SUL ROSS STATE UNIVERSITY
A Member of the Texas State University System

SRSU Policy: Confidential Data Policy
SRSU Policy ID: APM 7.09
Policy Reviewed by: Chief Information Officer
Approval Authority: Executive Cabinet
Approval Date: 7-23-2013
Next Review Date: 7-23-2015

Purpose
To protect confidential information vital to the University's business. Information includes but is not limited to: all transactional records, student and employee information, memos, reports, etc.

Policy Statement
All employees must safeguard University confidential business information as part of their daily actions and work routines. Confidential data is defined in the Data Classification Standard listed at the bottom of this policy.

Applies to
All employees

Responsibilities
• For authorized personnel confidential data may be made available on a need to know basis as and when required. For all other persons access to such information must be prohibited. (TAC 202.75.2.a)
• Unauthorized modification, transmitting or other dissemination of confidential information is strictly prohibited. Unauthorized dissemination of this information may result in disciplinary or legal action as appropriate.
• Confidential information should be safely stored and protected while on file servers, network drives, workstations, and during any type of transmission. Authorized access should be enforced. Confidential information should be erased securely from network drives, file shares etc. after proper authorization.
• Network or directory share information showing where the confidential information is stored must not be publicly viewable.
• Confidential data must not be emailed or faxed; unless there is no other method available to transmit the information. Upon prior authorization, confidential information sent via email must be sent from their official Sul Ross State University (username@sulross.edu) email account. (TAC 202.75.3.b)
• Confidential information sent via email off-site must be encrypted. (TAC 202.75.4.a)
• Employees must not download and store confidential information unless encrypted on their personal computers, external hard drives, thumb/ pen drives and CD/DVD, or any removable device. (TAC 202.75.4.b)
• Printed reports that contain confidential data must not be left available to the public. All printed confidential data must be shredded or disposed of into locked bins.
• Employees must not take printed or unencrypted confidential data off-campus.
• Employees must not discuss confidential data in public.
• All attachments or electronic files received from external sources must be scanned for viruses or malicious code in order to protect existing confidential information.
• The University will periodically audit employees to insure compliance and enforcement of policy. *(TAC 202.75.5)*
• Any incidents of non-compliance may be reported to the Chief Information Officer (CIO).

**Data Classification Standard** *(TSUS R&R III,19.2; TAC 202.71):*

**Confidential**

Data classified in this category is considered to be highly sensitive in nature. Such data should not be copied or removed from the institution’s operational control without department head permission. Confidential data is subject to the most restricted distribution and must be protected at all times. Compromise of data classified as Confidential could seriously damage the reputation, mission, safety, or integrity of the institution, its staff, or its constituents. It is mandatory to protect data at this level to the highest possible degree as is prudent or as required by law.

Examples: Personal Identifiable information such as Social Security Numbers, Driver’s License Numbers; Institution Finances; Employee Personnel data; Vendor Bids information; Ongoing audits and Investigations; HIPPA protected information; Student transcripts: FERPA; Student addresses;

**Restricted**

Restricted data is to be kept within the departments that manage it. It is sensitive, but does not rise to the level of Confidential. Data classified in this category is for internal institutional use only, the release of which must be approved prior to dissemination outside the institution. Its compromise may inconvenience the institution, but is unlikely to result in a breach of confidentiality, loss of value or serious damage to integrity. Protection of this information is required and would be determined by the institution.

Examples: Daily institutional finances; Research data; Test questions and answers; Minutes of meetings; Agenda for discussion

**Public**

Data classified in this category is for general use and is approved by the institution as available for routine public disclosure and use. Security at this level is the minimum required by the institution to protect the integrity and availability of this data. This data should be sent out or made available only through Institutional Communications and/or other approved departments.

Examples: Press material; Marketing content; Public posts; Annual Reports
<table>
<thead>
<tr>
<th>Data Classification</th>
<th>Confidential</th>
<th>Institutional</th>
<th>Public</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reputational risk</td>
<td>High</td>
<td>Med</td>
<td>Low</td>
</tr>
<tr>
<td>Financial Risk</td>
<td>High</td>
<td>Med</td>
<td>Low</td>
</tr>
<tr>
<td>Other institutional risks</td>
<td>Information in this category may provide access to physical or virtual resources</td>
<td>Protected data from a department’s point of view</td>
<td>General information</td>
</tr>
<tr>
<td>Legal requirements</td>
<td>Protection of data is required by law (State and federal laws and regulations, FERPA, HIPPA, GLB, DMCA, etc.)</td>
<td>SRSU has a contractual agreement or operational need to protect data in this category</td>
<td>Protection of this data is at the discretion of the data owner.</td>
</tr>
<tr>
<td>Access</td>
<td>Only designated SRSU employees who have a need to know and need to use may be provided access.</td>
<td>SRSU employees and non-employees (vendors) who have a need to know.</td>
<td>SRSU community, and general public</td>
</tr>
<tr>
<td>Examples</td>
<td>Social Security Numbers, bank account numbers, HIPPA information, Prospective student records with SSN, phone numbers and addresses, Financial bid information prior to bid submission, Credit Card numbers, Investigations and audit information, Tax Payer ID, Purchasing card information, and</td>
<td>Resources with access to restricted information, Research details Information for Institution internal use only and Financial transactions that do not include restricted data. Some parts of confidential information that may be reduced in sensitivity after a certain time; Employee personnel Information,</td>
<td>Campus maps, Community announcements, Business contact information, newsletters</td>
</tr>
</tbody>
</table>
Sul Ross State University has identified the following employees as Data Owners:

<table>
<thead>
<tr>
<th>Department</th>
<th>Data Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Human Resources</td>
<td>Judy Perry</td>
</tr>
<tr>
<td>Finance</td>
<td>Oscar Jimenez</td>
</tr>
<tr>
<td>Financial Aid</td>
<td>Melinda Cullins &amp; Mickey Corbett</td>
</tr>
<tr>
<td>Registrar</td>
<td>(Alpine: TBD)</td>
</tr>
<tr>
<td></td>
<td>(RGC: Claudia Wright)</td>
</tr>
</tbody>
</table>

OIT collaborates with data owners to develop procedures to document authorization requests. Requests for granular access to data by system users, will be made to the data owner. The data owner will recommend approval or disapproval to the ISO. ISO will approve or disapprove the request. Disputes will be resolved by the Executive Committee. Logs of these requests are maintained by OIT. Access privileges are to be reviewed every 90 days by respective Data owners.

Data owners will further define appropriate procedures for use of data under their control. Employees and student workers will be asked to sign non-disclosure agreements upon employment. Our Acceptable Use Policy further details user responsibilities and obligations. Dissemination of policy awareness will be included in the new employee orientation process managed by HR and the student orientation process by the Lobo Den.