แนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์และเครือข่าย ตามมาตรฐาน ISO/IEC 27001 กรณีศึกษาโรงแรมเดอะเบอร์เคลีย์

มงคล ใจมา

สารนิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
วิทยาศาสตร์มหาบัณฑิต (สาขาวิทยาการคอมพิวเตอร์และระบบสารสนเทศ)
คณะสถิติประยุกต์
สถาบันบัณฑิตพัฒนบริหารศาสตร์
2562

บทคัดย่อ

ชื่อสารนิพนธ์	แนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์และเครือข่าย ตามมาตรฐาน ISO/IEC 27001 กรณีศึกษาโรงแรมเดอะเบอร์เคลีย์
ชื่อผู้เขียน	นายมงคล ใจมา
ชื่อปริญญา	วิทยาศาสตร์มหาบัณฑิต (สาขาวิทยาการคอมพิวเตอร์และระบบสารสนเทศ)
ปีการศึกษา	2562
อาจารย์ที่ปรึกษา	รศ.ดร.วราภรณ์ จิรชีพพัฒนา รศ.ดร.นิธินันท์ ธรรมากรนนท์

กระบวนการศึกษาของโครงงานนี้ เป็นการนำเอาการบริหารจัดการความมั่นคงปลอดภัยตามมาตรฐาน ISO/IEC 27001 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มาเป็นแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์และเครือข่าย เพื่อให้องค์กรมั่นใจได้ว่าการดำเนินงานทางธุรกิจสามารถดำเนินไปได้อย่างต่อเนื่อง ลดความเสี่ยงและป้องกันการเข้าถึงระบบเทคโนโลยีสารสนเทศจากบุคคลอื่น และการให้บริการอินเตอร์เน็ตของโรงแรมมีรูปแบบและขั้นตอนการให้บริการที่สามารถติดตามหรือระบุตัวตนผู้ใช้งานได้

กิตติกรรมประกาศ

การศึกษาและการดำเนินงานของโครงการนี้ ประสบความสำเร็จได้ด้วยความกรุณาและความช่วยเหลือของ รศ.ดร.วราภรณ์ จิรชีพพัฒนา และ รศ.ดร.นิธินันท์ ธรรมากรนนท์ ซึ่งเป็นอาจารย์ที่ปรึกษา ที่ได้กรุณาสละเวลาและให้คำปรึกษาเป็นอย่างดี ทั้งการแนะนำแนวทางการดำเนินโครงงาน และองค์ความรู้ต่างๆ อันเป็นประโยชน์สำหรับการดำเนินโครงงานนี้ ส่งผลให้การศึกษาและการดำเนินโครงงานสำเร็จลุล่วงไปได้ด้วยดี ข้าพเจ้าขอขอบพระคุณอาจารย์เป็นอย่างสูง และขอบคุณเพื่อนๆ ที่มีส่วนช่วยเหลือในเรื่องต่างๆ มา ณ โอกาสนี้ด้วย

มงคล ใจมา

กุมภาพันธ์ 2563

สารบัญ

หน้า

บทคัดย่อ I

กิตติกรรมประกาศ II

สารบัญ III

สารบัญตาราง VII

สารบัญภาพ VIII

บทที่ 1 บทนำ 12

1.1 ที่มาและปัญหาของโครงการ 12

1.2 วัตถุประสงค์ 12

1.3 ขอบเขตการดำเนินงาน 12

1.4 วิธีดำเนินการ 13

1.5 ประโยชน์ที่คาดว่าจะได้รับ 13

บทที่ 2 พื้นฐานและทฤษฎีที่เกี่ยวข้อง 15

2.1 ทรัพยากรสารสนเทศ 15

2.2 ความมั่นคงปลอดภัยระบบคอมพิวเตอร์ 17

2.3 หลักการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ 18

2.4 ความเสี่ยงด้านเทคโนโลยีสารสนเทศ 23

2.5 การจัดการความเสี่ยง 24

2.6 แนวทางการบริหารจัดการความมั่นคงปลอดภัย 25

2.7 มาตรฐานที่เกี่ยวข้องกับการบริหารจัดการความมั่นคงปลอดภัย 28

2.8 มาตรฐาน ISO/IEC27001 29

2.9 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 30

2.10 การวิเคราะห์ช่องว่าง (Gap Analysis) ด้านการบริหารเทคโนโลยีสารสนเทศ.....33

บทที่ 3 การดำเนินงาน 35

3.1 วิเคราะห์โครงสร้างระบบคอมพิวเตอร์และเครือข่ายปัจจุบัน 35

3.1.1 โครงสร้างของระบบเครือข่าย 36

3.1.2 รายละเอียดอุปกรณ์ในระบบเครือข่าย.....37

3.1.3 ข้อมูลกำหนดให้ใช้เครือข่ายภายในองค์กร 38

3.1.4 อุปกรณ์เครื่องเซิร์ฟเวอร์ที่ใช้งาน 39

3.1.5 แอพพลิเคชั่นที่ใช้งาน.....40

3.1.6 ปริมาณผู้ใช้งานเครื่องคอมพิวเตอร์ 41

3.1.7 การกำหนดหมายเลข VLAN (Virtual LAN).....42

3.1.8 โครงสร้างการเดินสายสัญญาณระหว่างชั้น.....42

3.1.9 รายละเอียดการติดตั้งและการเชื่อมต่อระบบเครือข่าย.....43

3.2 วิเคราะห์ระบบสนับสนุนความปลอดภัยระบบคอมพิวเตอร์และเครือข่ายปัจจุบัน 44

3.3 วิเคราะห์ปัญหาในระบบคอมพิวเตอร์และเครือข่ายปัจจุบัน.....46

3.3.1 ช่องโหว่หรือข้อบกพร่องของระบบคอมพิวเตอร์และเครือข่ายปัจจุบัน 46

3.3.2 ความเสี่ยงในการเข้าถึงระบบเทคโนโลยีสารสนเทศ 49

3.3.3 การกระทำความผิดในแง่ของโอกาสที่จะเกิดขึ้นกับการให้บริการอินเตอร์เน็ต 52

3.4 การวิเคราะห์ช่องว่าง (Gap Analysis) 53

3.4.1 การวิเคราะห์ช่องว่างโครงสร้างระบบคอมพิวเตอร์และเครือข่าย.....53

3.4.2 การวิเคราะห์ช่องว่างการเข้าถึงระบบเทคโนโลยีสารสนเทศ 56

3.4.3 การวิเคราะห์ช่องว่างการให้บริการอินเตอร์เน็ตของโรงแรม 60

บทที่ 4 ผลการดำเนินงาน 62

4.1 การออกแบบโครงสร้างความมั่นคงปลอดภัยระบบคอมพิวเตอร์และเครือข่ายใหม่ 62

4.1.1 การปรับปรุงโครงสร้างอุปกรณ์และเครือข่าย 63
4.1.1.1 การเปลี่ยนสวิตซ์หลัก (Core Switch) 63
4.1.1.2 การเปลี่ยนสวิตซ์ในส่วนที่เชื่อมต่อกับผู้ใช้งานในแต่ละชั้น (Access Switch)...63
4.1.1.3 การเปลี่ยนสาย UTP จาก CAT5 เป็น CAT6 ทั้งหมด 64
4.1.1.4 การนำเครื่องเซิร์ฟเวอร์ของแต่ละแผนกมาจัดวางใหม่ที่ DMZ Zone 64
4.1.1.5 การติดตั้งสวิตช์เซิร์ฟเวอร์ 65
4.1.1.6 การติดตั้งสัญญาณอินเตอร์เน็ต (Internet ADSL) 65
4.1.1.7 การป้องกันการเข้าถึงอุปกรณ์ Access Switch และ Access point.....65
4.1.1.8 การใช้งาน Port Security.....66
4.1.1.9 การทำ Disable Port ของอุปกรณ์ Switch 67
4.1.1.10 การทำ Backup & Restore Configuration.....67
4.1.1.11 การทำเครื่องหมายหรือติดหมายเลขกำกับไว้ที่สายแลนที่เชื่อมต่อกับ Access Switch 68
4.1.1.12 การนำระบบ VLAN เข้ามาใช้งาน.....68
4.1.1.13 การทำ Inter VLAN Routing 70
4.1.1.14 การควบคุมการเข้าออกห้อง Server.....70
4.1.2 ออกแบบระบบสนับสนุนความปลอดภัยของระบบคอมพิวเตอร์และเครือข่าย 71
4.1.2.1 การปรับปรุงการตั้งค่าการทำงานของระบบความปลอดภัยคอมพิวเตอร์และเครือข่าย 71
4.1.2.2 แนะนำโปรแกรมหรือระบบรักษาความปลอดภัยบนระบบคอมพิวเตอร์และเครือข่าย 78
4.2 แนวทางปฏิบัติในการเข้าถึงระบบเทคโนโลยีสารสนเทศ ภายใต้มาตรฐาน ISO/IEC 27001 82
4.2.1 การลงทะเบียนผู้ใช้งานระบบสารสนเทศ.....82
4.2.2 การถอดถอนสิทธิ์ผู้ใช้งานระบบสารสนเทศ.....84
4.2.3 การบริหารจัดการสิทธิ์ในการเข้าถึงระบบสารสนเทศ 86
4.2.4 การบริหารจัดการสิทธิ์ในการเข้าถึงดาต้าเซ็นเตอร์ 87
4.2.5 การควบคุมการใช้งานสิทธิ์ Administrator.....88
4.2.6 การควบคุมการเข้าถึงเครือข่ายไร้สาย.....88
4.2.7 การกำหนด Policy ในการเข้าถึงระบบระบบคอมพิวเตอร์.....89

4.2.8 การควบคุมการเข้าถึงอุปกรณ์เครือข่าย 92
4.2.9 การควบคุมการติดรหัสผ่านไว้ที่หน้าจอคอมพิวเตอร์หรือบนโต๊ะทำงาน 93
4.2.10 การควบคุมการเข้าถึงเครือข่ายภายในจากระยะไกล.....94
4.2.11 การควบคุมการเข้าออกห้องเซิร์ฟเวอร์ 94
4.2.12 การควบคุมการเข้าถึงตู้ Switch แต่ละตามชั้น 96
4.2.13 การควบคุมการเปลี่ยนแปลงอุปกรณ์เครือข่าย 96
4.2.14 การป้องกันไวรัสและสแปม.....97
4.2.15 การจัดการช่องโหว่ของ Windows.....98
4.2.16 การป้องกันการเข้าถึงและโจมตีจากเครือข่ายภายนอก.....99
4.2.17 การควบคุมการเข้าถึงระบบงานหรือข้อมูลของคนอื่น 100
4.3 แนวทางปฏิบัติในการให้บริการอินเตอร์เน็ต ตามแนวทางพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550.....100
4.3.1 การให้บริการอินเตอร์เน็ตสำหรับลูกค้า In-House Guest 101
4.3.2 การให้บริการอินเตอร์เน็ตสำหรับลูกค้า Visitors.....102
4.3.2.1 การเข้าใช้บริการอินเตอร์เน็ตจากคูปอง.....102
4.3.2.2 การเข้าใช้บริการอินเตอร์เน็ตผ่าน Facebook.....102
4.3.3 การให้บริการอินเตอร์เน็ตสำหรับพนักงานของโรงแรม 103
บทที่ 5 สรุปผลการดำเนินงาน.....105
5.1 สรุปขั้นตอนการดำเนินงาน.....105
5.2 สรุปผลการดำเนินงาน.....106
5.3 ปัญหาและอุปสรรค.....107
5.4 ข้อเสนอแนะ.....108
บรรณานุกรม.....109
ภาคผนวก ก DOMAIN INTERNATIONAL STANDARD ISO/IEC 27001 111
ประวัติผู้เขียน 119

สารบัญตาราง

ตารางที่ **หน้า**

ตารางที่ 2.1 ฐานความผิดและบทกำหนดโทษ.....31
ตารางที่ 3.1 แสดงอุปกรณ์เครือข่าย.....36
ตารางที่ 3.2 แสดงภาพรวมเครือข่ายขององค์กร.....39
ตารางที่ 3.3 แสดงรายละเอียดอุปกรณ์เซิร์ฟเวอร์และเซอร์วิสที่ใช้งาน.....40
ตารางที่ 3.4 แสดงแอพพลิเคชั่นและระดับความสำคัญ.....40
ตารางที่ 3.5 แสดงจำนวนเครื่องคอมพิวเตอร์.....41
ตารางที่ 3.6 แสดงหมายเลย IP Address และหมายเลข VLAN.....42
ตารางที่ 3.7 ช่องโหว่หรือข้อบกพร่องของระบบคอมพิวเตอร์และเครือข่ายปัจจุบัน.....46
ตารางที่ 3.8 ความเสี่ยงในการเข้าถึงระบบเทคโนโลยีสารสนเทศ.....49
ตารางที่ 3.9 การกระทำความผิดในแง่ของโอกาสที่จะเกิดขึ้นกับการให้บริการอินเตอร์เน็ต.....52
ตารางที่ 3.10 การวิเคราะห์ช่องว่างโครงสร้างระบบคอมพิวเตอร์และเครือข่าย.....53
ตารางที่ 3.11 การวิเคราะห์ช่องว่างการเข้าถึงระบบเทคโนโลยีสารสนเทศ.....56
ตารางที่ 3.12 การวิเคราะห์ช่องว่างการให้บริการอินเตอร์เน็ตของโรงแรม.....60
ตารางที่ 4.1 แสดงการกำหนด Username และ Password ที่อุปกรณ์ Access Switch.....65
ตารางที่ 4.2 แสดงตัวอย่างการออกแบบ VLAN ของระบบเครือข่ายใหม่.....68
ตารางที่ 4.3 แสดงตัวอย่างการทำ Inter VLAN Routing ของแต่ละแผนกที่ทำงานใน Operation เดียวกัน.....70

สารบัญภาพ

รูปที่ **หน้า**

รูปที่ 2.1 องค์ประกอบสำคัญของการรักษาความมั่นคงปลอดภัยสารสนเทศ 19
รูปที่ 2.2 วงรอบการจัดการระบบบริหารจัดการการรักษาความมั่นคงปลอดภัยสารสนเทศ ISO 27001.....29
รูปที่ 3.1 โครงสร้างระบบเครือข่ายปัจจุบันขององค์กร 36
รูปที่ 3.2 ตัวอย่างอุปกรณ์ Core Switch.....37
รูปที่ 3.3 ตัวอย่างอุปกรณ์ Access Switch 37
รูปที่ 3.4 ตัวอย่างอุปกรณ์ Firewall 37
รูปที่ 3.5 ตัวอย่างอุปกรณ์ Firewall 38
รูปที่ 3.6 ตัวอย่างอุปกรณ์ Nas Storage 38
รูปที่ 3.7 ตัวอย่างอุปกรณ์ Access Point.....38
รูปที่ 3.8 ตัวอย่างโครงสร้างการเดินสายสัญญาณระหว่างชั้น.....42
รูปที่ 3.9 ตัวอย่างการติดตั้งอุปกรณ์เครือข่าย Core Switch 43
รูปที่ 3.10 ตัวอย่างการติดตั้ง Access Switch.....43
รูปที่ 3.11 ตัวอย่างการติดตั้ง Access Point 44
รูปที่ 4.1 แสดงผังการออกแบบผังโครงสร้างระบบเครือข่ายใหม่ 63
รูปที่ 4.2 ตัวอย่างอุปกรณ์ Core Switch ยี่ห้อ Aruba 3810M 48G.....63
รูปที่ 4.3 ตัวอย่างอุปกรณ์ Access Switch ยี่ห้อ รุ่น Aruba 2530 48G 64
รูปที่ 4.4 ตัวอย่างสาย UTP แบบ CAT6.....64
รูปที่ 4.5 ตัวอย่างการนำเครื่องเซิร์ฟเวอร์ของแต่ละแผนกมาจัดวางใหม่ที่ DMZ Zone 64
รูปที่ 4.6 ตัวอย่างการติดตั้งสวิตช์สำหรับเครื่องเซิร์ฟเวอร์ 65
รูปที่ 4.7 การติดตั้งสัญญาณอินเตอร์เน็ต (Internet ADSL) จากผู้ให้บริการ ISP 2 ราย.....65
รูปที่ 4.8 การกำหนดรหัสผ่านเข้าถึงอุปกรณ์ Access Switch.....66

