SECURITY BREACHES PROCEDURE

Procedure for Identifying Security Breaches

In determining whether or not private information has been acquired, or is reasonably believed to have been acquired by an unauthorized person or a person without valid authorization, the District shall consider:

1. Indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer, or other device containing information;
2. Indications that the information has been downloaded or copied;
3. Indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported; and
4. Any other factors that the District shall deem appropriate and relevant to such a determination.

Procedure for Security Breach Notification

The Superintendent or designee shall ensure that the District provides notice of any security system breach, following discovery, to any state resident whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person. In addition, the Superintendent or designee shall disclose to the attorney general by mail or e-mail any breach of the security system which exceeds two hundred fifty individuals. The disclosure will be made in the most expedient time possible and without unreasonable delay, except when a law enforcement agency determines and advises the District that notification will impede criminal investigation.

The District shall provide notice to the affected state residents by at least one of the following methods:

1. Written notice to the last known home address of the resident;
2. Electronic notice, if the notice is consistent with the provisions regarding electronic records and signatures set forth in section 7001 of title 15 of the United States Code; or
3. Substitute notice if the District can demonstrate that the cost of providing notice would exceed $250,000 or that the affected class of subject persons to be notified exceeds 500,000, or the District does not have sufficient contact information. Substitute notice shall consist of e-mail notice, conspicuous posting of the notice on the district's web site[1], and notification to major statewide media.

In addition, the following cybersecurity incidents must be disclosed to the North Dakota Information Technology Department in accordance with law as soon as reasonably possible:

1. Suspected breaches;
2. Malware incidents that cause significant damage;
3. Denial of service attacks that affect the availability of services;

[1] If your district has a web site, include this item in your regulations.

4. Demands for ransom related to a cybersecurity incident or unauthorized disclosure of digital records;
5. Identity theft or identity fraud services hosted by entity information technology systems;
6. Incidents that require response and remediation efforts that will cost more than ten thousand dollars in equipment, software, and labor; and
7. Other incidents the entity deems worthy of communication to the department.

End of Jamestown Public School District Administrative Regulation IDC-AR