Message from the CIO

As Texas Tech University moves strategically to achieve national research university status, we focus our November bulletin on research topics and activities in the TTU IT Division. The High Performance Computing Center (HPCC) has been collaborating with the High Energy Physics group to prepare infrastructure for the Hadron Collider project. In support of other research initiatives, TTU hosted the High Performance Computing Across Texas (HiPCAT) semi-annual conference that showcased TTU researchers partnering with the HPCC. In addition, we offer pertinent information on Grid Computing at TTU, as well as guidelines for classifying and securing research data. Information resources are important institutional assets for faculty research, and the TTU Office of the CIO has been proactive in soliciting funding to enhance IT infrastructure and services to provide the best possible resources for faculty. We join the campus in working toward national research university status and appreciate your support of our efforts.

-Sam Segran
Associate Vice President for IT and Chief Information Officer

Protecting Confidential and Sensitive Research Data

The TTU IT Division Security Program establishes strategies and controls for the protection of all TTU networks, computers, and data, including research data. HPCC works closely with the IT Division Security Team to maintain highly secure environments for its research clusters and grids. Researchers at TTU are strongly encouraged to observe “Best Practices” in the electronic collection, transmission, and storage of their research data.

We ask that researchers examine the data they are collecting and classify the data into one of the following categories:

- **Confidential Data** - Confidential information, as defined by the Texas Administrative Code, is information that must be protected from unauthorized disclosure or public release based on state or federal law. Texas Tech University OP 70.40 details procedures and safeguards regarding private or personally identifiable information;
- **Sensitive Data** - Information pertaining to Access Control data, Account Management Data, procedures, security documentation of Information Resources, or any other information TTU so designates; and
- **Public Data** – Information specifically designated by state or federal law as Public and/or in accordance with the Texas Public Information Act.

After determining the type of data being collected in your research, the next step is to evaluate the data as it pertains to the criticality of our institutional mission:

1. **Mission Critical** – Information considered essential to the function(s) of TTU, a TTU business unit, or a TTU official research project;
2. **Non-Mission Critical** – Information considered nonessential to the function(s) of TTU, a TTU business unit, or a TTU official research project.

The following matrix can be used as a guide to classify your research information and data:

<table>
<thead>
<tr>
<th>Data Classification Matrix</th>
<th>Confidential</th>
<th>Sensitive</th>
<th>Public</th>
</tr>
</thead>
<tbody>
<tr>
<td>TTU Mission Critical</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TTU Non-Mission Critical</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

Research data classified as mission critical and either confidential or sensitive (as indicated by an “X” above) have additional specific security requirements. Note that owners of Information Resources, as defined by the TTU IT Security Policies are responsible for upholding the related TTU IT Security Policies in regard to information stored on or processed by those Information Resources as well as specify any additional controls that may be necessary. In addition, custodians of Information Resources, as defined by the TTU IT Security Policies, are responsible for execution of the related TTU IT Security Policies. We encourage you to carefully review the TTU IT Security Policies (http://www.depts.ttu.edu/infotech/security). For additional information about classifying your data or state requirements, please contact the Information Security Officer, J Stalcup, at j.stalcup@ttu.edu or (806)742-8000. For assistance with securing servers and applications, please contact IT Help Central at (806)742-HELP (4357), via e-mail at ithelpcentral@ttu.edu or online at www.ithelpcentral.ttu.edu.

TTU Information Technology Division Hosts Distinguished Grid Scientists

The Texas Tech University IT Division hosted members of High Performance Computing Across Texas (HiPCAT) for their semi-annual conference in October. Mr. Sam Segran (Associate Vice President and for IT and CIO) and Dr. Taylor Eighmy (Vice President for Research) welcomed researchers from institutions across Texas. Texas Tech University showcased four researchers at the conference who presented their projects to the group:

- Sukanta Basu, Ph.D. - Geosciences
  “Emergent Challenges in Wind Power Meteorology Using High Performance Computing”
- Kelvin Cheng, Ph.D., and Liming Qiu - Physics
  “Multi-state Molecular Dynamics Simulation of Alzheimer’s Peptic Interactions with Neuronal Membrane Mimics”
- Rajesh Khare, Ph.D. – Chemical Engineering
- Bill Hase, Ph.D. – Chemistry and Biochemistry

Dell, Inc. sponsored a dinner for the conference and also briefed the group on future high performance computing initiatives at Dell. Participants also toured the new TTU High Performance Computing facility located in the Experimental Sciences Building.
TTU Prepares Computing Infrastructure for Large Hadron Collider Restart

Cooperation between the TTU High Performance Computing Center (HPCC) and High Energy Physics (HEP) group is helping to prepare Texas Tech University for participation in the Large Hadron Collider (LHC) as it resumes operation this year. The LHC is a particle accelerator instrument located on the border of Switzerland and France; many scientists believe that the enhanced ability to study the particles that it produces will greatly advance our understanding of the Universe. The HPCC and Physics departments are collaborating to upgrade, update, and ready computing cluster, storage, and display capabilities to facilitate this work.

