San Jose State University Group/Grid Computing Guidelines

INTRODUCTION

There are a number of computer screen savers and other software that use the spare computing cycles of desktop systems to perform a computational task such as find a cure for a disease or search for extraterrestrial life (often referred to as a group or grid computing endeavor). These programs typically run in the background as a screen saver and perform sets of calculations, the results of which are sent via the Internet to a central repository. While seemingly innocuous, these types of programs present clear and present security risks to SJSU systems. SJSU staff, faculty and students are restricted from installing and using such software unless authorization is specifically granted by the SJSU ISO and CSU ISSO after careful review and consideration of the following issues:

- **Legal Issues –** CSU Guidelines states that this activity constitutes improper use of government resources, unless allowing the use of spare computer cycles is set up as a sanctioned 'state government or CSU project.' Even if this activity is to be permitted, the following security risks are relevant and should be evaluated before final authorization is granted.
- **Unknown Software Code -** The code that drives the screen saver could install an undetected Trojan Horse or backdoor to the system so that undetected modifications or maintenance to the program could be performed without user knowledge. This backdoor access could put all SJSU systems at potential risk. For example, the SETI screen saver that lets users help in the search for extraterrestrial life was recently found to contain a security vulnerability that could put its users at risk.
- **Security of Receiving Site -** The screen saver program automatically communicates to a source outside of SJSU and we really don't know exactly what information from an SJSU computer would be sent or what would be done with it on the other end. Establishing automated connections with any outside site that SJSU does not control or have detailed security knowledge of is a potential security problem.
- **Bandwidth Overload -** There could potentially be an overload of SJSU's network bandwidth availability if a large number of SJSU-based systems had a particular group computing program running at the same time. This could impact critical SJSU operations and Service Level Agreements (SLAs).
- **Staff Resource Usage -** Permitting this screen saver program/computer cycle use by one user could set a precedent for other similar requests.

Each new request would require that staff research the background of these organizations and review the program code for Trojan Horses, backdoors and other vulnerabilities. This becomes a significant staff resource issue.

As a result of these concerns, SJSU guidelines is that the installation, downloading, and use of such software onto SJSU systems (whether state or personally owned) is not permitted without preauthorization/preapproval from the SJSU ISO and the CSU ISO. Users should contact the SJSU ISO prior to installing or using any screensaver (or other software) that is not provided with the operating system.

UCAT may monitor for the presence of such software reporting out to sites on the internet, and will block Internet access (Quarantine) for systems found to be violating this guidelines.

Compliance to Campus Guidelines, Guidelines and Standards

As the owners of the network infrastructure at SJSU, UCAT reserves the right to intervene as needed to enforce campus guidelines and/or protect network performance. Therefore, UCAT may act to shutdown any campus based grid/group computing system due to irresponsible, inappropriate or illegal activity in accordance with SJSU Information Technology Resources Responsible Use Policy.