รูปที่ 4.9 การกำหนดรหัสผ่านเข้าถึงอุปกรณ์ Access Point 66
รูปที่ 4.10 แสดงการทำ Port Security ของอุปกรณ์ Access Switch 67
รูปที่ 4.11 แสดงการ Disable Port ของอุปกรณ์ Switch ที่เชื่อมต่อไปยัง Outlet Lan 67
รูปที่ 4.12 ตัวอย่างการกำหนดรหัสผ่านเข้าถึงอุปกรณ์ Access Switch.....68
รูปที่ 4.13 ตัวอย่างแสดงการติดตั้ง Finger Scan และกล้องวงจรปิด CCTV 71
รูปที่ 4.14 ตัวอย่างแสดง Redundant internet connections 72
รูปที่ 4.15 ตัวอย่างแสดงการตั้งค่า Anti-Virus 72
รูปที่ 4.16 ตัวอย่างแสดงการตั้งค่า Web Filter 72
รูปที่ 4.17 ตัวอย่างแสดงการตั้งค่า DNS Filter.....73
รูปที่ 4.18 ตัวอย่างแสดงการตั้งค่า Application Control 73
รูปที่ 4.19 ตัวอย่างแสดงการตั้งค่า Intrusion Protection (IPS) 73
รูปที่ 4.20 ตัวอย่างแสดงการตั้งค่า Email Filter 74
รูปที่ 4.21 ตัวอย่างแสดง Limiting bandwidth with traffic shaping.....74
รูปที่ 4.22 ตัวอย่างแสดง IPsec VPN with FortiClient.....75
รูปที่ 4.23 ตัวอย่างการติดตั้งโครงสร้างออบเจ็คในระบบแอคทีฟไดเรกเทอรี่ 75
รูปที่ 4.24 ตัวอย่างการติดตั้ง Additional Domain Controller.....76
รูปที่ 4.25 ตัวอย่างการตั้งค่า Driver Maps ในระบบ Active directory 76
รูปที่ 4.26 ตัวอย่างการติดตั้ง Radius Server ในระบบ Active directory 77
รูปที่ 4.27 ตัวอย่างการติดตั้ง DHCP Server.....77
รูปที่ 4.28 ตัวอย่างการติดตั้งระบบ Access Point Controller 78
รูปที่ 4.29 ตัวอย่างระบบมอนิเตอร์อุปกรณ์เครือข่ายด้วยโปรแกรม IPswitch WhatsUp Gold 78
รูปที่ 4.30 ตัวอย่างการติดตั้งโปรแกรม Veeam Backup & Replication.....79
รูปที่ 4.31 ตัวอย่างการติดตั้งโปรแกรม ESET Security Management Center 80
รูปที่ 4.32 ตัวอย่างการติดตั้งโปรแกรม MalwareBytes 80
รูปที่ 4.33 ตัวอย่างการติดตั้งโปรแกรม SOFTNIX LOGGER (SLG) 81
รูปที่ 4.34 ตัวอย่างการติดตั้งโปรแกรม Snort 82

รูปที่ 4.35 แบบฟอร์มลงทะเบียนขอใช้บริการระบบสารสนเทศ.....83
รูปที่ 4.36 ตัวอย่างการทบทวนเอกสารสิทธิ์ของพนักงาน.....84
รูปที่ 4.37 ตัวอย่างรายชื่อพนักงานที่ออกแล้วที่ฝ่าย HR ส่งให้ฝ่ายไอที.....85
รูปที่ 4.38 ตัวอย่างพนักงานที่ออกแล้วต้องอยู่สถานะ Disable / Inactive.....85
รูปที่ 4.39 ตัวอย่างการจัดการสิทธิ์ผู้ใช้งานสำหรับโปรแกรม Metro.Brita.....86
รูปที่ 4.40 ตัวอย่างการจัดการสิทธิ์ผู้ใช้งานสำหรับโปรแกรม Epitome.....87
รูปที่ 4.41 ตัวอย่างโฟลเดอร์ในดาต้าเซ็นเตอร์สำหรับแต่ละแผนก.....87
รูปที่ 4.42 แสดงการ InActive ของ Account ที่ใช้เป็น Admin ร่วมกัน.....88
รูปที่ 4.43 ตัวอย่างการแบ่งแยก SSID สำหรับเครือข่ายไร้สาย.....89
รูปที่ 4.44 ตัวอย่างการจัดการ User Account ของผู้ใช้งานในแต่ละแผนก.....89
รูปที่ 4.45 ตัวอย่างการกำหนดเป็น Policy ใน GPO.....90
รูปที่ 4.46 ตัวอย่างการกำหนด Policy ป้องกันการ Brute Force.....91
รูปที่ 4.47 แสดงกำหนด Policy ในการล็อคหน้าจออัตโนมัติ.....91
รูปที่ 4.48 แสดงการล็อคหน้าจออัตโนมัติที่เครื่องคอมพิวเตอร์ของพนักงาน.....92
รูปที่ 4.49 แสดงการกำหนด Password ที่อุปกรณ์ Access Point.....92
รูปที่ 4.50 ตัวอย่างก่อนติดพาสเวิร์ดและหลังจากนำพาสเวิร์ดที่ติดไว้ออกจากจอคอมพิวเตอร์.....93
รูปที่ 4.51 แสดงโปรแกรมรีโมทระยะไกลที่ต้องลบออกจากเครื่องผู้ใช้.....94
รูปที่ 4.52 แสดงการติดตั้ง Finger Scan และกล้องวงจรปิด CCTV.....95
รูปที่ 4.53 แบบฟอร์มบันทึกการเข้าออกห้องเซิร์ฟเวอร์.....95
รูปที่ 4.54 แสดงการล็อคตู้แร็ค Switch ตามชั้นต่างๆ.....96
รูปที่ 4.55 แสดงการสำรอง Config ของอุปกรณ์ Switch.....97
รูปที่ 4.56 แสดงการติดตั้ง Antivirus.....98
รูปที่ 4.57 แสดงการ Update จากระบบ SECURITY MANAGEMENT CENTER.....98
รูปที่ 4.58 แสดงการ Update Patch Windows.....99
รูปที่ 4.59 แสดงการตั้งค่า Policy ของ Firewall (FortiGate 80E).....99
รูปที่ 4.60 แสดงการเข้ารหัสเอกสารจากโปรแกรม Excel.....100

รูปที่ 4.61 แสดงตัวอย่างระบบ Interface ในการเชื่อมต่อฐานข้อมูลของลูกค้า.....101
รูปที่ 4.62 แสดงตัวอย่างหน้า Login เข้าใช้บริการอินเตอร์เน็ต สำหรับลูกค้า In-House Guest 101
รูปที่ 4.63 แสดงตัวอย่างแบบฟอร์มในการแจกคูปอง 102
รูปที่ 4.64 แสดงตัวอย่างการเข้าใช้บริการอินเตอร์เน็ตผ่าน Facebook.....103
รูปที่ 4.65 แสดงตัวอย่างหน้า Login เข้าใช้บริการอินเตอร์เน็ต 103
รูปที่ 4.66 แสดงตัวอย่างแบบฟอร์มขอใช้บริการอินเตอร์เน็ต 104
รูปที่ 4.67 แสดงตัวอย่างหน้า Login เข้าใช้บริการอินเตอร์เน็ตสำหรับพนักงาน 104

บทที่ 1
บทนำ

1.1 ที่มาและปัญหาของโครงการ

โรงแรมเดอะเบอร์เคลีย์ เป็นหนึ่งในผู้ประกอบธุรกิจโรงแรมชั้นนำที่มีเอกลักษณ์การให้บริการแบบไทยในระดับมาตรฐานสากล เปิดให้บริการห้องพักรายวัน 24 ชั่วโมง สไตล์โมเดิร์น 788 ห้อง เหมาะกับการเข้าพักทุกรูปแบบ แพคเกจงานห้องประชุมสัมมนา พร้อมกับทีมจัดเลี้ยงที่คอยอำนวยความสะดวกและให้ความช่วยเหลือตั้งแต่ต้นจนจบงาน ห้องอาหารที่นำเสนอเมนูอาหารจากหลายหลายทวีปทั่วโลก ห้องจัดเลี้ยงสามารถปรับเปลี่ยนรูปแบบการจัดงานได้หลากหลายรูปแบบ ล๊อบบี้ให้บริการอาหารว่าง เบเกอรี่และเครื่องดื่มนานาชนิด ในเวลากลางวันสามารถนัดพบลูกค้า คุยงาน หรือแวะพักผ่อนระหว่างทริปการเดินทาง หรือให้บริการเบียร์เย็นๆ และเล่นดนตรีสด

ปัจจุบันโครงสร้างระบบคอมพิวเตอร์และเครือข่ายขององค์กร ยังเกิดช่องโหว่หรือข้อบกพร่องที่อาจส่งผลทำให้องค์กรขาดประสิทธิภาพในการดำเนินงาน ระบบหยุดชะงักทำงานไม่ต่อเนื่อง และเกิดความเสี่ยงต่อการบุกรุกจากผู้ไม่ประสงค์ดี พร้อมทั้งความเสี่ยงในการเข้าถึงระบบสารสนเทศของพนักงาน เนื่องจากพนักงานยังขาดความรู้ความเข้าใจในเรื่องความปลอดภัยสารสนเทศ และองค์กรยังไม่มีบทลงโทษสำหรับการละเมิดกฎข้อบังคับด้านความมั่นคงปลอดภัยสารสนเทศทั้งผู้ใช้งานและผู้ดูแลระบบ

นอกจากนี้ระบบการให้บริการอินเตอร์เน็ตของโรงแรม ยังอาจเกิดความเสี่ยงในการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เนื่องจากการ Login เข้าใช้งานอินเตอร์เน็ตจะให้กรอก Email Address เพื่อรับ Username และ Password ซึ่งทำให้ไม่สามารถติดตามหรือระบุตัวตนผู้ใช้งานได้

1.2 วัตถุประสงค์

เพื่อเสนอแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์และเครือข่ายต่อผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ

1.3 ขอบเขตการดำเนินงาน

- โครงสร้างความมั่นคงปลอดภัยระบบคอมพิวเตอร์และเครือข่ายภายในโรงแรม

- การเข้าถึงระบบเทคโนโลยีสารสนเทศภายใต้การควบคุมการเข้าถึง (Access control) ตามมาตรฐาน ISO/IEC 27001
- การให้บริการอินเตอร์เน็ตของโรงแรมให้ถูกต้องตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

1.4 วิธีดำเนินการ

- วิเคราะห์โครงสร้างความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และเครือข่ายปัจจุบันภายในองค์กร
- วิเคราะห์ช่องโหว่หรือข้อบกพร่องของโครงสร้างเครือข่ายปัจจุบัน ความเสี่ยงในการเข้าถึงระบบเทคโนโลยีสารสนเทศ และปัญหาเกี่ยวกับการกระทำความผิดในแง่ของโอกาสที่จะเกิดขึ้นกับการให้บริการอินเตอร์เน็ต
- วิเคราะห์ช่องว่าง (Gap Analysis) เพื่อระบุถึงความแตกต่างระหว่างระบบคอมพิวเตอร์และเครือข่ายปัจจุบันและระบบใหม่ที่ออกแบบไว้
- ออกแบบแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์และเครือข่ายตามมาตรฐาน ISO/IEC 27001 และการให้บริการอินเตอร์เน็ตของโรงแรมให้ถูกต้องตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550
- เสนอแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์และเครือข่าย ต่อผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ
- นำข้อเสนอแนะที่ได้จากผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ เพื่อมาปรับปรุงแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์และเครือข่ายให้ดีขึ้น

1.5 ประโยชน์ที่คาดว่าจะได้รับ

- เพื่อให้การปฏิบัติงานเป็นไปอย่างมีระบบ ทำงานได้อย่างต่อเนื่อง และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที เมื่อเกิดสถานการณ์ความไม่แน่นอน
- เพื่อลดความเสี่ยงที่อาจเกิดขึ้นจากการโจมตีโดยอาศัยช่องโหว่ของระบบคอมพิวเตอร์และเครือข่าย

- เพื่อป้องกันระบบเทคโนโลยีสารสนเทศและระบบฐานข้อมูลจากผู้บุกรุกและผู้ไม่มีสิทธิ์ในการเข้ามาใช้ระบบจากภายในองค์กร
- เพื่อเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบคอมพิวเตอร์และเครือข่าย
- เพื่อให้ผู้ใช้งานและผู้ดูแลระบบตระหนักถึงความปลอดภัยในการเข้าถึงระบบเทคโนโลยีสารสนเทศ
- เพื่อการบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศที่ดีและมีประสิทธิภาพ ตามมาตรฐาน ISO/IEC 27001
- เพื่อการปฏิบัติและหลีกเลี่ยงการละเมิดข้อกำหนดทางกฎหมายในการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550
- เพื่อเป็นแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์และเครือข่ายขององค์กร สำหรับการวางแผนพัฒนาและปรับปรุงต่อยอดเพิ่มประสิทธิภาพที่ดียิ่งขึ้นในอนาคต

บทที่ 2
พื้นฐานและทฤษฎีที่เกี่ยวข้อง

ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ มีความหมายครอบคลุมถึงการรักษาความลับ การรักษาความครบถ้วนสมบูรณ์ และการรักษาความพร้อมใช้ของทรัพยากรในระบบคอมพิวเตอร์ทุกๆ ระดับ เริ่มต้นตั้งแต่อุปกรณ์ฮาร์ดแวร์ ระบบปฏิบัติการ ซอฟต์แวร์ และการเชื่อมต่อกันเป็นเครือข่าย รวมถึงข้อมูลหรือสารสนเทศที่ถูกจัดเก็บและประมวลผลโดยอุปกรณ์และซอฟต์แวร์ที่เชื่อมต่อเป็นระบบ ซึ่งทางผู้จัดทำได้รวบรวมข้อมูลที่เกี่ยวข้องกับแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์และเครือข่าย ได้ดังต่อไปนี้

2.1 ทรัพยากรสารสนเทศ

ทรัพยากรสารสนเทศ มีความหมายครอบคลุมถึงเครื่องคอมพิวเตอร์ และอุปกรณ์เชื่อมต่อต่างๆ และครอบคลุมถึงองค์ประกอบอื่นๆ ดังต่อไปนี้

มนุษย์ (people) ได้แก่ ผู้ที่เกี่ยวข้องกับระบบคอมพิวเตอร์ เช่น ผู้ใช้งาน ผู้ดูแลระบบ โดยปกติแล้วมนุษย์จะถูกประเมินเป็นภัยคุกคามหลักต่อทรัพยากรสารสนเทศเนื่องจากมีเป็นทรัพยากรที่เป็นมีจุดอ่อนมากที่สุดในการรักษาความมั่นคงปลอดภัย แม้ว่าทรัพยากรอื่นๆ จะถูกปกป้องและกำหนดมาตรการอย่างรัดกุมที่สุดแล้ว หากผู้คนที่เกี่ยวข้องกับทรัพยากรนั้นละเลยหรือขาดความตระหนักรู้ ก็จะส่งผลให้ทรัพยากรนั้นถูกโจมตีสำเร็จ เช่น การให้บริการรับฝากไฟล์ผ่านอินเทอร์เน็ต ซึ่งเลือกใช้เทคโนโลยีการรักษาความมั่นคงปลอดภัยที่เข้มแข็งมาก แต่ผู้ใช้งานบันทึกข้อมูลสำหรับใช้พิสูจน์ตัวจริงและกำหนดสิทธิ์โดยเขียนลงบนกระดาษแปะไว้ที่หน้าจอมอนิเตอร์ ย่อมเป็นการเพิ่มความเสี่ยงที่จะมีผู้ไม่ประสงค์ดีใช้ข้อมูลดังกล่าวเข้าถึงข้อมูลที่ถูกจัดเก็บในระบบนั้น โดยอาจเปลี่ยนแปลง แก้ไข หรือลบข้อมูลนั้นโดยไม่ได้รับอนุญาต

