

AOE Test Security Incident Procedure

Purpose

This document defines the criteria of test security incidents and describes the actions of the Vermont Agency of Education (AOE) and expected action of schools and districts when testing security incidents occur. This document is a supplement of the [Test Administration Manual](#) and the [Test Coordinator Manual](#).

Test Security Importance

The security of assessment instruments and the confidentiality of student information are vital to maintaining the validity, reliability, and fairness of the results. It is of primary importance to maintain the security of students' personally identifiable information for student safety and privacy. Protecting the security of the testing environment (including test items and other proprietary information) provides confidence in the assessment's accuracy and precision in measuring what students know and can do. Finally, protecting the security of the assessment itself limits both risk to students in Vermont as well as students across the country who may see the same items on their tests.

Test Security Incident Definitions

Any deviation in test administration is known as a test security incident. Test security incidents, such as improprieties, irregularities, and breaches, are behaviors prohibited either because they give a student an unfair advantage or because they compromise the security of the assessments. Whether intentional or by accident, failure to comply with security rules, either by staff or students, constitutes a test security incident. Improprieties, irregularities, and breaches need to be reported in accordance with the instructions in this section for each severity level. Definitions for test security incidents are provided in **Table 1 below (See also Table 9 on p. 21 of the [Test Coordinator Manual](#))**.

Table 1. Definitions for Test Security Incidents

Type	Definition
Impropriety	A test security incident that has a low impact on the individual or group of students who are testing and has a low risk of potentially affecting student performance on the test, test security, or test validity. These circumstances can be corrected and contained at the school level. An impropriety should be reported to the District Test Administrator (DA) and School Coordinator (SC) immediately and submitted in the Appeals module of TIDE, if student testing is impacted. Details regarding how and when to submit an appeal, and specific examples of Testing Improprieties can be found in Table 10 of the Test Coordinator Manual .

Irregularity	A test security incident that impacts an individual or group of students who are testing and may potentially affect student performance on the test, test security, or test validity. These circumstances can be corrected and contained at the school or district level and submitted in the online Appeals system for resolution. An irregularity must be reported to the DA and SC immediately and submitted in the Appeals module of TIDE, if student testing is impacted. Details regarding how and when to submit an appeal and specific examples of Testing Irregularities can be found in Table 10 of the Test Coordinator Manual .
Breach	A test security incident that poses a threat to the validity of the test. Examples may include such situations as a release of secure materials or a security/system risk. These circumstances have external implications for the Consortium and may result in a Consortium decision to remove the test item(s) from the available secure bank. A breach incident must be reported to the DA and SC immediately and entered in TIDE (should an appeal be required). Details regarding how and when to submit an appeal can be found in the Test Coordinator Manual .

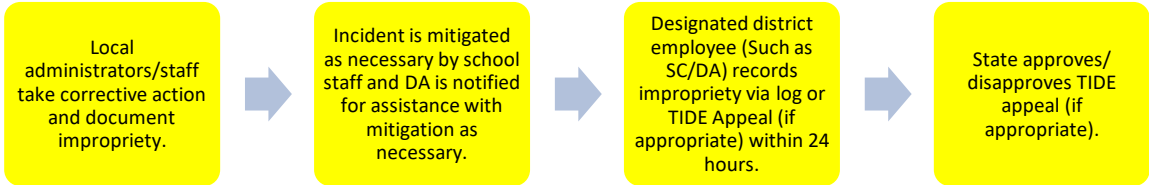
Note: The only security incidents that are reported in the Appeals system in TIDE are those that involve a student and test and that require an action for the test such as to reset, reopen, allow a grace period extension, restore, or invalidate a test that a student was taking at the time of the incident. TIDE does not serve as a log for all incidents.

Reporting Timelines and Action Steps

Improprieties

The test administrator must immediately report the incident to the school testing coordinator. The school testing coordinator will correct and contain the incident at the district/school or enter it in the Appeals module of TIDE, if student testing is impacted. Follow the steps in Section VII.II of the [Test Coordinator Manual](#) for Filing an Appeal in TIDE.

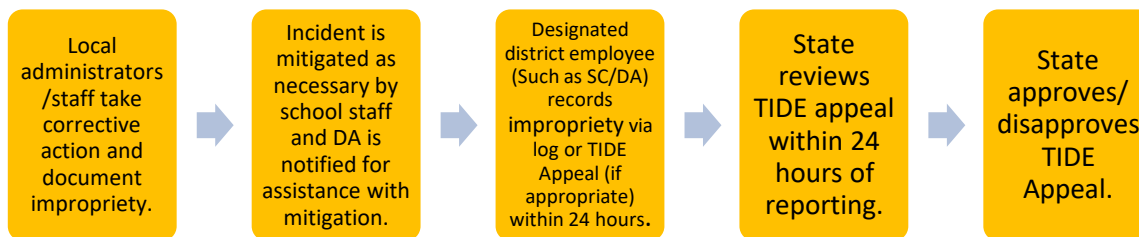
Figure 1. Improprieties Communication Flow



Irregularities

The Test Administrator must immediately report the incident to the District Test Administrator/School Coordinator (DA/SC). The DA/SC will submit the incident in the Appeals module of TIDE (if appropriate) by the end of the day of the incident. Follow the steps in Section VII.II of the [Test Coordinator Manual](#) for Filing an Appeal in TIDE for information on submitting an appeal.

