



# Test Security Policies and Procedures

---

The PED and Cognia™ classify security incidents into three categories: severe, moderate, and minor.

## Severe Irregularities

Security breaches, such as cheating or stealing test content, are events that pose a potential threat to the validity of the test. In addition, such incidents cause the loss of copyrighted assets and might result in the removal of the test item(s) from future testing. These breaches are considered SEVERE and may include but are not limited to:

- Student intentionally uses incorrect login (taking the test for someone else).
- Student copies answers or provides answers during testing.
- Students discuss test questions during breaks.
- Student accesses a cell phone, web browser, or recording device to find answers or to record test items.
- Student removes test materials from the testing room.
- Student or staff disseminates or discusses test content to others within school or district or via public forums (social media, websites) before, during, or after testing.
- Staff loses login information (printed tickets are missing) or a theft occurs of login information before testing.
- Staff provides students with materials or devices that are not allowed during testing.
- School or district staff coaches, provides answers, or modifies student responses.
- Staff resets a test to give student a second attempt at testing.
- Staff leaves room unsupervised during testing.
- Staff intentionally or unintentionally administers a secure test for practice.
- Unauthorized person(s) accesses online test content or student records.

If you need to have a test invalidated or you have evidence that test content has been made available outside of the test administration, call the New Mexico Help Desk immediately. Use the Testing Irregularity Reporting Form to report the incident within 24 hours.

## Moderate Irregularities

Serious misconduct before, during, or after testing might have high potential impact to individuals or groups who are testing. Such irregularities might affect student performance, test security, and validity. These irregularities are considered MODERATE and may include but are not limited to:

- Student unintentionally uses incorrect login.
- Student leaves the testing room without supervision or permission.
- Student moves ahead in test (session access codes provided by mistake).
- Staff provides incorrect accommodations for student.

- Staff intentionally provides session access codes before the appropriate time.
- Staff allows a test session to be tested over multiple days.
- Disruption of online access to testing system.

If a Moderate-level irregularity occurs that requires that the test be invalidated, use the Test Irregularity Reporting Form to contact Cognia within 24 hours of the occurrence.

## Minor Irregularities

Improper behavior or minor disruptions have low potential impact on individuals or groups who are testing, and they have low potential risk of affecting student performance, test security, or validity. These irregularities are considered MINOR and may include but are not limited to:

- Student arrives late.
- Student or staff makes distracting motions or sound while testing.
- Student is not focused on the test or constantly looking around.
- Student leaves the test due to illness.
- Student leaves an entire section or test blank.
- Student randomly marks answers on test or answers in a pattern.
- Student unintentionally submits test before completion.
- Staff gives incorrect instructions or deviates from the directions for administration.
- All students need to leave the room during testing (fire drill, emergency evacuation).

If a Minor irregularity occurs, the Test Coordinator and school staff can resolve the issue locally.

### General Guidance

Students and educators often wonder how far the rules on protecting test security extend. Clearly, broadcasting test item content and reading passages by posting on the web, using social media, or discussing them with colleagues or friends compromises test security. In addition, students and teachers may be aware of the main ideas of some test item content and reading passages before a test administration (e.g., by recalling a previous test administration). Cognia's position is that discussing the topic of a reading selection or the content of test items is most likely a security violation. Our advice is to avoid such discussions.

One exception may be family conversations, where parents may ask about their child's experience in taking the iMSSA. Here, general discussion of reading topics and the general nature of test items may be appropriate—as long as these general discussions do not extend beyond immediate family discussions.

# Protecting Data and Preventing Security Violations

Training can help avoid inadvertent test security threats and minimize the risk of intentional security breaches. Test coordinators are required to train all staff who administer and proctor the iMSSA to review essential information, including test security and ethics and roles/responsibilities. The *Test Administration Manual* identifies our requirements for all school personnel involved in test administrations.

For more information about testing roles and responsibilities, refer to the *Test Administration Manual*.

## Preventive Measures

Preventing test security violations may be the most important part of maintaining test integrity. The following table shows some common security incidents and ways to mitigate them.

Common Security Incidents	Preventive Measures
Disorderly testing sessions that can distract students and raise the risk of student cheating	Close familiarity with the iMSSA test administration and security policies and practices
	Rigorous training of all district and school staff involved in test administrations
	Promoting a culture of professional ethics and behavior in schools and throughout the school district
Exposure of secure test content, including test items, reading passages, etc., before, during, and after test administrations	Arranging online test administration locations that screen test content from viewing by anyone other than an examinee
	Identifying and training district and school staff who are responsible for protecting secure material
	Monitoring of testing sites and test administrations
Cheating during test administrations	Random and targeted observations of schools during testing and of test administration sessions

## Reporting Possible Test Irregularities and Security Violations

In the event of a security breach or infringement of its intellectual property, Cognia reserves the right to take appropriate action.

## Support

If you have questions regarding the security policies and procedures or need support throughout the irregularity reporting process, please contact the Cognia New Mexico Help Desk/Customer Care Center Team at 1-877-676-6722 or [nmtechsupport@cognia.org](mailto:nmtechsupport@cognia.org), or use the [live chat link](#) on the Help and Support Site.