Writing a Security Plan

Jane Powanda
Mitretek Systems/UI Information Technology Support Center

Abstract

Description of topic:
Writing a security plan can be a daunting task, particularly if you don't know where to start. Federal guidelines provide you with what you need to know about a security plan but not how to do it. This tutorial describes a method that will help you to develop a security plan for your application, system or organization. It will help you to ask yourself and your co-workers the right questions and will help you to be selective in determining what information you need to gather to complete the plan. It is based on NIST 800-18 Guide for Developing Security Operational Plans for Information Technology Systems and is enhanced by integrating information security management topics discussed in ISO 17799, Information Technology - Code of practice for information security management.

This tutorial, developed by Ms. Powanda, has been successfully used as part of multiple security training workshops for state employees involved with US Department of Labor programs. It leads the student through the writing of each of the sections of a Security Plan that includes:

- Introduction (Purpose, scope, intended audience, plan maintenance, etc.)
- The Application/System and its Environment (Hardware, Software, Operational environment, Data sensitivity, Threats, Security goals)
- Operational Plan (Roles and Responsibilities, Management controls, Operational controls, Technical controls)
- Other relevant topics
- Glossary

Biography

Ms. Powanda, a Senior Information Security Specialist and Program Manager at Mitretek Systems, is currently managing programs involving security, security training, and system modernization for the Unemployment Insurance Information Technology Support Center (ITSC), a U.S. Department of Labor program. Over the past five years, she has helped many state and federal organizations to write security and business continuity plans, and perform security risk assessments. Her 25 years experience in the information security field has given her the opportunity to solve security technology problems for the Department of Defense, foreign governments, many civil federal agencies as well as commercial enterprises. She has also had the opportunity to serve as a member of a National Security Standards Oversight Group, a subcommittee of the President's National

Security Telecommunications Advisory Committee (NSTAC). Prior to working in security, she distinguished herself as an expert in systems programming and computer programming languages.

Ms. Powanda holds a bachelors degree in math, computer science, and education from Penn State University and a Masters degree in Business from Temple University. In addition to her work in industry she has been an adjunct faculty member of Immaculata College and Villanova University where she taught Computer Literacy and Computer Programming Languages. Her outreach to local schools in helping young people to understand information security, using DISA's CyberProtect tool, has resulted in invitations to speak at the National Cyber Ethics Conference and the Virginia State Technical Educator's conference.