Hawaiʻi State Department of Education

Test Security Handbook

v3.2
November 2, 2018

Table of Contents

Scope

Contents of the *Hawai'i Test Security Handbook* pertain to all federally-mandated tests administered through the Hawai'i Department of Education. As of 2017, these tests include:

- Smarter Balanced Assessments (SBA)
  - English / Language Arts: Grades 3-8, 11
  - Mathematics: Grades 3-8, 11
- Hawai'i State Alternate Assessments (HSA-Alt)
  - English / Language Arts: Grades 3-8, 11
  - Mathematics: Grades 3-8, 11
  - Science: Grades 4, 8, 11
- Access for ELLs 2.0
  - Listening, Reading, Speaking, Writing: K-12
- Alternate ACCESS
  - Listening, Reading, Speaking, Writing: K-12
- Hawai'i State Science Assessments (HSA)
  - Science: Grades 4, 8
- End of Course Exams (EOC)
  - Biology I: High school students at conclusion mandatory core course
- KĀ'EO for Hawaiian language immersion students
  - Language Arts: Grades 3, 4
  - Mathematics: Grades 3, 4
  - Science: Grade 4

Descriptions and updates to these mandatory exams and their population parameters are available through the Department's annual memo entitled "*Hawai'i Statewide Assessment Program."* (Appendix D.10) The memo is released annually during the preceding summer.

Contents and Organization of HIDOE Test Security Manual

The main purpose of this Manual is to provide a central source and repository for all information related to test security in the state. The contents provide information for preventing and detecting irregularities on state assessments, such as cheating and test piracy, and for following up on suspected or confirmed examples of improper or unethical testing behavior by either students or test administration staff. .

The Manual is structured similarly to the recent report from the Technical Issues in Large-Scale Assessment (TILSA) report, *Preventing, Detecting, and Investigating Test Security Irregularities: A Comprehensive Guidebook on Test Security for States* (Olson & Fremer, 2013). It focuses on three key aspects of test security: prevention, detection, and follow-up activities.

1. Prevention – Standards for the test security aspects of the design, development, and operation of state assessment programs, for both multiple

choice response and performance measures, along with state policies and procedures that support implementation of the standards.

2. Detection – Guidelines and approaches for planning, implementing, and interpreting data forensics analyses, web monitoring, and the identification of possible test irregularities.

3. Follow-Up Consultation on Irregularities – Strategies for planning and conducting consultation activities and actions that the state may need to take based on findings from inquiries on testing irregularities.

This Security Manual includes definitions, policies, and procedures for the regulation of all aspects of test security, including information security, item/test development and design, assessment publication and assessment administration. In many cases, these policies and procedures represent operational security goals that are already in different stages of implementation by the HIDOE. The Security Manual provides documentation and actionable objectives. It can serve as a resource in renegotiating vendor contracts or restructuring operational aspects of the program.

Among other things, the elements of this Manual are intended to provide greater protection of HIDOE intellectual property, reduce test fraud and theft, and to maintain program standards and integrity. The Manual may also be used to train staff and as a reference to structure security roles, responsibilities, and performance expectations.

The Test Security Manual sets forth test security policies, procedures, and responsibilities for the Hawai'i State Department of Education (HIDOE). Internal policy and procedures documents included in a Caveon Test Security Audit (draft report issued January 7, 2015) are referenced in the compilation of this Manual. Note that many of the procedures described in this Manual are already in place, whereas others are recommended for consideration.

This Test Security Manual has been approved by the Administrator of the Assessment Section of the HIDOE and will be reviewed and revised no less than annually.

In summary**,** the test security manual provides:

- A flexible means to document the most critical processes related to test security activities of the HIDOE
- An electronic document usable in training based partially on the results of the security audit and further review of HIDOE documents
- A summary of state practices in the areas of prevention, detection, and consultation activities
- A single, comprehensive source defining procedures, processes, and regulations, including the escalation path to be followed in the event of a test security inquiry
- A historical document that can be built upon and expanded over the course of each assessment year that includes information on any audits, forensics

analyses, web patrol findings, or follow up inquiries that have been conducted in the state

Introduction and Overview

Importance of Test Security

The primary goal of test security is to protect the integrity of the assessment and to assure that results are accurate and meaningful. To ensure that trends in achievement results can be calculated across years in order to provide longitudinal data, a certain number of test questions must be repeated from year to year. If any of these questions are made public, the validity of the test may be compromised. If the reliability or validity of a test is compromised, the test scores of individual students or entire classes may be invalidated, and disciplinary actions may be taken.

Appropriate testing practices are not always universally understood or followed. Good testing practices are sometimes violated because the individual involved is not informed about what is appropriate for a standardized assessment administration. To help school staff securely administer the state assessment and have a common understanding of what practices are appropriate, the Hawai'i Department of Education (HIDOE) has prepared these guidelines.

Overview of Test Security Manual

This Test Security Manual focuses on best practice and guidelines for three main assessment integrity themes: prevention, detection, and follow-up consultation activities for inquiries of testing irregularities. Discussion and details of practices within these three themes include the following:

- Prevention
    - State policies and practices for test security
    - Standards for test integrity and the security aspects of the design, development, operation, and administration of state assessments to prevent irregularities from occurring.
- Detection
    - Guidelines for activities to detect possible testing irregularities
    - Monitoring, analysis, and reporting activities related to the security of the state assessment
- Follow-Up Consultation on Irregularities
    - Guidelines for the state, complex areas, and schools to work together on follow ups to testing irregularities
    - Remediation of irregularities to ensure valid results for all students

Test administration practices are subject to this ultimate question: Do all test administration procedures prior to, during, and after the test administration, lead to

student results that accurately reflect a valid and reliable measure of each student's unique and true educational knowledge, skills and abilities?

Dr. Greg Cizek in a recent NCME whitepaper on test integrity noted that following these guidelines will help ensure that all students have equal opportunities to show their knowledge, skills, and abilities. Educators, students, parents, school boards, legislators, researchers, and the public must have confidence that psychometrically-sound testing, scoring, and reporting will be handled ethically and in accordance with the best administrative practices.[1]

State assessments are an important and required tool used to monitor student achievement results; for assessments to yield fair and accurate results, they must be administered under the same standardized conditions to all students.
This document represents the expected professional conduct of all educators who administer state assessments. It is intended to be used by the HIDOE, its complex areas and schools, in the fair and appropriate administration of state assessments.

The best way to promote appropriate test administration practices is to ensure that teachers and administrators understand and recognize acceptable and unacceptable practices. While this document's primary purpose is for state-level administration, at its discretion, state-level HIDOE may consider sharing portions of this manual with complex areas and schools.

Test Security Goals for State Assessment

1. Provide secure assessments that result in valid and reliable scores
2. Adhere to high professional test administration standards
3. Maintain consistency across all testing occasions and sites (i.e., schools)
4. Protect the investments of resources, time and energy

Best Testing Practices for Security

The following is a compilation of best testing practices as they relate to test security. These testing practices should be used in determining whether or not a practice is consistent with the principles of performing one's duties with honesty, integrity, due care, and fairness to all. Following these practices will also ensure the integrity of the assessment process and the reliability and validity of any inference made from assessment results.

Schools must ensure that appropriate staff have training and knowledge of appropriate assessment practices; they must monitor staff practices to ensure compliance. As part of training, school duties should include the following:

[1] Based on the National Council on Measurement in Education Test and Data Integrity Document, Oct. 2012

Training:

- In writing, no less than once annually, define the standard of what constitutes an unethical or inappropriate practice.
- In writing, no less than once annually, define how test security standards will be monitored, under what circumstances sanctions apply, and what those sanctions are.
- In writing, no less than once annually, define security procedures as they relate to testing. Highlight changes and additions made since the previous communication.
- Insure that testing program personnel participate in test security training and are properly instructed.
- Require each test coordinator (TC) to complete the required assessment and security trainings and sign a Confidentiality Agreement. File these agreements with HIDOE.
- Require principals and school test coordinators to complete all required assessment trainings and sign a Principal or Test Coordinator Confidentiality Agreement. File these agreements with HIDOE annually.
- Require individuals who administer, handle, or have access to secure test materials at the school to complete each required assessment's training as appropriate: have them sign a Test Administrator's/Proctor's/Scribe's Confidentiality Agreement. File these agreements in the appropriate office each year.
- In writing, define what materials and practices are allowable for assessment preparation; communicate these procedures, materials, and practices at least once annually to all appropriate staff.
- Prohibit all personnel without sufficient and appropriate knowledge, skills, or training from administering an assessment.

Assessment Preparation:

- Prohibit teachers from preparation practices enacted solely for the result of raising scores or performance levels on assessments: where the intent is score-driven and absent standard curriculum protocol.
- Prohibit the use of questions, tasks, graphs, charts, passages, or other material included in an assessment where that material is the same as, paraphrased or overly similar in content to what is in the assessment.

Assessment Administration:

- Within the test environment, remove or cover all displays related to assessment content prior to the administration of the state test.
- Prohibit staff from prompting or assisting students in any manner with their answers.
- Secure prohibited electronic devices, including cell phones, during testing.
- Require students to follow the testing guidelines in the Test Administration Manual (TAM) on use of calculators.
- Administer tests only during the testing window established by the HIDOE.

- Require test administrators and proctors of standardized tests to rigorously follow the appropriate administrative procedures as directed in the TAM(s).
- Ensure that all test administrators and proctors strive to create a positive testing environment.
- Limit assistance by test administrators and proctors to only those issues concerning the mechanical aspects of marking answers, clarifying directions, and finding the right place on answer sheets or recording answers via an electronic device.
- Prohibit test administrators and proctors from indicating answers, pointing out the rationale of an item, or prompting students in any manner.
- During test administration, walk around unobtrusively to ensure appropriate test-taking test security measures are followed.
- Provide students with only the references or tools specifically designated for the test.
- Provide accommodations, as appropriate, for students with Individual Education Programs (IEPs), Section 504 Plans, or for English Language Learners (ELL).
- With the exception of allowable accommodations, designated supports, or administrative considerations, prohibit nonstandard changes for administering the assessment.

- During or immediately preceding testing, prohibit actions aiding a student in the assessment; such actions including the use of a gesture, facial expression, body language, language, or any other action or sound that may guide a student's response.
- Do not provide to a student any definition or clarification of the meaning of a word or term contained in an assessment, other than that specified in the TAM.
- Administer state assessments as prescribed in the TAM and/or the Test Coordinator's Guide by the appropriate grade and subject.
- Supervise students at all times during testing sessions.

Overall Assessment Security:

- Schools shall cooperate with HIDOE and others in conducting an inquiry of any alleged inappropriate assessment practice.
- Potential test security violations must be reported to the test coordinator who will determine whether HIDOE's Assessment Section needs to be contacted; Reportable issues include: missing materials, testing misadministration, copyright infringement, and other deviations from acceptable security requirements.
- When contacting the Assessment Branch, the TC will first complete the "Testing Incident Report Form" found in the appendix of this manual.
- Ensure that no one compromises test security or the accuracy of the test data (score) results by manipulating the test administration, demographic data, or the students' answers.
- Ensure that student test scores and test performance are not disclosed to any unauthorized person.
- Encourage community members to voice any concern about any test administration practice that they may consider inappropriate by contacting the Assessment Section.
- Follow written procedures on complaints, allegations, or concerns on inappropriate practices. These procedures ensure the protection of individuals' rights, the integrity of an assessment, and the integrity of assessment results.
- Prohibit the use of any assessment for purposes other than that for which it was intended.

Physical Security:

- Secure state assessment materials prior to, during, and following each test administration; prohibit unauthorized access to secure test questions at all times.
- Store physical test materials in a locked and secured central location by the TC in accordance with directions in the TAM.
- Prohibit students from having access to secure test questions or answer keys.
- Prohibit any form of cheating.
- Ensure that no secure test materials, test questions, or student responses are retained, reproduced, paraphrased, or discussed in any manner.
- Return all secure test materials to the state's assessment vendor (AIR) following the procedures outlined in the TAM. Establish and implement procedures to

ensure maximum test security and limit access of secure materials to authorized personnel only.
- Before each test administration, materials must be distributed and stored according to instructions provided with the test. Tests must be secured at all times during test administration, including all breaks in the testing sequence. All test booklets (used and unused) and answer sheets, if applicable, must be counted, reconciled, and returned to a centrally located, locked, and secured area immediately upon the completion of each daily testing session.

School Administration Violations:

- Engaging in or aiding others in inappropriate preparation activities.
- Engaging in or aiding others in inappropriate test-taking practices.
- Correcting or altering any student's test response during or following the administration of an assessment.
- Excluding students from an assessment because a student has not performed well, may not perform well, or because the aggregate performance of a group may be affected.
- Any practice that results in a potential conflict of interest or exerts an undue influence on a person administering or scoring an assessment.
- Any practice that either makes, or appears to make, an assessment process unfair.

Consequences of Test Security Violations

Administrators, certified and non-certified school staff, students, and parents must adhere to all best testing practices. Consequences of violations may include the invalidation of student test results and liability for copyright infringement. Disciplinary measures for educators and school staff may be determined at an employment level based on a school board's policy and the severity of the test security violations. Examples might include a written reprimand, suspension, or termination of contract. The HIDOE may also pursue its own sanctions of department-licensed individuals for testing irregularities.

Invalidation of test results for individual students or groups of students may have multiple consequences, including:

- Parents will not receive scores on their child's report.
- Public reporting will reflect all invalidated tests as "not tested." This may reduce the percentage of students meeting proficiency.
- Schools may have a more difficult time meeting adequate progress requirements.

Hawai'i Policies and Practices on Maintaining Security for the State Assessments

HIDOE continues to issue strong statements on test security policies and practices through its numerous training sessions.

"The security of assessment instruments and the confidentiality of student information are vital to maintaining the integrity of the assessments and the reliability of the results. Due to the importance of test security for all of the Hawai'i Department of Education's statewide student assessments"

1. Test security audits are routinely carried out to ensure that the current processes and procedures reflect best practices.
2. Quality Assurance visits are conducted in order to ensure communication consistent with current test security policy. Hawaii's next visit -- which includes external observation for impartiality -- takes place in October, 2018
3. Student scoring patterns are electronically monitored throughout the testing windows to identify and detect possible cheating and other irregularities. Consultation with the principal and test coordinator will take place as necessary when potential problems are identified.
4. Teams conduct on-site monitoring of schools at various times during testing windows to verify adherence to test administration procedures and provision of appropriate test accommodations, designated supports, and administrative considerations for identified students.
5. Web monitoring of social networking sites and other online venues has been activated to identify potential testing breaches.

The list of statewide school communication on test security includes:

- HIDOE Test Security Plan: Test Security Policy and Associated Procedures
- Maintaining Security and Understanding the Consequences
- Examples of Cheating / Inappropriate Behavior Scenarios Related to Statewide Student Assessments that Require Students' Scores to be Invalidated (memo dated 6/10/13)
- Testing Incident Report Form (document with reporting form)
- Policies: Student Confidentiality and Assessment
- Preventing Student Cell Phone Access during Testing
- Test Environment and Security
- SBAC State Smart Sheet for Operational Testing
- *SBAC State Procedures Manual—Item Risk Rubric:* Smarter Balanced Item Exposure Risk Analysis

Copies are provided in the appendix.

Test Security Standards and Guidelines

The HIDOE develops assessments and establishes professional conduct standards as related to test security which are based upon the following professional standards, guidelines and laws:

Standards for Educational and Psychological Testing. (2014). American Educational Research Association (AERA), American Psychological Association (APA), and National Council on Measurement in Education (NCME)

Operational best practices for statewide large-scale assessment programs. (2014). Council of Chief State School Officers (CCSSO) and Association of Test Publishers (ATP).

Technical Issues in Large-Scale Assessments (TILSA) Test Security Guidebook: Preventing, Detecting, and Investigating Test Security Irregularities. (2013). John F. Olson and John Fremer, CCSSO.

Family Education and Privacy Rights Act (FERPA). (1997). Code of Federal Regulations – Title 34, Volume 1, Parts 1 to 299.

National Council on Measurement in Education Test and Data Integrity Document (Oct. 2012)

Caveon™Test Security. (2015). *Test Security Standards. A*uthor.

Section I. Prevention

This section addresses policies, procedures, and standards for assessment integrity and security aspects of the design, development, operation, and administration of state assessments. In order to prevent test compromises, breaches, invalid administrations, or other irregularities from occurring, the following activities are required:

- Review of all state policies, procedures, and protocol related to test security.
- Provide integrity and security training to all staff, both when they move into jobs and then periodically to be sure they are current on security policies and procedures.
- Assign explicit responsibility for test security and monitor the effectiveness of the efforts.
- Implementation of a variety of well planned activities by the HIDOE to prevent irregularities.
- Adhere to the testing administration windows and testing schedules.
- Adhere to all test administration rules and policies.
    - Devote as much attention as possible to prevention.
    - Follow rules to discourage student or Test Administrator prohibited behavior.

Test Administration Manual

In 2015, Hawai'i began administering the Smarter Balanced Assessment Consortium (SBAC) as its new summative tests. HIDOE has adapted and is using much of the information provided by SBAC to its member states on test administration procedures.

The annual online *Smarter Balanced Summative Test Administration Manual* (TAM) is the key document used in preparing for and administering the SBAC assessments. Test security information is included in the TAM. For example, information on key responsibilities is provided on User Roles in the Online Testing System for staff listed below.

- Principal
- Test Coordinator (TC)
- Test Administrator (TA)
- Teacher (TE)

In addition, checklists for the first three groups listed here are provided in the appropriate TAM appendices. Note that the use of these checklists is a school decision.