Figure 2. Irregularities Communication Flow



Breaches

Breaches include test security incidents that pose a threat to the validity of the test. Breaches require immediate attention and escalation to AOE. Examples may include such situations as exposure of secure materials or a repeatable security/system risk (e.g., administrators modifying student answers; test items shared in social media). These circumstances have external implications that may impact students across VT and other states that share test items with VT. The Test Administrator must immediately report a breach to the District Test Administrator/School Coordinator. The DA must report the incident to the AOE (AOE.statewideassessment@vermont.gov) along with a written report documenting all pertinent details. (e.g., details of breach, specific test, date and time, TA, school, and number of students involved)

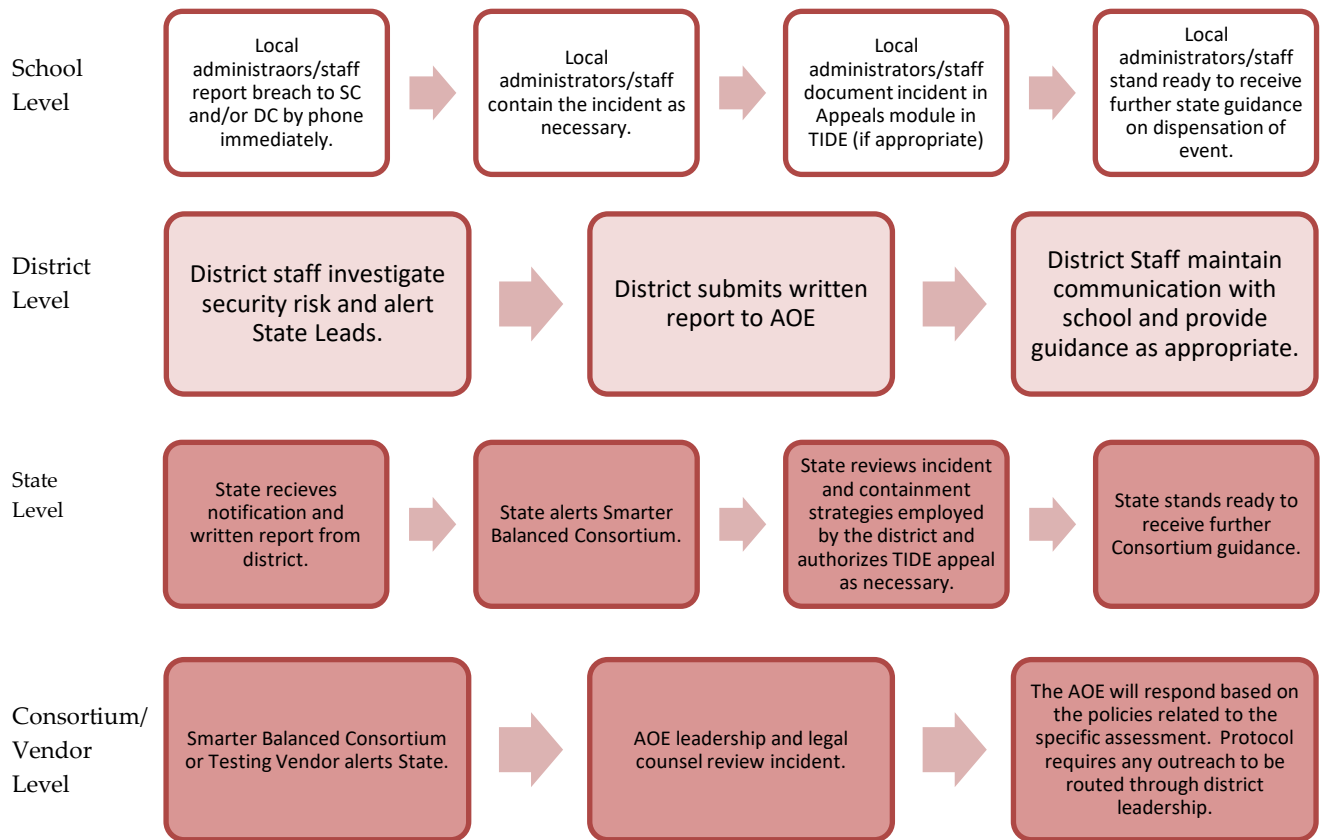
The AOE may instruct the DA to submit the incident through the Appeals module of TIDE.

If a test vendor notifies the AOE of a breach:

1. The AOE will communicate with the vendor to understand the details of the breach.
2. The Assessment Team will alert AOE leadership and legal counsel to determine the necessary course of action.
3. The AOE will alert the impacted district and follow through on any steps required by test vendors.

Please see Appendix H: Test Security Chart in the [Test Coordinator Manual](#) for a list of test security incident levels and examples of types of issues.

Figure 3. Breach Communication Flow



AOE Response

Violation of test security is a serious matter with far-reaching consequences. Breaches of test security include, but are not limited to, copying of test materials, sharing test materials, sharing test materials publicly (including social media,) failing to return test materials, coaching students, giving students answers, and/or changing students’ answers. Such acts may lead to the invalidation of an entire school district’s student test scores, disruption of the test system statewide and nationally, and legal action against the individual(s) committing the breach including revocation of the individual’s license to teach in Vermont.

A breach of test security, if initiated by an educator or administrator, may constitute a violation of the Code of Professional Responsibility for Teachers, as well as a violation of other pertinent state and federal law and regulation. In certain cases, security breaches could jeopardize licensure for certified and administrative staff. The AOE will investigate all such matters and pursue appropriate follow-up action. (See [Test Coordinator Manual p. 2](#))