

TECHNOLOGY RESOURCES  
CYBERSECURITY

CQB  
(LOCAL)

<b>Plan</b>	The District shall develop a cybersecurity plan to secure the District's cyberinfrastructure against a cyberattack or any other cybersecurity incidents, determine cybersecurity risk, and implement appropriate mitigation planning.
<b>Technology Operations</b>	<p>All technology resources shall be backed up on a regular basis according to the security procedures. Virus protection shall be running and regularly updated on computers running on the District's network.</p> <p>All software installed on District workstations and network shall comply with the software's licensing agreement and the District's change control and approval procedures.</p>
<b>Coordinator</b>	The Superintendent shall designate a cybersecurity coordinator. The cybersecurity coordinator shall serve as the liaison between the District and the Texas Education Agency in cybersecurity matters.
<b>Training</b>	<p>The Board delegates to the Superintendent the authority to:</p> <ol style="list-style-type: none"><li>1. Determine the cybersecurity training program to be used in the District;</li><li>2. Verify and report compliance with training requirements in accordance with guidance from the <del>Department of Information Resources</del> <a href="#">Texas Cyber Command</a>; and</li><li>3. Remove access to the District's computer systems and databases for noncompliance with training requirements as appropriate.</li></ol> <p>The District shall complete periodic audits to ensure compliance with the cybersecurity training requirements.</p>
<b>Security Breach and Cybersecurity Incident Notifications</b>	<p>Upon discovering or receiving notification of a breach of system security or a <del>security</del> <a href="#">cybersecurity</a> incident, as defined by law, the District shall disclose the breach or incident to affected persons or entities <a href="#">and provide any other notices</a> in accordance with the time frames established by law. The District shall give notice by using one or more of the following methods:</p> <ol style="list-style-type: none"><li>1. Written notice.</li><li>2. Email, if the District has email addresses for the affected persons.</li><li>3. Conspicuous posting on the District's websites.</li><li>4. Publication through broadcast media.</li></ol> <p>The District shall disclose a breach or incident involving sensitive, protected, or confidential student information as required by law.</p>