



OPERATING IN LEAST PRIVILEGE MODE

Summary to the full White Paper

Information Technology Services

May 22, 2009

In order to meet and comply with Federal and state statutes in addition to business agreements, Penn State is moving toward practicing in the least privilege mode. In addition to the statutes, the threat vector of the Internet continues to become more complex, posing an urgent need to secure and protect the information with which we work at Penn State. The practice of least privilege includes, but is not limited to, restricting access to sensitive information to only those who have a business need to know and mitigating the risk of Personally Identifiable Information (PII) exposure to unauthorized users, both physically and electronically.

An essential initiative is underway at Penn State to help mitigate the risk of compromises and loss of PII by restricting the use of local administrative privileges on computers that are connected to the Internet. Machines that are never connected to the Internet or network may not require as stringent security measures with administrative privileges. A report from BeyondTrust based on all vulnerabilities published in Microsoft's 2008 Security Bulletins and Reports, indicates 92% of critical vulnerabilities can be mitigated by removing administrative privileges.

Users with a valid requirement for administrative privileges may be granted elevated privileges by applying for an exception through their chain of command. This does not mean the requester may operate as an administrator, but rather they will operate with a set of regular user privileges and work in an elevated mode when it is required by the software or to perform a particular task. When the task is complete, they should switch back to normal privileges. Such mechanisms may include, but not limit, creating two accounts; one with an elevated privilege and one with limited privileges; running a virtual environment for the elevated privilege mode; or using a software program to manage the privileges.

A need for an exception may include, but is not limited to, faculty or staff who: a) connect to certain equipment or devices that cannot, within reason, be upgraded or replaced to the modern versions not requiring administrative access to operate; b) frequently test or use new software; c) travel frequently and have needs which require specific setting changes.

Prior to implementing the least privilege mode, it is recommended that a team be organized within your area to embark upon the project and determine the best mechanisms for those who qualify for an exception. The team may also be tasked with conducting an initial assessment, determining criteria for valid exceptions, creating policies around the initiative, developing awareness sessions and prioritizing areas to target first.

Several departments at Penn State have successfully gone through removing local administrative privileges in their respective areas. A significant decline in helpdesk requests has been reported after removing administrative privileges. When properly planned and implemented, the process of operating in a least privilege mode will successfully help to mitigate the overall risk and unauthorized exposure of sensitive employee, student, alumni and customer data.

Supporting documentation moving towards the initiative of operating in the least privilege mode includes, but does not limit, the Data Classification Scheme Security Matrix (reference 3.1.4) and University policy AD20 "Computer and Network Security" (reference section f).

For additional resources on available tools and implementation mechanisms, review the full White Paper on Operating in Least Privilege Mode located: <http://www.ipas.psu.edu/phase2/supportingdocs2.html>.