ฮาร์ดแวร์และอุปกรณ์ต่อเชื่อมต่างๆ (hardware and its peripheral) มีความหมายรวมถึงเครื่องคอมพิวเตอร์ แท็บเล็ต และสมาร์ทโฟน ซึ่งมีความสามารถในการรับข้อมูล ประมวลผล แสดงผลและเชื่อมต่อกับเครือข่ายคอมพิวเตอร์ได้ ความไม่มั่นคงปลอดภัยของอุปกรณ์เหล่านี้อาจเกิดขึ้นเนื่องจากมีภัยคุกคามเกิดขึ้นกับอุปกรณ์โดยตรง เช่น การขโมย ซึ่งส่งผลให้เจ้าของไม่สามารถใช้งานได้หรือนำข้อมูลส่วนบุคคลในอุปกรณ์นั้นไปเปิดเผยทำให้ความลับของข้อมูลนั้นถูกทำลายลง หรืออาจเกิดจากไฟฟ้ากระชากและทำให้ข้อมูลที่จัดเก็บในอุปกรณ์นั้นๆ เสียหาย

นอกจากนี้ยังรวมถึงการที่ฮาร์ดแวร์นั้นๆ ถูกทำลายหรือทำให้ใช้การไม่ได้โดยมีสาเหตุจากธรรมชาติ เช่น น้ำท่วม ฟ้าผ่าอุปกรณ์

ซอฟต์แวร์ (software) ที่ถูกพัฒนาขึ้นมักมีข้อบกพร่องที่เกี่ยวข้องกับความมั่นคงปลอดภัย เนื่องจากคุณสมบัตินี้มักถูกละเลยในระหว่างขั้นตอนการวิเคราะห์และพัฒนาซอฟต์แวร์นั้นๆ ทำให้เมื่อมีการนำมาใช้งานมักจะมีช่องโหว่ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย เช่น อุปกรณ์เราเตอร์สำหรับใช้งานอินเทอร์เน็ตสำหรับเชื่อมต่อผ่านระบบเอดีเอสแอลบางรุ่นมีข้อบกพร่องเกี่ยวกับความมั่นคงปลอดภัย และเมื่อผู้ไม่ประสงค์ดีโจมตีระบบสำเร็จจะสามารถปลอมแปลงกระบวนการสอบถามโดเมนเนมได้ ดังนั้นผู้ใช้งานหรือผู้ดูแลระบบจะต้องดำเนินการการปรับปรุง คุณสมบัติซอฟต์แวร์ตามหลังอยู่เสมอๆ ทั้งนี้การปรับปรุงคุณสมบัติดังกล่าวผู้พัฒนาซอฟต์แวร์อาจสร้างช่องโหว่ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยเพิ่มมากขึ้นโดยไม่ได้ตั้งใจก็เป็นได้

ข้อมูลและสารสนเทศ (data and information) เป็นทรัพยากรที่สำคัญต่อบุคคลหรือองค์กรที่เป็นผู้สร้างประมวลผล และรับส่งข้อมูลสารสนเทศนั้นๆ ด้วยเหตุนี้ทรัพยากรนี้จึงเป็นเป้าหมายหลักของการโจมตีของผู้ไม่ประสงค์ดีโดยผลเสียหายที่เกิดขึ้นมักจะเกิดขึ้นในสามลักษณะสำคัญคือ การเปิดเผยความลับ การแก้ไขข้อมูลโดยไม่มีสิทธิ์ และการทำให้ข้อมูลนั้นๆ ไม่สามารถเข้าถึงได้ เช่น ถูกลบ เปลี่ยนแปลงสิทธิ์หรือถูกเข้ารหัสลับเพื่อเรียกค่าไถ่

ขั้นตอนระเบียบวิธีปฏิบัติ (procedure) ขั้นตอนการดำเนินการกับข้อมูลมักถูกละเลยจากผู้ที่เกี่ยวข้องทำให้มีช่องโหว่ที่อาจทำให้เกิดการละเมิดความมั่นคงปลอดภัยได้ เช่น องค์กรต่างๆ มักมีการฝึกอบรมพนักงานให้ดำเนินการอย่างใดอย่างหนึ่งกับซอฟต์แวร์ที่ใช้ในองค์กรในรูปแบบของคู่มือการทำงาน ทำให้พนักงานที่มีหน้าที่คล้ายคลึงกันสามารถใช้งานซอฟต์แวร์ได้เหมือนๆ กัน โดยมักละเลยการสร้างความตระหนักรู้เกี่ยวกับการใช้งานซอฟต์แวร์อย่างมั่นคงปลอดภัยเป็นผลให้เกิดช่องโหว่ของการรักษาความมั่นคงปลอดภัยได้ เช่น พนักงานบัญชีคนหนึ่งอาจเข้าใช้งานระบบเงินเดือนค้างไว้โดยไม่ได้ล็อกหน้าจอขณะพักรับประทานอาหารกลางวัน ผู้ไม่ประสงค์ดีอาจเข้าใช้งานซอฟต์แวร์และปรับเปลี่ยนข้อมูลในระบบบัญชีได้

เครือข่าย (network) ระบบสารสนเทศในปัจจุบันถูกเชื่อมต่อเข้าด้วยกันผ่านเครือข่าย การรับส่งข้อมูลไม่ว่าจะเป็นเครือข่ายส่วนตัว เครือข่ายเฉพาะบริเวณ และเครือข่ายอินเทอร์เน็ต แม้ว่าการเชื่อมต่อกันดังกล่าวจะสร้างความสามารถในการใช้งานทรัพยากรสารสนเทศร่วมกันจากระยะทางไกล และทำให้เกิดการใช้งานทรัพยากรอย่างมีประสิทธิภาพมากยิ่งขึ้น การเชื่อมต่อกันเป็นเครือข่ายยิ่งมีขนาดมากเท่าไรย่อมเป็นการเพิ่มความเสี่ยงที่ทรัพยากรจะถูกโจมตี และเพิ่มความยากในการรักษาความมั่นคงปลอดภัยมากยิ่งขึ้น เมื่อกล่าวโดยนัยแล้วจะเห็นว่า ทรัพยากรสารสนเทศมีองค์ประกอบสำคัญๆ ดังที่ได้กล่าวมา อย่างไรก็ดีทรัพยากรสารสนเทศอาจถูกนิยามได้ใน

ความหมายที่ใกล้เคียงกันแต่ถูกนิยามขึ้นมาในระยะเริ่มต้น คือ ระบบคอมพิวเตอร์ ซึ่งประกอบด้วย ฮาร์ดแวร์ ซอฟต์แวร์ มนุษย์ และข้อมูล ซึ่งจะขาดองค์ประกอบสำคัญคือ เครือข่ายและขั้นตอนวิธีปฏิบัติ ซึ่งเป็นองค์ประกอบที่สำคัญในปัจจุบัน เนื่องจากการประยุกต์ใช้งานเทคโนโลยีสารสนเทศและการสื่อสารในปัจจุบัน มีการแลกเปลี่ยนทรัพยากรกันผ่านช่องทางการสื่อสารและระบบเครือข่าย ตลอดจนการประมวลผลข้อมูลในปัจจุบันมีความซับซ้อนมากขึ้นกว่าในอดีต ดังนั้นเมื่อกล่าวถึงระบบคอมพิวเตอร์ในปัจจุบันจึงนิยมใช้คำว่าทรัพยากรสารสนเทศ ซึ่งมีความหมายครอบคลุมถึงทรัพยากรเครือข่ายและขั้นตอนวิธีปฏิบัติที่เกี่ยวข้อง

2.2 ความมั่นคงปลอดภัยระบบคอมพิวเตอร์

การรักษาความมั่นคงปลอดภัย หมายถึง การทำให้มั่นใจได้ว่าทรัพยากรสารสนเทศที่มีอยู่มีความถูกต้องสมบูรณ์ และพร้อมใช้งานสำหรับผู้ใช้งานที่ได้รับสิทธิ์ในการเข้าถึงทรัพยากรนั้นๆ ดังตัวอย่างการรักษาความมั่นคงปลอดภัยของเครื่องคอมพิวเตอร์ส่วนบุคคล ซึ่งจัดเก็บข้อมูลอาจมีข้อมูลที่ไม่ต้องการให้ผู้อื่นล่วงรู้ ตลอดจนต้องการรักษาความครบถ้วนสมบูรณ์ของไฟล์ต่างๆ ที่ถูกจัดเก็บไว้ในคอมพิวเตอร์ไม่ให้ถูกทำลายโดยมัลแวร์ และป้องกันการแพร่ระบาดของหนอนอินเทอร์เน็ต ซึ่งอาจทำให้เครื่องคอมพิวเตอร์ไม่สามารถใช้งานได้ อาจพิจารณาตั้งพาสเวิร์ดเพื่อควบคุมการเข้าถึงเข้าถึงเครื่องคอมพิวเตอร์ จัดการเข้ารหัสลับฮาร์ดดิสก์ ติดตั้งซอฟต์แวร์ตรวจจับคอมพิวเตอร์ไวรัส และเปิดการใช้งานไฟร์วอลล์ส่วนบุคคล เป็นต้น โดยทั่วไปการจัดการความมั่นคงปลอดภัยของทรัพยากรสารสนเทศสามารถจำแนกตามเป้าหมายของการรักษาความมั่นคงปลอดภัยได้ ดังต่อไปนี้

ความมั่นคงปลอดภัยเชิงกายภาพ (physical security) เพื่อป้องกันอุปกรณ์ สิ่งของ หรือบริเวณให้ปราศจากการเข้าถึงโดยไม่ได้รับอนุญาต และการใช้งานที่ไม่ถูกต้อง เช่น การตั้งรหัสผ่านเพื่อเข้าใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล สร้างห้องปฏิบัติการสำหรับระบบคอมพิวเตอร์และเครือข่าย การจัดให้มีระบบไฟสำรอง การจัดให้มีระบบดับเพลิง การจัดให้มีการพิสูจน์ตัวจริงก่อนเข้าถึงฮาร์ดแวร์หรือห้องที่ใช้จัดเก็บฮาร์ดแวร์ตลอดจนทรัพยากรเครือข่ายที่เกี่ยวข้อง

ความมั่นคงปลอดภัยส่วนบุคคล (personnel security) เพื่อรักษาบุคลากรหรือกลุ่มของผู้ใช้งานที่ได้รับสิทธิ์ให้เข้าถึงและดำเนินงานได้อย่างมั่นคงปลอดภัย เช่น การกำหนดสิทธิ์ให้กับเจ้าหน้าที่ตามความรับผิดชอบ โดยกำหนดให้เจ้าหน้าที่ทั่วไปไม่สามารถอ่านข้อมูลที่ถูกสร้างขึ้นโดยหัวหน้างานของตนเอง แต่สามารถแก้ไขและตรวจสอบผู้ทำการแก้ไขทรัพยากรนั้นๆ ได้ การบังคับให้ผู้ใช้งานเปลี่ยนรหัสผ่านเมื่อเข้าสู่ระบบในครั้งแรกและทุกๆ สามเดือน

ความมั่นคงปลอดภัยของการดำเนินงาน (operation security) เพื่อปกป้องหรือป้องกันกระบวนการทำงาน ตลอดจนกิจกรรมอื่นๆ ที่เกี่ยวข้อง

ความมั่นคงปลอดภัยของการสื่อสาร (communication security) เพื่อป้องกันสื่อนำสัญญาณข้อมูลต่างๆ ที่รับส่งผ่านช่องทางการสื่อสาร โดยมุ่งเน้นการรักษาความมั่นคงปลอดภัยของอุปกรณ์ต่างๆ ที่เชื่อมต่อกันเป็นระบบสื่อสาร รวมถึงการแพร่สัญญาณให้มีความมั่นคงปลอดภัย เช่น การกำหนดมาตรการเฝ้าตรวจการดักรับข้อมูล การเข้ารหัสข้อมูลที่มีการรับส่งกันในเครือข่ายหรือระหว่างเครือข่าย การใช้บริการวีพีเอ็นในการเชื่อมต่อระบบคอมพิวเตอร์ระหว่างสาขา ซึ่งทำให้มั่นใจได้ว่าการรับส่งข้อมูลระหว่างจุดจะถูกเข้ารหัสทำให้ผู้ไม่ประสงค์ดีที่ดักรับข้อมูลได้ไม่สามารถวิเคราะห์หรือแปลความหมายข้อมูลที่ดักรับได้

ความมั่นคงปลอดภัยของเครือข่าย (network security) เพื่อป้องกันการเข้าถึงอุปกรณ์เครือข่ายต่างๆ และอุปกรณ์ที่นำมาเชื่อมต่อเข้ากับเครือข่าย เช่น การแบ่งเครือข่ายออกเป็นเครือข่ายย่อยๆ เพื่อจำแนกกลุ่มผู้ใช้งานและระบบบริการต่างๆ รวมถึงการจัดให้มีการเฝ้าตรวจความมั่นคงปลอดภัย และการจัดให้มีการพิสูจน์ตัวจริงของผู้ใช้งานก่อนจึงจะสามารถใช้งานเครือข่ายได้ จะเห็นได้ว่ามีความแตกต่างจากความมั่นคงปลอดภัยของการสื่อสาร โดยมีขอบเขตที่แคบกว่าและพิจารณาที่การเชื่อมต่อในบริเวณที่เกี่ยวข้อง เช่น ระบบเครือข่ายภายในบ้าน ระบบเครือข่ายภายในบริษัท

ความมั่นคงปลอดภัยของข้อมูลข่าวสาร (information security) เพื่อรักษาความลับ ความครบถ้วนสมบูรณ์ และความพร้อมใช้ขององค์ประกอบต่างๆ ที่ถูกผนวกรวมเข้าเป็นระบบสารสนเทศ นับตั้งแต่กระบวนการสร้าง ประมวลผล และการรับส่งสารสนเทศนั้นๆ

2.3 หลักการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์

ในการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ ประกอบด้วย 2 หลักการ ได้แก่ หลักการพื้นฐาน และหลักการอื่นๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัย

หลักการพื้นฐาน การรักษาความมั่นคงปลอดภัยจะสำเร็จได้ก็ต่อเมื่อองค์กร ได้มีการจัดการกำหนดนโยบายที่เกี่ยวข้อง การควบคุมการดำเนินการให้เป็นไปตามนโยบาย การเสริมสร้างความรู้ความเข้าใจที่เกี่ยวข้อง การฝึกอบรม การสร้างความตระหนักรู้ และการประยุกต์ใช้เทคโนโลยีที่เกี่ยวข้องอย่างเหมาะสม

1) การรักษาความลับ (confidentiality) หมายถึง กระบวนการ มาตรการ และการจัดการที่เกี่ยวข้องกับการรักษาความลับของสารสนเทศที่ถูกประมวลผล ส่งต่อ และจัดเก็บให้สามารถเข้าถึงได้เฉพาะผู้ที่มีสิทธิ์เข้าถึงทรัพยากรนั้นๆ ตัวอย่างข้อมูลที่ควรมีการจัดเก็บและมีการกำหนดมาตรการควบคุมการเข้าถึงเพื่อรักษาความลับของข้อมูลที่สำคัญ เช่น ข้อมูลผู้ป่วยในระบบสารสนเทศของโรงพยาบาล ข้อมูลส่วนบุคคลอื่นๆ

เช่น หมายเลขประจำตัวประชาชน กำหนดการของบุคคลสำคัญ รายชื่อผู้โดยสารของเที่ยวบินต่างๆ

2) การรักษาความครบถ้วนสมบูรณ์ (integrity) หมายถึง กระบวนการ มาตรการ และการจัดการที่เกี่ยวข้องกับการตรวจสอบความครบถ้วนสมบูรณ์ของสารสนเทศที่ถูกประมวลผล ส่งต่อ และจัดเก็บให้มีความถูกต้องสมบูรณ์ และสามารถตรวจสอบความครบถ้วนสมบูรณ์นั้นได้ เช่น หากมีการแก้ไขไฟล์ที่ถูกสร้างขึ้นแล้วมีการส่งผ่านไฟล์นั้นเข้าสู่เครือข่ายคอมพิวเตอร์ ผู้ที่เกี่ยวข้องจะต้องสามารถตรวจสอบได้ว่าไฟล์นั้นว่าถูกแก้ไขเปลี่ยนแปลงไประหว่างการส่งผ่านช่องทางการสื่อสารหรือไม่

