

สารบัญ

	หน้า
คำนำ.....	(3)
รายละเอียดชุดวิชา.....	(7)
วิธีการศึกษา	(8)
 หน่วยที่ 6 ความมั่นคงปลอดภัยของระบบปฏิบัติการวินโดวส์.....	 6-1
แผนการสอนประจำหน่วย	6-2
ตอนที่ 6.1 ความรู้เบื้องต้นเกี่ยวกับระบบปฏิบัติการวินโดวส์.....	6-4
เรื่องที่ 6.1.1 ระบบความมั่นคงปลอดภัยของระบบปฏิบัติการวินโดวส์.....	6-5
เรื่องที่ 6.1.2 การจัดการความมั่นคงปลอดภัยของระบบปฏิบัติการวินโดวส์	6-15
ตอนที่ 6.2 การป้องกันภัยคุกคามต่อระบบปฏิบัติการวินโดวส์	6-18
เรื่องที่ 6.2.1 การปิดช่องโหว่ในระบบปฏิบัติการวินโดวส์	6-19
เรื่องที่ 6.2.2 การป้องกันความมั่นคงปลอดภัยในระบบปฏิบัติการวินโดวส์	6-28
ตอนที่ 6.3 การบริหารความมั่นคงปลอดภัยของระบบปฏิบัติการวินโดวส์	6-31
เรื่องที่ 6.3.1 การยกระดับและการติดตั้งแพตช์	6-32
เรื่องที่ 6.3.2 การบำรุงรักษาความปลอดภัยระบบปฏิบัติการวินโดวส์.....	6-35
เรื่องที่ 6.2.3 การป้องกันการโจมตีในระบบปฏิบัติการวินโดวส์.....	6-38
บรรณานุกรม	6-41
 หน่วยที่ 7 ความมั่นคงปลอดภัยของระบบปฏิบัติการยูนิกซ์.....	 7-1
แผนการสอนประจำหน่วย	7-2
ตอนที่ 7.1 ระบบความมั่นคงปลอดภัยของระบบปฏิบัติการยูนิกซ์.....	7-4
เรื่องที่ 7.1.1 พื้นฐานระบบปฏิบัติการยูนิกซ์	7-5
เรื่องที่ 7.1.2 การจัดการความมั่นคงปลอดภัยของระบบปฏิบัติการยูนิกซ์	7-9
ตอนที่ 7.2 การควบคุมความมั่นคงปลอดภัยของระบบปฏิบัติการยูนิกซ์	7-17
เรื่องที่ 7.2.1 การควบคุมโพรเซสของระบบปฏิบัติการยูนิกซ์.....	7-18
เรื่องที่ 7.2.2 การควบคุมผู้ใช้ระบบปฏิบัติการยูนิกซ์	7-22
เรื่องที่ 7.2.3 การเข้ารหัสลับของระบบปฏิบัติการยูนิกซ์	7-25
ตอนที่ 7.3 การบริหารความมั่นคงปลอดภัยของระบบปฏิบัติการยูนิกซ์.....	7-27
เรื่องที่ 7.3.1 การทดสอบความมั่นคงปลอดภัยของระบบปฏิบัติการยูนิกซ์.....	7-28
เรื่องที่ 7.3.2 การป้องกันการโจมตีระบบปฏิบัติการยูนิกซ์.....	7-31
บรรณานุกรม	7-40

