

# Network Protection for Design Professionals

## Access Controls

### Background:

Managing system user access privileges or Access Control is the means of controlling what information users can utilize, the programs they can run and the modifications they can make. Access Control may be built into the operating system, incorporated into applications, or may be implemented through add-on security packages. Access controls help protect:

- Operating systems and other system software from unauthorized modification or manipulation.
- The integrity and availability of information by restricting the number of users and processes with access.
- Confidential information from being disclosed to unauthorized individuals.

### How to implement appropriate controls:

- Define access controls based on “need-to-know” or “least privilege”, which refers to the granting users only the access required to perform their duties.
- Access Controls should be centrally administered, so that one office or individual is responsible for configuring access controls. Restricting the ability to make changes to very few individuals allows for strict control over information.
- Formal procedures should be put in place to revoke user access privileges as soon as possible after a change in these privileges, such as the when an individual leaves the organization. In the case of an “unfriendly” termination initiated by the organization, consideration should be given to revoking privileges at the same time as or even before the employee is notified of the dismissal.

### Resources:

**An Introduction to Computer Security: The NIST Handbook Chapters 10 and 17**, National Institute of Standards and Technology,

<http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf>

**Common Sense Guide to Prevention and Detection of Insider Threats**, United States Computer Emergency Readiness Team,

[http://www.us-cert.gov/reading\\_room/](http://www.us-cert.gov/reading_room/)



VICTOR O.  
SCHINNERER  
& COMPANY, INC.