Information is provided in the TAM on those "Personnel Who May Serve as Test Administrators" and the related requirements for administering the assessment, as follows:

- General Education Teacher
- Special Education Teacher
- School Counselor
- Instructor in content areas where there is a shortage
- Long-term substitute teacher
- Identified public charter school employees
- Test Coordinator

Additional information is included in the TAM on “Ensuring Test Security”. It is important that all summative test items and test materials are secured and must be appropriately handled, since secure handling protects the integrity, validity, and confidentiality of assessment items, prompts, and student information. Any deviation in test administration must be reported as a test security incident to ensure the validity of the assessment results.

This section of the TAM goes on to emphasize that the security of assessment instruments and the confidentiality of student information are vital to maintaining the validity, reliability, and fairness of the results. All summative test items and test materials are secure and must be appropriately handled. Secure handling protects the integrity, validity, and confidentiality of assessment items, prompts, and student information. Any deviation in test administration must be reported as a test security incident to ensure the validity of the assessment results.

Security of the Test Environment is also described in Table 6 of the TAM, where it describes security requirements for the test environment before, during, and after testing. The test environment refers to all aspects of the testing situation while students are testing and includes what a student can see, hear, or access (including access via technology). TAs and TCs or other individuals who have witnessed, been informed of, or suspect the possibility of a test security incident that could potentially affect the integrity of the assessments or the data should follow the steps outlined in the section *Responding to Testing Improprieties, Irregularities, and Breaches* in the TAM.

Definitions for Test Security Incidents

HIDOE uses the following definitions from SBAC to categorize security incidents and rate them on their level of severity. Details are provided in the TAM. More details are provided in the appendix.

Impropriety (Low Severity)

An unusual circumstance 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 state level and do not need to be reported to the Consortium.

Examples of various incidents are provided:

- Student(s) making distracting gestures/sounds or talking during the test session that creates a disruption in the test session for other students.
- Student(s) leave the test room without authorization.
- Administrator or Coordinator leaving related instructional materials on the walls in the testing room.

Irregularity (Medium Severity)

An unusual circumstance 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 state level and do not need to be reported to the Consortium.

Examples of irregularities are given:

- Student(s) cheating or providing answers to each other, including passing notes, giving help to other students during testing, or using hand-held electronic devices to exchange information.
- Student(s) accessing the Internet or any unauthorized software or applications during a testing event.
- Student(s) accessing or using unauthorized electronic equipment (e.g., cell phones, PDAs, iPods, or electronic translators) during testing.

Breach (High Severity)

An event 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.

Finally, several examples of breaches are described:

- Administrator or Coordinator modifying student responses or records at any time.
- Adult or student posting items or test materials on social media (Twitter, Facebook, etc.).
- Adult or student copying, discussing, or otherwise retaining test items, reading passages, writing prompts, or answers for any reason. This includes the use of photocopiers or digital, electronic, or manual devices to record or communicate a test item.

HIDOE Test Security Memorandum

In a memo from the HIDOE issued in 2014, a section titled *"Consequences for Students and School Staff Who Use Electronic Devices to Breach the Security of Any Test Item*

Included in a Statewide Student Assessments" was shared with schools. This policy is currently still in effect. A copy of this memo is provided in the appendix. The memo provides the following information regarding the administration of the tests. It states that "Due to the importance of test security for all of the statewide assessments, any school that has a student or staff member who uses an electronic device which results in the breach of a test item will be subject to the following actions/consequences:

1. The involved student's incomplete test or complete test that has been scored will be invalidated by the Department of Education's Student Assessment Section.
2. The school administration will be responsible for determining the consequences for the involved student per the Hawai'i Administrative Rules, Title 8, Chapter 19 and/or the consequences for the involved certificated or classified staff member per the Office of Human Resources procedures.
3. The school administration and test coordinator must retrain the staff regarding the test security requirements for all statewide assessments during a face-to-face meeting.
4. The test administrator who was conducting the test session when an electronic device was used by one or more students or a staff member will be required to retake the Test Administrator Certification Course in order to administer any additional assessments to students.
5. The school will be required to have a second adult present in the testing room with the test administrator who was conducting the test session when the electronic device was used to breach the security of one or more test items during each subsequent test session for the remainder of the current school year.
6. The school will be required to pay for the cost of each test item that was posted on a social networking site which required its removal from the current online, adaptive item bank.
7. The school must submit its detailed testing schedule that includes the date, time, and student seating chart for each test session for all statewide assessments administered during the remainder of the current school year and the next school year.
8. Unannounced site monitoring by the Complex Area Superintendent's identified staff and the Assessment Section's staff or designees as determined by [the Superintendent] may extend beyond one school year."

HIDOE has reinforced the message contained in this memo in its interactions with complex areas and schools. This is a strong message that shows the seriousness that is being taken regarding test security.

HIDOE Letter on Test Security Policy and Associated Procedures

A letter that was issued in 2014 to schools and Complex Areas from the HIDOE on Test Security Policy and Associated Procedures is provided in Appendix D. It provides very good context and a summary on why the security of assessment instruments and the

confidentiality of student information are vital to maintaining the validity, reliability, and fairness of the results. It also provides more details on the levels of severity that were described above.

In the letter, HIDOE states that "All test items and test materials are secure and must be appropriately handled. Secure handling protects the integrity, validity, and confidentiality of assessment items, prompts, and student information. Any deviation in test administration must be reported as a test security incident to ensure the validity of the assessment results. Failure to honor security severely jeopardizes student information and/or puts the operational test at risk.

Everyone who administers or proctors the online Smarter Balanced English Language Arts or Mathematics Field Test is responsible for understanding the test security procedures for administering the field tests. Test security incidents, such as improprieties, irregularities, and breaches, are behaviors prohibited during the field test administration, either because they give a student an unfair advantage or because they compromise the secure administration of the field test items. Whether intentional or by accident, failure to comply with test 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 provided in the Smarter Balanced Online Field Test Administration Manual."

Guidance on Test Security Activities related to Prevention

For the State of Hawai'i to administer a secure assessment program, many areas need to be addressed in its planning and implementation. These areas include managing the program, budgeting for the work, item and test development, and administering the state assessment. In the following parts of this section of the HIDOE Test Security Manual, a summary of activities is provided that need to be done to maintain security in the following areas:

- Management:
- Budgets
- Assessment Development
- Maintenance of Intellectual Property
- Secure Item and Test Design
- Administration of the Assessment

Test Security Management:

1. Management. An individual (the Security Coordinator) will be responsible for the overall leadership and management of the Hawai'i test security program set forth in this Manual, under the leadership of the Administrator or Director of the Assessment Section.

a. Authority. The Security Coordinator with the approval of the Director will make final determinations regarding the application of these policies and procedures, and from time-to-time, will recommend appropriate changes to these policies and procedures as well as to the resources and legal requirements for test security.

b. Budget & Finance. It is recommended that an annual test security budget be prepared for the Director with supporting rationale and consistent with budgeted funds.

c. Reporting. Periodic scheduled reporting will provide information regarding security related activities, security incidents, security trends, and recommendations for change.

d. Coordination. To effectively implement test security across the entire state assessment program it is recommended that a Security Coordinator be appointed to oversee security objectives and activities with participating groups, including assessment development, operations, vendor management, legal counsel, investigations, and research.

e. Research. It is recommended that ongoing research be conducted related to the security policies and procedures in place focusing in part on:

    i. The effectiveness (and cost effectiveness) of existing security measures;

    ii. The identification of new or emerging security issues;

    iii. Maintenance of testing industry security standards;

    iv. The impact of security measures on existing and potential testing practices.

f. Compliance. The Coordinator should oversee compliance with these policies and procedures directly or indirectly with the following training and compliance responsibilities:

    i. Training. Develop appropriate training materials predicated on these policies and procedures as well as those in operation manuals and procedural documents. Provide regular test security training, including security responsibilities associated with each program regular staff position, to all personnel, contractors and suppliers involved in assessment development, assessment publication, assessment administration, and assessment data management.

ii. Alignment. Maintain the alignment of employee, contractor, vendor, and test taker pledges and agreements with these policies and procedures. Review all agreements annually to insure their alignment.

iii. Operations. Oversee assessment processes for compliance with these policies and procedures and make appropriate modifications to training materials and messages to address any identified shortcomings.

iv. Quality Assurance. Together with the test security vendor, establish a set of criteria to identify schools for quality assurance site visits. These site visits will include interviews with test coordinators, test administrators, and other members of the assessment team to assess familiarity and compliance with established security procedures.

v. Enforcement. Establish procedures for adjudicating alleged or suspected incidents of test fraud and theft, to include guidelines for determining the authenticity of an incident and the initiation of a formal investigation as specified in the Test Security Incident Response Plan described within this Manual.

g. Monitoring. The Department will continue to monitor assessment activity within the Department, at vendors and in schools, for evidence of test fraud, theft and distribution of test content either directly or indirectly. The statewide assessments that are subject to routine monitoring by HIDOE or Caveon are Smarter Balanced Summative Assessments, HSA-Alts, ACCESS for ELLs Online and Alternate ACCESS assessments, End-of-Course exams, HSA Science assessments, the ACT, and Kaiapuni Assessment of Educational Outcomes (KA'EO). The following strategies should be employed:

i. Testing. Monitoring of assessment administration activities for indications of test fraud and theft, including violations of assessment administration policies. Secure timely reports from the test delivery vendor and schools across the state, of irregularities during test administration.

ii. Distribution of Protected Assessment Content. Formal monitoring of "test prep" materials on the Internet and elsewhere for use of protected assessment content and coordinating appropriate enforcement measures with legal counsel.

iii. Vendor Performance. Monitoring of vendor compliance with contracted security responsibilities and preparation of reports on related findings and recommendations.

iv. Incident Investigation. Overseeing the investigation of alleged or suspected incidents of test fraud and theft.

2. Review Panel. It is recommended that the Director appoint an internal Review Panel, chaired by the Security Coordinator, to review all allegations of test fraud, theft, and violations of other policies and procedures and to make decisions regarding appropriate actions to be taken.

3. Interim Management. The Director should develop a plan for the interim distribution of test security management responsibilities to insure security functions are maintained without interruption.

Budget and Finance

1. Budget Preparation. It is recommended that the Security Coordinator prepare for the Director an annual test security budget that maintains and enhances existing security functions, responds to new threats, and invests in preventive measures.

2. Justification of Budget Request. The annual test security budget proposal should contain justifications for each of the major categories of proposed test security expenditure.

3. Return on Investment (ROI) Calculation : Using an approach similar to the "Caveon ROI Risk Calculator Model" (see Appendix B), estimations of the return on new and existing test security investments may be identified, at a minimum, for each of the following:

    a. The results of the Internet monitoring and other forms of test fraud and theft monitoring described in these policies and procedures;

    b. Avoidance of unplanned assessment redevelopment activities;

    c. Maintenance of program goodwill and reputation;

    d. The cost and frequency of security incident response;

    e. Confidence of stakeholders and others in the State assessment results.

4. Regular Security Expenditures. The annual test security budget should cover, at a minimum, funding the routine test security management, monitoring, and training activities ("Regular Security Activities") set forth in these policies and procedures without interruption, including;

    i. Maintenance of security management, monitoring and training activities;

    ii. Monitoring assessment administration security provided by School Test Coordinators and Test Administrators;

iii. Maintenance of routine security management, monitoring, and training activities of those who are engaged in assessment security;

iv. Analyzing examination data using Data Forensics.

5. Incident-Related Expenditures. The annual test security budget should include funds reasonably necessary to ensure that the HIDOE Assessment Section can respond to unforeseeable security issues and incidents in a manner consistent with these policies and procedures.

6. Security Upgrades. The annual test security budget should include appropriate funds to keep pace with program growth and emerging security issues.

7. Budget Review. The test security budget should be developed annually and reviewed for its adequacy in promoting and maintaining the test security goals set forth in this Security Manual.

Assessment Development

1. Oversight & Reporting

   Oversee the security of the assessment development process and provide periodic reports on the maintenance of security and the status of specified objectives.

2. Qualification of Personnel

   Prior to commencing work, all employees, vendors and contractors ("Assessment Development Personnel") involved in the development of assessments will be qualified as follows:

   a. Legal Agreements. In keeping with existing practice, all Assessment Development Personnel will be required to enter a legal agreement controlling the confidentiality of the assessment development process and materials, as well as HIDOE ownership of resulting assessment content and other materials.

   b. Review. The form of each agreement will be reviewed and approved by the State's legal counsel and maintained consistently without modification.

   c. Training. All Assessment Development Personnel should, at a minimum, undergo training regarding the elements of the security policies and procedures relevant to their roles and responsibilities, as follows:

      i. All new Assessment Development Personnel (including employees, contractors and Subject Matter Experts) will receive test security training

materials and opportunities for related instruction prior to commencing assessment development work;

ii. Security updates and related instruction will be provided to all personnel on an annual basis;

iii. At the discretion of HIDOE management, training outcomes may be verified by assessment.

3. Replacement Assessments

Attempts should be made to procure sufficient resources for assessment development to develop large item pools or alternate forms for computer based tests. This will permit prompt responses in the event of security compromises, with as little disruption as possible in testing activity.

4. Control & Monitoring of Materials

a. Electronic Material. The item authoring and banking systems and associated assessment development data should be hosted on a secure, password protected, server. The server should be located in a secure controlled area.

i. The assessment development software system should be capable of tracking access and modification of assessment materials including the time and identity of the individual responsible for the modification.

ii. Electronic access to secure materials should be monitored and modified as needed to limit access based on individual job responsibility (scope) and by project (duration).

iii. All modifications to assigned access rights should be individually approved by the responsible manager.

iv. Access passwords, other than those limited by project duration, should be modified on at least a three-month basis, and on the departure of a Program staff member.

b. Secure Areas. Ensure physical assessment security in all work areas. Where necessary, use electronic combination door locks allowing physical access by only those Program staff and facilities service personnel whose job responsibilities require access to the secure area as well as files, cabinets, and offices containing protected assessment material.

i. Monitor physical access to secure areas including access occurring after business hours, on weekend and holidays;

ii. Retain all keys and passwords in a secure location

iii. Transfer of Materials. All assessment development materials delivered to contractors and vendors will be transferred by secure, verifiable means along with appropriate confidentiality markings and reminders, and will be returned or destroyed by permanent erasure from computer systems or cross-shredding of hard-copy materials, upon the completion of work.

iv. Sensitive assessment materials and information, including assessment documents, item pools, and test taker databases and answer keys, will be transferred via secure file transfer protocol (SFTP) or via a bonded carrier with shipment tracking capabilities.

v. Sensitive assessment materials (e.g., assessment items) should not be included in or attached to e-mail messages.

vi. Employees, contractors, and vendors should inspect sensitive assessment materials upon receipt for errors and discrepancies that are indicative of tampering.

vii. Each employee, contractor, or vendor should be required to formally acknowledge that received assessment materials have been returned and destroyed upon completion of a project.

c. Consequences of Noncompliance. The HIDOE, working in concert with the State Attorney General's Office, should make clear in Test Security Policy guidelines and state statutes that failure to comply with these assessment material control policies and procedures could result in adverse employment or contract action, according to the terms and conditions set forth in the corresponding employment, contractor, or vendor agreements.

Maintenance of Intellectual Property & Test Taker Privacy

1. Intellectual Property. To ensure confidentiality and preserve the State's intellectual property rights in assessment items and forms, the Security Coordinator should ensure that the following precautions are observed:

   a. Personnel Agreements. All assessment development personnel and contractors should enter into an appropriate agreement assigning all proprietary rights and interests in assessment materials and information to HIDOE and prohibiting disclosure of assessment materials to any individual or organization unless expressly authorized.

   b. Teacher/Instructor, Test Administrator, and Test Coordinator Agreements. Individuals in schools and elsewhere providing assessment administration

and management services will enter into an agreement including binding commitments to:

i. Safeguard assessment materials and information;

ii. Adhere to all prescribed test administration procedures for all students, including the administration of approved testing

iii. Accommodations for special populations

iv. Manage security compromise incidents as directed;

v. Allow unannounced reviews of test security operations;

vi. Provide regular reports on all test security activities.

c. Other Precautions. In cooperation with legal counsel, intellectual property rights in assessment materials and information will be preserved as follows:

i. Copyright interests in active assessment items and forms should be registered by the HIDOE Assessment Section or the testing vendor with the U.S. Copyright Office using the “secure test” registration procedure prior to their release;

ii. Copyright notations should be prominently displayed in all assessment materials and information;

iii. Infringing uses of assessment materials and information should be monitored and vigorously opposed.

2. Test Taker Privacy. In the interest of maintaining test taker privacy, detailed assessment results as well as test taker identification and contact information:

a. Will be regarded as confidential protected assessment material and safeguarded in a way comparable to that of assessment content and development materials;

b. Will not be released or used in any manner inconsistent with standing test use agreements.

Secure Item and Test Design

1. Test and Item Design. A combination of item and test design strategies will be implemented to hamper efforts by instructors, test administration personnel, test takers (students) and others to memorize and later use or disclose sensitive assessment content, and to otherwise limit the effects of test exposure. HIDOE uses a CAT for its summative assessment, which is a good strategy for enhanced security, along with some of the following activities.

Sample strategies include:

a. Item Design

i. Creating large item pools for computer based testing or multiple forms for paper-based assessments.

ii. Requiring randomization of items and answer options during assessment delivery.

c. Test Design

i. Randomized presentation of equivalent items from two or more assessment forms

ii. Scrambling of items within CBT and paper and pencil forms.

2. Implementation

a. Ensure that the assessment delivery system:

i. Is capable of implementing the item and assessment design strategies set forth in this Section and is capable of accommodating future design strategies.

b. Establish item and assessment replacement processes for the:

i. Statistical detection of exposure effects on items and assessments.

ii. Rapid replacement of items and assessment forms when a security compromise is detected or when pre-established item/test exposure criteria are reached.

3. Evaluation. Item exposure analyses should be conducted at least quarterly to evaluate the effectiveness of the measures set forth in this Section for increasing test security and reducing item exposure. A report may be issued on the status of the findings.

4. Assessment Validation

a. To the extent possible, the excellent current practice should be continued of field testing items by "seeding" proposed items into active assessments or item pools. Test Takers may be informed that non-scored beta items will be included in the assessment, but not which items.

