Cohesive Plan for Testing Breach Protocols and Procedures

I. Common Types of Breaches

- Unauthorized Access: When test questions or answers are accessed by individuals not authorized to view them.
- Cheating: Instances where students or staff engage in dishonest practices to gain an unfair advantage.
- Procedural Violations: Not adhering to the guidelines set for administering assessments, such as not following the correct timing or environment for testing.

II.Prevention and Proactive Security Measures

- Cultivate a Security Culture: Foster an effective security culture within the organization to prioritize test integrity, including all educators and test proctors completing the annual testing ethics training.
- Robust Authentication and Access Control: Minimize user accounts, implement passwordless approaches (MFA, biometrics like FIDO2/WebAuthn & CTAP), utilize role-based permissions, enforce strong password policies, restrict access with client certificates, deploy multi-factor authentication (MFA), regularly audit employee access, centralize logging of authentication attempts, and implement posture checking/network admission control.
- Secure Domain Management: Regularly audit registrar control panel access, use role accounts (e.g., hostmaster@) for domain contacts, deploy internal DNS resolvers, and implement DNS Response Policy Zone (DNSRPZ) to block malicious sites.
- Endpoint and Data Protection: Deploy endpoint protection, implement desktop firewalling, and utilize full disk encryption.
- Academic Honesty Education and Environment:
    - Ensure educators establish a classroom environment conducive to learning and academic risk-taking, provide support in research and study skills, offer further guidance on academic integrity, require students to cite sources and provide evidence, and annually evaluate the effectiveness of measures to promote academic integrity.
    - Educating students on the purpose and benefits of the assessments including the opportunity to demonstrate what they know.
    - Use appropriate proctoring practices during classroom assessments to set expectations prior to the summative assessment (see annual testing ethics training for appropriate proctoring practices).

- AI Responsible Use: Develop and annually review a District-wide AI Plan and AI Responsible Use Guidelines, ensure AI-enabled tools comply with State and federal law, provide staff training and student instruction on AI use, and require staff, students, and parents/guardians to sign authorizations for electronic network and unsupervised AI use.

III. Identification and Reporting of Breaches to Proper Entities

- Monitoring and Auditing: Monitor ongoing security management of systems, code base, and processes, centralize logging of all authentication attempts and monitor for abnormal activity, and regularly audit employee access to systems.
- Academic Dishonesty (Malpractice) Recognition: Educate staff and students on what constitutes academic dishonesty, including improper aid to students, plagiarism, collusion, and falsification.
- Electronic Device Usage Violations: Identify and address inappropriate use of personal electronic devices during school hours.
- Unauthorized Network Access: Recognize and restrict unauthorized access ("hacking") and disclosure of personal identification information on District networks.

IV. Incident Response and Remediation

- Incident Response Process: Establish a clear incident response process that addresses how the incident occurred, what the perpetrator did, how to return to business as usual, and how to prevent recurrence.
- Addressing Academic Dishonesty: Treat incidences with equity, consistency, procedural fairness, and timely resolution; ensure documentation of violations is confidential, and administer appropriate consequences for violations, which may include conferences, warnings, parent contact, detention, Friday School, suspension, etc.
- Electronic Device Confiscation: For violations of electronic device usage, confiscate devices and follow the LEA's policy for electronic devices.
- Network and AI Policy Violations: Failure to follow policies or administrative procedures will result in loss of privileges, disciplinary action, and/or legal action, based on the LEA's policies and procedures.
- Confidentiality of Student Records: Maintain confidentiality of student records and implement reasonable measures to protect against unreasonable access before loading confidential student information onto the network.

