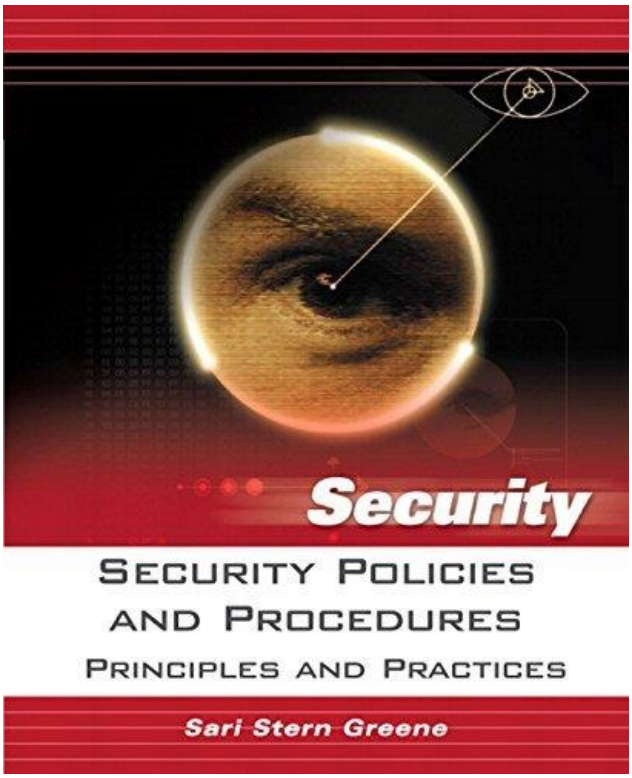
บทวิจารณ์หนังสือ

นิตยา วงศ์ภินันท์วัฒนา
ภาควิชาระบบสารสนเทศเพื่อการจัดการ คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์



Title: Security policies and procedures: principles and practices
Author: Sari Stern Greene
Edition: 1st Edition, 2006
Publisher: Prentice Hall
Number of pages: 544

หนังสือ Security policies and procedures: principles and practices เป็นหนังสือที่กล่าวว่าองค์กรควรวางแผนอย่างไรเพื่อป้องกันทรัพย์สินด้านสารสนเทศทั้งที่จับต้องได้และไม่ได้ นอกจากนี้ยังกล่าวว่า รูปแบบของนโยบายเป็นสิ่งที่มีความสำคัญอย่างมากต่อการทำความเข้าใจของเจ้าหน้าที่ขององค์กร โดยมีแนวความคิดสองแบบเกี่ยวกับรูปแบบของนโยบาย แนวความคิดที่หนึ่งกล่าวว่าควรเขียนนโยบายทั้งหมดรวมกันในเอกสารฉบับเดียวโดยแยกออกเป็นหัวข้อย่อยๆ (write one large policy document) อีกแนวคิดหนึ่ง คือ แยกเขียนนโยบายออกเป็นส่วนๆ ที่เป็นอิสระจากกัน ในที่นี้จะใช้แนวคิดสุดท้าย คือ แยกเขียนนโยบายออกเป็นส่วนย่อยๆ แยกจากกัน

หนังสือเล่มนี้ยังกล่าวถึงการกำหนดปัจจัยต่างๆ ที่จะนำมาจัดทำนโยบายการรักษาความมั่นคงปลอดภัย โดย องค์กรต้องวิเคราะห์ความเสี่ยงและพิจารณาว่าจะยึดหลักหรือแนวปฏิบัติเกี่ยวกับการรักษาความมั่นคงปลอดภัยของหน่วยงานใด เช่น ISO, COBIT หรือ ITIL เป็นต้น หนังสือเล่มนี้มีตัวอย่างการกำหนดนโยบายการรักษาความมั่นคงปลอดภัยตามมาตรฐานการรักษาความมั่นคงปลอดภัยของ ISO 17799-2000 หรือ BS 7799 เป็นหลักในการกำหนด domain ที่จะต้องจัดทำนโยบายการรักษาความมั่นคงปลอดภัย ซึ่งมาตรฐานดังกล่าว กำหนด domain ของการรักษาความมั่นคงปลอดภัยดังนี้ (1) นโยบายการรักษาความมั่นคงปลอดภัยองค์กร (2) นโยบายการจัดชั้นทรัพย์สินและขั้นตอนการปฏิบัติงาน (3) นโยบายบุคลากรและขั้นตอนการปฏิบัติงาน (4) นโยบายการรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อมและขั้นตอนการปฏิบัติงาน (5) นโยบายการจัดการการสื่อสารและการปฏิบัติการและขั้นตอนการปฏิบัติงาน (6) นโยบายควบคุมการเข้าถึงและขั้นตอนการปฏิบัติงาน (7) นโยบายการพัฒนาระบบและบำรุงรักษาและขั้นตอนการปฏิบัติงาน (8) นโยบายการฟื้นฟูระบบจากภัยพิบัติและความต่อเนื่องของการดำเนินธุรกิจและขั้นตอนการปฏิบัติงาน