3) การรักษาความพร้อมใช้ (availability) หมายถึง กระบวนการ มาตรการ และการจัดการที่เกี่ยวข้องกับการรักษาความพร้อมใช้ของสารสนเทศที่ถูกประมวลผล ส่งต่อ และจัดเก็บให้มีความพร้อมใช้อยู่เสมอ ทำให้ผู้ใช้ที่มีสิทธิ์เข้าถึงและใช้งานทรัพยากรสารสนเทศนั้นๆ สามารถเข้าใช้งานได้ เช่น เมื่อกล่าวถึงความพร้อมใช้ของระบบบริการธนาคารอิเล็กทรอนิกส์ อาจหมายถึงลูกค้าสามารถเข้าถึงและใช้งานบริการนั้นได้เสมอตลอด 24 ชั่วโมง และอาจหมายรวมถึงเจ้าหน้าที่ๆ เกี่ยวข้องสามารถเข้าถึงและบริหารจัดการซอฟต์แวร์นั้นได้

รูปที่ 2.1 องค์ประกอบสำคัญของการรักษาความมั่นคงปลอดภัยสารสนเทศ

จากรูปที่ 2.1 จะเห็นว่าทรัพยากรสารสนเทศที่ต้องการให้มีความมั่นคงปลอดภัยนั้นอาจถูกจัดเก็บอยู่ในฮาร์ดแวร์ (hardware) ซอฟต์แวร์ (software) หรือถูกส่งผ่านระบบการสื่อสาร (communication) ก็เป็นได้ และการสร้างความมั่นคงปลอดภัยให้กับทรัพยากรสารสนเทศนั้นจะมีความเกี่ยวเนื่องกับการรักษาความมั่นคงปลอดภัยทางกายภาพ (physical security) ในทุกระดับโดยการจัดให้มีเทคโนโลยีและกระบวนการที่เหมาะสมสำหรับการเข้าถึงทางกายภาพต่อฮาร์ดแวร์ ซอฟต์แวร์ และระบบการสื่อสาร นอกจากนี้ยังมีความจำเป็นต้องสร้างการรักษาความมั่นคงปลอดภัยส่วนบุคคล (personal security) เนื่องจากมนุษย์เป็นจุดอ่อนที่สุดของระบบการรักษาความมั่นคงปลอดภัย และมักละเมิดกฎเกณฑ์ที่จำเป็น ทั้งนี้อาจแก้ไขได้โดยการสร้างความตระหนักรู้ถึงเหตุผลและความสำคัญของการรักษาความมั่นคงปลอดภัย เป็นต้น มาตรการและเทคโนโลยีที่นำมาใช้จะต้องมีการกำหนดให้สอดคล้องกับการจัดการรักษาความมั่นคงปลอดภัยในระดับองค์กร โดยการกำหนดยุทธศาสตร์ นโยบายและกฎระเบียบที่เกี่ยวข้อง ตลอดจนมีการกำกับดูแลอย่างเหมาะสม

หลักการที่เกี่ยวข้องกับความมั่นคงปลอดภัย การรักษาความมั่นคงปลอดภัยทรัพยากรสารสนเทศจึงเป็นกระบวนการเชิงบริหารที่นำเอานโยบาย การดำเนินงาน และการประยุกต์ใช้เทคโนโลยีที่เกี่ยวข้องเพื่อป้องกันและจำกัดผลเสียหายต่อการรักษาความลับ ความครบถ้วนสมบูรณ์ และความพร้อมใช้ของทรัพยากรสารสนเทศนั้นๆ

1) **ช่องโหว่ (vulnerability)** คือ ความบกพร่องหรือจุดอ่อนที่มีอยู่ในทรัพยากรสารสนเทศ โดยเป็นผลมาจากการออกแบบ การพัฒนาซอฟต์แวร์ การจัดการกระบวนการทำงาน หรือการบำรุงรักษาระบบนั้นๆ เช่น ช่องโหว่ของระบบปฏิบัติการ ช่องโหว่ของซอฟต์แวร์เว็บเบราว์เซอร์ การอนุญาตให้ผู้ไม่มีบัตรเข้าถึงห้องสำคัญๆ ที่เกี่ยวข้องกับกระบวนการทำงานโดยไม่มีการตรวจสอบ หรือการไม่ควบคุมให้มีการตรวจสอบเอกสารลับก่อนการทิ้งขยะ เป็นต้น เมื่อพิจารณาตามกลุ่มของทรัพยากรจะสามารถจำแนกประเภทของช่องโหว่ได้ 3 ลักษณะ ดังต่อไปนี้
   - ช่องโหว่ที่เกี่ยวข้องกับฮาร์ดแวร์ หมายถึง ข้อบกพร่องที่เกี่ยวข้องกับความมั่นคงปลอดภัยของฮาร์ดแวร์ เช่น ช่องโหว่ของการเข้ารหัสของระบบขายปลีกครบวรจร (Point of Sale; POS) ซึ่งส่งผลให้ผู้โจมตีสามารถขโมยข้อมูลบัตรเครดิตของผู้ใช้บริการ หรือช่องโหว่ของระบบสมองกลที่ใช้ควบคุมรถยนต์ที่เมื่อถูกโจมตี

ผ่านเครือข่ายแล้วจะทำให้ผู้โจมตีสามารถควบคุมการระบบควบคุมภายในรถยนต์คันนั้นๆ ได้

- ช่องโหว่ที่เกี่ยวข้องกับซอฟต์แวร์ หมายถึง ข้อบกพร่องที่เกี่ยวข้องกับซอฟต์แวร์ต่างๆ ที่เมื่อเกิดการโจมตีต่อซอฟต์แวร์นั้นๆ แล้วจะส่งผลกระทบต่อความมั่นคงปลอดภัยของซอฟต์แวร์และซอฟต์แวร์ระบบอื่นๆ ที่เกี่ยวข้อง เช่น ช่องโหว่ของระบบปฏิบัติการที่เกี่ยวข้องกับการแชร์ไฟล์ผ่านระบบเครือข่ายคอมพิวเตอร์ ที่หากผู้ไม่ประสงค์ดีโจมตีต่อบริการแชร์ไฟล์สำเร็จอาจทำการลบโฟลเดอร์ หรือไฟล์ต่างๆ โดยไม่ได้รับอนุญาต
- ช่องโหว่ที่เกี่ยวข้องกับการบริหารจัดการข้อมูล หมายถึง ข้อบกพร่องที่เกี่ยวข้องกับการจัดการข้อมูลต่างๆ ทั้งที่เป็นข้อมูลที่ไม่ได้จัดเก็บในรูปแบบดิจิทัล และข้อมูลในรูปแบบดิจิทัล เช่น หากองค์กรหรือบุคคลจัดเก็บข้อมูลซึ่งใช้ในการพิสูจน์ตัวจริงอย่างไม่เหมาะสม เมื่อข้อมูลนั้นรั่วไหลออกไปอาจส่งผลให้เกิดการโจมตีต่อองค์กรนั้นๆ ได้ หรือเปิดโอกาสให้มีการโจมตีต่อทรัพยากรอื่นๆ

2) **ภัยคุกคาม (threat)** คือ บุคคลหรือผู้ใดก็ตามที่สามารถใช้ประโยชน์จากช่องโหว่ที่มีเข้าถึงและทำลายความมั่นคงปลอดภัยของทรัพยากรสารสนเทศได้ ภัยคุกคามต่อทรัพยากรสารสนเทศจำแนกได้ 4 ลักษณะคือ

- การดักรับ (interception) หมายถึง เหตุการณ์ที่ผู้ไม่ประสงค์ดีเข้าถึงหรือดักรับข้อมูลโดยปราศจากสิทธิ์โดยถูกต้อง เช่น การดักรับที่รับส่งกันระหว่างผู้รับและผู้ส่งในระบบเครือข่ายคอมพิวเตอร์ (sniffing) การแอบอ่านข้อมูลจากหน้าจอของผู้อื่น การแอบฟังผู้อื่นพูดคุยกันเพื่อให้ได้ข้อมูลที่ตนเองไม่มีสิทธิ์เข้าถึง
- การขัดจังหวะ (interruption) หมายถึง เหตุการณ์ที่ผู้ไม่ประสงค์ดีกระทำแล้วส่งผลให้ผู้ใช้งานที่มีสิทธิ์ไม่สามารถเข้าถึง หรือใช้งานทรัพยากรนั้นๆ ได้ เช่น การตัดสายสัญญาณเครือข่ายการลบไฟล์ข้อมูล การทำลายคอมพิวเตอร์ หรือการนำเข้าข้อความที่ระบบประมวลผลแล้วทำให้ระบบปฏิเสธการให้บริการ
- การดัดแปลงแก้ไข (modification) หมายถึง การเข้าถึงและแก้ไขทรัพยากรสารสนเทศโดยไม่มีสิทธิ์ เช่น การเปลี่ยนแปลงการปรับตั้งค่าต่างๆ ของ

ระบบปฏิบัติการ การอนุญาตให้มีการเข้าถึงจากระยะไกลโดยไม่มีการพิสูจน์ตัวจริง ซึ่งอาจส่งผลกระทบต่อความมั่นคงปลอดภัย การดักรับโดยการเปลี่ยนเส้นทางและการเปลี่ยนแปลงข้อมูลที่ถูกรับส่งผ่านเครือข่าย โดยการดัดแปลงแก้ไขดังกล่าวอาจกระทำได้ในกรณีอื่นๆ เช่น เพื่อนของนักศึกษาอาจแก้ไขไฟล์รายงานของนักศึกษาที่ถูกบันทึกไว้ในสื่อจัดเก็บข้อมูล เช่น แฟลชไดร์ฟโดยที่นักศึกษาไม่ทราบ เมื่อนักศึกษาส่งรายงานไปยังอาจารย์จึงพบว่าข้อมูลนั้นไม่ใช่ข้อมูลที่ถูกต้อง

- การปลอมแปลง (fabrication) หมายถึง การสร้างข้อมูลหรือสิ่งแปลกปลอมเข้าสู่ระบบสารสนเทศ เช่น การเพิ่มข้อมูลลงในระบบจัดการฐานข้อมูล การตั้งเครือข่ายไร้สายที่มีชื่อสถานีเหมือนกับเครือข่ายเป้าหมาย เพื่อดักรับข้อมูลต่างๆ และการปลอมแปลงหมายเลขไอพีเพื่อหลบเลี่ยงกลไกพิสูจน์ตัวจริงเพื่อเข้าใช้งานเครือข่าย การปลอมแปลงตนเองเป็นบุคคลอื่นเพื่อหลอกถามข้อมูล วัตถุประสงค์หลักของการปลอมแปลงจึงเกี่ยวข้องกับการล่อลวงให้เหยื่อเข้าใจผิดว่าข้อมูลหรือสารสนเทศนั้นเป็นข้อมูลหรือตัวตนจริงๆ ของผู้นั้น หากเหยื่อตายใจและให้ข้อมูลหรือเปิดเผยข้อมูลสำคัญจะทำให้เกิดการละเมิดความมั่นคงปลอดภัยต่อเหยื่อนั้นๆ เช่น การส่งจดหมายโดยอ้างว่าผู้ส่งเป็นหัวหน้างานและให้ส่งความลับขององค์กรไปยังอีเมล หรือให้จัดพิมพ์เอกสารแล้วส่งไปยังผู้โจมตี

3) **การโจมตี (attack)** คือ การกระทำหรือผลที่เกิดขึ้นเมื่อเกิดภัยคุกคามต่อช่องโหว่ต่างๆ ที่มีอยู่ในทรัพยากรสารสนเทศ ทั้งนี้การโจมตีอาจไม่ได้มีต้นกำเนิดจากผู้ไม่ประสงค์ดีแต่เพียงอย่างเดียวก็เป็นได้ เช่น ทรัพยากรสารสนเทศหนึ่งมีความลับไม่ควรถูกเผยแพร่ให้ผู้ไม่มีหน้าที่เกี่ยวข้องรับทราบ แต่ไม่ถูกกำหนดมาตรการควบคุมการเข้าถึงอย่างเหมาะสม อาจถูกเข้าถึงโดยผู้ใช้งานทั่วไป และนำข้อมูลนั้นไปเผยแพร่ อันเป็นการทำลายความลับของทรัพยากรนั้นๆ ทั้งนี้ การกระทำดังกล่าวอาจเกิดขึ้นโดยเจตนาหรืออาจเกิดขึ้นจากอุบัติเหตุ การโจมตีอีกลักษณะหนึ่งที่ได้รับความนิยมคือ การโจมตีต่อโครงสร้างพื้นฐานที่สำคัญของเป้าหมาย เช่น การทำให้ระบบปฏิเสธการให้บริการ และการโจมตีด้วยเทคนิคเชิงสังคมอื่นๆ เช่น การแอบอ้างเป็นพนักงานคอลเซนเตอร์

เพื่อล่อลวงเป้าหมายให้กระทำการอย่างใดอย่างหนึ่งโดยเปิดเผยข้อมูลพิสูจน์ตัวจริง หรือการหลอกลวงให้ทำรายการบัญชีผ่านเอทีเอ็ม

4) **ผู้ไม่ประสงค์ดี (attacker)** คือ บุคคลหรือกระบวนการที่เกิดขึ้นจากมนุษย์เพื่อกระทำการโจมตีต่อทรัพยากรสารสนเทศเป้าหมาย จากนิยามดังกล่าวจะเห็นได้ว่ามีความหมายใกล้เคียงกับภัยคุกคามแต่จำกัดสาเหตุไว้ที่มนุษย์เท่านั้น ซึ่งผู้ไม่ประสงค์ดีอาจมีแรงจูงใจในการโจมตีต่อระบบที่แตกต่างกันออกไป เช่น ความประมาท ค่าตอบแทน และความสะใจ เป็นต้น ในปัจจุบันนิยมใช้คำว่า แฮกเกอร์ (hacker) สามารถจำแนกประเภทจากแรงจูงใจในการโจมตีต่อระบบได้หลายลักษณะ เช่น แฮกเกอร์สมัครเล่น แฮกเกอร์หมวกขาว แฮกเกอร์หมวกดำ

5) **เอกซ์พลอยต์ (exploit)** คือ แม้ว่าเอกซ์พลอยต์จะมีความหมายตามพจนานุกรมว่า “การใช้ประโยชน์หรือการทำประโยชน์” แต่เอกซ์พลอยต์ในที่นี้จะหมายถึงการโจมตีต่อช่องโหว่ที่มีในระบบสารสนเทศ เพื่อทำลายความมั่นคงปลอดภัยหรือเข้าใช้ประโยชน์จากช่องโหว่ที่มีอยู่ เช่น ช่องโหว่ของระบบจัดการเนื้อหาผ่านเว็บที่ถูกค้นพบและรายงาน อาจมีผู้ไม่ประสงค์ดีพัฒนาโปรแกรมที่สามารถโจมตีต่อช่องโหว่ดังกล่าวสำเร็จ แล้วแจกจ่ายให้กับผู้ที่สนใจนำโปรแกรมนี้ไปโจมตีต่อช่องโหว่นั้น นอกจากนี้ยัง หมายถึงเทคนิควิธีที่ใช้ในการโจมตีด้วยเทคนิควิศวกรรมเชิงสังคม เช่น การพยายามตีสนิทกับเหยื่อ ซึ่งทำหน้าที่สำคัญในระบบสารสนเทศเพื่อให้ได้มาซึ่งข้อมูลที่เป็นประโยชน์ต่อการโจมตี หรือการล่อลวงเพื่อใช้ประโยชน์จากเหยื่อในการเข้าถึงทรัพยากรสารสนเทศ

2.4 ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ความเสี่ยงด้านเทคโนโลยีสารสนเทศขององค์กร สามารถจัดแบ่งออกเป็น 6 ประเภท ดังนี้