Administration of the Assessment

1. CBT/CAT Distribution. To insure the safety of secure assessment materials, the distribution path should be charted and monitored to confirm:

    a. That all secure data is encrypted to meet the established standards.

    b. That data transmission to the delivery vendor is performed through a secure data pathway.

    c. That the point of SFTP receipt is secured by the vendor to meet industry standards.

    d. That the transfer of the secure assessment data to the assessment delivery system is performed using secured data transmission pathways.

    e. That the encryption implemented at the time of release is maintained during all handling of the secure assessment data.

    f. That policies and procedures governing the above handling of the secure assessment data are in place internally and with the test delivery vendor.

2. Assessment Administration. To maintain consistently high levels of security surrounding the administration of assessments, administrative arrangements should meet the following requirements:

    a. Physical Security. Ensure that the physical conditions at testing locations facilitate secure testing, as follows:

        i. Provide sufficient space for test takers to be seated well apart from one another if there are not privacy panels between individual workspaces;

        ii. Maintain a seating chart of all individuals being tested for each session and make the seating chart available upon request;

        iii. Ensure that access to materials, computers, and testing information is disabled upon an employee leaving the Department;

        iv. Maintain all assessments, assessment results and test taker information in strict confidence, in secure systems and facilities.

    b. Assessment Proctoring

        i. Consistent with the division of responsibility between the state, complex areas, and schools, every effort should be made to

insure that test takers do not have access to bags/purses, books, papers, pagers, cell phones, calculators, or any electronic device that can be used to capture/record assessment content.

ii. Confirm that there is no information related to the assessment content that is visible on charts, posters, or other materials in the testing environment that might be sources for examination answers.

iii. Insure that students are continuously monitored throughout the assessment administration through the use of teachers or other qualified educational professionals. If a Test Administrator must leave the room, or is otherwise disengaged from the direct monitoring of test takers, a replacement Test Administrator should be assigned immediately so that students are never left un-proctored.

iv. Insure access to computer-based assessments is under strict control of the Test Administrator at all times. This includes all assessment related materials, examination access codes, and login information.

v. Confirm that every edition of the Test Coordinator's Guide and the Administrator Manual specifies assessment delivery and proctoring procedures with sufficient specificity to support a secure test administration environment.

3. Irregularity Reporting. In accordance with HIDOE test security policies, any variation from established procedures in the administration of the State assessments should be reported as soon as reasonably possible to the HIDOE Assessment Section by direct contact by local school personnel, typically a Test Coordinator or Test Administrator, or by the delivery vendor. This includes:

   a. Copies of Testing Incident Report Forms submitted by the Test Administrator addressing situations that could threaten the security of assessment data.

   b. Any suspicious activity, including, but not limited to test taker misconduct such as student disruptions, observations of answer-copying, discussing assessment questions with others, use of cell phones, and use of unauthorized materials, missing and lost or stolen assessment materials.

   c. Testing location disruptions, including but not limited to lapses in monitoring/proctoring, outside distracting noises, other distracting activities or noises from others within the testing environment.

4. Qualification of Test Administration Personnel

    a. All Test Administration Personnel (Test Coordinators and Test Administrators) will undergo annual training regarding the elements of the policies and procedures relevant to their roles and responsibilities.

    b. Following training, employ a means of evaluating Test Coordinators' and Test Administrators' understanding of the test administration procedures.

    c. Utilize periodic communications to all Test Administration Personnel to issue security alerts or procedural modifications.

5. Conflicts of Interest

    a. Test Administration Personnel may not use their knowledge of assessment content to violate the security and integrity of the assessment through acts of coaching, or other prohibited actions.

6. Qualification of Test Takers

    a. Testing Rules. Prior to testing all test takers must:

        i. Have their identity confirmed by school personnel or present one form of personal identification if they are not known by the Test Administrator or other individuals involved in the process, such as the classroom teacher or school counselor;

        ii. Submit to physical monitoring at all times during assessment administration as well as monitoring of assessment response data;

        iii. Hold all assessment content in confidence indefinitely;

        iv. Refrain from the following forms of assessment misconduct :

            1) Accessing materials known or represented to be active assessment content prior to testing;

            2) Possessing in the testing area, writing materials, cameras, PDAs, personal computers brought to the testing room, tablets, communication devices such as cellular telephones, reference materials, or non-approved calculators;

            3) Communicating about test content with other students either in the testing area or in any other location, both during and after the assessment;

4) Recording or memorizing assessment content;

5) Disrupting other test takers or the testing process;

6) Violating or attempting to violate published assessment retake rules;

v. Submit, if misconduct is detected, to reasonable requests for the production of information and materials;

vi. Abide by local school board or HIDOE determinations regarding alleged misconduct;

vii. Abide by all sanctions imposed by local school boards or the HIDOE for misconduct or any other violation of these Testing Rules.

b. It is recommended that these prohibited actions be covered in an acknowledgement page on the computer screen that the student must read and "sign" at the beginning of the test session. There should also be a stipulation that each student's electronic acknowledgement should be recorded and be recoverable by the vendor if needed at a future time.

7. Security Incident Management. To preserve the integrity of assessment materials and assessment scores, when misconduct (as defined elsewhere in this Section) is suspected, testing site personnel (Test Coordinators or Test Administrators) will be required to:

a. Call on one or more additional Test Administrators to confirm the misconduct;

b. Take reasonable, non-physical measures to:

i. Interrupt the assessment and arrange for the implicated test taker(s) to leave the testing area;

ii. Prevent test takers from leaving the testing area with secure assessment materials;

iii. Preserve evidence of test taker use of unauthorized materials without inappropriately, under school rules, confiscating or otherwise attempting to deprive test takers of their belongings (e.g., photographs or video recordings).

c. Follow requirements for handling security incidents in the local school district's code of student conduct. The Security Coordinator and other HIDOE staff should work with local districts to be sure that student misconduct, during or after assessment testing sessions as outlined in this Manual are mentioned as a basis for disciplinary action under the local code of student conduct.

d. Apprise the suspected student(s) of the potential consequences of misconduct (as set forth in these policies and procedures) and provide contact information for the responsible local school district personnel regarding the disposition of examination results.

d. Organize a Security Incident Report utilizing the Testing Incident Report Form consisting of the following:

    i. A description of the observed misconduct, including information provided by the Test Administrators and other personnel or students who observed the misconduct.

    ii. A list of actions taken by the school and district, including steps to avoid future incidents of the same nature and disciplinary measures for any individuals involved.

Section II. Detection

This section addresses guidelines and best practice for monitoring test administrations to minimize the risk of errors and activities for the detection of test irregularities. The activities discussed include:

- Assessment Monitoring Procedures
- Testing Irregularities Detection Activities: Statistical Analysis (Data Forensics)
- Guidelines for Test Security Detection Activities

In the following parts of this section, an overview of each detection activity is given. Later in the section, detailed guidelines for each activity are provided.

Assessment Monitoring Procedures

Assessment monitoring activities conducted by states typically follow this process. During any day of testing a monitor may present themselves to the front office of the school at the beginning of the school day. These monitors will deliver a signed letter, on HIDOE letterhead, to the Principal of the school. The monitor will then ask for the schedule of testing for the school and choose a room to monitor.

Once they arrive in the room they will introduce themselves to the Test Administrator and any proctors and quietly sit at the back of the room and observe the test administration. The monitor has a checklist of questions that they will mark to indicate if they see any irregularities and if any best practices are observed during testing. The monitors are unable to answer any questions about the test administration. All questions should be directed to the School/Building Assessment Coordinator or the Complex Area.

After the test is complete the monitor will immediately report any testing irregularities that may cause an invalidation of scores to HIDOE. The Assessment Section will work with the school to find a resolution. If no irregularities are found, HIDOE will send a copy of the checklist to the Principal for information or to suggest possible process improvements.

Testing Irregularities Detection Activities: Statistical Analysis (Data Forensics)

During and after online test administrations, HIDOE conducts multiple analyses on student assessments. These analyses help the state in detecting testing irregularities. Online testing permits detailed analyses of the response times of testing students and can detect testing anomalies. An anomaly may be detected when testing students obtain very different response times from most other students. Extreme response patterns will be monitored. For example, on occasion, students may proceed quickly through a test, answering all questions correctly and using much less time than would be normal or appropriate. These students may well be “harvesting” test questions to facilitate cheating at a later time. In other situations, it may be detected that students are

taking much longer than would be normal or appropriate, in which case, the HIDOE may, through the analysis of test data, identify the situation and diagnose the anomaly.

Here are the kinds of questions that data forensics methods help answer:

- Does it appear that two or more test takers colluded before or during a test?
- Does it appear that some students had advance knowledge of specific test questions?
- Is there evidence that the responses of two or more students in a class are far more similar than would have occurred if they were working independently?
    - For online test administrations, does the timing of responses to questions very considerably from the timing of responses of other students?
    - Are there changes to test scores for an individual or a class from one test administration to another that are much greater than one would expect for the test that was administered?

The following table looks at some of the data forensics methods that HIDOE is using and the types of testing irregularities they help detect.

DATA FORENSICS ANALYSIS	TESTING IRREGULARITIES
Unusual Score Gains and Losses	Coaching on actual test content, "helping" during a test administration.
Similarity	Sharing answers during testing, teachers helping before or during testing, illicit use of stolen test questions.
Corrective Change	Changing answers by educators, inappropriate assistance during testing.
Person Fit Analysis	Inconsistent response patters such as answering difficult questions correctly while missing easy questions.
Other Data Forensics Methods (e.g., response time analyses)	Varies

Unusual Score Gains and Losses

The data forensic approach has a very long history of use in admissions and licensure/certification testing and other assessments and makes comparisons of scores from one testing occasion to another. This approach is essentially the same regardless of the test delivery method. This analysis can show extreme changes in performance level changes by group and by cohort.

Similarity Analysis

A very effective data forensics approach is to examine, on a response by response basis, the answers given on each question, in every subject for every possible pair or group of students who took the same test or set of questions. This type of analysis is done for a substantial sized group when a data analyst has access to the data that

emerge from item responses for individual students using an online test administration or from scanning student answer sheets in a paper/pencil test administrations.

Corrective Change Analysis

In the past, when a paper/pencil test administration was done, an erasure analysis was performed for each administered assessment. An erasure analysis looks at changed responses on scanned student answer documents. Similar analyses are performed for online test administrations, where HIDOE reviews changes made by a student after first choosing a response to a particular question. For online test administrations, a comparison is made between the first responses chosen and subsequent choices. Testing systems can provide precise details of any changes made, which affords a higher degree of accuracy in determining actual student behaviors. If a particular student consistently answers incorrectly and then changes to the correct response, one must be skeptical that the student(s) was relying on his or her knowledge and skills. Both CAT and CBT forensic analyses will examine the number, type, and frequency of changes of answer choices.

Person Fit Analysis

Another method of data forensics analysis for state assessments is the person-fit analysis, which examines the consistency of students' responses across all questions on a test. In general, students will perform better on those questions that most other students also answer correctly, not as well on questions of moderate difficulty, and least well on the most difficult questions on a test. If a student generally performs well in a particular area such as mathematics, the same student may answer correctly all questions of low and moderate difficulty and miss only some of the most difficult questions. However, there are instances when a student's, or a group of students', test responses do not adhere to this pattern, perhaps departing from it in very significant ways. In this case, a student, or a group of students does significantly better on the most difficult questions on a test than the less difficult ones. A pattern such as this would prompt the application of the person-fit analysis to determine whether prohibit behavior has occurred.

Other Data Forensics Methods

At times, other data forensics methods may be employed. For online test administrations, an analysis of response times to test questions sometimes exposes patterns of shorter response times than would be required to read a passage, analyze a data table. There are also methods that are variations on the methods described above. For example, a form of similarity analysis counts the longest string of identical answers between two testing students. This same approach is best suited for the analysis of computer based "fixed form" tests, but less suitable for analyzing computerized adaptive tests (CAT), because of the variability of test items presented amount groups of students.

Guidelines for Test Security Detection Activities

In the following part of this section of the Security Manual, details are provided on the guidelines that should be used for various activities focused on detecting possible irregularities in the assessment. Specific information is provided for these areas:

- Monitoring Test Scores and Statistical Analyses
- Internet & Media Monitoring (i.e., Web Patrol)
- External Reporting Mechanism

Monitoring Assessment Data, Scores, & Results

To enhance the trustworthiness of assessment results, to assess the effectiveness of other security efforts and to enhance the security and service-life of assessments, the Coordinator, in conjunction with assessment development staff, will implement and oversee proactive efforts to detect test fraud and theft by monitoring assessment-response and event data, as well as the unauthorized disclosure of sensitive assessment materials, by monitoring the Internet and other media.

a. Forensic Analysis of Assessment results data - All test taker response data should be analyzed to develop, at a minimum, the following information:

i. Individual Test Administrators with elevated levels of irregular assessment administration activity and the effect of those irregularities on assessment scores and pass rates on all assessments administered by others;

ii. Individual assessment results showing irregularities which may be indicative of test fraud or test theft; examples include unusual response times, unusual gains or losses, unusual individual response patterns, and where there are a sufficient number of common items between pairs of test takers, unusual similarities of responses

1) Groups of test takers suspected of organized test fraud or theft (collusion);

2) The effects of suspected test fraud and theft activity on aggregate assessment scores and pass rates;

3) The combined effect of suspected test fraud and theft on assessment and item performance over the life of the assessment.

2. Interpretation of Analyses. The Security Coordinator, in conjunction with the Director of Assessment and Accountability, will establish appropriate standards for the interpretation of the analyses conducted under this Section and for the imposition of sanctions specified elsewhere in these policies and procedures.

a. When testing irregularities are identified, the following options may be available to the school regarding the results for the affected test takers:

    i. that their assessment score is “indeterminate” (i.e., may not be a valid measure of the student’s abilities as measured by the assessment);

    ii. that the assessment score will be cancelled unless the school can confirm the validity of the student’s assessment score via re-test; or

    iii. that misconduct is suspected and that the assessment score will be withheld pending further investigation.

b. When testing irregularities are identified using data forensic analysis, and further indicate high rates of irregularities by a Test Administrator, it is recommended that the Security Coordinator, following existing HIDOE policies on Investigations, consider :

    i. Recommending that the school issue a reprimand to the Test Administrator;

    ii. Requesting that the Test Administrator’s activities be reviewed for evidence of irregularities;

        1) Monitoring a classroom or school site with either announced or unannounced visits, to evaluate assessment administration practices based on the procedures specified in the delivery vendor’s Test Administrator Manual:

            a) Using a checklist to verify correct procedures are followed;

            b) Issuing a warning if procedures are not followed;

            c) If a second “audit” is warranted, evaluating procedures a second time and imposing appropriate sanctions within HIDOE rules and the context of the standing agreement with the test delivery vendor.

Internet & Media Monitoring

To combat the unauthorized disclosure of sensitive assessment materials on the Internet and in other print and computer-based “test prep” media, and to evaluate the effectiveness of other security measures, the HIDOE should continue its efforts in Web Patrol to regularly monitor such activity to the extent that resources allow and report the

findings of those efforts. Depending on the scope of monitoring, HIDOE may want to consider the use an external entity with expertise in monitoring.

a. Scope. Monitoring activities should include:

   i. Conducting monitoring of the Internet for the assessments that are administered;

   ii. Monitoring the Internet including web sites, discussion forums, auction sites, search engines, and other publicly accessible Internet venues where stolen assessment content may be shared or sold;

   iii. Print and computer-based "test prep" materials such as books, guides, and practice assessments.

b. Frequency.

   i. Internet monitoring and reporting should occur on at least a quarterly basis. However, additional activities may be scheduled to coincide with important testing events, such as the summative assessments administered in the Spring;
   ii. Print and computer-based "test prep" materials including practice tests should be acquired and analyzed immediately upon publication.

c. Training. Personnel or vendors assigned to perform monitoring activities should receive training as needed to ensure that monitoring activities are comprehensive, thorough and produce actionable information.

d. Reports. Monitoring reports should include the following information:

   i. Ownership, contact, publication and distribution information (if available) for each identified source of actual or potential assessment disclosure ("Source"), as well as IP address, hosting and legal agent information for Internet-based sources;

   ii. An estimate of the probable risk posed by each Source (High, Medium, Low) based on:

      1) Whether the proffered materials are aligned with the content of currently administered assessments;

2) An analysis of marketing and other positioning language regarding the proffered materials (e.g., the materials contain “real assessment content”);

3) A determination of how the material is advertised, whether the site provides guarantee of passing the assessment, and the associated cost of purchasing the website materials;

4) Whether the proffered materials are sold or shared (i.e., commercial activity presents a higher risk);

5) Evidence that the content is being sold and for what price;

6) Whether content is being shared by other test takers (forums, chat rooms, blogs, etc.);

7) The results of a comparison of Source materials with sensitive assessment materials to determine the actual level of disclosure;

8) The percentage of overlap between website content and actual assessment content;

10) Whether the content of the advertising or positioning statements of the source has changed from the most recent report.

11) Whether the website suggests they are offering something additional or different than from the previous report;

12) Updates on the status of previously identified sources, including steps taken against those sources;

13) Given the changeable nature of Internet sources, once identified, each source should be saved or “cached” in order to preserve evidence for comparative analysis and other follow-up activities.

iii. An estimate of the relative security of the administered assessments (Compromised, At Risk, Not at Risk).

iv. For each source deemed to pose a significant risk, determine:

1) The appropriate measures to be taken against the source owner/operator, and as specified in the Security Incident Response plan contained in these policies and procedures;

2) The appropriate measures to be taken to safeguard the assessment and the assessment results.

