity, Certainty, and Celerity (or swiftness of response). NOTE: These three factors of deterrence are only effective if they are relayed to test takers through deliberate, direct, effective communication by the testing organization.



SEVERITY

When building your incident response matrix, design your punishments to be harsh enough that an audience will be fearful of receiving them. This is a delicate balancing act. If punishment is too harsh, the audience may cry "foul" and protest. If the punishments are too lenient, they may not prevent test cheats and pirates from subverting your rules.



CERTAINTY

It is important to ensure that the prescribed punishment takes place whenever a misdeed is committed. Of course, in the world of test security, this is a lofty goal to achieve! However, if individuals realize that being caught is probable, and punishment always follows being caught, many may choose to stick to the rules.



CELERITY

The closer the punishment is to the misdeed, the greater the likelihood that other offenders will realize that rule-breaking is a mistake. When punishment is appropriately severe, certain, and swift, a test taker may carefully consider the possible gains against the consequences of fraud and be deterred from engaging in wrongful actions.

DETERRENCE TACTICS TO CONSIDER FOR YOUR PROGRAM

Here's a small sampling (by no means an exhaustive list) of deterrence tactics. Which tactics might benefit your program? What needs to be done to implement each task? Who on your team could head up each assignment?

IN THE TESTING SPACE

- ☐ Posters in the room
- ☐ Verbal announcements
- ☐ Messages about the security measures in place
- ☐ Proctors present

ON THE INTERNET

- ☐ Social media reminders
- ☐ Legal Disclaimers on website
- ☐ Email messages to candidates
- ☐ Web Patrol efforts

DURING REGISTRATION

- ☐ Pop-up during online registration
- ☐ Privacy policy during registration
- ☐ Honor code during registration
- ☐ Security message at testing sign-in

IMPLEMENTATION

[illegible]

WITHIN THE TEST

- ☐ Opening disclaimers
- ☐ Honor code agreement
- ☐ Non-disclosure agreement
- ☐ Proctors present

AFTER THE TEST

- ☐ Research the effectiveness of deterrent methods used
- ☐ Survey examinees & test administrators
- ☐ Conduct Data Forensics

GOT MORE IDEAS?

IMPLEMENTATION

[illegible]

NOTES / BRAINSTORMING PAGE

TO-DO LIST

TASKS	PRIORITY	DUE DATE	
			<input type="checkbox"/>
			<input type="checkbox"/>
			<input type="checkbox"/>
			<input type="checkbox"/>
			<input type="checkbox"/>

WHAT'S NEXT?

CONGRATS ON FINISHING PART 1!

Security Boot Camp Part 2:
Technology will explore the mechanics of secure testing. What threats face your program? What tools exist to mitigate them?

DOWNLOAD PART 2



Learn more over at
caveon.com