1. POLICY STATEMENT

The purpose of this Data Incident Notification Policy ("Policy") is to encourage prompt reporting of incidents involving the unauthorized or inadvertent disclosure, use of, or access to Sensitive Data maintained by or on behalf of TCS Education System ("TCSES").

2. PURPOSE

TCSES, for itself and on behalf of its affiliates, processes, maintains and accesses a significant amount of Sensitive Data which is essential to the mission and operations of TCSES and its affiliates. TCSES values the privacy and security of such Sensitive Data, seeks to comply with legal obligations related to data privacy and security, and recognizes that data privacy and security issues continue to expand and evolve. Where TCSES suspects or becomes aware that Sensitive Data has been compromised, TCSES seeks to take prompt and appropriate action in accordance with applicable law and institutional policies.

In order to do so, TCSES employees and personnel and Affiliate employees and personnel who suspect or become aware of a Data Incident are required to immediately report such incidents pursuant to this Policy. Prompt reporting is critical to ensure that TCSES is able to (1) investigate, address, and remediate such incidents; (2) timely comply with any applicable notification or reporting requirements under local, state, federal, or international law; (3) submit any applicable claims for insurance coverage or indemnity against third-parties; and (4) take any other necessary and appropriate action to mitigate actual or potential harm to individuals, TCSES, or its Affiliates. The intent of this Policy is to reduce overall risks and address the continued importance of robust data security and privacy policies.

3. APPLICABILITY

This Policy applies to all TCSES and Affiliate employees, contractors, temporary workers, student workers, and agents who have access to and handle Sensitive Data. This Policy covers all computer systems, network devices, and any additional systems that store, process, transmit or access Sensitive Data. This Policy also applies to all information systems, regardless of ownership or location, used to store, process, transmit or access Sensitive Data maintained by or on behalf of TCSES and/or an Affiliate(s) (this includes, for example, an employee's personal system(s)/device(s) if that system/device is used to store, process, transmit or access Sensitive Data on behalf of TCSES and/or an Affiliate(s)).

4. DEFINITIONS

4.1 Data Incident

A Data Incident occurs when an event or collection of events or activities is suspected to have caused or resulted in the exposure (regardless of whether a device or system is encrypted or unencrypted) of Sensitive Data maintained by or on behalf of TCSES to persons not authorized to have or access such Sensitive Data. The suspected or actual disclosure of information subject to this Policy may occur through theft, mistake, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other

than authorized users and for an other than authorized purpose have access or potential access to Sensitive Data, whether physical or electronic.

A Data Incident also occurs when a suspected or actual exposure of Sensitive Data may constitute the violation or imminent threat of violation of any applicable law or regulation, or TCSES policies or procedures.

A Data Breach is a specific type of Data Incident that may require notification to affected individuals, regulatory agencies (including the U.S. Department of Education), or credit reporting agencies under applicable law, or to other individuals or entities pursuant to contractual obligations.

4.2 Sensitive Data

For purposes of this Policy, Sensitive Data includes any one or more of the following data elements about an individual:

- Social security number
- Driver's license number or state identification card number
- Passport or Foreign Visa number
- Financial account number, or credit card or debit card number
- FERPA protected information (e.g., student information and grades)
- HIPAA protected information (e.g., health, medical, or psychological information)

The categories of information that constitute "Sensitive Data" under this Policy may be different from the categories of information that constitute "Highly Sensitive Data" or "Personal Information" under other policies.

5. PROCEDURE

5.1. Immediate Reporting

Any individual who suspects that a Data Incident has occurred must immediately notify his/her immediate supervisor with a copy to both the Office of General Counsel ("OGC") via email to OfficeGeneralCounsel@tcsedsystem.edu and the Information Technology Department ("IT") via email to TCS-CyEmergency@tcsedsystem.edu, and include a description of the Data Incident with as much detail as is available at the time, including without limitation, the following information:

- the date and time of the Data Incident
- the method of disclosure,
- the number of individuals whose Sensitive Data may have been impacted,
- the categories of Sensitive Data involved,
- the number of unauthorized recipients of the Sensitive Data,
- if a Data Incident originated with a third-party, a copy of any notification received from the third-party pertaining to the matter, and

- if the Data Incident involves data maintained on behalf of TCSES or an Affiliate by a third-party, a copy of any and all contracts between TCSES/Affiliate and the third-party.

Immediate reporting is critical as there may be time sensitive requirements to report the matter to, among others, impacted individuals; state, federal or international authorities; insurance carriers; or other third-parties.

5.2. Investigation by TCSES

IT, in consultation with OGC, will investigate reported Data Incidents to confirm whether an incident is a Data Breach and reportable to any applicable authority or third-party. If a Data Breach has occurred, OGC will advise the involved business units on what notifications, reports or other actions are required to be taken under applicable law and contracts. If a Data Incident does not implicate any IT infrastructure, OGC may appoint a party other than IT to investigate the reported Data Incident.

6. ENFORCEMENT

Failure to follow this policy can result in disciplinary action, up to and including termination.

7. CONTACTS

- Office of General Counsel
- Information Technology