External Reporting Mechanism

To complement efforts to monitor test taker or Test Administrator misconduct, as well as the unauthorized taking and disclosure of sensitive assessment materials, establish and maintain a simple mechanism for the internal reporting of suspicious activity before, during, or after testing:

i. The reporting mechanism should at a minimum include an email address dedicated to the receipt and handling of such reports;

ii. Only those reports containing detailed, actionable information regarding the alleged perpetrator and the circumstances of the alleged misconduct should be processed.

1) Reports submitted anonymously should be processed as thoroughly as possible given available information.

iii. The Security Coordinator should recommend to the Director the possible use of incentives, such as nominal rewards, for information leading to the identification and/or prosecution of individuals for violations of these policies and procedures.

3. Formal Response Planning. The Security Coordinator should establish a process for responding to potential security incidents, including internal roles, responsibilities, decision criteria, and authorized actions for the handling, investigation and resolution of reported allegations of misconduct.

Section III. Follow-Up Consultation on Testing Irregularities

This section addresses guidelines for the HIDOE to work together with other entities in the state to follow up on irregularities and conduct consultation inquiry activities. These activities may include having HIDOE ask the school or complex area to conduct its own inquiry and produce a self-report. The more thorough the inquiry, the more likely HIDOE and the school can come to some determination of an irregularity and the required remediation.

HIDOE will determine the potential seriousness of the irregularity or may have additional questions and will assign an independent fact-finder, also known as an independent consultant to gather all the information regarding a potential irregularity. It is incumbent on the schools to provide complete cooperation to the consultants to identify all of the facts in the case.

This section also addresses the importance of reporting test irregularities and working with HIDOE to remediate irregularities in order to ensure valid results for all students. Remediation can differ based on the severity of a confirmed allegation or misadministration. There are limited options for HIDOE to resolve these irregularities after the testing window is over, but the goal of HIDOE is to ensure valid test scores, and for all students to have an equal opportunity to show their knowledge, skills, and abilities through their engagement with the test.

Many irregularities can be corrected if they are detected and attended to during the test administration window. Schools need to report and work with HIDOE to remediate and resolve irregularities as soon as possible. It is important to realize that the state has limited options if an irregularity is detected after the fact and must follow state board-approved guidelines for remediation.

Consequences of Testing Incidents

In one of its policy documents related to test security (in the appendix), the HIDOE has stated the possible consequences of testing irregularities and incidents. This includes the following:

“If testing incidents occur during administration of an assessment, the Department of Education may invalidate impacted assessments that have been wholly or partially completed. However, invalidation will not occur automatically. The Department will not invalidate an assessment until it verifies the facts associated with the alleged testing incident with the School Administrator and Test Coordinator.

- If an assessment or exam is invalidated, the test results and student responses will not be included in the testing, reporting, and accountability systems (regardless of whether the incident was initiated by an adult or a student)
- An invalidated assessment will count toward one of the student’s online HSA Science testing opportunities.

- An invalidated EOC test will result in no score for a student because only one opportunity is provided.
- In extremely rare instances, rather than invalidating an assessment or exam, the Department may reset a student's assessment or exam at the request of the school if the Department determines that the student's actions did not compromise the integrity of the assessment or exam. If an online HSA Science Assessment is reset, the student's initial responses will be removed and the student may retake this opportunity.

Department of Education employees may be held personally responsible for any violation of copyright laws or breaches in test security. The Office of Human Resources will use the current regulations to determine the disciplinary actions that may be taken for certified and classified employees who have been determined to be directly involved in misconduct that affected the integrity of the assessments or exams. Similarly, school principals will apply the current student disciplinary action regulations that may be taken with students who have been determined to be directly involved in a security incident that affected the integrity of an assessment or exam. There is a Department of Education memo dated February 28, 2014 which specifically addresses the consequences for students and school staff who use electronic devices to breach the security of any test item."

More information on the HIDOE's policies regarding testing incidents are provided in the appendix, along with a memo with examples of cheating or inappropriate behavior that may lead to invalidations. In addition, a Sample Security Incident Matrix is shown in Appendix A.

Guidelines for Consultations on Testing Irregularities

In the following part of this section, guidelines are presented on identification of test irregularities and steps that need to be taken if security has been violated. Details on use of a "Security Incident Response Plan" are also provided.

Test Security Violations

Test Security violations will be handled according to the procedures for Violations of the Code of Ethics for HIDOE Assessment Administration, as presented in formal HIDOE Test Security Policies

1. Test Fraud, as applied in this Test Security Manual, includes any attempt by an individual or individuals in collusion to subvert the testing process through actions including but not limited to:

    a. Unauthorized access to secure assessment materials;

    b. Use of stolen assessment materials through memorization or any other means;

c. Engaging others to take an assessment on another test taker's behalf;

d. Giving or receiving unauthorized assistance during the administration of an assessment;

e. Possession and/or use of unauthorized materials during the administration of an assessment including: notes, recording and communication devices;

f. Altering assessment scores;

g. Disclosing and/or distributing protected assessment material.

2. Test Theft, as applied in this Manual, includes any attempt by an individual or individuals in collusion to misappropriate protected assessment materials before, during, or after assessment administration, through actions including but not limited to:

a. Possession and/or use of recording or communication devices during the administration of an assessment;

b. Reproduction of assessment materials by any means, including reconstruction through memorization;

c. Storage and use of assessment materials to be used as test prep for test takers;

d. Providing answers or assisting in test administration to test takers before, during, or after the testing event.

Security Incident Response Plan

This Security Incidence Response Plan (SIRP) is an effort to maximize test security and to minimize risks. The SIRP is meant to provide a proactive approach to preventing cheating and promoting fair and valid testing in the State assessment program.

1) Irregularity Consultation Activities. This section describes how allegations and other information of test theft and fraud allegations should be followed up.

a) All reasonably detailed reports, assessment data analyses, and information received from monitoring efforts containing actionable information of alleged cheating and/or test theft (hereafter "possible Misconduct") by a test taker, test administration personnel, teacher, school administrator, or assessment support staff should be reviewed by the Security Coordinator as follows:

i) Confirmation of Time Sensitive Information: Within the time lines specified in existing policies issue reports containing information regarding possible misconduct should:

(1) Confirm the identity of alleged perpetrator(s);

(2) Confirm witness statements, including the names and contact information of other potential witnesses;

(3) Confirm statistical findings of assessment administration irregularity, as applicable;

(4) Archive images of websites engaged in unauthorized disclosure of secure assessment material on the Internet and elsewhere, as applicable.

ii) Collection of Related Information: Within the schedule determined by the HIDOE Assessment and Accountability Branch, instruct school districts or initiate action to collect the following information:

(1) Any available evidence which tends to refute or corroborate the original evidence or allegation(s);

(2) Available background information regarding the alleged perpetrator(s);

(3) Contact and ownership information regarding offending websites and other materials, as applicable.

iii) Establish the Scope of the Security Failure: Examine whether the alleged perpetrator(s) were the source or a "symptom" of a larger security failure by one or more of the following means:

(1) Analyze assessment data for patterns of individual and organized test fraud and theft;

(2) Analyze materials containing unauthorized disclosures of sensitive assessment material to establish whether the materials originated from source materials (e.g. the order of items and the accuracy of the text) or was collected from other sources on a piecemeal basis.

iv) Preservation of Evidence: Whether or not an Investigation Report results in sanctions or other remedies, the Security Coordinator should ensure that every Investigation Report is securely electronically preserved along with a record of all decisions and actions taken by the Coordinator, the Complex Area or school, including appeals.

2) Incident Management. This section discusses how to manage security incidents including assessment misconduct, leaks and mishandling of protected assessment material, coaching, etc.

a) Preservation of Assessments: On the receipt of a report or other information containing allegations of misconduct, the Security Coordinator will:

i) Within the time lines established by existing polices, receive reports and information, and evaluate whether the alleged incident(s) pose a threat to security of the State assessment content or assessment results, based on the results of the following inquiries:

(1) The availability of reliable evidence;

(2) The importance of the assessment content and assessment results;

(3) The number of individuals or organizations alleged to be involved in the incident(s);

(4) The prevalence of similar incidents;

(5) Patterns of suspected misconduct with the same individual or school, through analysis of assessment-response and event data;

(6) The presence of commercial activity (e.g. the buying & selling of assessment content or proxy services);

(7) The probable level of public and stakeholder interest in the alleged incident;

(8) The potential effect on HIDOE's reputation and confidence in the test results.

ii) Within 10 business days, and in conjunction with the examination publication and administration schedule, consider implementing any or all of the following measures:

a) Suspension of scheduled assessment administrations in a school on a comprehensive or selected basis;

b) Deployment of replacement assessment forms or CBT/CAT item pools;

c) Suspension of assessment results;

d) Evaluation of ongoing assessment results for indications of test fraud and/or theft.

b) Confidentiality: To preserve confidence in the assessment content and assessment results, and to ensure fairness and privacy, all information relating to alleged misconduct or disclosure will be regarded as "confidential."

3) Decision Making. This section discusses how supported allegations of misconduct will be documented and decided.

a) Investigation Report: Once collected, the Coordinator will analyze the existing evidence and derive concise, supportable findings in an Investigation Report including:

i) Those policies and/or legal commitments the alleged incident or activities would violate if confirmed;

ii) A description of the quantity and credibility of existing evidence, and what additional evidence or information, if any, would confirm or rebut that evidence;

iii) Conclusions stating whether the existing evidence supports one of the following findings:

(1) One or more State policies and/or legal commitments have been violated; or

(2) Additional investigation is needed to make a determination (if there is a strong possibility that additional investigation would produce important new evidence); or

(3) The existing evidence is insufficient to support the alleged violation.

b) Review Panel: A Review Panel (as described earlier) should be organized to evaluate the Investigation Report submitted by the Security Coordinator. The Panel's responsibilities shall include evaluation of the reasonableness of the Security Coordinator's findings and, identifying and recommending sanctions and/or other remedies as follows:

i) Test Takers. Depending on the clarity of evidence (circumstantial to "red-handed"), the student shall be subject to the following:

(1) At the discretion of the Division of Assessment and Accountability, the test score of the student may be invalidated and the student may be declared ineligible to retake the test until the next official testing opportunity;

(2) Be subjected to such disciplinary action as deemed appropriate to the school district;

ii) Any individual other than a student who violates any of the security provisions shall be subject to the following:

(1) Such personnel sanctions as might otherwise be imposed by the school for an act of misconduct;

(2) Be subjected to a hearing conducted by the HIDOE to determine revocation of any license issued to such individual pursuant to the provisions HIDOE policies and procedures;

(3) Payment of any costs incurred by the State or Division as a result of the violation.

iii) Third Parties. Recommendations to pursue any or all of the following remedies against individuals or organizations (e.g. brain dump sites, chat rooms, forums, Internet auction houses), involved in the taking and disclosure of assessment materials:

(1) Notices requesting that the individual(s) or organization(s) cease and desist from the unauthorized disclosure of assessment materials;

(2) Notices authorized by the Digital Millennium Copyright Act requesting Internet hosting organizations, search engine and auction operators remove or "takedown" offending website material;

(3) Institution of legal action to obtain damages or injunctions.

c) Appeal: To further ensure the fairness of decisions rendered against test takers or others, the HIDOE may provide affected parties with the following form of appeal:

i) Requests for Appeal. Upon the receipt of a notice of decision from the Department, the test taker or school staff member will have 30 business days to file with the Director of Assessment and Accountability a written request for appeal including new evidence for consideration.

ii) Review. Within 10 business days of a request for appeal, the Director will follow up on the request by referring the appeal along with the prior Investigation Report to the Review Panel. The Review Panel will:

(1) Review the investigative report and any new evidence;

(2) Determine whether the substance and credibility of the new evidence requires any modification of the Panel's original decision or sanctions.

(3) Recommend to the Director a course of action to be presented to the Associate Superintendent of HIDOE.

4) Identifying and Managing Assessment Threats. This section describes the means of using data-driven analysis to investigate possible testing misconduct.

a) The HIDOE should use data forensic statistical analysis periodically to identify and manage assessment threats. In particular, the following should be reviewed:

i) Abnormal examinee results;

ii) Cheating, proxy test taking, collusion, unusual score gains;

iii) Aberrant Test Administrator results;

iv) Unusually high pass rates and collusion patterns;

v) Extreme variations in assessment performance and unusual examination event results.

b) The HIDOE should use informal analysis to examine test-taking patterns. The following will be asked to determine if a student shows an abnormal test-taking pattern:

i) Does the student or class have an extremely high pass percentage?

ii) Where computer-based tests are used, are the response times for both items and the overall assessment extreme (too fast or too slow)?

5) Professional Benchmarks. The HIDOE can measure itself against other State assessment programs by:

a) Tracking developments in other states related to security and comparing Hawai'i's results against those of other state programs;

b) Participating in, and contributing to multi-state assessment security initiatives to learn more about what other professional programs are doing with regard to assessment security, such as the TILSA SCASS test security workgroup;

c) Attending appropriate conferences, such as the CCSSO National Conference on Student Assessment and presenting the results of their security initiatives.

6) Communication Plan. This section discusses whether and how incidents of misconduct will be communicated to stakeholders.

   a) The HIDOE Assessment and Accountability Branch may, without names or other identifying information, publish accounts of actions taken in confirmed cases of misconduct (rather than actions taken on the basis of the invalidity of an assessment result described elsewhere in this Plan).

APPENDICES

Appendix A – Sample Security Incident Matrix

Appendix B - Caveon Risk Calculator Model

Appendix C – Sample Seating Charts

Appendix D – HIDOE Policies and Procedures on Test Security

1. HIDOE Test Security Plan: Test Security Policy and Associated Procedures
2. Maintaining Security and Understanding the Consequences
3. Examples of Cheating / Inappropriate Behavior Scenarios Related to Statewide Student Assessments that Require Students' Scores to be Invalidated (memo dated 6/10/13)
4. Testing Incidents (document with reporting form)
5. Policies: Student Confidentiality and Assessment
6. Preventing Student Cell Phone Access during Testing -- Updated 7/23/13
7. Test Environment and Security
8. SBAC State Smart Sheet for Operational Testing
9. *SBAC State Procedures Manual—Item Risk Rubric:* Smarter Balanced Item Exposure Risk Analysis
10. Hawaii Statewide Assessment Program, School Year 2017-18

Appendix E. Glossary of Test Security Terms

Appendix A – Sample Security Incident Matrix

Severity	Types of Suspected Activity: Test Administrators	Possible Remedies
High	Sharing assessment content BEFORE the exam	• Scores invalidated • Permanent ban • Order investigation • Legal action
High	Sharing assessment content DURING the exam	• Scores invalidated • Permanent ban • Order investigation • Legal action
High	Coaching one or more test takers through assessment process	• Scores invalidated • Permanent ban • Order investigation • Legal action
High	Allowing proxy assessment-taking	• Warning letter • Probation • Order investigation
High	Second offense for suspected activity	• Permanent ban • Order investigation • Legal action
High	Test Administrator acting as a proxy test taker	• Scores invalidated • Permanent ban • Order investigation • Legal action
High	Forging assessment-related documents	• Scores invalidated • Order investigation • Legal action •
Medium	Violation of Procedures such as improper test taker check-in procedures. Fails to collect test taker possessions before assessment; fails to supervise assessment room, etc.	• Warning letter • Order investigation
Medium	Unauthorized delivery of an assessment	• Warning letter • Order investigation • Legal Action
Medium	Violation of Copyright or Trademarks	• Warning letter • Order investigation • Legal action

Appendix B - Caveon Return on Investment™ Calculator Model

caveon Test Security

Test Security ROI

Costs for Security Breach			Security Investments	
Lost Revenue & Strategic Position				**Physical test security**
test revenues				identity authentication
education revenue				proctoring
other lost revenue (partner programs, etc.)	0	0		
Unplanned Test Redevelopment				**Virtual Security**
subject matter expert time and travel				Web Patrol™
project manager time and travel				Data Forensics™
psychometric consulting				
test question beta testing	0	0		
Program Goodwill: loss of credibility & prestige				**Increased Test/Item Development**
defection of test takers to other programs				Production cost
marketing & PR expense to recover position				
staff time dealing with test taker complaints	0	0		
				Security management
Loss of test reliability				Security Audit
Legal liability from certifying/licensing unqualified test taker	0	0		Security Manager
Incident response				
Time, travel, system recovery costs	0			
Opportunity Cost	0			
TOTAL	0	0		**TOTAL**

Appendix C – Sample Seating Charts

Seating charts must be completed for each test session conducted by the school, including sessions that result from students being moved or relocated for any reason and even if there is only one student. Seating charts will assist with the tracking of online test administrations, secure assessment materials, and attendance.

