4.2.6 Information and Information Technology Policy for Security Breaches and Suspected Security Breaches

This policy applies to data in electronic form and not to hard copies of same.

4.2.6.1 Definitions

Security Breach means when unencrypted confidential and restricted information of an individual is reasonably believed to have been acquired by an unauthorized person. Acquisition of Personal Information by a KCTCS employee or agent for bona fide KCTCS business purposes does not constitute a Security Breach, provided that the Personal Information is not used or subject to further unauthorized disclosure.

Security Breach Coordinator, for purposes of this Policy, is the individual or functional position to whom suspected Security Breaches are reported and with overall responsibility for ensuring compliance with this Policy, by his/her respective KCTCS college or functional area.

Suspected Security Breach means when a System containing Personal Information is, among other possibilities, lost or stolen, accessed in unauthorized fashion or infected by a virus or worm, but it is not yet known whether the Personal Information has been compromised to meet the level of a Security Breach.

System, for purposes of this policy, is any computer or computing device, including, but not limited to, desktops, laptops, PDAs, removable media such as CDs, USB flashdrives or iPods used as storage devices.

4.2.6.2 Responsibilities and Duties

College Presidents and KCTCS Vice Presidents must designate a Security Breach Coordinator and ensure that that individual reads this Policy and understands his/her responsibilities thereof. Changes to a designated Security Breach Coordinator must be approved by the appropriate official and communicated to system-level Information Security Officer.

Security Breach Coordinators are responsible for:

- Ensuring that all Suspected Security Breaches within their respective college, division or unit are investigated and reported to the KCTCS Chief Information Officer.
- Acting as liaison between their respective college, division or unit and the system-level Information Security Officer to facilitate investigation of such Suspected Security Breaches.
- Making arrangements for implementing notification requirements, including the actual distribution of notification letters or emails and the setting up of a hotline for inquiries if appropriate.

Other related duties and responsibilities may be assigned to a Security Breach Coordinator as deemed necessary.
KCTCS Chief Information Officer is the designated KCTCS authority responsible for:
- Reporting all Security Breach incidents, in writing, to the KCTCS President, KCTCS Chancellor, KCTCS Vice President primarily responsible for Institutional Advancement, KCTCS legal services, and their ultimate resolution.
- Making a final determination as to whether the Suspected Security Breach is an actual Security Breach, based on the recommendation from the system-level Information Security Officer.
- As appropriate, may also report Suspected Security Breaches to KCTCS President, KCTCS Chancellor, KCTCS Vice President primarily responsible for Institutional Advancement, KCTCS legal services where a decision has been made not to notify.

System-level Information Security Officer is responsible for:
- Ensuring that the Security Breach incident response process is followed;
- Ensuring that system wide and, if applicable, college notification procedures are followed; and
- Coordinating with appropriate KCTCS officials and personnel, to analyze and recommend, in writing, to the KCTCS Chief Information Officer, whether a Suspected Security Breach is an actual Security Breach requiring notification.

4.2.6.3 Notification Requirements

In the event of a Security Breach, KCTCS must provide notification of the breach to those individuals whose unencrypted confidential and restricted information Personal Information is reasonably believed to have been acquired by an unauthorized person. Notification must occur without unreasonable delay, except:
- When law enforcement agency has determined that notification will impede a criminal investigation (in this case, notification must occur as soon as the law enforcement agency determines that it will not compromise the investigation), or
- In order to discover the scope of the Security Breach and restore the integrity of the System.

4.2.6.4 Security Breach Incident Response Process

Any instance of a Suspected Security Breach must be reported immediately to the appropriate Security Breach Coordinator who will initiate the incident response process described below.

Initial Reporting and Analysis

<table>
<thead>
<tr>
<th>RESPONSIBILITY</th>
<th>ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Breach Coordinator</td>
<td>When notified of a Suspected Security Breach, ensures that appropriate action is expeditiously taken to secure the affected System.</td>
</tr>
<tr>
<td></td>
<td>Immediately notifies the KCTCS Chief Information Officer.</td>
</tr>
<tr>
<td></td>
<td>Immediately notifies the KCTCS legal services if criminal activity is suspected to be responsible for the Security Breach.</td>
</tr>
<tr>
<td>KCTCS Chief</td>
<td>As appropriate, notifies the KCTCS President, KCTCS Chancellor, KCTCS</td>
</tr>
<tr>
<td>Information Officer</td>
<td>Vice President primarily responsible for Institutional Advancement, KCTCS legal services. Notifies the System-level Information Security Officer.</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| System-level Information Security Officer | In conjunction with the Security Breach Coordinator:  
  - Works with appropriate technical staff to complete technical analysis of the affected System.  
  - Works with KCTCS legal services and other staff as appropriate to recommend to the KCTCS Chief Information Officer as to whether this is an actual Security Breach or not. The analysis leading to the recommendation shall be documented in writing. |
| KCTCS Chief Information Officer | Based on the recommendation from the System-level Information Security Officer, makes a final determination as to whether this is a Security Breach or not. |

**Security Breach Notification**

If a Security Breach has occurred, the following steps should be taken:

<table>
<thead>
<tr>
<th>RESPONSIBILITY</th>
<th>ACTION</th>
</tr>
</thead>
</table>
| Security Breach Coordinator | In conjunction with the System-level Information Security Officer, works with the KCTCS Chief Information Officer, KCTCS Vice President primarily responsible for Institutional Advancement, and KCTCS legal services to:  
  - Develop an appropriate notification letter.  
  - Determine a substitute method of notice if sufficient contact information is not available for direct hard copy or email notice. |
| KCTCS Chief Information Officer | In consultation with the KCTCS Chancellor, KCTCS Vice President primarily responsible for Institutional Advancement, KCTCS legal services, and the appropriate college official whose college or unit experienced the Security Breach, determines the most appropriate college official to sign the notification letter. |
| Security Breach Coordinator | Arranges for the logistics to implement notification. |
The KCTCS Chief Information Officer will notify the KCTCS President of the final disposition of the Security Breach incident, including a description of the incident, the response process, the notification process, and the actions taken to prevent further breaches of security.