1) **ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม** หมายถึง ความเสี่ยงที่เกิดจากภัยคุกคามทางธรรมชาติสิ่งแวดล้อมที่มนุษย์กระทำขึ้น ลักษณะทางกายภาพและสิ่งแวดล้อมทั้งโดยเจตนาและไม่เจตนา เช่น วาตภัย อุทกภัย ฟ้าผ่า น้ำท่วม กระแสไฟฟ้าขัดข้อง เพลิงไหม้ และการไม่มีระบบควบคุมการเข้า-ออกห้องคอมพิวเตอร์แม่ข่าย

2) **ความเสี่ยงด้านบุคลากร** หมายถึง ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสานสนเทศ รวมถึงการวางแผนการตรวจสอบการทำงาน การมอบหมายหน้าที่และสิทธิ์ของบุคลากรที่มีส่วนเกี่ยวข้องกับการดำเนินการทุกฝ่าย ตลอดจนบุคลากรภายนอกที่เกี่ยวข้องทั้งทางตรงและทางอ้อมล้วนแต่เป็นความเสี่ยง

3) **ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ** หมายถึง ความเสี่ยงที่เกิดจากความผิดพลาดช่องโหว่ของภัยคุกคามที่เกิดขึ้นกับอุปกรณ์ ไม่ว่าจะเป็นความเสี่ยงที่ที่เกิดจากทำงานผิดพลาดของอุปกรณ์ ช่องโหว่ของอุปกรณ์ ตลอดจนการเคลื่อนย้ายตัวอุปกรณ์ การติดตั้งอุปกรณ์ในพื้นที่ไม่เหมาะสม การถูกภัยคุกคามจากภัยต่างๆ ไวรัสคอมพิวเตอร์

4) **ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์** หมายถึง ความเสี่ยงที่เกิดจากระบบงานโปรแกรมต่างๆ ที่ได้จัดทำและพัฒนาขึ้นสำหรับโครงการด้านเทคโนโลยีสารสนเทศ รวมถึงโปรแกรมประยุกต์อื่นๆ ประกอบการใช้โปรแกรมและระบบงาน ตัวอย่างเช่น การใช้โปรแกรมที่ไม่มีลิขสิทธิ์ ความผิดพลาดที่เกิดขึ้นจากการเขียนโปรแกรม โปรแกรมที่พัฒนาขึ้นมาแล้วมีผู้บุกรุกเข้ามาแก้ไขเปลี่ยนแปลงคำสั่ง และการถูกผู้ไม่หวังดีทำลายระบบ (Hacker)

5) **ความเสี่ยงด้านระบบเครือข่าย** หมายถึง ความเสี่ยงหรือภัยต่างๆ ที่เกิดขึ้นกับระบบเครือข่ายขององค์กรทั้งระบบอินทราเน็ต (Intranet) และอินเตอร์เน็ต (Internet) รวมถึงภัยที่มีสาเหตุมาจากปัญหาพื้นฐานของโพรโตคอล (Protocol) TCP/IP ด้วย เช่น ความเสี่ยงด้ายกายภาพ ความเสี่ยงด้านระบบปฏิบัติการ ความเสี่ยงระบบแม่ข่าย ความเสี่ยงจากการบุกรุกระบบเครือข่าย และความเสี่ยงจากภัยคุกคามต่างๆ

6) **ความเสี่ยงดด้านข้อมูล** หมายถึง ความเสี่ยงที่เกิดจากฐานข้อมูลต่างๆ ในระบบสารสนเทศอันอาจจะก่อให้เกิดความเสี่ยหาย ข้อมูลถูกทำลาย ความเสี่ยงจากผู้บุกรุก การโจรกรรมข้อมูลสำคัญ การลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูล

2.5 การจัดการความเสี่ยง

ความเสี่ยง (Risk) หมายถึง เหตุการณ์หรือการกระทำใดๆ ที่อาจจะเกิดขึ้นภายในสถานการณ์ที่ไม่แน่นอน และจะส่งผลกระทบหรือสร้างความเสียหาย (ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน) หรือก่อให้เกิดความล้มเหลวหรือลดโอกาสที่จะบรรลุวัตถุประสงค์และเป้าหมายขององค์กร

ทั้งในด้านยุทธศาสตร์การปฏิบัติงาน การเงิน และการบริการ ซึ่งอาจเป็นผลกระทบทางบวกด้วยก็ได้ โดยวัดจากผลกระทบ (Impact) ที่ได้รับ และโอกาสที่จะเกิด (Likelihood) ของเหตุการณ์

ปัจจัยเสี่ยง (Risk Factor) หมายถึง ต้นเหตุหรือสาเหตุที่มาของความเสี่ยงที่จะทำให้ไม่บรรลุวัตถุประสงค์ที่กำหนดไว้ โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นจะเกิดที่ไหน เมื่อใด และเกิดขึ้นได้อย่างไรและทำไม ทั้งนี้สาเหตุของความเสี่ยงที่ระบุควรเป็นสาเหตุที่แท้จริง เพื่อจะได้วิเคราะห์และกำหนดมาตรการลดความเสี่ยงในภายหลังได้อย่างถูกต้อง

การประเมินความเสี่ยง (Risk Assessment) หมายถึง กระบวนการระบุความเสี่ยง การวิเคราะห์ความเสี่ยง และจัดลำดับความเสี่ยง โดยการประเมินจากโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact) เมื่อทำการประเมินแล้ว ทำให้ทราบระดับของความเสี่ยง (Degree of Risk) หมายถึง สถานะของความเสี่ยงที่ได้จากการประเมินโอกาสและผลกระทบของแต่ละปัจจัยเสี่ยง แบ่งออกเป็น 4 ระดับ คือ สูงมาก สูง ปานกลาง และต่ำ

การบริหารความเสี่ยง (Risk Management) หมายถึง กระบวนการที่ใช้ในการบริหารจัดการ ให้โอกาสที่จะเกิดเหตุการณ์ความเสี่ยงลดลง หรือผลกระทบของความเสียหายจากเหตุการณ์ความเสี่ยงลดลงอยู่ในระดับที่องค์กรยอมรับได้ ซึ่งการจัดการความเสี่ยง อาจแบ่งโดยสรุปได้เป็น 4 แนวทางหลัก คือ การยอมรับ การลด/ควบคุม การยกเลิก และการโอนย้ายหรือแบ่งความเสี่ยง

การควบคุม (Control) หมายถึง นโยบาย แนวทาง หรือขั้นตอนปฏิบัติต่างๆ ซึ่งกระทำเพื่อลดความเสี่ยง และทำให้การดำเนินการบรรลุวัตถุประสงค์ แบ่งได้ 4 ประเภท คือ การควบคุมเพื่อการป้องกัน การควบคุมเพื่อให้ตรวจสอบ การควบคุมโดยการชี้แนะ และการควบคุมเพื่อการแก้ไข

2.6 แนวทางการบริหารจัดการความมั่นคงปลอดภัย

การประยุกต์ใช้งานเทคโนโลยีร่วมกับการบริหารจัดการความมั่นคงปลอดภัยอย่างเหมาะสม โดยเฉพาะอย่างยิ่งการกำหนดนโยบาย การประยุกต์ใช้งานเทคโนโลยีที่เกี่ยวข้อง และควบคุมการปฏิบัติให้เป็นไปตามที่กำหนดในนโยบายจะสร้างความมั่นใจได้ว่าการผลิต ประมวลผล จัดเก็บ และแสดงผลทรัพยากรสารสนเทศนั้นๆ มีความมั่นคงปลอดภัย

1) การควบคุมการเข้าถึงทรัพยากร

การควบคุมการเข้าถึงทรัพยากรสารสนเทศจะถูกดำเนินการโดยการกำหนดและใช้งานมาตรการควบคุม (access control) ซึ่งหมายถึง กระบวนการ วิธีการ หรือระบบซึ่งจะทำการตรวจสอบผู้ใช้งานก่อนอนุญาตให้ผู้ใช้งานที่ผ่านการตรวจสอบนั้นเข้าถึงทรัพยากรสารสนเทศใดๆ ได้ ยกตัวอย่าง มาตรการควบคุมสำหรับการเข้าใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลโดยทั่วไปที่นิยมใช้คือ การป้อนรหัสผู้ใช้งานและรหัสผ่าน มาตรการควบคุมสำหรับการผ่านเข้าออกห้องอาจมี

การติดตั้งระบบคีย์การ์ดให้เฉพาะผู้ที่มีการ์ดเท่านั้นจึงจะสามารถเข้าออกได้ หรือแม้กระทั่งการแจกจ่ายกุญแจเฉพาะเจ้าหน้าที่ผู้มีหน้าที่เกี่ยวข้องในการเข้าถึงห้องใดห้องหนึ่ง ก็จัดเป็นมาตรการการควบคุม ทั้งนี้มาตรการควบคุมสามารถจำแนกเป็น 3 ประเภท คือ

การควบคุมการเข้าถึงภาพบังคับ (mandatory access control) หมายถึง หลักการควบคุมการเข้าถึงแบบที่ผู้ใช้งานไม่สามารถเปลี่ยนแปลงสิทธิ์การเข้าถึงทรัพยากรได้ด้วยตนเอง เหมาะสำหรับการควบคุมทรัพยากรที่มีข้อมูลและสิทธิ์ของผู้ใช้งานมีความชัดเจน เนื่องจากผู้ใช้งานแต่ละคนจะถูกแบ่งมอบสิทธิ์ในการเข้าถึงทรัพยากรเป็นกลุ่มๆ (class or category) ในแต่ละกลุ่มจะมีการจัดลดับความมั่นคงปลอดภัย เช่น การแบ่งข้อมูลออกแบบลับที่สุด ลับมาก ลับ และไม่จัดลำดับชั้นความลับ เป็นต้น

การควบคุมการเข้าถึงโดยผู้ใช้ (discretionary access control) มีหลักการการควบคุมการเข้าถึงทรัพยากรในลักษณะของการให้สิทธิ์แก่เจ้าของหรือผู้ได้รับสิทธิ์นั้น เมื่อมีการร้องขอการพิสูจน์สิทธิ์จากผู้ใช้งาน กลไกการตรวจสอบสิทธิ์ที่ได้รับอนุญาตของผู้ใช้งานจะถูกตรวจสอบ และกลไกนี้จะเป็นผู้ส่งต่อสิทธิ์ที่ผู้ใช้งานได้รับให้สามารถเข้าถึงทรัพยากรได้อีกต่อหนึ่ง ซึ่งกลไกนี้เป็นกลไกมาตรฐานที่ระบบฐานข้อมูลนิยมใช้ในการควบคุมการเข้าถึง โดยทั่วไปเป็นที่เข้าใจได้ว่าผู้ใดสร้างหรือเป็นเจ้าของทรัพยากรผู้นั้นจะสามารถเข้าถึงและมอบสิทธิ์การเข้าถึงให้แก่ผู้อื่นได้

การควบคุมการเข้าถึงตามบทบาท (role-based access control) เป็นการควบคุมการเข้าถึงทรัพยากรตาม “หน้าที่” ที่ผู้ใช้งานมีต่อทรัพยากรสารสนเทศ กลไกควบคุมการเข้าถึงแบบนี้มีความเหมาะสมต่อการควบคุมการเข้าถึงทรัพยากรในระบบสารสนเทศ หรือโครงสร้างพื้นฐานระบบสารสนเทศที่มีความซับซ้อนเนื่องจากในระบบที่มีความซับซ้อนมากๆ มักมีความต้องการควบคุมทรัพยากรที่หลากหลาย หน้าที่ของผู้ใช้งานจึงถูกนำมาพิจารณาในการกำหนดสิทธิ์ ทำให้มั่นใจได้ว่าจะไม่มีผู้ใช้งานคนใดที่สามารถเข้าถึงหรือบริหารระบบได้ทั้งหมด การที่มีผู้สามารถเข้าถึงหรือบริหารระบบได้แต่เพียงผู้เดียวย่อมมีความเสี่ยในการที่ข้อมูลหรือสารสนเทศในระบบนั้นจะถูกเปลี่ยนแปลงแก้ไขอย่างไม่ถูกต้อง ตัวอย่างหนึ่งของการควบคุมการเข้าถึงตามบทบาทคือ การควบคุมการเข้าถึงซอฟต์แวร์ที่ใช้ในการปรับแต่งคุณสมบัติของระบบปฏิบัติการซึ่งกำหนดให้ผู้ใช้งานต้องได้รับสิทธิ์เป็นผู้ดูแลระบบ (administrator)

2) กลไกการควบคุมการเข้าถึงทรัพยากร

โดยปกติมาตรการการควบคุมที่ได้กล่าวมา มักถูกใช้ร่วมกับกลไกสำคัญต่อไปนี้ การแสดงตนการพิสูจน์ตัวจริง การกำหนดสิทธิ์ และการกำหนดความรับผิดชอบ ในกรณีนี้จะยกตัวอย่าง

มาตรการควบคุมการเข้าถึงและใช้บริการธุรกรรมผ่านอินเทอร์เน็ตของสถาบันการเงินแห่งหนึ่ง ซึ่งลูกค้าสามารถเข้าใช้งานได้ผ่านเว็บเบราว์เซอร์ และซอฟต์แวร์ที่ทำงานบนโทรศัพท์เคลื่อนที่

การแสดงตน (identification) เป็นกลไกที่ใช้ในการควบคุมผู้ใช้งานที่ต้องการเข้าถึงทรัพยากรตามช่องทางที่ทรัพยากรนั้นๆ กำหนดขึ้น ในกรณีนี้ผู้ใช้งานจะต้องใช้งานอาจถูกร้องขอให้ใช้งานผ่านเว็บเบราว์เซอร์ที่ได้รับความนิยมใช้งาน (เช่น ไฟร์ฟอกซ์ กูเกิ้ลโครม) และซอฟต์แวร์ที่ถูกพัฒนาขึ้นโดยสถาบันการเงินแห่งนั้นเท่านั้น หากการร้องขอใช้งานจากซอฟต์แวร์อื่นๆ เช่น เบราว์เซอร์ หรือซอฟต์แวร์ที่ไม่ได้ถูกพัฒนาขึ้นโดยสถาบันการเงินแห่งนั้นจะไม่เข้าถึงและพิสูจน์ตัวจริงได้

การพิสูจน์ตัวจริง (authentication) เป็นกลไกที่ใช้ในการตรวจสอบความถูกต้องของผู้ที่มแสดงตนขอเข้าถึงทรัพยากรสารสนเทศ การพิสูจน์ตัวจริงนิยมกระทำด้วยการตรวจสอบ “ความถูกต้อง” ของข้อมูลสำหรับการพิสูจน์ตัวจริง โดยแบ่งลักษณะของข้อมูลนั้นได้ 3 ลักษณะ คือ

1) ข้อมูลที่ผู้แสดงตนทราบ (something you know) เช่น ชื่อผู้ใช้งาน รหัสผ่าน หมายเลขพินสำหรับใช้งานเอทีเอ็ม

2) ข้อมูลที่ผู้แสดงตนมี (something you has) เช่น บัตรเอทีเอ็ม หมายเลขบัตร

3) ข้อมูลที่ผู้แสดงตนเป็น (something you are) เช่น ข้อมูลลายนิ้วมือ ข้อมูลม่านตา

สำหรับกรณีการเข้าถึงบริการธนาคารอิเล็กทรอนิกส์ในปัจจุบันนิยมใช้กลไกในการพิสูจน์ตัวจริงโดยใช้แหล่งที่มาของข้อมูลร่วมกัน เพื่อให้มั่นใจได้ว่าผู้ที่แสดงตนนั้นเป็นผู้ที่มีสิทธิ์เข้าถึงทรัพยากรนั้นจริงๆ โดยการใช้ข้อมูลชื่อผู้ใช้งาน รหัสผ่าน ร่วมรหัสผ่านแบบใช้ครั้งเดียว (One-Time Password; OTP) ที่ระบบจะเป็นผู้ส่งรายละเอียดไปยังโทรศัพท์มือถือเป็นครั้งๆ ไป