Schools can create seating chart templates that best suit their needs; however, the following minimal information must be collected for each test session:

- School name, room number, and date the test was administered
- Name of the test, grade level, and subject
- Name of the Test Administrator
- Test session start and stop times
- If the test is administered with paper/pencil (P/P) indicate the booklet number; if the test is administered online, indicate the students login name but do not include the password

Test Administration Seating Chart – Sample 1

School:	**Rm #:**	**Date:**
Test Administered:	**Subject/Grade Level:**	
Test Administrator:		
Start Time:	**End Time:**	

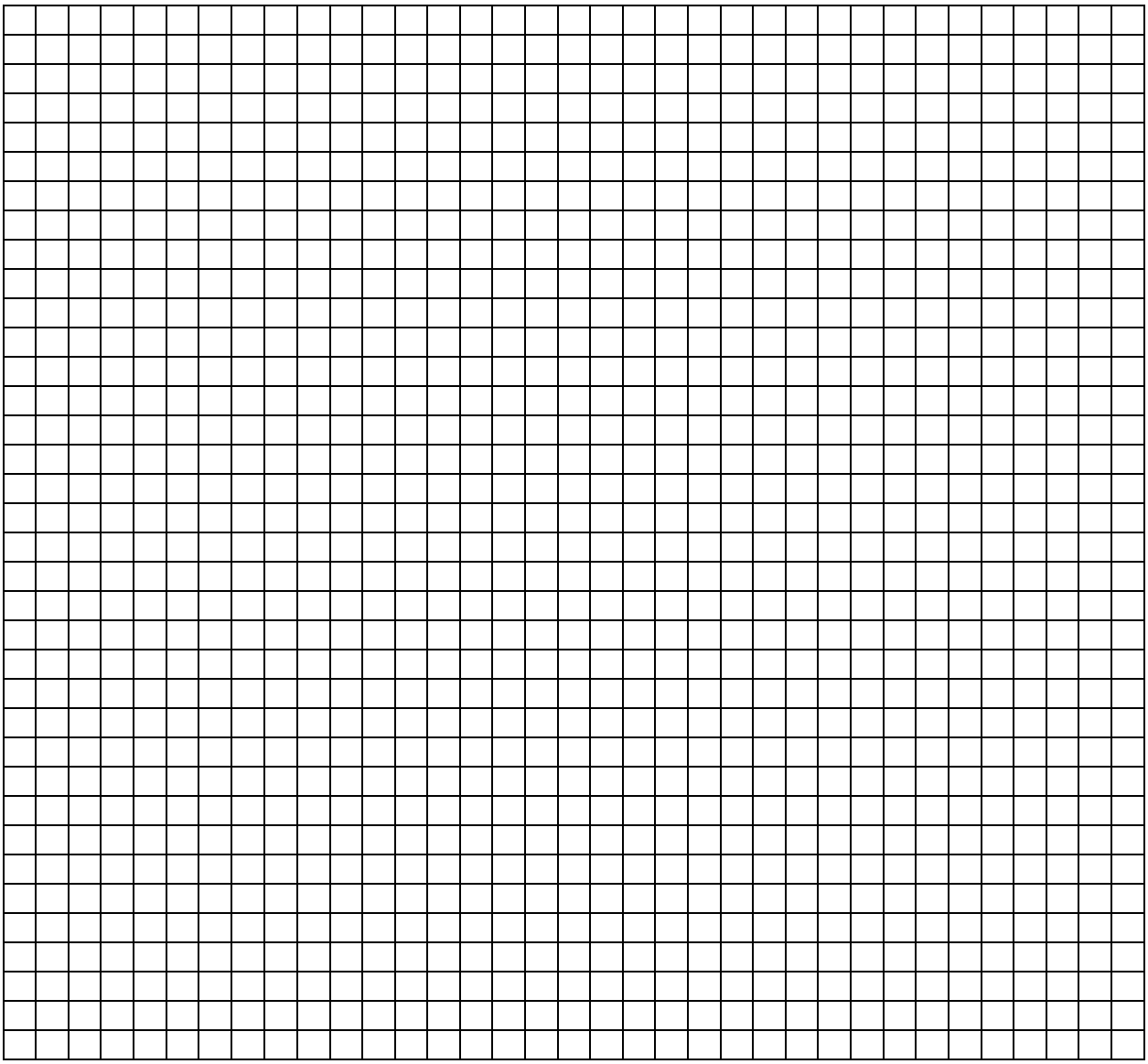
1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21	22	23	24
25	26	27	28	29	30

Seat #	Student Name	P/P - Test Booklet Number CBT – Student Login ID	Form #	Test Completed
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				
26				
27				
28				
29				
30				

Test Administration Seating Chart – Sample 2

School:	**Rm #:**	**Date:**
Test Administered:	**Subject/Grade Level:**	
Test Administrator:		
Start Time:	**End Time:**	

Instructions for the grid below:
1. Draw the location of and indicate the corresponding seat number for each student.
2. Complete the information on the corresponding table for each student.



Seat #	Student Name	P/P - Test Booklet Number CBT – Student Login ID	Form #	Test Completed
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				
26				
27				
28				
29				
30				

Test Administration Seating Chart – Sample 3

School:	**Rm #:**	**Date:**
Test Administered:	**Subject/Grade Level:**	
Test Administrator:		
Start Time:	**End Time:**	

Student 1	**Student 2**	**Student 3**	**Student 4**	**Student 5**
Name: **ID:** **Book #:** **Form #:**	**Name:** **ID:** **Book #:** **Form #:**	**Name:** **ID:** **Book #:** **Form #:**	**Name:** **ID:** **Book #:** **Form #:**	**Name:** **ID:** **Book #:** **Form #:**
Student 6	**Student 7**	**Student 8**	**Student 9**	**Student 10**
Name: **ID:** **Book #:** **Form #:**	**Name:** **ID:** **Book #:** **Form #:**	**Name:** **ID:** **Book #:** **Form #:**	**Name:** **ID:** **Book #:** **Form #:**	**Name:** **ID:** **Book #:** **Form #:**
Student 11	**Student 12**	**Student 13**	**Student 14**	**Student 15**
Name: **ID:** **Book #:** **Form #:**	**Name:** **ID:** **Book #:** **Form #:**	**Name:** **ID:** **Book #:** **Form #:**	**Name:** **ID:** **Book #:** **Form #:**	**Name:** **ID:** **Book #:** **Form #:**
Student 16	**Student 17**	**Student 18**	**Student 19**	**Student 20**
Name: **ID:** **Book #:** **Form #:**	**Name:** **ID:** **Book #:** **Form #:**	**Name:** **ID:** **Book #:** **Form #:**	**Name:** **ID:** **Book #:** **Form #:**	**Name:** **ID:** **Book #:** **Form #:**
Student 21	**Student 22**	**Student 23**	**Student 24**	**Student 25**
Name: **ID:** **Book #:** **Form #:**	**Name:** **ID:** **Book #:** **Form #:**	**Name:** **ID:** **Book #:** **Form #:**	**Name:** **ID:** **Book #:** **Form #:**	**Name:** **ID:** **Book #:** **Form #:**
Student 26	**Student 27**	**Student 28**	**Student 29**	**Student 30**
Name: **ID:** **Book #:** **Form #:**	**Name:** **ID:** **Book #:** **Form #:**	**Name:** **ID:** **Book #:** **Form #:**	**Name:** **ID:** **Book #:** **Form #:**	**Name:** **ID:** **Book #:** **Form #:**

Appendix D. Collection of Important Documents on HIDOE Policies and Practices

STATE OF HAWAI'I

DEPARTMENT OF EDUCATION
P.O. BOX 2360
HONOLULU, HAWAI'I 96804

Spring 2014 Smarter Balanced Field Test Test Security Plan

Test Security Policy and Associated Procedures

The security of assessment instruments and the confidentiality of student information are vital to maintaining the validity, reliability, and fairness of the results.

All test items and test materials are secure and must be appropriately handled. Secure handling protects the integrity, validity, and confidentiality of assessment items, prompts, and student information. Any deviation in test administration must be reported as a test security incident to ensure the validity of the assessment results. Failure to honor security severely jeopardizes student information and/or puts the operational test at risk.

Everyone who administers or proctors the online Smarter Balanced English Language Arts or Mathematics Field Test is responsible for understanding the test security procedures for administering the field tests. Test security incidents, such as improprieties, irregularities, and breaches, are behaviors prohibited during the field test administration, either because they give a student an unfair advantage or because they compromise the secure administration of the field test items. Whether intentional or by accident, failure to comply with test 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 provided in the Smarter Balanced Online Field Test Administration Manual.

Item security rules include but are not limited to the following:

- Unless assigned as an accommodation, no copies of the test items, stimuli, reading passages, performance task materials, or writing prompts may be made or otherwise retained. This includes using any digital, electronic, or manual device to record or retain an item.

- Descriptions of test items, stimuli, printed reading passages, or writing prompts must not be retained, discussed, or released to anyone. All printed test items, stimuli, and reading passages must be securely shredded immediately following a test session.
- Test items, stimuli, reading passages, or writing prompts must never be sent by email or fax, or replicated/displayed electronically.
- Secure test items, stimuli, reading passages, or writing prompts must not be used for instruction.
- No review, discussion, or analysis of test items, stimuli, reading passages, or writing prompts at any time, including before, during, or between sections of the test, is allowed by students, staff, or test administrators. Student interaction with test content during a test is limited to what is dictated for the purpose of a performance task.
- No form or type of answer key may be developed for test items.

Test administrators or other individuals who have witnessed, been informed of, or suspect the possibility of a test security incident that could potentially affect the integrity of the tests or the data should follow the steps outlined below and the *TIDE User Guide located at:* https://smarterbalanced.alohahsap.org/resources/test-administration/

❑ **Impropriety (Low Severity Level)**

Unusual circumstances that have a low impact on the individual or group of students who are testing and have a low risk of potentially affecting student performance on the field test, test security, or test validity. Examples include, but are not limited to, the following:

- Student(s) making distracting gestures or sounds during a field test session that creates a disruption in a field test session for other students
- Student(s) leave the testing room without supervision
- Student(s) accessing or using electronic equipment (e.g., cell phones, PDAs, iPods, or electronic translators) during testing for purposes other than cheating or sharing test information
- Students talking during testing
- Student(s) accessing the Internet during a field test session
- Administrators or Coordinators leaving instructional materials on the walls in the testing room

These circumstances can be corrected and contained at the school level using the test security required action steps.

Impropriety Reporting Procedure:

1. School administrator/staff take corrective action and document impropriety in the Testing Incident Report Form. (The log can be downloaded at https://smarterbalanced.alohahsap.org/test-administration-forms.stml.)

2. Incident is mitigated as necessary by school staff and state coordinator notified of mitigation.
3. Designated school coordinator records the impropriety in TIDE within 24 hours of the incident.
4. Designated state coordinator reviews TIDE record of impropriety according to state protocols and authorizes TIDE appeal.

❑ **Irregularity (Moderate Severity Level)**

Unusual circumstances that impact an individual or group of students who are testing and may potentially affect student performance on the field test, test security, or test validity. Examples include, but are not limited to, the following:

- Student cheating or providing answers to each other
- Disruptions to a field test session, e.g., fire drill, school-wide power outage
- Administrators or Coordinators failing to ensure administration and supervision of the Smarter Balanced Field Tests by qualified, trained personnel
- Administrator gives incorrect instructions that are not corrected prior to testing
- Administrator or teacher does not present class activity prior to Performance Task administration
- Administrators or coordinators giving our the username and password for authorized users to other individuals, including other authorized users
- Administrator allowing students to continue testing beyond the close of the selected testing window
- Administrator or teacher coaching or providing any type of assistance to students that may affect their responses
- Administrators providing students with non-allowable materials or devices during the field test administration or allowing inappropriate accommodations during field test administration
- Administrator allowing anyone other than a student to log into the Field Test unless prescribed as an allowable accommodation in the student's IEP.
- Administrator or Coordinator sending a student's name and SSID together in an email message.
- Administrator providing a student access to another person's work/responses

The circumstances causing the irregularity should be corrected at the school level, but submitted in the Smarter Balanced Field Test online system for resolution of the Appeal for testing impact.

Irregularity Reporting Procedure:

1. School administrators/staff report/document impropriety in the Testing Incident Report Form. (The log can be downloaded at https://smarterbalanced.alohahsap.org/test-administration-forms.stml.)

2. Incident is mitigated as necessary by school staff and state staff is notified of mitigation.
3. Designated state coordinator records the irregularity in TIDE by the end of the day that the incident is discovered.
4. Designated state coordinator authorizes TIDE appeal.
5. State reviews TIDE record of irregularity within 24 hours of reporting.

❑ **Breach (High Severity Level)**

An event that poses a significant threat to the validity of the field test. Examples may include such situations as a significant release of secure materials or a significant repeatable security/system risk. Examples include, but are not limited to, the following:

- Administrator or Coordinator modifying student responses or records at any time
- Administrator allowing students to take home field test items, reading passages, writing prompts, or scratch paper that was used during the Field Tests or failing to otherwise securely store field test materials
- Administrators or students copying, discussing, or otherwise retaining test items, stimuli, reading passages, writing prompts, or answers for any reason. This includes the use of photocopiers or digital, electronic, or manual devices to record or communicate a test item. This also includes using secure test items, modified secure test items, reading passages, or writing prompts for instructional purposes.
- Secure test materials are shared with the media by anyone
- Administrator, Coordinator, or student improperly removing secure testing materials such as test items, stimuli, reading passages, writing prompts, or scratch paper from the testing environment.

These circumstances have external implications for the Consortium and may result in a Consortium decision to remove the test question(s) from the available secure bank. Severe incidents requiring immediate attention (such as a release of secure materials or a repeatable security/system risk), are to be reported immediately to the Student Assessment Section at (808) 733-4100, and, for the Field Test, to the Smarter Balanced Help Desk at 1-855-833-1969 or smarterbalancedhelpdesk@ets.org.

Breach Reporting Procedure:

1. School administrator/staff report breach to the state coordinator by phone.
2. School administrator/staff contain the incident as necessary.
3. School administrator/staff document the incident in the Testing Incident Report Form and in TIDE if necessary. (The log can be downloaded at https://smarterbalanced.alohahsap.org/test-administration-forms.stml.)

4. School administrator/staff stand ready to receive further state guidance on dispensation of the event.
5. State lead alerts Smarter Balanced Help Desk by phone and follows up with written submission.
6. State coordinator reviews the incident and containment strategies employed by the school and authorizes TIDE appeal, if necessary.
7. State stands ready to receive further Consortium guidance.
8. Smarter Balanced Help Desk contacts designated Smarter Balanced staff.
9. Designated Smarter Balanced staff contacts the state lead and assist in state level mitigation.
10. If necessary, Smarter Balanced communicates mitigation strategies to all Consortium members.

Test Administrators and School Test Coordinators who have witnessed, been informed of, or suspect the possibility of a test security incident that could potentially affect the integrity of the field tests and data should follow the steps outlined in the Smarter Balanced Online Field Test Administration Manual.

The Hawai'i Department of Education's Office of Human Resources will use the current regulations that detail the disciplinary actions that may be taken for certified and classified employees who have been determined to be directly involved in a Smarter Balanced Field Test security incident that affected the integrity of the field tests and data. School principals will use the current student disciplinary action regulations that may be taken with students who have been determined to be directly involved in a Smarter Balanced Field Test security incident that affected the integrity of the field tests and data.

At the completion of the administration of all Smarter Balanced Field Tests at a school, the School Test Coordinator shall fax the Testing Incident Report Form to the Student Assessment Section at (808) 733-4483. The school shall archive the original document and provide it upon request. If a school has no test security incidents to report then no faxed document will be required.

Test Security Training Plan and Associated Procedures

A webinar that includes a power point presentation and questions and answers regarding the Smarter Balanced Administration and Test Security Procedures will be provided for the principals and test coordinators at each school prior to the beginning of each the testing window. The webinar information will be posted on the Hawai'i Department of Education's Smarter Balanced site for access and review by staff members at schools who are not able to participate in the webinar.

To ensure consistent administration across all participating schools in every Smarter Balanced state, all Test Administrators (TAs) should complete the Test Administration

training modules located on the Smarter Balanced Assessment Portal, at https://smarterbalanced.alohahsap.org/resources/trainings-and-webinars/

The principal of each school is responsible for ensuring that Test Administrators and any individuals who will be administering the Smarter Balanced Assessment have read and understand the Smarter Balanced Assessment Test Administration Manual (TAM), the Smarter Balanced Usability, Accessibility, and Accommodations Guidelines, and associated Smarter Balanced training modules.

The Hawai'i Department of Education will use its current criteria that describe which individual (staff or otherwise) may be designated as test administrators or other roles related to the administration of all statewide student assessments including the spring 2014 Smarter Balanced Field Test.

Consequences for Students and School Staff Who Use Electronic Devices to Breach the Security of Any Test Item Included in a Statewide Student Assessment

The Test Administrator must direct each student who enters the testing room with a cell phone or any other electronic device to turn it off, put it in a back pack or bag, and place the back pack or bag in a designated, secure area in the testing room that cannot be accessed during the test session. If a student does not have a back pack or bag, the Test Administrator will provide a box in which the electronic device will be placed after the student's name is written on a post-it-note and affixed to the electronic device. The box will also be placed in the designated, secure area in the testing room. This is a new test administration requirement that is being implemented beginning with 2013-14 to ensure students do not use these electronic devices to access the Internet in order to obtain information that can be used to answer any online or paper/pencil test items. This test security procedure also prevents students from using their phones to take pictures of test items and post them on social networking sites. **Any of these actions constitute a breach in test security and will result in the invalidation of a student's score for an assessment or exam.**

Due to the importance of test security for all of the statewide assessments, any school that has a student or staff member who uses an electronic device which results in the breach of a test item will be subject to the following actions/consequences:

1. The involved student's incomplete test or complete test that has been scored will be invalidated by the Department of Education's Student Assessment Section.

2. The school administration will be responsible for determining the consequences for the involved student per the Hawai'i Administrative Rules, Title 8, Chapter 19 and/or the consequences for the involved certificated or classified staff member per the Office of Human Resources procedures.

3. The school administration and test coordinator must retrain the staff regarding the test security requirements for all statewide assessments during a face-to-face meeting.

4. The test administrator who was conducting the test session when an electronic device was used by one or more students or a staff member will be required to retake the Test Administrator Certification Course in order to administer any additional assessments to students.

5. The school will be required to have a second adult present in the testing room with the test administrator who was conducting the test session when the electronic device was used to breach the security of one or more test items during each subsequent test session for the remainder of the current school year.

6. The school will be required to pay for the cost of each test item that was posted on a social networking site which required its removal from the current online, adaptive item bank.

7. The school must submit its detailed testing schedule that includes the date, time, and student seating chart for each test session for all statewide assessments administered during the remainder of the current school year and the next school year.

8. Unannounced site monitoring by the Assessment Section staff, and other staff as determined by Superintendent Kishimoto may extend beyond one school year.

The school administration and the test coordinator are directed to use the current procedures in the Test Administration Manual to report test security violations and cheating for the English Language Arts and Mathematics Assessments, HSA Science Assessment, Hawai'i State Alternate Assessments for Reading, Mathematics, and Science, End-of-Course Assessment for Biology I, and the ACT Plus Writing Tests.