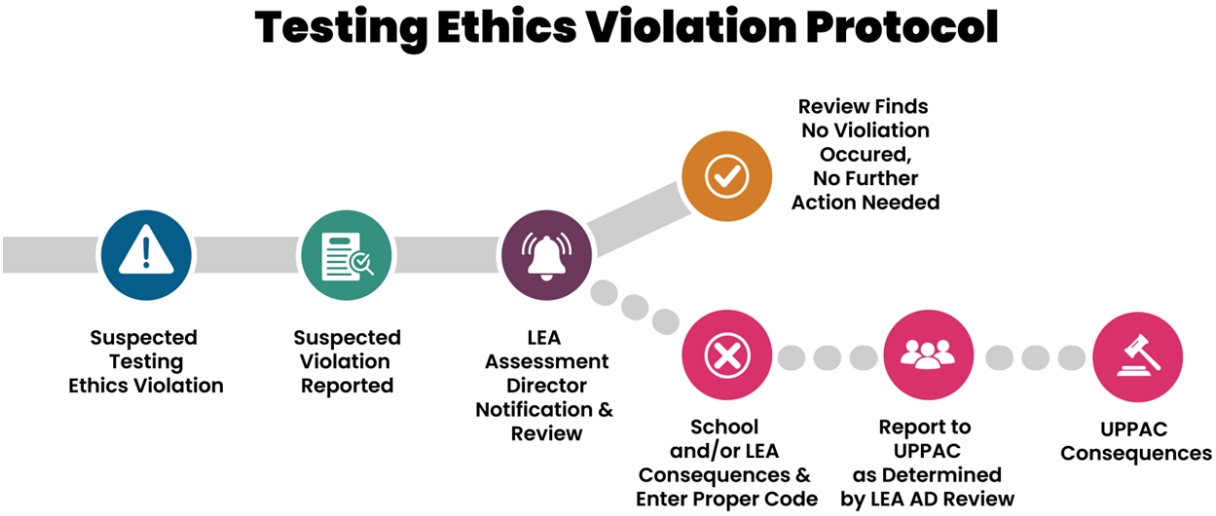
V. Student, Staff, and LEA Responsibilities

- Student Responsibilities: Produce authentic work based on individual, original ideas, fully acknowledge the ideas and work of others, citing sources, understand and abide by policies regarding cheating, inappropriate testing aids, copying, and electronic device use.
- Staff Responsibilities: Be familiar with emergency procedures and reporting; treat academic honesty professionally and follow guidelines; administer appropriate consequences for violations; and ensure electronic communications ensure student/staff privacy, safety, and security.
- LEA Responsibilities: Foster and maintain an atmosphere where educators feel safe to report possible ethical violations; ensure the school and LEA administrators know the LEA plan for ethical violations; ensure the assessment directors investigate ethical breaches and follow the LEA and state policies for remediation.

VI. Procedures for Ethical Violations

UT Admin Code R277-404-8 outlines the responsibilities of educators to comply with assessment requirements, protocols, and test security for both general and alternate assessments. The Board of Education in Utah values local control for LEAs, including matters of procedure in regards to addressing and remediating testing ethical violations or security breaches. Therefore, much of the processes for remediation of test security violations are left to LEAs to determine, with support from USBE as needed. The Standard Test Administration and Testing Ethics Policy outlines unethical testing practices and provides the following protocol LEAs should follow for remediating such violations:

- Testing ethics violations are to be reported to the supervisor of the person who may be investigated, the school administrator, the LEA assessment director, or the USBE Assessment department.
- Each LEA must determine local policies and procedures regarding ethics violations.
- In most cases, an initial investigation should be conducted at the school level.
- The LEA assessment director will review the initial investigation and determine findings.
- If the violation is of sufficient concern, the incident may also be forwarded to the Utah Professional Practices Advisory Commission (UPPAC) for review.
- If inappropriate practices are substantiated, educators or other staff may receive further training, a reprimand, be subject to disciplinary action, be terminated, and/or lose their Utah teaching license.



VII. Procedures for Detected Breaches at USBE

If a breach in test security is detected, USBE will implement the following procedure to notify LEAs:

1. Report to local school leaders to determine escalation status—USBE Assessment will inquire what LEA procedures will be followed.
2. The school leader follows up and reports back to USBE Assessment the results of their investigation.
3. USBE will determine what remediation, additional steps (if any), or further action that may be needed.
   a. State and LEA ethics policies and Utah Code violations may be reported to appropriate oversight personnel for possible referral to UUPAC and/or school board.
   b. LEA assessment directors may recommend USBE invalidate scores where security has been compromised; USBE will make the final determination to invalidate student test scores.