การกำหนดสิทธิ์ (authorization) คือ กลไกในการตรวจสอบและส่งมอบสิทธิ์สำหรับการเข้าถึงทรัพยากรสารสนเทศให้กับผู้ใช้งานที่ผ่านการพิสูจน์สิทธิ์ตามที่ได้กำหนดไว้ในมาตรการการควบคุมการเข้าถึงสารสนเทศสำหรับผู้ใช้งานรายนั้นๆ ซึ่งการกำหนดสิทธิ์ก็จะสอดคล้องกับประเภทของการควบคุมการเข้าถึง

การกำหนดความรับผิดชอบ (accountability) เป็นกลไกที่ทำให้มั่นใจได้ว่าผู้ใช้งานที่เข้าใช้งานตลอดจนผู้ไม่ประสงค์ดีที่พยายามเข้าใช้งานจะสามารถถูกตรวจสอบและเป็นผู้รับผิดชอบผลของการกระทำที่มีต่อทรัพยากรสารสนเทศนั้นๆ ได้ วิธีการและเทคโนโลยีสำคัญที่ใช้ในการตรวจสอบและกำหนดความรับผิดชอบคือ การจัดเก็บข้อมูลการจราจร การจะดเก็บประวัติการใช้งานหรือที่นิยมเรียกว่าล็อก (log) ของทรัพยากรต่างๆ ที่มี

2.7 มาตรฐานที่เกี่ยวข้องกับการบริหารจัดการความมั่นคงปลอดภัย

เพื่อให้การบริหารจัดการความมั่นคงปลอดภัยของทรัพยากรสารสนเทศเป็นไปอย่างสอดคล้องกันตามคุณลักษณะเฉพาะและรูปแบบการดำเนินงานขององค์กร และสอดคล้องกับกฎหมายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย องค์กรที่ทำหน้าที่คิดค้นและกำหนดมาตรฐานต่างๆ จึงกำหนดมาตรการและแนวทางที่เกี่ยวข้องเพื่อให้องค์กรต่างๆ นำไปประยุกต์ใช้สร้างความมั่นคงปลอดภัยให้กับทรัพยากรต่างๆ ขององค์กร ทั้งนี้หากองค์กรที่นำแนวทางที่กำหนดขึ้นไปใช้และผ่านการตรวจสอบมาตรฐานย่อมส่งผลดีต่อภาพลักษณ์ขององค์กรซึ่งเป็นการสร้างความน่าเชื่อถือและความมั่นใจต่อผู้มีส่วนได้เสียต่างๆ เช่น ผู้ถือหุ้น พนักงาน และตัวชี้วัดการจัดการความมั่นคงปลอดภัยของทรัพยากรสารสนเทศในองค์กรไปพร้อมๆ กัน ทั้งนี้มาตรฐานต่างๆ ที่กำหนดขึ้นเป็นมาตรฐานสากลย่อมมีความน่าเชื่อถือสูงเนื่องจากเป็นที่ยอมรับและถูกนำไปใช้อย่างแพร่หลาย มาตรฐานสำคัญๆ เช่น ชุดมาตรฐาน ISO 27000 เป็นต้น

ชุดมาตรฐาน ISO 27000 เป็นชุดมาตรฐานที่พัฒนาโดยองค์กรระหว่างประเทศว่าด้วยการมาตรฐาน (International Organization for Standardization; ISO) ต่อจากมาตรฐาน ISO 17799 โดยมีการรวบรวมมาตรการพื้นฐานหลากหลายมาตรฐาน ได้แก่ BS 7799-1, BS 7799-2, BS 7799-3 โดยมีเนื้อหาสำคัญเกี่ยวข้องกับการจัดการความเสี่ยงที่เกี่ยวข้องกับความมั่นคงปลอดภัย เช่น ความเสี่ยงเกี่ยวกับความมั่นคงปลอดภัยของข้อมูล วิธีและกระบวนการประเมินความเสี่ยง การปฏิบัติเพื่อลดความเสี่ยงและการบริหารจัดการความเสี่ยง ขั้นตอนวิธีการดำเนินการบริหารความเสี่ยง เป็นต้น ในชุดมาตรฐานนี้จะประกอบด้วยมาตรฐานที่สำคัญๆ เช่น

- ISO 27000 เป็นชุดมาตรฐานที่รวบรวมนิยามศัพท์ต่างๆ ที่เกี่ยวข้องกับการจัดการความมั่นคงปลอดภัยสารสนเทศ
- ISO 27001 เป็นมาตรฐานที่กำหนดคุณลักษณะเฉพาะที่เกี่ยวข้องกับการบริหารจัดการรักษาความมั่นคงปลอดภัยโดยวัตถุประสงค์หลักในการสร้างมาตรการควบคุมที่จำเป็นในการรักษาความมั่นคงปลอดภัยที่ถูกเรียกว่าระบบบริหารจัดการการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System; ISMS)
- ISO 27002 เป็นมาตรฐานที่กำหนดหลักปฏิบัติ แนวทางการจัดการความมั่นคงปลอดภัยที่มีการรวบรวมวัตถุประสงค์ วิธีการสร้างมาตรการควบคุม และรายละเอียดการปฏิบัติที่เกี่ยวข้องในการควบคุมความมั่นคงปลอดภัย
- ISO 27003 เป็นแนวทางการประยุกต์ใช้งานมาตรฐานในชุด ISO 27000

- ISO 27004 กำหนดแนวทางการตรวจวัดประสิทธิภาพการจัดการรักษาความมั่นคงปลอดภัย เพื่อช่วยในการประเมินผลหรือตรวจวัดประสิทธิภาพ
- ISO 27005 กำหนดแนวทางการจัดการความเสี่ยงที่เกี่ยวข้องกับทรัพยากรสารสนเทศ
- ISO 27006 กำหนดแนวทางการออกใบรับรองและการลงทะเบียนให้กับหน่วยงานต่างๆ ที่เกี่ยวข้อง

จะเห็นได้ว่าหลักสำคัญของชุดมาตรฐานนี้คือ การสร้างระบบบริหารจัดการการรักษาความมั่นคงปลอดภัยสารสนเทศ (ISMS) โดยผู้ที่จะนำมาตรฐานนี้มาประยุกต์ใช้จะต้องมีการกำหนดแผนและการปฏิบัติหลายประการในการสร้างการบริหารจัดการที่เหมาะสม โดยมีการดำเนินการเป็นวงรอบประกอบด้วยการวางแผน การปฏิบัติตามแผน การตรวจสอบ และการปรับปรุง ดังแสดงในรูปที่ 2.2

รูปที่ 2.2 วงรอบการจัดการระบบบริหารจัดการการรักษาความมั่นคงปลอดภัยสารสนเทศ ISO 27001

2.8 มาตรฐาน ISO/IEC27001

ปัจจุบันเป็นเวอร์ชั่น ISO/IEC27001:2005 หรือเรียกว่า ISMS (Information Security Management System) เป็นมาตรฐานการจัดการข้อมูลที่มีไว้เพื่อให้ธุรกิจดำเนินการต่อไปได้อย่างต่อเนื่อง ข้อกำหนดต่าง ๆถูกกำหนดขึ้นโดยองค์กรที่มีความน่าเชื่อถือว่า ISO (The International Organization for Standardization) และ IEC (The International Electro technical Commission) การนำ ISMS มาใช้สามารถช่วยให้กิจกรรมทางธุรกิจดำเนินไปอย่างต่อเนื่องไม่สะดุด ช่วยป้องกันกระบวนการทางธุรกิจจากภัยร้ายแรง เช่น ภัยธรรมชาติ และป้องกันความเสียหายของระบบข้อมูล

ได้ ISMS สามารถนำมาใช้งานได้ครอบคลุมทุกกลุ่มอุตสาหกรรมและทุกกลุ่มธุรกิจ ห้อข้อสำคัญในมาตรฐาน ISO/IEC27001 : 2005 ประกอบด้วย 11 โดเมนหลักได้แก่

1. นโยบายความมั่นคงขององค์กร (Security Policy)
2. โครงสร้างความมั่นคงปลอดภัยในองค์กร (Organization of information security)
3. การจัดหมวดหมู่และการควบคุมทรัพย์สินขององค์กร (Asset Management)
4. มาตรฐานของบุคคลเพื่อสร้างความมั่นคงปลอดภัยให้กับองค์กร (Human Resources Security)
5. ความมั่นทางด้านกายภาพสื่อการและการดำเนินงานของระบบสารสนเทศขององค์กร (Communications and Operations Management)
6. การบริหารจัดการด้านการสื่อการและการดำเนินงานของระบบสารสนเทศขององค์กร (Communications and Operations Management)
7. การควบคุมการเข้าถึงระบบสารสนเทศขององค์กร (Access Control)
8. การพัฒนาและดูแลระบบสารสนเทศ (Information Systems Acquisition, Development and Maintenance)
9. การบริหารจัดการเหตุการณ์ละเมิดความมั่นคงปลอดภัย (Information Security Incident Management)
10. การบริหารความต่อเนื่องในการดำเนินงานขององค์กร (Business Continuity Management)
11. การปฏิบัติตามข้อกำหนดทางด้านกฎหมายและบทลงโทษของการละเมิดนโยบาย (Compliance)

2.9 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

หมวด 1 ความผิดเกี่ยวกับคอมพิวเตอร์

กระทำต่อคอมพิวเตอร์

มาตรา 5 การเข้าถึงระบบคอมพิวเตอร์ฯ

มาตรา 6 การล่วงรู้และเปิดเผยมาตรการการป้องกันการเข้าถึง

มาตรา 7 การเข้าถึงข้อมูลคอมพิวเตอร์ฯ

มาตรา 8 การดักรับข้อมูลคอมพิวเตอร์ฯ

มาตรา 9 การรบกวนข้อมูลคอมพิวเตอร์ฯ

มาตรา 10 การรบกวนระบบคอมพิวเตอร์ฯ ใช้คอมพิวเตอร์กระทำความผิด

มาตรา 11 Spam mail

มาตรา 14 การปลอมแปลงข้อมูลคอมพิวเตอวเตอร์ เผยแพร่เนื้อหาอันไม่เหมาะสม

มาตรา 15 ความรับผิดชอบของผู้ให้บริการ

มาตรา 16 การเผยแพร่ภาพจากการตัดต่อ/ดัดแปลง

ตารางที่ 2.1 ฐานความผิดและบทกำหนดโทษ

ฐานความผิด	โทษจำคุก	โทษปรับ
มาตรา 5 เข้าถึงคอมพิวเตอร์โดยมิชอบ	ไม่เกิน 6 เดือน	ไม่เกิน 10,000 บาท
มาตรา 6 ล่วงรู้มาตรการป้องกัน	ไม่เกิน 1 ปี	ไม่เกิน 20,000 บาท
มาตรา 7 เข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ	ไม่เกิน 2 ปี	ไม่เกิน 40,000 บาท
มาตรา 8 การดักข้อมูลคอมพิวเตอร์	ไม่เกิน 3 ปี	ไม่เกิน 60,000 บาท
มาตรา 9 ทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง	ไม่เกิน 5 ปี	ไม่เกิน 100,000 บาท
มาตรา 10 ทำให้ระบบไม่สามารถทำงานได้ตามปกติ	ไม่เกิน 5 ปี	ไม่เกิน 100,000 บาท
มาตรา 11 สแปมเมล์	ไม่มี	ไม่เกิน 100,000 บาท
มาตรา 12 กระทำผิดมาตรา 9 หรือมาตรา 10	ไม่เกิน 10 ปี	ไม่เกิน 200,000 บาท
ก่อให้เกิดความเสียการแก่ประชาชน	3 ปี ถึง 15 ปี	60,000–300,000 บาท
กระทบต่อความมั่นคงปลอดภัยของประเทศ/เศรษฐกิจ วรรคท้าย เป็นเหตุให้ผู้อื่นถึงแก่ชีวิต	10 ปี ถึง 20 ปี	ไม่มี
มาตรา 13 การจำหน่าย/เผยแพร่ชุดคำสั่ง	ไม่เกิน 1 ปี	ไม่เกิน 20,000 บาท
มาตรา 14 การเผยแพร่เนื้อหาอันไม่เหมาะสม	ไม่เกิน 5 ปี	ไม่เกิน 100,000 บาท
มาตรา 15 และ มาตรา 26 ความรับผิดชอบของผู้ให้บริการ	ไม่เกิน 5 ปี	ไม่เกิน 100,000 บาท
มาตรา 16 การตัดต่อภายผู้อื่น	ไม่เกิน 3 ปี	ไม่เกิน 60,000 บาท
มาตรา 17 การกระทำความผิดนอกราชอาณาจักรต้องรับโทษในราชอาณาจักร		

หมวด 2 พนักงานเจ้าหน้าที่

อำนาจหน้าที่ (มาตรา 18)

1) มีหนังสือ/เรียกเพื่อให้ถ้อยคำ/เอกสาร
2) เรียกข้อมูลจราจร
3) สั่งให้ส่งมอบข้อมูลที่อยู่ในครอบครอง

4) ทำสำเนาข้อมูล

5) สั่งให้ส่งมอบข้อมูล/อุปกรณ์

6) ตรวจสอบ/เข้าถึง

7) ถอดรหัสลับ

8) ยึด/อายัดระบบ

หน้าที่ของผู้ให้บริการ

มาตรา 26 เก็บข้อมูลจราจรไม่น้อยกว่า 90 วัน แต่ไม่เกิน 1 ปี

มาตรา 26

ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่า 90 วัน นับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็นพนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกิน 90 วัน แต่ไม่เกินหนึ่งปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้

ผู้ให้บริการจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการ นับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การใช้บริการสิ้นสุดลง

ความในวรรคหนึ่งจะใช้กับผู้ให้บริการประเภทใด อย่างไร และเมื่อใด ให้เป็นไปตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา

บทกำหนดโทษ ผู้ให้บริการผู้ใดไม่ปฏิบัติตามมาตรานี้ ต้องระวางโทษปรับไม่เกินห้าแสนบาท

หน้าที่ของผู้ให้บริการ

ดังนั้นทางโรงแรมเดอะเบอร์เคลี่ย์เปิดให้ลูกค้าใช้บริการอินเตอร์เน็ตฟรี กฎหมายถือว่าเป็น “ผู้ให้บริการ” จะต้องเก็บข้อมูลการใช้งานคอมพิวเตอร์และอินเตอร์เน็ต เรียกว่า ข้อมูลการจราจรคอมพิวเตอร์ (Log file) ไว้เป็นเวลาขั้นต่ำ 90 วัน และสูงสุด 1 ปี นับตั้งแต่มีการใช้งานระบบ และจะต้องส่งข้อมูลให้เจ้าหน้าที่ ภายใน 7-15 วัน หากเจ้าหน้าที่ร้องขอ

ข้อมูลการจราจรคอมพิวเตอร์

ข้อมูลการจราจรคอมพิวเตอร์ คือ ข้อมูลเส้นทางการใช้งานอินเตอร์เน็ตหรือการเชื่อมต่อสื่อสารกันระหว่างเครื่องคอมพิวเตอร์ รวมถึงมือถือและแท็บเล็ต ประกอบด้วยข้อมูลดังต่อไปนี้

- ระบุว่าใครเป็นผู้ใช้งาน

- ระบุว่าใช้งานจากเครื่องไหน
- ระบุว่าใช้งานวันที่เท่าไหร่ และช่วงเวลาใด
- ระบุว่าใช้งานจากที่ใด (IP Address)
- ระบุว่าเข้าใช้งานที่เว็บไซต์ไหน
- ระบุเส้นทาง

ผู้ให้บริการต้องปรับโทษ

หากไม่เก็บข้อมูบการจราจรคอมพิวเตอร์หรือไม่สามารถระบุตัวตนผู้ใช้งานได้จะต้องระวางโทษ ปรับสูงสุด 500,000 บาท

หากไม่ส่งข้อมูลการจราจรคอมพิวเตอร์ตามคำสั่งของเจ้าหน้าที่ จะต้องระวางโทษปรับสูงสุด 200,000 บาท และปรับเป็นรายวัน วันละ 5,000 บาท จนกว่าจะทำให้ถูกต้อง