Maintaining Security and Understanding the Consequences

The security of assessment instruments and the confidentiality of student information are vital to maintaining the integrity of the assessments and the reliability of the results. Due to the importance of test security for all of the Hawai'i Department of Education's statewide student assessments, the following measures will be in place during the 2014-2015 school year:

1. A test security audit will be carried out to ensure that the current processes and procedures reflect best practices.
2. Student scoring patterns will be electronically monitored throughout the testing windows to identify and detect possible cheating and other irregularities. Consultation with the principal and test coordinator will take place as necessary when potential problems are identified.
3. Teams will conduct on-site monitoring of schools at various times during testing windows to verify adherence to test administration procedures and provision of appropriate test accommodations for identified students.
4. Web monitoring, including social networking sites, will take place to identify potential testing breaches.

If testing incidents occur during administration of an assessment, the Department of Education may invalidate impacted assessments that have been wholly or partially completed. However, invalidation will not occur automatically. The Department will not invalidate an assessment until it verifies the facts associated with the alleged testing incident with the School Administrator and Test Coordinator**.**

- If an assessment or exam is invalidated, the test results and student responses will not be included in the testing, reporting, and accountability systems (regardless of whether the incident was initiated by an adult or a student)
- An invalidated assessment will count toward one of the student's online HSA Science testing opportunities.
- An invalidated EOC test will result in no score for a student because only one opportunity is provided.
- In extremely rare instances, rather than invalidating an assessment or exam, the Department may reset a student's assessment or exam at the request of the school if the Department determines that the student's actions did not compromise the integrity of the assessment or exam. If an online HSA Science Assessment is reset,

the student's initial responses will be removed and the student may retake this opportunity.

Department of Education employees may be held personally responsible for any violation of copyright laws or breaches in test security. The Office of Human Resources will use the current regulations to determine the disciplinary actions that may be taken for certified and classified employees who have been determined to be directly involved in misconduct that affected the integrity of the assessments or exams. Similarly, school principals will apply the current student disciplinary action regulations that may be taken with students who have been determined to be directly involved in a security incident that affected the integrity of an assessment or exam. There is a Department of Education memo dated February 28, 2014 which specifically addresses the consequences for students and school staff who use electronic devices to breach the security of any test item.

Student Assessment Section
Phone: 808-307-3636
Fax: 808-733-4483
Email: hsa/SAS/HIDOE@notes.k12.hi.us
(The full Lotus Notes address is required)

NEIL ABERCROMBIE
GOVERNOR

KATHRYN S. MATAYOSHI
SUPERINTENDENT

STATE OF HAWAI'I

DEPARTMENT OF EDUCATION
P.O. BOX 2360
HONOLULU, HAWAI'I 96804

OFFICE OF THE SUPERINTENDENT

SYSTEMS ACCOUNTABILITY OFFICE

June 10, 2013

TO: Kathryn S. Matayoshi, Superintendent

FROM: Cara Tanimura, Director
Systems Accountability Office

SUBJECT: **Examples of Cheating / Inappropriate Behavior Scenarios Related to Statewide Student Assessments that Require Students' Scores to be Invalidated**

The required test security and administration procedures for each of the Department of Education's (Department) statewide student assessments are provided in the appropriate online test administration manual for review and use by all qualified school level personnel who are involved in administering the assessments to students. The examples of cheating / inappropriate behavior scenarios that require students' scores to be invalidated have been included in this memo to emphasize the consequences for staff members, students, and their schools.

Adult Initiated:

1. A Test Administrator was testing a small group of SPED students and a proctor was present in the testing room. The proctor observed the Test Administrator walking around the testing room and pointing to the correct answers on the computer screen for different students who were answering multiple-choice test questions. The Test Administrator also showed different students how to move objects to the correct location on the computer screen for constructed response test questions. The proctor reported these actions to the principal. The principal interviewed the Test Administrator who had taken and passed the mandatory online certification course that addressed the test security and administration requirements. The Test Administrator stated that he or she did not think such assistance to students was wrong or inappropriate. The teacher was no longer allowed to serve as a Test Administrator during the remainder of the testing window. The Principal handled any necessary personnel action. The students' scores for this content area assessment opportunity were invalidated.

2. A Test Administrator permitted students to use behaviors that are not allowed for statewide student assessments during a test session, i.e., talk to each other while taking the assessment, ask the Test Administrator to read and explain test questions, and sit next to smarter students who could help them pass the assessment. Students shared this information with their

classmates and this led to some teachers being informed who then reported the Test Administrator's actions to the principal. The teacher was no longer allowed to serve as a Test Administrator during the remainder of the testing window. The Principal handled any necessary personnel action. The students' scores for this content area assessment opportunity were invalidated.

3. A Principal and a Test Coordinator were monitoring students' scores in the Online Reporting System to identify students who had not received a passing score of 300 or higher for various content area assessments. When they saw a number of students who had increases of 60 – 100 scale score points for a third opportunity assessment, they were concerned and interviewed each student individually. Some students shared that the Test Administrator walked around the testing room and pointed to test questions on the computer screen that they had just answered and said, "Check your answer; try again." Other students said, "The teacher pointed to the formula sheet and the equation for certain test questions; some students said, "I gotta pass this test." The Principal handled any necessary personnel action. The students' scores for this content area assessment opportunity were invalidated.

4. A Test Administrator wrote a test question on a piece of paper after a student reported that there was no correct answer. The Test Administrator paused the student's test and gave the test question to the school's Test Coordinator. The Test Coordinator told the Test Administrator that no one may write a test question on a piece of paper or take a screen shot of it on the computer screen. The protocol that a Test Administrator needs to use for reporting a test question that does not load properly on the computer screen, does not display all of the answer options, or appears to have no correct answer includes the following:

   - Pause the student's test.
   - Write the student's name, 10-digit ID number, number of the test question displayed on the student's screen, and the Test Session ID on a piece of paper.
   - Give this information to the Test Coordinator who will report it to the Help Desk Staff so the appropriate action can be taken by the testing contractor to address the issue.

   In this scenario, there was a correct answer to the test question. So the student was told to choose the answer he or she thought was correct even if the student did not think there was a correct answer.

5. After a content area assessment opportunity had been completed, a teacher told colleagues in the teachers' lounge, "I explained test questions to the students but they still didn't do well." One of the colleagues informed the Principal because this action could hurt their school's reputation and the entire staff if the students went home and told their parents that their teacher helped them answer the test questions. The Principal handled any necessary personnel action. The students' scores for this content area assessment opportunity were invalidated.

6. A school decided to have teachers who served as Test Administrators conduct makeup testing sessions for students who were absent during the initial administration of an assessment in their classrooms during regular instruction to reduce the need to pull students out of their regular classes to be tested by support staff who were also certified as Test Administrators in addition to their other professional duties. Students who were taking makeup tests were directed to wear headphone to block the noise of regular classroom activities and to face their chairs and desks toward the back of the classroom. The Test Coordinator reported the following test security breach that occurred in one classroom. The teacher was conducting a video production project with the students and staff members from Olelo were present in the classroom to assist the students while they practiced their videotaping skills. A student videotaped a few test questions that were displayed on students' computer screens from a distance. However, this action

involved two test security breaches, i.e., students must be tested in a room where no other instructional or non-instructional activities are being conducted, no electronic device may be used to record and store pictures of test questions. The Principal handled any necessary personnel action. The students' makeup test scores for this content area assessment opportunity were invalidated.

7. A Test Administrator forgot to activate the text-to-speech feature for a group of ELL students immediately **before** they began a Mathematics test session. When the students raised their hands and said that they could not listen to the test questions being read by the electronic voice, the Test Administrator asked a support staff member to come to the computer lab to provide assistance even though the Test Administrator had passed the certification course and had been taught how to activate this feature during the previous school year. The support staff member incorrectly thought that the feature could be activated for each student **after** he or she had already started a test session. So the support staff member decided to log into the test session using the legal first name and 10-digit ID number of an absent student and answer the first test question to determine whether the text-to-speech feature could be activated. This was a test security breach because no other student or school staff member may log into a test session using a student's identification information. Due to the support staff member's action, the absent student's second opportunity for this content area assessment was invalidated. The Principal and Test Coordinator decided to review this test security requirement and the procedures for presetting online testing features for identified students prior to the beginning of a test session, e.g., text-to-speech. The Principal handled any necessary personnel action.

8. A Test Administrator told the class the day before a content area assessment was administered that it would be an interesting experiment to find out which answer option (A, B, C, or D) occurred the most on a test by having student control groups that only chose options A, B, C, or D. Some students shared the experiment information with teachers who taught some of their other classes. These teachers informed the Principal and the Test Coordinator. All Test Administrators were told to inform students that the online assessments are adaptive so it is important for them to answer each test question carefully because their answer will determine the next question or set of questions assigned to them depending on the content area assessment. The Principal handled any necessary personnel action. The students' scores for this content area assessment opportunity were not invalidated because the school worked as a professional team to ensure that students were given the correct information about the importance of answering each test question carefully.

9. A Test Administrator left the testing room 10 minutes before the end of the test session to prepare for the next class while students were still answering test questions. The Test Administrator thought that this action was okay because a proctor was present in the testing room even though this staff member was not allowed to take and pass the certification course which is a requirement to serve as a Test Administrator. This is a violation of test security because only the Test Administrator is allowed to pause students' tests at the end of a test session if they have not answered all of the test questions using the computer assigned to the Test Administrator. The Test Coordinator came to the testing room to pause the students' incomplete tests. The Principal handled any necessary personnel action. The students' scores for this content area assessment opportunity were not invalidated.

10. A Test Administrator tested two small groups of students in separate computer alcoves where only the students in one of the two alcoves could be monitored at any point in time. Each small group included approximately 8-10 students. The logistics for these two small groups did not adhere to the required test security requirements. First, a Test Administrator must be able to view all of the students in a test session throughout that test session. Second, a proctor must also be present in the testing room with a small group that includes 9-12 students. When

students were interviewed about their behavior while the Test Administrator was not present in their computer alcove, they stated that they talked about their plans after school but not about the test questions. Since students' actual behavior could not be verified, their scores for this content area assessment opportunity were invalidated. The Principal and the Test Coordinator reviewed the acceptable logistics for testing groups of students with all Test Administrators to ensure that the correct test security procedures were followed for the remaining test sessions scheduled during the testing window.

Student Initiated:

1. A student was observed looking at the computer screen of another student seated next to him who happened to be answering the same set of test questions for the same reading passage. This is possible for an adaptive assessment because the online system is programmed to display the entire set of test questions for a reading passage while only one test question for any other content area is displayed on the computer screen. The student clicked on the same multiple-choice answer for two of the test questions that he saw on the other student's computer screen. The student was told to leave the testing room and the incomplete Reading Assessment opportunity was invalidated.

2. A student was using a cell phone during a test session and refused to turn off the phone or give it to the Test Administrator. The student was told to leave the testing room and the incomplete content area assessment opportunity was invalidated. The Principal and the Test Coordinator reminded all Test Administrators to tell the students to turn off their cell phones and any other electronic devices and put them in their pockets or bags as soon as they enter the testing room and to walk around the testing room to confirm that the students are following this test security requirement.

3. A student was singing loudly during a test session about how dumb the test was and would not stop singing when told to do so three times. The student was told to leave the testing room and the incomplete content area assessment opportunity was invalidated.

4. A student used a camera phone to take screen shots of test questions displayed on the computer screen and posted them on Instagram. The student's friends at other schools saw the test questions when they were at school or at home and informed their teachers or parents. The Principals at the schools of the student's friends were informed. The student who took the screen shots of the test questions had his or her score for the test invalidated. When a secure test question is posted on a social media site, it can no longer be used for future test administrations. The cost of developing, reviewing, field testing, and verifying the statistics for one multiple-choice test question is $1,000 and $1,500 for a constructed response test question that involves typing, dragging and dropping objects and words, drawing lines and arrows, etc. to indicate answers.

5. While students were being tested in their classroom, a student took a notebook out of his or her desk and began reviewing the handwritten notes on various pages to locate specific information that would help to answer some of the test questions. The Test Administrator told the student that the notebook could not be used during the test session and placed it on his or her own desk. Since the student did not have an opportunity to use the information in the notebook to answer any of the test questions, the content area assessment opportunity did not need to be invalidated. The Principal and Test Coordinator met with all of the Test Administrators and explained that they need to inform students that they cannot use any of the instructional materials and tools in their desks or the classroom work centers to answer test questions before each test session begins.

6. A Test Administrator saw a student using a personal multi-function calculator for a Mathematic test session instead of the required four function calculator when the student had answered more than half of the test questions. When the Test Administrator asked the student why he or she was using the personal calculator instead of the one that was placed beside the computer, the student said that it was easier to use the personal computer because he or she knew where each key was located. The student's content area assessment opportunity was invalidated because the multi-function calculator gave him or her an advantage in answering some of the test questions that involved more complex functions.

If you have any questions, please contact Cara Tanimura, Director, Systems Accountability Office at (808) 586-3283 or via Lotus Notes.

CT:PI:kb

c: Ronn Nozoe, Deputy Superintendent
Systems Accountability Office

Testing Incidents

Occasionally an incident may occur that will disrupt testing. A testing incident is any event that could potentially impact the integrity of the assessments or exams and the test results before, during, or after the test administration. Testing incidents are behaviors that may give a student an unfair advantage or may compromise the secure administration of an assessment. Reportable incidents, whether intentional or accidental, include security violations, cheating and improper assistance by adults or students, and other test administration problems. These testing incidents are classified into one of three categories: an impropriety, an irregularity, or a breach depending upon the seriousness of the situation.

Improprieties are unusual circumstances that 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. Examples of improprieties include:

- Student(s) making distracting gestures or sounds during a test session that creates a disruption for other students
- Student(s) leave the testing room without supervision
- Student(s) accessing or using electronic equipment (e.g., cell phones, PDAs, iPods, or electronic translators), during testing for purposes other than cheating or sharing test information except those allowed as part of an IEP or accommodation.
- Students talking during testing except as appropriate in individual testing situations.
- Student(s) accessing the Internet during a test session
- Administrators or Coordinators leaving instructional materials on the walls in the testing room

Irregularities are unusual circumstances that impact an individual or group of students who are testing and may potentially affect student performance on the test, test security, or test validity. Examples if irregularities include:

- Student(s) cheating or providing answers to each other
- Disruptions to a test session, e.g., internet outage, a fire drill, a school-wide power outage
- Administrators or Coordinators failing to ensure administration and supervision of the assessments by qualified, trained personnel
- Administrator gives incorrect instructions that are not corrected prior to testing
- Administrators or coordinators giving our the username and password for authorized users to other individuals, including other authorized users
- Administrator allowing students to continue testing beyond the close of the selected testing window
- Administrator or teacher coaching or providing any type of assistance to students that

may affect their responses

- Administrators providing students with non-allowable materials or devices or allowing inappropriate accommodations during the test administration
- Administrator allowing anyone other than a student to log into the assessment unless prescribed as an allowable accommodation in the student's IEP.
- Administrator or Coordinator sending a student's name and SSID together in an email message.
- Administrator providing a student access to another person's work/responses

Breaches are events that pose a threat to the validity of the test. Examples may include such situations as a release of secure materials or a repeatable security/system risk. These circumstances have implications beyond the school and beyond Hawaiʻi. A breach incident must be reported immediately! Examples of breaches include:

- Administrator or Coordinator modifying student responses or records at any time
- Administrator allowing students to take home test items, reading passages, writing prompts, or scratch paper that was used during the assessment or failing to otherwise securely store assessment materials.
- Administrators or students copying, discussing, or otherwise retaining test items, stimuli, reading passages, writing prompts, or answers for any reason. This includes the use of photocopiers or digital, electronic, or manual devices to record or communicate a test item. This also includes using secure test items, modified secure test items, reading passages, or writing prompts for instructional purposes. (TAs are allowed to produce materials for students who have Braille, Print on Request, or Large Print accommodations is allowed. These materials must be secured and shredded until shredded and cannot be retained from one test session to another.)
- Secure test materials are shared with the media by anyone.
- Administrator, Coordinator, or student improperly removing secure testing materials such as test items, stimuli, reading passages, writing prompts, or scratch paper from the testing environment.

The following descriptions provide further guidance for dealing with some specific testing incidents.

- If a student becomes ill while taking an assessment or exam, pause the student's test session and allow the student to complete the assessment or exam at a later time.
- If a student cheats, remove the student from the testing room immediately. Pause the student's assessment or exam. The School Administrator must contact the student's parents immediately to inform them of their child's cheating and the associated consequences.
- If a student becomes disruptive, remove the student from the testing room immediately.

Pause the student's assessment or exam. The student may be given another opportunity to finish the assessment or exam at a later time. The School Administrator must contact the student's parents immediately to inform them of their child's disruption and the associated consequences.

- If there is a major disruption such as: internet outage, a fire drill, a school-wide power outage, or a natural disaster, and if the Test Administrator can safely access the Test Administrator workstation before leaving the testing room, then he or she should pause all assessments. If he or she cannot safely access the Test Administrator workstation, then he or she should evacuate and secure the testing room consistent with the school's evacuation policy. Upon returning to the testing room, the Test Administrator should pause all assessments or exams before students return to their stations. This helps ensure that a student does not view or complete another student's assessment or exam if he or she sits at the wrong computer by mistake.

  In cases where the assessment has been paused for more than 20 minutes due to a major disruption the programming of the online system will not allow a student to review previously answered questions. In such cases, the Test Coordinator should contact the Student Assessment Section by phone, fax or e-mail.

