Classification of IT Resources for ISORA

Categorization and Classification of IT Resources

There are a variety of categories and classifications of not only data, but also the criticality of resources, such as servers. A server that contains only publicly available research data, but that is critical for teaching or supporting other research might be considered critical for “Availability” and “Research”, two classifications that can be assigned in the ISORA application.

System and Data Classifications

The ten classifications of a machine contained within ISORA are listed below:

<table>
<thead>
<tr>
<th>Classification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - Confidentiality</td>
<td>Need to strictly limit read access to data.</td>
</tr>
<tr>
<td>2 - Integrity</td>
<td>Data must be accurate, users must be able to trust its accuracy.</td>
</tr>
<tr>
<td>3 - Availability</td>
<td>Data must be accessible to authorized persons, entities, or devices.</td>
</tr>
<tr>
<td>H - Health</td>
<td>Confidential information on the health of individuals.</td>
</tr>
<tr>
<td>N - Financial</td>
<td>Confidential information on finances</td>
</tr>
<tr>
<td>S - SSN</td>
<td>Social security numbers and the names with which they are associated.</td>
</tr>
<tr>
<td>R - Research</td>
<td>Research data, software or systems.</td>
</tr>
<tr>
<td>U - Critical UT</td>
<td>Critical to the operations or interests of the University.</td>
</tr>
<tr>
<td>D - Critical Department</td>
<td>Critical to the operations or interests of the Department.</td>
</tr>
</tbody>
</table>

System Data Categorization

There is a strong state mandated policy to protect highly sensitive data, that which is called Category I. Any of the above criteria could cause the system on which it resides to be classified as a Cat I system.

A host is considered to be a Category I device if:

- There is a high need for confidentiality, integrity, availability (CIA) of the data processed with the host
- The host is used to store, process, or otherwise manipulate Category I data
- The host is considered to be critical for University or Department operations

So, what are the data categories?

Category-I Data

University data protected specifically by federal or state law or University of Texas rules and regulations (e.g., HIPAA; FERPA; Sarbanes-Oxley, Gramm-Leach-Bailey; the Texas Identity Theft

CNS TSC Resources

- What is a TSC?
- ISORA
  - Classification of IT resources
- Net.Contacts
- ISO Ticket Remediation

External links

Here are some useful TSC resources that are located on other sites:

- TSC Tools: From here you can navigate to Net.Contacts, as well as the many other tools made available to TSCs to help them better analyze manage their networks and systems.
- ISO's ISORA page: Here you’ll find more in depth information published by the Information Security Office.
- The ISORA application: The actual ISORA Web application. When you push out ISORA, Net.Contacts will populate the application with your systems.
- Information Security Office (ISO) Wiki: ISO’s best practices, checklists procedures and more all in one handy location that is regularly updated.
Enforcement and Protection Act; University of Texas System Business Procedure Memoranda; specific donor or employee data). University data that are not otherwise protected by a known civil statute or regulation, but which must be protected due to university contractual agreements requiring confidentiality, integrity, or availability considerations (e.g., Non Disclosure Agreements, Memoranda of Understanding, Service Level Agreements, Granting or Funding Agency Agreements, etc.) are also included (see some basic examples of Cat I data or an extended list of Category I data classification examples)

**Category-II Data**

University data not otherwise identified as Category-I data, but which are releasable in accordance with the Texas Public Information Act (e.g., contents of specific e-mail, date of birth, salary, etc.) The release of such data is still considered sensitive and the data must be appropriately protected to ensure a controlled and lawful release. Cat-II could also be data that could have greater impact in aggregate. (A floor plan may not be sensitive data, but the plans for the whole campus might be since a terrorist could use it to plan an attack.) Cat-II is data for which the release of the data might result in:

- Short-term loss of reputation.
- Short-term loss of research funding.
- Short-term loss of critical departmental service.
- Unauthorized tampering of research data.
- Individuals put at risk for identity theft.

**Category-III Data**

University data that are not otherwise identified as Category-I or Category-II data (e.g., publicly available). Such data have no requirement for confidentiality, integrity, or availability. Examples include:

- Professor's personal blog
- Student's personal laptop with their own work not covered by copyright or otherwise protected

Acknowledgement: Much of this information was pulled from pages located on The College of Education Information Technology and The Center for Computational Biology and Bioinformatics pages on data categorization.

**Related articles**

- Page: ChemDraw
- Page: CrashPlan UT Backup
- Page: Instructional Use Laptop program
- Page: Admin Responsibility Matrix
- Page: Classification of IT Resources for ISORA