Unacceptable Computer Use – DOs and DON’Ts for Departmental Personnel

Prohibited Activities:
University policy 7000: Acceptable Use and Administration of Computer and Communication Systems, specifically prohibits use of university resources for personal gain, harassment or intimidation of another individual, and any other illegal act. Various state laws and standards specifically prohibit downloading, viewing, or storing sexually explicit material.

DO:
- Do your job! It is always acceptable for employees to perform their duties.
- Do STOP investigating further once department personnel become aware of situations that may need further review by central offices.
- Do contact Internal Audit and the IT Security Office before proceeding. This helps ensure consistent handling of similar situations across the university, preventing unfair treatment and reducing the possibility of lawsuits against the university and its employees.
- Do remember it is not your fault that someone in your department has potentially violated state law and university policies and you are doing your duty when reporting to central offices.

DON’T:
- Do not conduct your own investigation! Other university personnel have undergone extensive computer forensic training.
- Do not allow deletion of the questionable material. If need be, isolate the machine until further review can be performed.
- Do not interview the personnel that may be involved until after contacting Internal Audit and the IT Security Office. This will allow for a complete uniform investigation or review (if needed).
- Do not share the details of the investigation among the department beyond requisite management personnel. There is always the possibility that there is no violation of laws and university policies.

Information to be gathered in the event of an incident:
- The 5 W’s (Who, What, When, Where, Why) of the incident.
- Example: Steve Jones, IT support staff, discovered potentially inappropriate material when reviewing the reasons for Joan Stevens’ machine slow-down. This review happened in Room 238 of University Hall at approximately 3:00 pm on May 17, 2013. The material in question appeared to be of a sexually explicit nature. The machine has been stored in a locked office.

Section 2.2-2827 of the Code of Virginia prohibits employees from using an agency-owned or agency-leased computer to access, download, print, or store sexually explicit content. Sexually explicit content is described as any description of or any picture, photograph, drawing, motion picture film, digital image, or visual representation of sexual conduct or nudity, as defined in Section 18.2-390 of the Code of Virginia. Section 2.2-2827 is an administrative prohibition and is not a criminal offense.

The university’s Statement of Business Conduct Standards (Standards) states that “State law prohibits employees from accessing, downloading, printing, or storing information with sexually explicit content.” The Standards also state that “Personal use of university assets is prohibited, although some limited, personal use of computer or communications systems may be permitted.”

State Department of Human Resource Management (DHRM) Standard 1.75, Use of Electronic Communications and Social Media, also prohibits accessing, uploading, downloading, transmitting, printing, posting, or storing information with sexually explicit content as prohibited by law (see Code of Virginia §2.2-2827). The Standard adds that employees who engage in prohibited activities may be subject to disciplinary action according to DHRM Standard 1.60, Standards of Conduct.

Brian J. Daniels
Associate Director of Internal Audit
Phone: 231-5883
Email: bdaniels@vt.edu

Randolph C. Marchany
University IT Security Officer
Phone: 231-1688
Email: marchany@vt.edu