The central local computing engine for the project, the 240-core Antaeus cluster located at the Reese Technology Center, has been updated to the latest versions of the Rocks and Lustre software that are used to run its computing and storage capabilities. In addition, several related auxiliary support systems have also been upgraded. The group also anticipates expanding its storage and computing capacity further in the near future.

In the Science building, the HPCC has helped the HEP group develop, design, and implement large multi-monitor displays, such as the one shown in the accompanying picture. Such large display arrays are common features at the LHC, and are needed to go through the large amount of data to monitor both the online and offline performance of the experiment.

This picture shows a set of 10 offline processing monitoring screens, each displaying multiple tabs of information related to the analysis of data from the Compact Muon Solenoid (CMS) experiment. Drs. Nural Akchurin of Physics (standing), Ravi Vadapalli of the HPCC, and Sung-won Lee of Physics are going through the displays, each of which must be checked multiple times during a typical 8-hour offline computing shift. Dr. Alan Sill of the HPCC (not shown) helped the group to assemble and configure the displays. The entire staff of the HPCC, including Dr. James Abbott (Associate Director), Srirangam Addepalli (Senior Programmer Analyst), Huijun Zhu (Programmer Analyst) and Poonam Mane (Student Assistant) also participated in the operation of the storage and clusters.

Best Practices for Grid Computing at Texas Tech University

What is the Grid?

The Grid refers to an infrastructure that enables the integrated, collaborative use of high-end computers, networks, databases, and scientific instruments owned and managed by multiple TTU areas and units. Grid computing is an application that harnesses unused computer cycles, typically from campus computers not in use during a particular time period, to process large computational programs. Grid applications allow secure resource sharing across organizational boundaries; computational projects are not easily handled by today's Internet and Web infrastructures.

What is TechGrid?

TechGrid is a collection of about 800 Windows PC's located on the TTU campus and the TTU IT HPCC (High Performance Computing Center) Linux multiprocessors organized into a computational grid. It may be accessed using Condor (all platforms) or Globus (Linux) software. TechGrid utilizes unused CPU power from idle desktop workstations. For instance, TechGrid can be configured to only use desktop machines where the keyboard and mouse are idle. Idle computer time is donated by many areas and units on campus, such as the Rawls College of Business, the Department of Mathematics and Statistics, the College of Education, the English Department, and the TTU IT Division Technology Support Department.

Grid Best Practices:

1. Make sure your code has been thoroughly tested on your local machine, before trying to run it on the grid. This will reduce development time and reduce grid run-time errors.
2. Know the run-time of your application. Most grid jobs run for less than 8 hours. If your application runs longer than 8 hours then let us know so that we can allocate the appropriate computing resource for your application.
3. Know how much data your application produces. Most grid resources have a limit of 2 GB for data provisioning and storage. If your application generates more than 2 GB of data, let us know so that we can allocate the appropriate computing resource for your application.
4. If you need more computing resources beyond the TechGrid, we may move your application to run on larger grid resources found in cluster computing environments.
5. If your application works locally, however not on the grid, please let us know so that we can help you tailor a grid submission script.

Please contact the HPCC at HPCC@ttu.edu for more information.

Contributions by: Katherine Austin, Ph.D., Darrell Bateman, Fisayo Delano, Jerry Perez, Philip Smith, Ph.D., J Stalcup, Alan Sill, Ph.D., Britta Tye, Laura Webb, and Allen Young.

Safe Computing Practices Committee: Sam Segran, Katherine Austin, Ph.D., Darrell Bateman, Pulin Bhatt, Shannon Cepica, Paco Diaz, Scott Hall, Mark Holwerda, Michael Horton, Danny Mar, Alvin Mills, Yung Ng, Mike Simmons, J Stalcup, Britta Tye, John Vandygriff, Allen Young, and assistance from IT Division leadership and staff.