Procedure for Handling a Testing Security Breach

1. **Reporting**
    - Any staff member who observes or suspects a breach must report it immediately to the school's assessment director.
2. **Incident Documentation**
    - A formal **incident report** is completed, detailing:
        - What occurred
        - Who was involved
        - When and where it happened
        - Evidence (e.g., screenshots, photos, witness statements)
3. **Investigation**
    - The school/district conducts an **internal investigation**.
    - Students or staff may be interviewed.
    - Digital logs (e.g., test platform activity, computer use) may be reviewed.
4. **Containment**
    - Immediate steps are taken to **limit the breach's impact**, such as:
        - Stopping testing temporarily
        - Replacing compromised test content
        - Confiscating unauthorized materials (e.g., phones, scratch paper)
5. **Corrective Action**
    - Depending on the breach's severity:
        - Staff may receive retraining or disciplinary action.
        - Students may have test scores invalidated or retake the test.
        - In severe cases, legal or employment consequences may follow.
6. **Notification to State Office**

- The school or district must submit a report to the **state education office**, who may determine if further actions are needed.

7. **Prevention Plan**

   - Schools may be required to submit a **corrective/preventive action plan** outlining how similar breaches will be avoided in the future.