หน่วยที่ 8 ความมั่นคงปลอดภัยของระบบเครือข่ายคอมพิวเตอร์.....	8-1
แผนการสอนประจำหน่วย.....	8-2
ตอนที่ 8.1 ความรู้เบื้องต้นเกี่ยวกับการรักษาความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์.....	8-4
เรื่องที่ 8.1.1 พื้นฐานการรักษาความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์.....	8-6
เรื่องที่ 8.1.2 โครงสร้างระบบเครือข่ายคอมพิวเตอร์เพื่อป้องกันภัยคุกคาม.....	8-13
ตอนที่ 8.2 ช่องโหว่ ภัยคุกคาม และการรักษาความมั่นคงปลอดภัยของระบบเครือข่ายคอมพิวเตอร์.....	8-23
เรื่องที่ 8.2.1 ช่องโหว่การสื่อสารบนระบบเครือข่ายคอมพิวเตอร์.....	8-25
เรื่องที่ 8.2.2 ภัยคุกคามบนระบบเครือข่ายคอมพิวเตอร์.....	8-31
เรื่องที่ 8.2.3 การรักษาความปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์.....	8-34
ตอนที่ 8.3 โพรโทคอลการรักษาความปลอดภัยระบบเครือข่ายคอมพิวเตอร์.....	8-39
เรื่องที่ 8.3.1 โพรโทคอลการพิสูจน์ตัวตนในระบบเครือข่ายคอมพิวเตอร์.....	8-41
เรื่องที่ 8.3.2 โพรโทคอลการพิสูจน์ตัวตนเพื่อการเข้าถึงระยะไกล.....	8-47
เรื่องที่ 8.2.3 โพรโทคอลการรักษาความมั่นคงปลอดภัยเลเยอร์ที่ 2 และเลเยอร์ที่.....	8-54
บรรณานุกรม.....	8-61
 หน่วยที่ 9 เทคโนโลยีการรักษาความมั่นคงปลอดภัยระบบเครือข่ายคอมพิวเตอร์.....	9-1
แผนการสอนประจำหน่วย.....	9-2
ตอนที่ 9.1 ไฟร์วอลล์.....	9-4
เรื่องที่ 9.1.1 ความสำคัญ คุณสมบัติ และประเภทของไฟร์วอลล์.....	9-6
เรื่องที่ 9.1.2 สถาปัตยกรรมการทำงานของไฟร์วอลล์.....	9-14
เรื่องที่ 9.1.3 ชุดของข้อกำหนดและผลิตภัณฑ์ไฟร์วอลล์.....	9-20
ตอนที่ 9.2 ระบบตรวจจับการบุกรุกระบบเครือข่ายคอมพิวเตอร์.....	9-29
เรื่องที่ 9.2.1 ความหมาย ข้อดี และประเภทของระบบตรวจจับการบุกรุกระบบเครือข่ายคอมพิวเตอร์.....	9-30
เรื่องที่ 9.2.2 การตรวจจับการบุกรุกระบบเครือข่ายคอมพิวเตอร์.....	9-41
ตอนที่ 9.3 ตัวอย่างการใช้เทคโนโลยีการรักษาความมั่นคงปลอดภัยระบบเครือข่ายคอมพิวเตอร์ ..	9-49
เรื่องที่ 9.3.1 เทคโนโลยีการรักษาความมั่นคงปลอดภัยระบบทรีสต์.....	9-50
เรื่องที่ 9.3.2 เทคโนโลยีการรักษาความมั่นคงปลอดภัยระบบประมวลผลแบบกลุ่มเมฆ.....	9-55
บรรณานุกรม.....	9-61

หน่วยที่ 10 ความมั่นคงปลอดภัยของระบบเครือข่ายไร้สาย	10-1
แผนการสอนประจำหน่วย	10-2
ตอนที่ 10.1 ความรู้เบื้องต้นเกี่ยวกับเครือข่ายแลนไร้สาย	10-4
เรื่องที่ 10.1.1 รูปแบบการเชื่อมต่อและการเข้าใช้ช่องสัญญาณของเครือข่ายแลนไร้สาย	10-5
เรื่องที่ 10.1.2 มาตรฐานเครือข่ายแลนไร้สาย	10-10
เรื่องที่ 10.1.3 ความถี่ในการใช้งานและเทคโนโลยีในการส่งสัญญาณในเครือข่ายแลนไร้สาย	10-17
ตอนที่ 10.2 การรักษาความมั่นคงปลอดภัยในเครือข่ายแลนไร้สาย	10-22
เรื่องที่ 10.2.1 ภัยคุกคามในเครือข่ายแลนไร้สาย	10-23
เรื่องที่ 10.2.2 การรักษาความปลอดภัยในมาตรฐาน IEEE 802.11	10-28
บรรณานุกรม	10-38