2.10 การวิเคราะห์ช่องว่าง (Gap Analysis) ด้านการบริหารเทคโนโลยีสารสนเทศ

การทำ GAP Analysis เพื่อรายงานสรุปสถานะขององค์กรที่เกี่ยวข้องกับกิจรรมและการให้บริการในปัจจุบันว่าในทางปฏิบัติที่เป็นอยู่จริง ยังมีกิจกรรมหรืองานใดที่อาจเป็นช่องว่างหรือเป็นส่วนที่ยังไม่มี เมื่อเทียบกับมาตรฐานที่พึงปฏิบัติที่ดี ซึ่งอาจจะเรียกเป็น Best Practice โดยหน่วยงานกำกับหรือมาตรฐานสากลที่กำหนด โดยองค์กรและหน่วยงานอาจคาดหวังผลเพื่อบรรลุเป้าหมายที่กำหนด เป็นการประเมินอย่างเป็นอิสระโดยบุคคลภายนอกหรือสายงานอื่นที่ไม่ใช่เป็นผู้ปฏิบัติงาน หรืออาจใช้วิธีการที่เรียกว่า CSA (Control Self-Assessment) ที่ปฏิบัติโดยหน่วยงานภายในองค์กรนั้นๆ เอง ทั้งนี้ผลการวิเคราะห์ช่องว่าง (Gap Analysis) จะนำมาเพื่อทำแผนดำเนินการ (Action Plan) เพื่อลดช่องว่างที่มีอยู่เพื่อก้าวสู่ระดับการบริหารที่ดีขึ้น

ความหมายของสัญลักษณ์ที่ใช้วิเคราะห์ช่องว่าง

ในการสรุปผลการวิเคราะห์รายงานช่องว่างตามเกณฑ์ของหน่วยงาน ซึ่งอาจจะมีแนวทางในการกำกับแตกต่างกันไปนั้น ในการทำ Gap Analysis ให้ยึดหลักหรือเกณฑ์ปฏิบัติในการกำกับหน่วยงานนั้นๆ เป็นเกณฑ์ และในกรณีที่ใช้มาตรฐานสากลเป็นหลักในเรื่องที่เกี่ยวข้อง ก็ต้องยึดแนวทางในการเปรียบเทียบการปฏิบัติจริงขององค์กรนั้นๆ กับเกณฑ์มาตรฐานสากล ซึ่งอาจจะจัดทำโดยทีมงานที่เกี่ยวข้องหรือร่วมประชุมกันในกลุ่มงานที่เกี่ยวข้องหลังจากที่ได้ประชุมกลุ่มฯ เพื่อให้การสื่อสารกันได้อย่างชัดเจน ก็จะนำช่องว่างดังกล่าวมาจัดทำ Action Plan เพื่อลดช่องว่างในการก้าวไปสู่ Best Practice หรือมาตรฐานในการกำกับที่เกี่ยวข้อง ซึ่งอาจจะใช้วิธีการได้หลากหลาย

การนำเสนอในที่นี้จึงเป็นการนำเสนอในรูปแบบเพื่อให้เข้าใจโดยง่าย การทำ Gap Analysis จะใช้แนวทางตามเกณฑ์การประเมินเป็นบรรทัดฐาน เพื่อการเปรียบเทียบกับการปฏิบัติจริง โดยมีคำอธิบายดังนี้

1. “เกณฑ์การประเมิน” คือรายการ หรือ หัวข้องานที่ทางหน่วยงานจะใช้ในการประเมิน ซึ่งจะเปลี่ยนแปลงทุกปีตามความคาดหวังของหน่วยงาน

2. “การปฏิบัติ” หมายถึง ในเกณฑ์การประเมินหรือเปรียบเทียบกับมาตรฐาน หรือ Best Practice หัวข้อนั้น ทางองค์กรได้ปฏิบัติหรือไม่ และมีความพึงพอใจหรือไม่ หรือมีข้อที่ควรอาจปรับปรุงแก้ไขอื่นใดได้อีก เป็นต้น

ก. สัญลักษณ์ ● เป็นการปฏิบัติอย่างสมบูรณ์ หมายถึง คำชี้แจงของคณะทำงานขององค์กร ว่าได้ดำเนินการโครงการตามเกณฑ์อย่างครบถ้วน และองค์กรมีเอกสารพร้อมที่จะยืนยันและชี้แจงเมื่อต้องการ อย่างไรก็ดี คุณภาพและการปฏิบัติจริง รวมทั้งผลงานที่ได้รับขึ้นกับความถูกต้อง ความครบถ้วน ความสมบูรณ์ ความสามารถในการใช้งานได้ในเวลาตามที่ต้องการของผู้ที่เกี่ยวข้อง

ข. สัญลักษณ์ ◖ เป็นการปฏิบัติบางส่วน หมายถึง คำชี้แจงของคณะทำงานขององค์กร ว่าได้ดำเนินการตามเกณฑ์ได้เพียงบางส่วน และมีเอกสารแสดงสถานะของโครงการ อย่างไรก็ดี คุณภาพและการปฏิบัติจริง รวมทั้งผลงานที่ได้รับขึ้นกับความถูกต้อง ความครบถ้วน ความสมบูรณ์ ความสามารถในการใช้งานได้ในเวลาตามที่ต้องการของผู้ที่เกี่ยวข้อง

3. “ความคิดเห็นที่ประชุม” หมายถึง ข้อสรุปในเบื้องต้นที่ได้หารือกันภายในการประชุมระหว่างคณะทำงานขององค์กรและผู้ที่เกี่ยวข้องกับโครงการหรือแผนงานเพื่อที่จะลดช่องว่าง (Gap) ต่อไป

4. “ข้อสังเกตและข้อเสนอแนะเบื้องต้นจากหน่วยงานประเมิน” หมายถึง ข้อสังเกต และคำแนะนำจากหน่วยงานประเมินในเบื้องต้น

5. “Action Plan” หมายถึง แผนการดำเนินงานที่จำเป็นต้องปฏิบัติ เพื่อให้เป็นไปตามการประเมินตามเกณฑ์ เพื่อยกระดับกระบวนการจัดการที่ดี

ก. ✓ หมายถึง ต้องการทำแผนการดำเนินงานเพื่อให้สามารถกำหนดผู้รับผิดชอบได้ และระยะเวลาในการปฏิบัติได้อย่างสมเหตุสมผล

ข. ✕ ไม่ต้องการทำแผนการดำเนินงานเพราะที่ประชุมมีข้อสรุปว่าได้ดำเนินการแล้ว หรือเป็นแผนที่ดำเนินงานต่อเนื่องจากปีก่อนหน้านี้

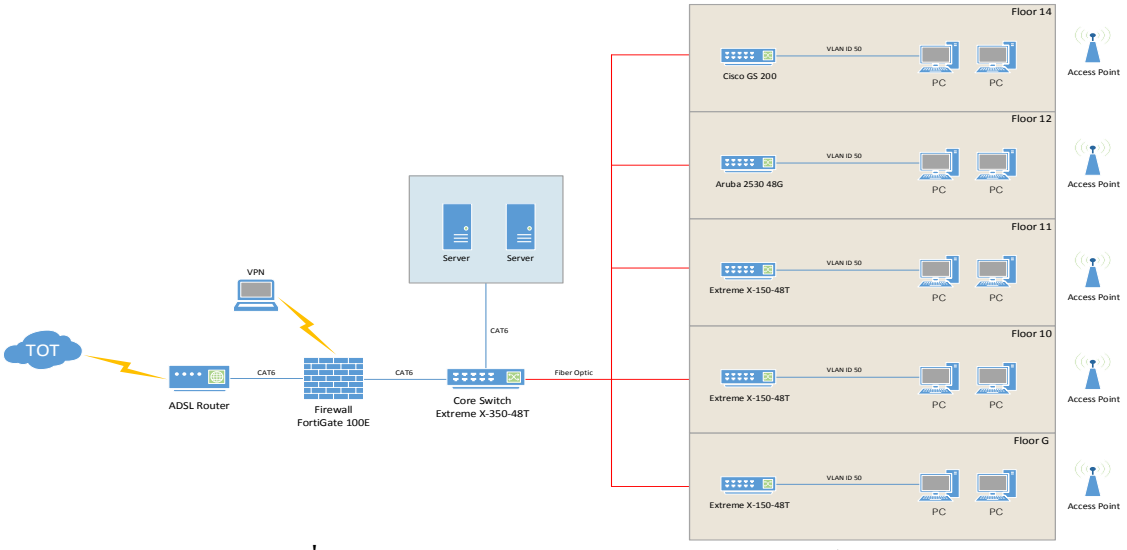
บทที่ 3
การดำเนินงาน

หลังจากได้จัดเตรียมคู่มือการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์และเครือข่าย มาตรฐานการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ ISO/IEC 27001 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 เพื่อเสนอการออกแบบแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์และเครือข่าย ให้ทางผู้จัดการฝ่ายเทคโนโลยีสารสนเทศรับทราบและอนุญาตให้สามารถจัดทำได้ ซึ่งมีขั้นตอนดำเนินงาน ดังนี้

3.1 วิเคราะห์โครงสร้างระบบคอมพิวเตอร์และเครือข่ายปัจจุบัน

โครงสร้างระบบเครือข่ายปัจจุบันขององค์กร เป็นลักษณะเครือข่ายโทโปโลยีแบบสตาร์ โดยใช้อุปกรณ์สวิตซ์ทำการกระจายสัญญาณไปยังสวิตซ์ตัวอื่นๆ ที่อยู่ตามชั้นต่างๆ แล้วกระจายไปยังเครื่องคอมพิวเตอร์ของพนักงาน โดยเป็นสวิตซ์ Layer 2 แบบ Managed และ Unmanaged แต่ไม่ได้มีการทำ VLAN เอาไว้ ซึ่งการเชื่อมต่อของสวิตซ์ เป็นลักษณะเชื่อมต่อจากศูนย์กลางที่ตั้งอยู่ในห้องเซิร์ฟเวอร์ที่ชั้น 10 ทำหน้าที่รับการเชื่อมต่อจากสวิตซ์ตัวอื่นๆ ที่อยู่ตามแต่ละชั้น สวิตซ์ทุกตัวทำการเชื่อมต่อผ่านกันไประหว่างสวิตซ์ โดยไม่ได้ตั้งค่าคอนฟิกใดๆ ปลายทางเชื่อมต่อไปยังเครื่องเซิร์ฟเวอร์และอุปกรณ์ไฟร์วอลล์ในการเชื่อมต่ออินเตอร์เน็ต การกำหนดไอพีแอดเดรส (IP Address) อยู่ภายใต้ซับเนต (Subnet) เดียวกันทั้งหมด ทุกเครื่องสามารถเชื่อมต่อถึงกันได้

ซึ่งแผนผังโครงสร้างระบบเครือข่ายปัจจุบันขององค์กร มีรายละเอียดดังต่อไปนี้



รูปที่ 3.1 โครงสร้างระบบเครือข่ายปัจจุบันขององค์กร

3.1.1 โครงสร้างของระบบเครือข่าย

โครงสร้างระบบเครือข่ายประกอบด้วยอุปกรณ์เครือข่ายต่างๆ ดังต่อไปนี้ ตารางที่ 3.1 แสดงอุปกรณ์เครือข่าย

Description	Quantity
ADSL Router (TOT)	3
Firewall FortiGate 80E	1
Extreme X-350-48T (Core Switch)	1
Extreme X-350-48T (Access Switch)	2
Aruba 2530 48G (Access Switch)	1
Extreme X-350-24T (Access Switch)	1
Cisco GS 200 (Access Switch)	3
Linksys LGS326P (Access Switch)	1
HP V1910-24G (Access Switch)	1
Extreme X-150-48T (Access Switch)	1
Eugenius EWS330AP (Access Point)	15

3.1.2 รายละเอียดอุปกรณ์ในระบบเครือข่าย

องค์กรมีจำนวนโหนดที่เชื่อมต่อจำนวนไม่มาก โดยแบ่งเป็นอุปกรณ์ข่ายที่เป็นสวิตช์สำหรับใช้งานได้ 2 ประเภท คือ Core Switch และ Access Switch และอุปกรณ์เชื่อมต่อต่างๆ

อุปกรณ์สวิตซ์ (Switch) ยี่ห้อ Extreme X-350-48T (Layer 2) เป็นอุปกรณ์สวิตซ์ตัวหลัก (Core Switch) ใช้สำหรับกระจายสัญญาณไปยังสวิตซ์ทุกจุดภายในองค์กร

รูปที่ 3.2 ตัวอย่างอุปกรณ์ Core Switch

อุปกรณ์สวิตซ์ (Switch) ยี่ห้อ Cisco GS 200 และ Extreme X-150-48T ทำหน้าที่เป็น Access Switch คืออุปกรณ์สวิตซ์ที่เชื่อมต่อไปยังเครื่องคอมพิวเตอร์ของผู้ใช้งาน (ซึ่งมีหลายรุ่นหลายยี่ห้อ) และอุปกรณ์ที่สามารถเชื่อมต่อเข้ากับระบบเครือข่ายภายในองค์กรของแต่ละแผนก

รูปที่ 3.3 ตัวอย่างอุปกรณ์ Access Switch

อุปกรณ์ ADSL Modem ของ TOT ใช้สำหรับเชื่อมต่อสัญญาณอินเตอร์เน็ตจากผู้ให้บริการ ISP

รูปที่ 3.4 ตัวอย่างอุปกรณ์ Firewall

อุปกรณ์ไฟร์วอลล์ (Firewall) ยี่ห้อ FortiGate 80e ใช้สำหรับตรวจสอบข้อมูลที่มาจากอินเตอร์เน็ตหรือเครือข่ายภายในองค์กร

รูปที่ 3.5 ตัวอย่างอุปกรณ์ Firewall

อุปกรณ์ (Nas Storage) QNAP TS-453 Pro 4-Bay ใช้สำหรับ Backup ข้อมูลจาก File server

รูปที่ 3.6 ตัวอย่างอุปกรณ์ Nas Storage

อุปกรณ์แอสเซสพอยท์ (Access Point) ยี่ห้อ Eugenius EWS330AP ใช้สำหรับแพร่กระจายสัญญาณของเครือข่ายชนิดไร้สาย (Wireless) ภายในอาคาร

รูปที่ 3.7 ตัวอย่างอุปกรณ์ Access Point

3.1.3 ข้อมูลกำหนดให้ใช้เครือข่ายภายในองค์กร

ภายในองค์กรมีจำนวนเครื่องคอมพิวเตอร์ และ Notebook รวมกันประมาณ 180 เครื่อง ซึ่งทางฝ่ายเทคโนโลยีสารสนเทศได้กำหนดการใช้งานเครือข่าย ดังนี้

- กำหนดให้ใช้ไอพีแบบสแตติก (Static) โดยใช้ไอพีภายใน คือ 192.168.54.0/23
- ไอพีเซิฟเวอร์ = 192.168.54.1 - 192.168.54.50

- ไอพีไคลเอ็นต์ (Client) = 192.168.55.1 - 192.168.55.254
- ซับเน็ตมาสค์ (Subnet Mask) = 255.255.254.0
- เกทเว (Gateway) = 192.168.54.1
- ดีเอ็นเอส (DNS) = 192.168.54.20
- ลิงค์ผู้ใช้บริการเครือข่าย 1 (Link ISP 1) = 300 Mbps