Reporting Testing Incidents

All staff members at a school are required to report testing incidents to the School Administrator. Testing incidents that do not involve the Test Coordinator should also be reported immediately to the Test Coordinator. School Administrators who have witnessed, been informed of, or suspect the possibility of a testing incident that could potentially impact the integrity of the assessments or exams and test results should immediately contact the Student Assessment Section:

Breaches pose a serious threat to the integrity of the assessment and requires that the incident is addressed to the extent possible at the school site, that it be reported to the appropriate school personnel right away, and that both the Complex Area Superintendent and Student Assessment Section be contacted by telephone. A more complete report of the incident should be submitted to the Student Assessment Section using the Testing Incident Report Form, found in Appendix L, by the end of the school day during which the incident occurs. Depending upon the exact nature of the Breach, these reports may be forwarded to the Office of the Superintendent.

Improprieties and Irregularities should be reported to the Student Assessment Section within 24 hours. These are to be reported using either the Testing Incident Report Form or using the Testing Incident section of the online TIDE system. The TIDE system should only be used to report incidents

that involve a student and test and that require an action for the test such as to invalidate, reset, reopen, revert a test that was invalidated, grant a grace period, or report a problem with an item (Refer to the TIDE User Guide pp. 40-52) . The Testing Incident Report Form should be used to report any other Improprieties and Irregularities. The completed form can be faxed to the Student Assessment Section at (808) 733-4483 or scanned and e-mailed to hsa/SAS/HIDOE@notes.k12.hi.us. (The full Lotus Notes address is required)

Student Assessment Section staff will review each report and notify the TC and other relevant school-level personnel of the resolution in a timely manner. In some cases there may be a need for additional communication and clarification prior to final resolution.

2014–2015 Hawai'i Assessment: Testing Incident Report Form		
School:	School Code:	Today's Date:
School Telephone Number:	Test Coordinator Name:	
Person Completing this Report:	Test Administrator Name:	

Severity Level: ☐ Impropriety ☐ Irregularity ☐ Breach

Initiated by: ☐ Adult(s) ☐ Student(s)

Assessment: ☐ SB Math Non-PT ☐ SB Math-PT ☐ SB ELA Non-PT ☐ SB ELA-PT ☐ HSA Science ☐ HAS-Alt

End of Course Exam: ☐ Biology ☐ Algebra I ☐ Algebra II ☐ US History ☐ Expos Writing ☐ HAS-Alt

Date and Time of Incident:	Grade Level:	Test Session ID:

Description of Incident

Description of Action Taken

Adults Involved:

Name	Assessment Role	Description of Involvement	Action Taken

Students Involved:

SSID	Description of Involvement	Action Taken

Attach additional sheets if necessary.

The completed form should be faxed to the Student Assessment Section at (808) 733-4483 or scanned and e-mailed to hsa/SAS/HIDOE@notes.k12.hi.us (The full Lotus Notes address is required.)

Policies: Student Confidentiality and Assessment

Federal law (the Family Educational Rights and Privacy Act) prohibits the public disclosure of student information or test results. The following are examples of prohibited practices:

- Giving out TIDE login information (username and password) either to other authorized TIDE users or to unauthorized individuals
- Sending a student's name and 10-digit State Student Identification Number (SSID) together in an email message. If information must be sent via email or fax, include only the SSID, not the student's name
- Giving students the wrong SSID during the login process, causing students to log in and test under another student's SSID

Student test materials and reports must not be exposed in such a manner that student names can be identified with student results, except to authorized individuals with an educational need to know.

10-Digit State Student ID Numbers

All students must be enrolled at their testing schools before they can take the online assessment. If a student is not enrolled at the testing school, this information must be updated in the student information system before the student can be tested. Data from the Department's student information system will be uploaded nightly into the online TIDE system. Student information will appear in TIDE about 48–72 hours after it has been entered into eSIS/SSES.

Students will log into an online assessment using their legal first names, their SSID, and a Test Session ID. They should have their SSID prior to testing. The SSIDs may be printed on cards and distributed to the students at the beginning of each test session so they can log into the system. However, student personal information, including the SSID, is confidential. If papers or cards containing both the student name and the SSID are distributed, these papers or cards must be collected before the students leave the testing room and stored at a secure location until they are needed for the next test session. All student personal information printed on paper or cards must be shredded after students have completed the appropriate online assessments for 2014–2015.

Only students may log into their online testing session. Test Administrators, proctors, or other staff may not log in using a student's SSID (except when called for in a student's IEP), although they may assist students with logging in.

Preventing Student Cell Phone Access during Testing

Updated 7/23/13

The Rule: Page 17 of the 2013-2014 Test Administration Manual prohibits students from "accessing or using electronic equipment (e.g., cell phones, PDAs, iPods, or electronic translators) during testing."

Promising Practices: Preventing students from accessing cell phones during testing is an important part of ensuring security of the test environment. However, enforcing this rule poses a variety of challenges for districts. Various districts have reported using a combination of the following methods to prevent student cell phone access during testing:

- Student handbooks contain the policy that cell phone access/use is prohibited on the school premises, during school hours, and / or during testing.
- TAs require that students leave cell phones in their lockers. If students bring cell phones into to the testing environment, TAs instruct students to "check in" their phones with the TA. The TA holds onto the phones until the students leave the testing environment. To prevent theft, some districts have TAs lock phones in a secure place accessible only to the TA.
- TAs remind students before each testing event that cell phones are not allowed. To increase awareness, some districts have also sent home reminders about the district policy to parents.
- Districts have established disciplinary policies for students who break the rule, ranging from detentions to suspension depending on the severity of the violation.

SBAC State Smart Sheet for Operational Testing

Technology

Test-Taking Devices and Approved Secure Browsers - Smarter Balanced requires that testing devices meet certain minimum requirements and that they run on an approved secure browser. The official Smarter Balanced policy regarding testing devices can be reviewed in the Technology Strategy Framework and Testing Device Requirements. The current list of approved secure browsers, corresponding devices, and sunset dates are available on the Smarter Balanced website.

iPad Application Installation – The Apple iPad is an approved device for use with the Smarter Balanced assessments. In order to meet test security requirements, all testing devices must run an approved secure browser. Smarter Balanced strongly recommends that iPads used for testing run iOS 8.1.3. For additional information, please reference the Smarter Balanced guidelines for the configuration of iOS devices.

See *Appendix C* of the *Test Administration Manual* for additional information about using secure browsers and ensuring tech readiness.

Test Security

Smarter Balanced has a vested interest in ensuring that assessments are supported by security protocols that establish both fairness for student engagement and validity in the interpretation of results. Maintaining test security during administration of the summative assessment is critical to preserving the integrity of the test. The *Guidance for Social Media Summative Assessment Monitoring* is available in *Appendix F* of the *State Procedures Manual* and provides recommendations for how states can monitor social media to identify instances of test items being posted online.

- The UCLA student clerks and Smarter Balanced Communications Specialist Nicole Siegel will monitor social media Monday through Friday, 6 a.m. to 5 p.m. PST. When a summative or interim assessment item is identified, all relevant information will be shared with the appropriate State Lead via email. States should contact the school the student attends and take necessary actions to have the item removed from social media. Please send a follow up email to sb@smarterbalanced.org on the resolution.
- Consult *Appendix G: Item Risk Rubric* of the *State Procedures Manual* to determine whether the breach requires the item to be removed from the assessment. If you have concerns about an item breach and believe the item should be removed, please email sb@smarterbalanced.org. You will receive a response within two hours.
- If a member of the state education agency is monitoring social media and identifies an item of concern, please flag for Smarter Balanced by sending an email to sb@smarterbalanced.org. The subject line of the email should read:

Social Media Test Security Issue. In this email, please include the following information:
    - A description of the image
    - Social media site where the image was posted
    - Hyperlink to the image or a copy of the image itself
    - Date published
    - Date removed
- Primary search criteria will include the following terms: @SmarterBalanced @smarterbalance @smartbalance #sbac #smarterbalance(d) #commoncore #ccss #supportthecore #assessments.
- The UCLA student clerks will conduct secondary searches for state-specific test names.

Helpful Materials

Test Administration Manual – The *Test Administration Manual* provides instructions and guidance for the Smarter Balanced online, **open-source system**. It is expected that all states will need to customize this manual to meet state-specific needs.

State Procedures Manual – The *State Procedures Manual* is designed to help state leadership prepare for the administration of the Smarter Balanced assessments. It includes information for the summative assessments, interim assessments, data warehouse/reporting system, and Digital Library. The manual provides a general overview of Smarter Balanced policy topics such as test security, test scheduling, and general administration of the summative and interim assessments.
To access the Smarter Balanced State Procedures Manual, visit the Assessment Training and Operations Folder on the secure FTP site.

Educator Communication Toolkit – The Educator Communications Toolkit is intended to assist educators in communicating about the Smarter Balanced Assessment System. The toolkit includes many helpful resources like talking points and common misperceptions about Smarter Balanced. The toolkit should be customized by states prior to distribution.

School – District Leader Communication Toolkit – The School – District Leader Communication Toolkit is intended to assist leaders at the district and school level in communicating about the Smarter Balanced Assessment System to a variety of key stakeholders. The toolkit includes many helpful resources like suggested outreach tips, a press release template, and talking points.

Additional materials you may find helpful are available on the Smarter Balanced Secure FTP site including a variety of accessibility resources like Audio Guidance Tips for TAs, Read Aloud Guidelines and the Scribing Protocol.

Refusal

- Collect the number of students refusing to take the test to provide accurate

information to state leaders and the media.

- Federal guidance requires all students be assessed. The US Department of Education notes that federal funds could be at risk and if numbers fall below 95 percent of the state's accountability plan. Cite state law as well.
- Suggested talking points:
    - Assessments help to provide valuable information to parents, teachers, and students, and the state is committed to ensuring that they are as accurate as possible and welcome feedback on ways to improve them.
    - Ultimately, the greatest penalty for avoiding these assessments is not being able to provide meaningful information on where a student stands on their path to success.
    - [If applicable] College and universities will use Grade 11 assessment results to help determine whether admitted students are exempt from non-credit bearing courses. If a high school student does not take the assessments, he or she will not have that opportunity to earn an early exemption from these developmental or remedial courses.

Communications Tips

- Connect with a local school district to have the chief and other key leaders observe Smarter Balanced testing in person.
- Request that your vendor provide you with daily or weekly numbers of students that have started and completed the assessments.
- Consider organizing a survey to obtain information from key stakeholders, such as students, teachers, or administrators on successes and challenges.
- Describe the value of Smarter Balanced when engaging with reporters. Focus on key messages including the following: that Smarter Balanced is a quality assessment system, that teachers helped build the assessment, and that the consortium is a state-led organization.
- Consider adding daily vendor meetings to your schedule (at least for the first few weeks of testing) to discuss and troubleshoot any emergent issues.

SBAC State Procedures Manual—Item Risk Rubric

Smarter Balanced Item Exposure Risk Analysis

Smarter Balanced States have an individual and collective interest in maintaining the security of the summative assessment items. States may use the following rubric to evaluate the risk that item exposure creates.

A greater degree of exposure and/or a longer duration of exposure increases the threat to the validity of the test.

Exposure Duration	Levels of Risk
1. Degree of cumulative exposure	a. Newspaper/mainstream media – High Risk b. Social Media – Medium Risk c. Local Exposure - Medium Risk
2. Duration of exposure	a. Permanent (e.g. paper exposed) – High Risk b. Moderate (online, but removed within 24 hours) – Medium Risk

The nature content that is exposed will help to determine the threat to the validity of the test. Content that isn't accessible to a large portion of the student population and/or otherwise isn't likely to be present on their tests constitutes a lower risk to the tests' validity.

Exposure Scope	Levels of Risk
1. What type/portion of the item is exposed	a. All information is self contained – High Risk b. Items that have an External Reference – High Risk c. Stimuli – Medium Risk
2. What is the likelihood students will see the exposed content on their tests	a. Likely – High Risk b. Unlikely – Medium Risk
3. Presentation of item	a. English – High Risk b. Language other than English – Medium Risk c. Braille and ASL –Medium Risk

Smarter Balanced will collaborate with states and service provides to determine whether the action states need to take. The test that the Consortium will apply are described by following questions:

- Will the validity of the Test be improved based on removing the item from the pool?

  - If the item is highly exposed but unlikely to be seen by a student, the risk of interacting with the item pool may not be offset by the reduction of risk to validity.
  - If the item measures a unique dimension of the construct (either via content or difficulty) the validity of the test could be reduced by eliminating the item
- Will public perception of the test be improved by the Action?
  - The Consortium needs to take a strong stance on test security
  - Removing exposed items may be necessary to retain public confidence

If the Consortium determines that an action is required, the Consortium will notify the states' designated service providers, the state project managers identified on the MOU, and the K-12 state lead of the item ID that must be removed from the pool. Service providers will need to remove the item within 1 business day.

Unless otherwise determined by the Consortium on a case by case basis, states do not need to re-score tests for students who respond to an item exposed between the time the item was exposed and when the item was removed from the service providers systems.

Test Environment and Security

Students are to be provided with a quiet environment free of distractions that might interfere with their ability to concentrate or otherwise compromise the testing conditions. In addition, the security of assessment instruments and the confidentiality of student information are vital. Everyone who administers or proctors a Hawaiʻi online assessment is responsible for ensuring that there is a quiet environment and that the test security requirements in the table below are met.

Requirement	Description
School Administrators understand the guidelines and processes for the test environment and test security	
Test Coordinator and Teat Administrators are qualified and trained	All Test Coordinators (TCs) and Test Administrators (TAs) must meet qualification requirements (i.e. have a professional license). TCs must participate in training and TAs must be certified.
Test materials are kept secured	All assessment materials must be kept in a secure location accessible to only the TC and TAs.
TIDE usernames and passwords are kept confidential	Giving out TIDE login information (username and password) either to other authorized TIDE users or to unauthorized individuals is prohibited.
Access to the assessments is restricted	Providing access to secure assessments to anyone before, during, or between sections of any assessment as well as reviewing or discussing secure test items or student responses during or after an assessment administration are prohibited. This includes analysis of test items, stimuli, reading passages, or writing prompts at any time.
Confidentiality of student personal information is maintained	The confidentiality of student personal information is maintained as prescribed by the Family Educational Rights and Privacy Act. Any documents, papers or cards that contain both the student name and the State Student Identification Number (SSID) must be collected before the students leave the testing room and either securely stored to be used in a subsequent test session or shredded. All printed student personal information must be shredded after students have completed the assessments.
Students with Braille, Print on Request, and Large Print, as well as HSA accommodations are tested individually.	Students taking the HSA-Alt as well as those with Braille, Print on Request, and Large Print accommodations are to be tested individually. The testing of these students should take place in an environment out of the sight and hearing of other students. Note: All HSA-Alt students are tested individually in an environment out of the sight and hearing of other students.

Requirement	Description
Information displayed in the testing environment is limited	Displaying content- or process-related information on bulletin boards, chalkboards or dry-erase boards, or charts is not allowed. Any displays that might assist students in answering questions must be removed or covered.
Access to the testing environment is limited	Access to the testing environment is strictly limited to the TC, authorized TAs and the students being assessed. Unauthorized individuals must not be in the room where a test is being administered. Note: An aide or other staff member accompanying a student as called for in an IEP are allowed in the room during testing but cannot interact with the assessment. Note: Second Raters, when called for in the testing guidelines are allowed in the room during testing.
Electronic devices including cell phones are off and put away	All cell phones and other electronic devices must be turned off and put away during testing, preferably put in a backpack or bag, and placed in a designated, secure area in the testing room. Note: Students are allowed to use appropriate assistive technologies identified in their IEPs. Note: HSA-ALT students may use i-Pads for the online administration using the secure browser.
The testing environment minimizes student opportunities to see the work of others	Students should be seated so there is enough space between them to minimize opportunities to look at each other's work, or should be provided with table-top partitions or other types of barriers.
Testing is carried out using the secure browser	All online assessments must be carried out using the secure browser and student computers in the testing environment should not have any other access to the Internet.
Students log themselves in using their own SSID	A student being tested must log him/herself into the assessment using their unique SSID unless otherwise prescribed as an allowable accommodation in the student's IEP. Outside of the accommodation previously mentioned, adults are not allowed to access the online testing system using an SSID.
Students only have access to approved resources	Students should have access to and use of only those allowable resources that are permitted for each specific assessment. The use of unapproved resources is prohibited. Note: Approved resources include those identified in a student's IEP or in accommodations identified for that student in TIDE.
Students demonstrate appropriate behavior during testing	Students are actively supervised and there is quiet environment, without talking or other distractions, including gestures and sounds that might interfere with a student's ability to concentrate or might compromise the testing situation.
Students receive no assistance which will affect their results.	TCs, TAs, proctors, and other students are prohibited from coaching or providing any other type of assistance that may affect a student's responses. Neither adults nor students may alter the response(s) of another student or encourage a student to alter his or her response(s). This includes students cheating or providing answers to each other by talking, passing papers or sharing materials or information by any means.

Requirement	Description
Students cannot leave the testing environment without permission	Students cannot leaving the testing environment without permission and until their test is paused. Note: In the case of the HAS-Alt, the assessment may be paused and breaks taken at the discretion of the TA when such a pause is deemed necessary based upon student needs.
Students with Print on Request and Braille accommodations must be tested individually	The TA may print the stimulus or test questions for an online assessment including the Braille version if these accommodations are identified for a student. Secure materials must be printed in the testing room and these materials cannot be retained from one test session to the next. Students with these accommodations should be tested individually.
All printed test materials must be collected, secured and shredded	All printed secure test materials including: braille materials; test items, stimuli, reading passages, or writing prompts printed as part of accommodations; and, allowable paper resources, as well as scratch paper and any paper students write on during testing, must be collected immediately after each test session and secured until shredded. These materials cannot be retained from one test session to the next. In the case of the HSA –Alt, all materials in the Test Kit, except the physical manipulatives provided, as well as any TA created picture cards that were substituted for picture symbols, brailed materials and Second Rater Student Worksheets and Answer Keys must be inventoried and returned to AIR. Note: For HAS-ALT scratch paper, etc., is moved to the shred category Note: The one exception is in the case of SB Performance Tasks Parts 1 and 2, the TA may collect and secure student scratch paper and note s at the end of Part 1 and return it to them at the start of Part 2. At the end of Part 2, all scratch paper and notes must be collected and secured until shredded.
All reproducing, photographing, or recording is prohibited	Reproducing, photographing, or recording any information from secure assessments, excluding the allowable reproduction and printing described in the TAM, is strictly prohibited. Test items, stimuli, reading passages, or writing prompts must never be released to anyone, sent by email or fax, or replicated/displayed electronically. Note: Producing materials for students who have Braille, Print on Request, or Large Print accommodations is allowed. These materials must be secured and shredded until shredded and cannot be retained from one test session to another.
The disclosure of any information from secure test materials is prohibited	Disclosure of any information from secure assessment materials to anyone, including other students or unauthorized adults such as parents, other relatives, or friends is strictly prohibited. This includes discussions about the test and the improper removal of any secured materials from the testing room.

