

Find information

- answers.vt.edu
- computing.vt.edu
- [CNS FAQs](#)
- [Online Course Support](#)
- [Software Skills Gateway](#)
- security.vt.edu
- antivirus.vt.edu
- [Annual Report](#)
- [CSC-4help](#)
- [Staff Senate](#)

In this issue

CTU changes	1
Security reviews	1
ACCS presenters	2
Junk Mail Manager	2
Educause Security Professionals	2
Effective Practices	2
Office of the VP-IT	

CTU changes

Collaborative Technologies Unit (CTU) is transitioning from Secure Enterprise Technology Initiatives (SETI) to Enterprise Systems. Responsibilities for the My VT portal move with the unit, and the portal itself takes on new roles in support of research administration for university research offices, principal investigators, and grants administrators. CTU will also retain its responsibilities in support of the coming content management system.

Responsibilities for CAS, the central authentication service, will move to Middleware.

Security reviews

Data exposure is one of the biggest threats facing Virginia Tech today. Each university department must comply with applicable regulations to protect data from misuse or exposure.

The university's obligation to protect sensitive data falls under the regulation of state and Federal privacy laws and regulations. These include (but are not limited to) the Family Educational Rights and Privacy Act or FERPA and the Gramm-Leach-Bliley Act, as well as the Payment Card Industry security standard requirements. The state and Federal agencies responsible for enforcement take their responsibilities seriously, and constituents within the university could be contacted for a detailed review by an outside entity.

The IT Security Office reviews areas with the greatest risks, selected with guidance from the executive vice president's office and the controller's office. Reviews help departments to manage potential risks of data exposure and system reliability, to ensure that appropriate measures for security are being taken, and to prepare for future audits. The security reviews focus on:

- End-system security
- CIS benchmarks
- Network access
- Network application security
- Software patching
- SSN Scanner
- File sharing
- Web applications
- Host firewalls & antivirus
- Physical access
- Running services & open ports
- Online databases
- Backup mechanisms

Security reviews may take two to four weeks depending on the size and complexity of the department being reviewed. A plan for doing security reviews will be prepared for the next fiscal year, and departments will be appropriately contacted. If your department is interested in ensuring your security, send an e-mail to randy.marchany@vt.edu.

ACCS

The Association of Collegiate Computing Services of Virginia is holding their Spring 2007 meeting April 18 through 20 at the University of Virginia. Among the program presenters are staff from Virginia Tech:

Joe Kelley and Patty Branscome, “Software Distribution at Virginia Tech: Methods and Technology”

Rob Sprague and Raven Jennings with Rick Reo (George Mason University), “Innovative Uses for Collaborative Support Tools”

Zeb Bowden, “Reducing the Risk of Data Theft with BitLocker and EFS”

Marc DeBonis, “Architecting an MS WSUS Solution for the .edu Environment”

Richard Hach and Wendy Wigen (EDUCAUSE), “Communications Assistance for Law Enforcement Act (CALEA)”

Ron Angert (Residential Programs) and Clay Calvert (University of Mary Washington), “Promoting Security Awareness”

Vice President for Information
Technology
Earving Blythe
1700 Kraft Drive, Mailstop

**Information Technology
at Virginia Tech**

Phone: 540-231-4227

Website: www.it.vt.edu

Along with Connie Sadler from Brown, Mary Dunker has been named co-chair of the Educause Security Task Force Effective Practices & Solutions Working Group. The working group focuses on identifying and promoting practices, tools, and procedures that higher education institutions have found to be practical solutions to preventing or responding to security problems with an emphasis on technology and process solutions.

Junk Mail Manager

The junk mail quarantine system, Junk Mail Manager or JMM, is currently in beta testing. JMM is a quarantine system that uses the Mirapoints to determine spam and then holds messages tagged as junk. JMM puts more control of spam management in each user’s hands. Users can configure their own allow/deny lists. All items still in the quarantine are summarized so that each person can ensure that desired e-mail is delivered. Each user may opt out of the JMM system, or opt back in at a later time. Initially, all individual e-mail accounts will be set to use the JMM.

Educause Security Professionals

Randy Marchany from the IT Security Office is one of the leaders of the Educause pre-conference workshop of the Security Professionals conference. The seminar is “IT Security Incident Handling: Tools, Techniques, and Processes.” The three other leaders of the seminar are from Cornell University.

The seminar examines the six steps of incident response: preparation, detection, containment, eradication, recovery, and follow-up. The seminar leaders also provide templates, demonstrations of security tools, and forensic techniques to participants.

Nora Lucas has moved to the Office of the Vice President and has taken on additional duties as the administrative assistant to the VPIT. Nora takes over for Cindy Woods who has joined the Test and Deployment group within SETI.