Requirement	Description
Secure materials and information cannot be used for instruction	Secure test items, stimuli, reading passages, or writing prompts must not be used for instruction. Activities that are based upon information gained from your role as a TC or TA and are created or implemented for the sole purpose of increasing test scores are a violation of ethical assessment administration.
Testing sessions must be free from major disruptions	To the extent possible, testing sessions should be scheduled so they are free of major disruptions such as fire drills, computer network down times, and school-wide power outages. Hardware and software should be tested prior to the beginning of testing.
Any deviation in test administration (Testing Incidents) must be reported	Any deviation in test administration, including not meeting the requirements described above, must be reported as a testing incident. Test administrators or other individuals who have witnessed, been informed of, or suspect the possibility of a testing incidence that could potentially affect the integrity of the tests should report the incidence immediately following the steps described in **Testing Incidents** in the **Test Administration Manual.**

DAVID Y. IGE
GOVERNOR

KATHRYN S. MATAYOSHI
SUPERINTENDENT

STATE OF HAWAI`I

DEPARTMENT OF EDUCATION

P.O. BOX 2360

HONOLULU, HAWAII 96804

Office of Strategy, Innovation and Performance

June 27, 2017

TO: Complex Area Superintendents
Principals (All)
Public Charter School Executive Director
Public Charter School Directors (All)
Test Coordinators (All)

c: Assistant Superintendents
State Public Charter School Commission
Superintendent's Office Directors
Office of Curriculum, Instruction and Student Support
Office of Information Technology Services
Assessment & Accountability Branch

F R O M: Tammi Chun
Assistant Superintendent

SUBJECT: Hawaii Statewide Assessment Program, School Year 2017-18

The Hawaii Statewide Assessment Program's (HSAP) portfolio of assessments provide data annually on student, school and system educational performance. Statewide assessment data provides feedback on students' progress and informs planning for improvements. HSAP fulfills requirements of Board Policies E-102, 102-3, and 102-6, Chapter 302A-201 of the Hawaii Revised Statutes, and the Every Student Succeeds Act (ESSA). Additionally Strategic Plan Indicators of student success include student assessments and are reported annually as part of Strive HI and provides data to support Goal 3, Objective 3b of the Strategic Plan: "Provide user-friendly data to support strategic decision-making and accountability for Student Success." This memo describes HSAP for School Year 2017-18 (SY 2017-18). This memo supersedes the prior memo regarding SY 2017-18 testing windows (published on May 30, 2017).

The HSAP portfolio of assessments support implementation of standards-based education in every public school in Hawaii. HSAP's standards-based assessments are aligned to the learning expectations of every student and measure students' progress towards being on the pathway of college and career readiness. These results complement teacher and school-selected assessments to inform instructional practice and collaborative, honest conversations about the extent to which students' academic progress is satisfactory or needs to further be supported.

The state's assessment portfolio is reviewed annually and adjustments are made based upon the current priorities, policies, and technical developments. A number of changes are being made for SY 2017-18 to streamline the assessment portfolio in alignment with the Strategic Plan which states, "The federal Every Student Succeeds Act requires standardized testing. In addition to federally required tests, schools may

choose to assess students to inform planning for learning… and to validate and report on students' academic progress… This Strategic Plan does not mandate additional testing (Strategic Plan, 2017-2020, page 8)."

SMARTER BALANCED ASSESSMENTS

The Smarter Balanced Assessments in English Language Arts (ELA)/Literacy and Mathematics serve as the statewide assessment of Hawaii's rigorous college and career ready academic standards. Smarter Balanced Assessments are administered across 15 states, the U.S. Virgin Islands, and the Bureau of Indian Education. The Smarter Balanced Assessments are fully aligned to the Hawaii Common Core Standards and measure the depth and breadth of student knowledge and skills. These assessments are administered to all HIDOE and public charter school students in grades 3-8 and 11. All students in tested grades should take the Smarter Balanced Assessments, with the exception of students taking the Hawaii State Alternative Assessments (HSA-Alt) or Kaiapuni Assessment of Educational Outcomes, as described below.

A revised version of the Smarter Balanced assessments will be administered beginning SY 2017-18. This revised version uses more efficient test questions and streamlines the performance tasks. The computer adaptive test, with some modifications, will continue to be administered for both ELA/Literacy and Mathematics. The ELA/Literacy performance task will be reduced to one research item and the full-write assignment. The mathematics performance task will not be continued as part of the summative assessment.

The revised Smarter Balanced Assessments will measure the same standards and provide the same information with reliability and validity. These changes are anticipated to reduce the test taking time by 1.5 hours per student, on average. We anticipate a greater impact in the lower grades where testing times were longer and less in 11th grade where testing times were shorter. The reduced time for test administration provides more time for teacher-designed instruction and assessment to advance student learning and success.

Smarter Balanced Summative Assessments

Assessment	Content Areas	Grade(s)		Testing Window	
				Open	Close
Smarter Balanced	ELA/Literacy Mathematics	3 – 8 and 11		02/20/18	05/31/18
Smarter Balanced	ELA/Literacy Mathematics	First Semester Students at Block Schedule Schools ONLY	11	11/27/17	05/31/18
Smarter Balanced	ELA/Literacy Mathematics	Multi-track Schools	3 – 8 Yellow Track	02/20/18	05/31/18
			3 – 8 Red, Blue, and Green Tracks	03/19/18*	06/22/18*

*Subject to change

HAWAII STATE SCIENCE ASSESSMENTS

Hawaii public schools began implementation of Next Generation Science Standards (NGSS) in SY 2016-17, with full implementation targeted for SY 2019-20 (DOE Memo – August 5, 2016). During SYs 2017-18 and 2018-19, schools will transition from the Hawaii Content and Performance Standards III (HCPS III) to

the NGSS. This transition phase requires the administration of "bridge" assessments that measure the subset of standards that are shared by both the HCPS III and the NGSS.

Beginning SY 2017-18, the bridge version of the HSA Science Assessments will be administered to students in grades 4 and 8; students will have up to two opportunities to take the test in Spring 2018. At the high school level, the bridge version of Biology 1 End-of-Course Exam will be administered to all students enrolled in a Biology 1 course.

These assessments are required and meet federal ESSA requirements for science testing. All students in tested grades should take the HSA-Science, with the exception of students taking the Hawaii State Alternative Assessments (HSA-Alt) or Kaiapuni Assessment of Educational Outcomes, as described below.

Hawaii State Science Assessments Administration

Assessment	Content Area	Grades	Number of Opportunities	Testing Window	
				Open	Close
HSA	Science	4 and 8	2	01/10/18	05/31/18
HSA	Science Multi-track Schools	4 and 8	2	01/10/18	06/22/18*

*Subject to change

HAWAII STATE ALTERNATE ASSESSMENTS (HSA-ALT)

Students with significant cognitive disabilities participate in the Hawaii State Alternate Assessments (HSA-Alt) because their performance cannot be accurately assessed using the general statewide assessments even with appropriate accommodations. These assessments are administered to students in grades 3-8 and 11 who meet the participation requirements for the alternate assessment.

Hawaii State Alternate Assessments (HSA-Alt) Administration

Assessment	Content Areas	Grades	Mode	Testing Window	
				Open	Close
HSA-Alt	ELA/Literacy Mathematics	3 – 8 and 11	Online	02/20/18	05/31/18
			Paper/Pencil*	02/20/18	05/25/18
HSA-Alt	Science	4, 8 and 11	Online	02/20/18	05/31/18
			Paper/Pencil*	02/20/18	05/25/18

* Paper/Pencil administration must be verified by the Assessment Section

KAIAPUNI ASSESSMENT OF EDUCATIONAL OUTCOMES (KÂ'EO)

The Kaiapuni Assessment of Educational Outcomes (KÂ'EO) in Language Arts, Mathematics and Science are developed and administered in the Hawaiian language. The language arts and mathematics assessments are administered to grades 3 and 4 public school students in the Hawaiian Language Immersion Program. The science assessment is administered to grade 4 students in the program. Kaiapuni students in grades 3 and 4 take KÂ'EO instead of Smarter Balanced and HSA Science.

In SY 2017-18, KÂ‘EO assessments in Language Arts and Mathematics are being developed for grades 5-8 and a Science assessment is being developed for grade 8. These newly developed KÂ‘EO assessments will be field tested in Spring 2018; student and school reports of results for field test assessments will not be available during this development year. The Department is negotiating with the U.S. Department of Education to allow Kaiapuni students taking the field test versions to take the field test only, foregoing student and school reports for SY 2017-18 ("double testing waiver"). The outcome of those negotiations impacts whether Kaiapuni students will also take the Smarter Balanced Assessments for grades 5-8 and HSA-Science for grade 8 in 2017-18. The Assessment Section is responsible for the planning and communication of these issues with the Office of Hawaiian Education.

Kaiapuni Assessment of Educational Outcomes (KÂ‘EO) Administration

Assessment	Content Areas	Grades	Testing Window	
			Open	Close
KÂ‘EO	Language Arts Mathematics	3 and 4	04/02/18*	05/31/18
KÂ‘EO	Science	4	04/02/18*	05/31/18
KÂ‘EO Field Test	Language Arts Mathematics	5 - 8	04/02/18*	05/31/18*
KÂ‘EO Field Test	Science	8	04/02/18*	05/31/18*

*Subject to change

END-OF-COURSE EXAMS

The End-of-Course (EOC) exams measure students' levels of proficiency for the standards and benchmarks assigned to the course. The Algebra 1 and Algebra 2 EOC Exams measure students' levels of proficiency for the Hawaii Common Core Standards in Mathematics for respective courses; these exams may be given to students in any grade level for whom the tests are appropriate. These tests are provided to support schools' and teachers' instruction, but administration of these tests are optional. Costs of these optional EOCs are covered by the Department for all public schools.

The Biology 1 EOC Exam is required to be administered to all public school students enrolled in Biology 1 since it is Hawaii's statewide assessment to meet federal assessment requirements of the Every Student Succeeds Act (ESSA); this is described on page 2 as part of HSA-Science Assessments.

Due to low participation rates and the transition to C3-based Social Studies standards (scheduled for Board of Education approval in June 2018), the U.S. History EOC Exam will no longer be administered.

End-of-Course Exams Administration

EOC Exam	Administration	Testing Window	
		Open	Close
Algebra 1 (Optional) Algebra 2 (Optional) Biology 1** (Required)	Fall (block schedule schools only)	11/27/17	12/21/17
Algebra 1 (Optional) Algebra 2 (Optional) Biology 1** (Required)	Spring	04/23/18	05/31/18
Algebra 1 (Optional) Algebra 2 (Optional) Biology 1** (Required)	Multi-track Schools	06/12/18	06/22/18*
Algebra 1 (Optional) Algebra 2 (Optional)	Summer	06/12/18*	07/19/18*

Biology 1** (Required)			

*Subject to change
**Required as statewide assessment to meet federal ESSA requirements for assessment in science

COLLEGE ADMISSIONS EXAM

The Department will continue to offer the ACT college admissions exam for high school juniors in SY 2017-18. However, this exam is now optional. The exam is being offered to support schools and students' college and career preparation to meet our Strategic Plan Goal 1, Objective 1: "All students are empowered in their learning to set and achieve their aspirations for the future." To expand options for students and to support schools, the Department will cover the cost of the ACT college admissions exam.

DOE schools, in consultation with their school community and complex area superintendent, will have the option of administering the ACT to grade 11 students either a) for the entire grade level on the statewide administration date, 02/27/18, or online during the school days as listed in the table below or b) on an individual basis at a national testing center on 02/10/18 through vouchers provided by the Department. Charter schools should make this decision in consultation with their school communities and local governing boards. Schools will need to notify the Assessment Section of their plan for offering the exam by November 2017; Assessment Section will coordinate this step via test coordinators.

The ACT Aspire assessments are no longer being offered as part of the HSAP or Hawaii's statewide contract with ACT.

ACT College and Career Readiness Assessments Administration

Assessment	Content Area	Grade	Location	Mode	Testing Window	
					Open	Close
The ACT	English Mathematics Reading Science Writing	11 *(optional, based on consultation with school community and CAS)*	School	Online (Tu, W, Th only)	02/27/18	03/08/18
				Paper/Pencil	Administration Date: 02/27/18	Make Up Testing Date: 04/03/18*
			ACT National Testing Center	Voucher	Administration Date: 02/10/18*	N/A

*Subject to change

ACCESS for ELLs 2.0 ONLINE

The ACCESS for ELLs 2.0 is an English language proficiency assessment administered to all English Learners in Kindergarten through 12th grade to monitor students' progress and proficiency in acquiring academic English. ACCESS is required for all English Learners by ESSA. Beginning SY 2017-18, all schools will administer the assessments online.

ACCESS for ELLs 2.0 Online Administration

Assessment	Content Area	Grades	Mode	Testing Window	
				Open	Close
ACCESS for ELLs 2.0 Online and Alternate ACCESS	Listening Reading Speaking Writing	Kindergarten through 12	Online Paper/Pencil**	01/16/18	02/26/18*

*Subject to change
**Paper/Pencil administration in K (all domains) and grades 1-3 (writing only)

NATIONAL ASSESSMENT OF EDUCATIONAL PROGRESS (NAEP)

Hawaii will continue to participate in federally mandated assessments. ESSA requires state participation in Reading and Mathematics which are administered in odd-numbered years to a sample of schools and grade 4 and 8 students. There are no mandatory NAEP assessments in SY 2017-18.

During SY 2016-17, Superintendent informed the U.S. Department of Education National Assessment of Education Progress staff and the State of Hawaii Board of Education that non-mandatory NAEP assessments will not be administered to minimize mandatory testing in our schools.

If you have questions regarding the testing windows, please contact Brian Reiter, Administrator, Assessment Section, at (808) 733-4100 or via Lotus Notes email. If you have questions regarding the changes in the HSAP, please contact Tom Saka, Director, Assessment & Accountability Branch, at (808) 586-3283 or via Lotus Notes email.

KH/TC/SM:ja

APPENDIX E. Glossary of Test Security Terms

Breach
(1) an event, intentional or not, that results in the inappropriate exposure of test items or answers that could potentially impact the accuracy of the test results; OR
(2) an action by others before, during, or after a test administration to impact student test scores (e.g., educators changing student answer sheets).

Cheating
General term that can include educator or student misconduct or improprieties that includes intentional misbehavior or unethical practices. Note that this term is not used in every state. Some states avoid the use of the word “cheating” in their communications and use different terminologies.

Compromise
Disclosure of test items or forms; can be intentional or unintentional. May also refer to changing the interpretation of a test score or changing the test score itself.

Data Forensics
The use of analytic methods to identify or detect possible cheating. Procedures can include evaluation of score gains, aberrance or person fit, erasures, latency analysis, similarity analysis, and examination of changes in student responses (wrong-to-right, right-to-wrong, wrong-to-wrong).

Impropriety
Inappropriate misconduct; a more serious offense than an irregularity. The difference between impropriety and irregularity is usually defined in perception of the degree, intent, and/or effect of the misconduct.

Irregularity
This includes many different activities, not necessarily cheating, but anything unusual that happened during testing, such as the fire alarms went off or a power outage.

Misconduct
Misbehavior during testing, such as inappropriate proctoring or other violations of standard testing protocol.

Security Investigation
Follow-up activities regarding possible cheating or piracy of test materials. Typically involves the collection of evidence, review of available information, interviews of suspected staff, and summary of findings from the investigation.

Test Integrity
As presented in the NCME white paper from Greg Cizek (2012), test integrity emphasizes that valid testing requires the results to be useful, interpretable, accurate, and comparable. The technical merits of the test scores must meet industry standards with respect to fairness, reliability, and validity; however, cheating and security breaches can pollute the data, reducing or eliminating their value.

Test Piracy
Stealing of test forms, items, prompts, or other secure testing materials, often for the purpose of selling the materials to others.

Test Security Kit
A document for states that may provide instructions about a state's security-related procedures, processes, and regulations, including the escalation path to be followed in the event of a test security breach.

Validity
Validity refers to the extent to which a test accurately measures what it purports to measure. In the fields of psychological testing and educational testing, "Validity refers to the degree to which evidence and theory support the interpretations of test scores entailed by proposed uses of tests". In relation to test security, it is the most important aspect of an assessment. As Greg Cizek stated in his NCME whitepaper (2012), "Assessment requires that results be: accurate, fair, useful, interpretable, and comparable. The technical merits of test scores must meet professional and industry standards with respect to fairness, reliability, and validity. Test data must be free from the effects of cheating and security breaches **and** represent the true achievement measures of students who are sufficiently and appropriately engaged in the test administration. Cheating, falsifying data, security breaches, and other actions of academic fraud compromise the standards of fairness, reliability, and validity by polluting data."

Web Monitoring or Web Patrol

A process that can be used to address the risk to tests and items posed by illicit discussion, distribution, and sale of test content on the Internet. Web monitoring/patrol leverages technology tools and human expertise to identify, prioritize, and monitor

websites, discussion forums, peer-to-peer servers, etc., where sensitive test information may be disclosed or at risk of disclosure.