ส่วนรายละเอียดอื่นๆ ขององค์กร แสดงอยู่ในตารางที่ 3.2

ตารางที่ 3.2 แสดงภาพรวมเครือข่ายขององค์กร

โครงสร้างเครือข่าย (Topology)	เลเยอร์ 2 สวิตซ์ (Switch) เชื่อมต่อแบบสตาร์ (Star)
การเชื่อมต่อ (Connectivity)	แบบยูทีพี (UTP) และไฟเบอร์ออฟติก (Fiber Optic)
การใช้งานเครื่องเซิร์ฟเวอร์	แอพพลิเคชั่นเซิร์ฟเวอร์ (Application Server), ไฟล์เซิฟเวอร์ (File Server)
การเชื่อมต่ออินเตอร์เน็ต	ลีดไลน์ (Lead line)
การใช้งานอินเตอร์เน็ต (Internet)	เปิดให้ใช้สำหรับทุกเครื่องในองค์กร โดยสามารถใช้งานได้อย่างอิสระไม่มีการจำกัดสิทธิ์
ลิงค์สำรองการเชื่อมต่ออินเตอร์เน็ต	ไม่มี
ระบบความปลอดภัย (Security)	ใช้ฟอติเกตไฟร์วอล์ (FortiGate Firewall) ในการกำหนดค่าการใช้งานอินเตอร์เน็ต เป็นไฟร์วอล์ ชนิดยูทีเอ็ม(UTM) สามารถตั้งค่าได้ทั้งผ่านหน้าเว็บและคอมมานไลน์ (Command Line)
การจัดการเครือข่าย (Network Management)	ใช้การเทลเน็ต (Telnet) ไปบริหารจัดการตัวอุปกรณ์เครือข่าย

3.1.4 อุปกรณ์เครื่องเซิร์ฟเวอร์ที่ใช้งาน

จากการสำรวจเครื่องเซิร์ฟเวอร์ที่ใช้งาน ทำให้ทราบจำนวนเครื่องเซิร์ฟเวอร์และเซอร์วิสที่ใช้งานในแต่ละเครื่อง ดังต่อไปนี้

ตารางที่ 3.3 แสดงรายละเอียดอุปกรณ์เซิร์ฟเวอร์และเซอร์วิสที่ใช้งาน

Server Name	Service
Epitome	PMS, POS
METRO BRITA	Brita, Web base
Touchpoint	PMS, POS
Eagle	Eagle
Opera	Oracle, Web base
File Share	File Share
Winpac	Winpac, Liaison, IPU, Magnegate, PMS
Engineer Job	Web base
IT Job	Web base
ESET Endpoint	ESET Endpoint Antivirus (NOD32)
Active Directory	DNS, Active Directory

3.1.5 แอพพลิเคชั่นที่ใช้งาน

แอพพลิเคชั่นที่ใช้งานโปรแกรมในปัจจุบัน มีดังต่อไปนี้

ตารางที่ 3.4 แสดงแอพพลิเคชั่นและระดับความสำคัญ

Server Name	Description	Priority
Epitome	โปรแกรมระบบจองห้องพัก	Critical
Touchpoint	โปรแกรมระบบขายอาหารและเครื่องดื่ม	Critical
Opera	โปรแกรมระบบจัดการห้องสัมมนา	Critical
Metro Brita	โปรแกรมระบบสั่งซื้อสินค้า	High
Eagle	โปรแกรมระบบงานบุคคล	High
Engineer Job	โปรแกรมแจ้งงานช่าง	Important
IT Job	โปรแกรมแจ้งงาน IT	Important

3.1.6 ปริมาณผู้ใช้งานเครื่องคอมพิวเตอร์

จากการสำรวจแต่ละแผนกทำให้ทราบถึงจำนวนเครื่องคอมพิวเตอร์ในการทำงานของพนักงานที่ใช้งาน มีดังต่อไปนี้

ตารางที่ 3.5 แสดงจำนวนเครื่องคอมพิวเตอร์

Department	Amount	Application
Information Technology	6	Internet, EPITOME, TOUCHPOINT, Metro Brita
Executive	5	Internet, EPITOME
Finance & Accounting	13	Internet, TOUCHPOINT, Metro Brita, Eagle
Account Receivable	5	Internet, EPITOME, Metro Brita
Cost	4	Internet, TOUCHPOINT, Metro Brita
Receiving	4	Internet, Metro Brita
Purchasing	7	Internet, Metro Brita
Reservation	6	Internet, EPITOME, Metro Brita
Human Resource	6	Internet, Metro Brita, Eagle
Food & Beverage	7	Internet, TOUCHPOINT, Metro Brita
Housekeeping	8	Internet, EPITOME, Metro Brita
Catering	8	Internet, EPITOME, Metro Brita
Sales	11	Internet, EPITOME, Metro Brita
Business Development	4	Internet, EPITOME, Metro Brita
Engineer	5	Internet, Metro Brita
Security	3	Internet, Metro Brita
Front Office	23	Internet, EPITOME, Metro Brita
Kitchen	11	Internet, Metro Brita
Graphic	3	Internet, Metro Brita
Notebook/Laptop	18	Internet, EPITOME, Metro Brita
POS	10	TOUCHPOINT

3.1.7 การกำหนดหมายเลข VLAN (Virtual LAN)

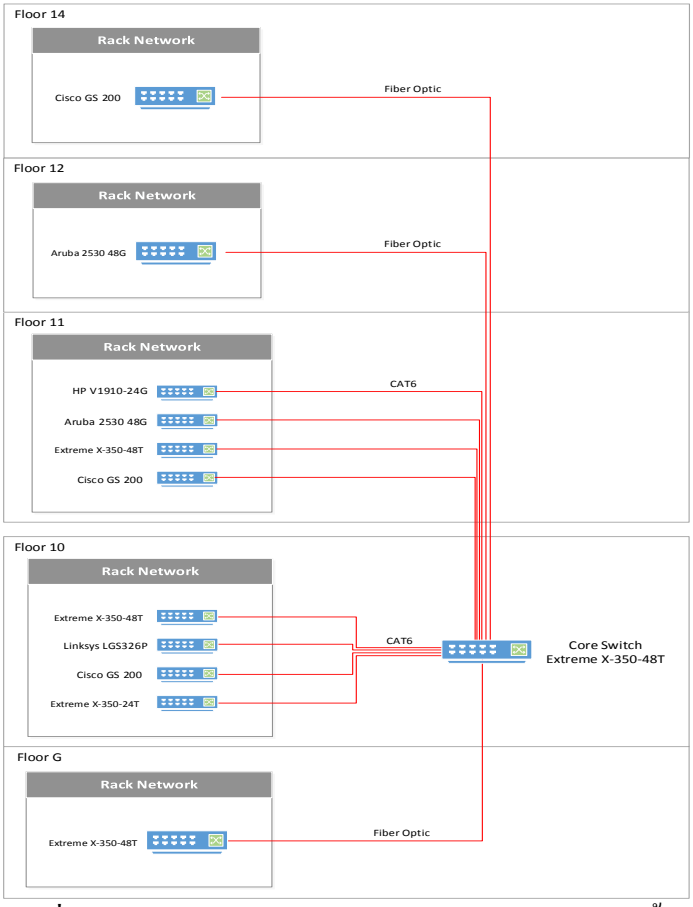
หมายเลข VLAN จะแบ่งออกเป็น 3 วง อาทิ Internal Network, Wireless Office และ Wi-Fi Hotspot รายละเอียดดังตารางที่ 3.6

ตารางที่ 3.6 แสดงหมายเลย IP Address และหมายเลข VLAN

Network Name	IP Address	Subnet Mark	VLAN
Internal Network	192.168.54.1	255.255.254.0	50
Wireless Office	192.168.60.1	255.255.255.0	60
Wi-FI Hotspot	10.10.0.1	255.255.252.0	100

3.1.8 โครงสร้างการเดินสายสัญญาณระหว่างชั้น

การเดินสายสัญญาณระหว่างห้องเซิร์ฟเวอร์ชั้น 10 ขึ้นไปตู้แร็คชั้น 11, 12, 14 และลงไปตู้แร็คชั้น G ของอาคาร จะเชื่อมต่อโดยการใช้สาย Fiber Optic และสาย UTP เชื่อมต่อเข้ากับอุปกรณ์สวิตช์แต่ละตัว โดยเชื่อมจาก Core Switch ไปยัง Access Switch แต่ละตัว

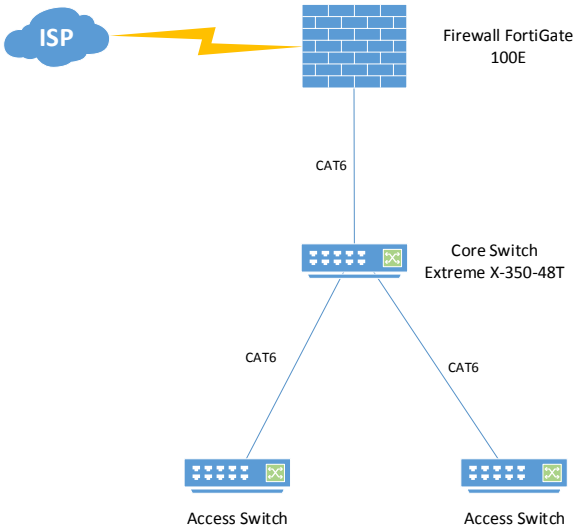


รูปที่ 3.8 ตัวอย่างโครงสร้างการเดินสายสัญญาณระหว่างชั้น

3.1.9 รายละเอียดการติดตั้งและการเชื่อมต่อระบบเครือข่าย

การติดตั้งอุปกรณ์เครือข่าย Core Switch

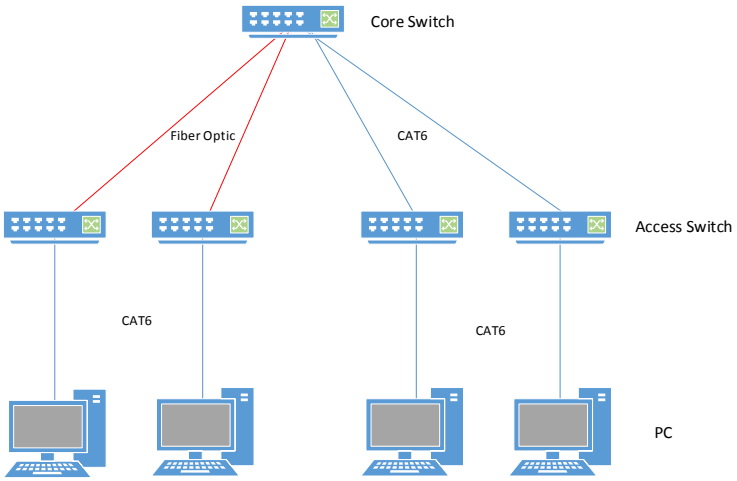
จากรูปที่ 3.9 จะเห็นได้ว่า Core Switch Extreme X-350-48T เป็นอุปกรณ์หลักทำหน้าที่เป็นศูนย์กลางของระบบเครือข่าย ซึ่งมีการเชื่อมต่อไปยังสวิตช์และไฟร์วอลล์ เพื่อเชื่อมโยงระบบเครือข่ายทั้งหมดเข้าไว้ด้วยกัน



รูปที่ 3.9 ตัวอย่างการติดตั้งอุปกรณ์เครือข่าย Core Switch

การติดตั้ง Access Switch

ในการติดตั้งอุปกรณ์ Access Switch มีจำนวน 10 เครื่องที่ห้องชั้น 10, 11, 12, 14 และชั้น G เพื่อใช้สำหรับเชื่อมต่อกับเครื่องคอมพิวเตอร์ของพนักงาน และเชื่อมต่อกับ Core Switch



รูปที่ 3.10 ตัวอย่างการติดตั้ง Access Switch

การติดตั้ง Access point

ในการติดตั้งอุปกรณ์ Access Point เพื่อใช้สำหรับเชื่อมต่อกับโน้ตบุ๊กหรือโทรศัพท์มือถือของพนักงาน ซึ่ง Access Point แต่ละตัวจะใช้สาย UTP ในการเชื่อมต่อกับอุปกรณ์ Access Switch ประจำชั้นหรือตามแผนกต่างๆ

รูปที่ 3.11 ตัวอย่างการติดตั้ง Access Point

3.2 วิเคราะห์ระบบสนับสนุนความปลอดภัยระบบคอมพิวเตอร์และเครือข่ายปัจจุบัน

จากผังของระบบคอมพิวเตอร์และเครือข่ายปัจจุบัน จะแสดงรายละเอียดของระบบที่คาดว่าสนับสนุนการดำเนินงานด้านความปลอดภัย ดังนี้

ระบบ: Firewall

ระบบกรองข้อมูลการสื่อสาร ควบคุมการเข้าถึงระหว่างเน็ตเวิร์กภายนอกที่ไม่ปลอดภัย บังคับใช้นโยบายด้านความปลอดภัย โดยการกำหนดกฎให้กับไฟร์วอลล์ว่าจะอนุญาตหรือไม่ให้ใช้เซอร์วิสชนิดใดผ่าน บันทึกกิจกรรมต่างๆ ที่ผ่านเข้าออกเน็ตเวิร์ก

ฟังก์ชันระบบงานหลัก คือ

- Security Profiles
- VPN
- Policy-based routing
- Port forwarding
- VLAN
- DHCP Server

ระบบ: Active Directory (AD)

ระบบศูนย์กลางที่เก็บรวบรวมทรัพยากรที่ใช้งานบนเครือข่ายภายในองค์กร เพื่อให้ง่ายต่อการค้นหาและบริหารจัดการ เช่น บัญชีรายชื่อผู้ใช้งาน, บัญชีเครื่องคอมพิวเตอร์หรือเครื่อง server, Share Folder รวมไปถึงสามารถกำหนดสิทธิ์ในการใช้ทรัพยากรและคุณสมบัติของผู้ใช้งาน ทั้งแบบเป็นกลุ่มและรายทรัพยากรได้

ฟังก์ชั่นการทำงานของระบบ

- Management Profile
- File Share
- Policy

ระบบ: File Share

ใช้ในการแชร์ Folder สำหรับแต่ละแผนก โดยทำงานอยู่บนเครื่อง Server ให้บุคคลกรในองค์กร Access เข้าไปถึงทรัพยากรที่อยู่ในภายใน Folder เหล่านั้น และมีการกำหนด Permissions ในการถึง File Share ที่แตกต่างกันตามแต่ละแผนก

ฟังก์ชั่นการทำงานของระบบ

- Sharing
- Permissions
- Network path

ระบบ: System Log

เพื่อนำมาใช้เก็บข้อมูลการใช้งานและเข้าถึงอินเตอร์เน็ตด้วยคอมพิวเตอร์ รวมถึงการระบุตัวตนของผู้ใช้งานและเก็บข้อมูลจราจรบนเครือข่ายคอมพิวเตอร์ เพื่อป้องกันการใช้งานระบบเครือข่ายคอมพิวเตอร์ในทางที่ผิด และตรวจสอบสถานะของผู้ใช้งานอินเตอร์เน็ต เพื่อลดความเสี่ยงในการให้บริการอินเตอร์เน็ต

ฟังก์ชั่นการทำงานของระบบ

- Syslog
- Local Traffic
- Wireless Traffic
- VPN Traffic

ระบบ: ESET Endpoint antivirus

โปรแกรมรักษาความปลอดภัยที่ใช้ทรัพยากรของระบบน้อยที่สุด เพื่อป้องกันการแฝงตัวจากไวรัส สปายแวร์ ม้าโทรจัน เวิร์ม แอดแวร์ รูทคิท และการโจมตีอื่นๆ โดยไม่ขัดขวางประสิทธิภาพการทำงานของระบบหรือรบกวนคอมพิวเตอร์

ฟังก์ชั่นการทำงานของระบบ

- Computer Protection
- Network Protection
- Web and Email Protection

ระบบ: Nas Storage

ใช้สำหรับ Backup ข้อมูลของแต่ละแผนกผ่านเครือข่าย โดยการสร้าง bat file เพื่อกำหนดค่าในการ Backup ในแต่ละวัน โดยมีข้อมูลล่าสุดอย่างน้อย 3 วัน

ฟังก์ชั่นการทำงานของระบบ

- Schedule Automatic Backup
- Backup File Share
- File Storage

3.3 วิเคราะห์ปัญหาในระบบคอมพิวเตอร์และเครือข่ายปัจจุบัน

จากการสำรวจถึงปัญหาในระบบคอมพิวเตอร์และเครือข่าย ก่อนทำการออกแบบและพัฒนาระบบใหม่ สามารถจัดแบ่งปัญหาได้เป็น 3 ส่วน ดังนี้

- ☐ ช่องโหว่หรือข้อบกพร่องของระบบคอมพิวเตอร์และเครือข่ายปัจจุบัน
- ☐ ความเสี่ยงในการเข้าถึงระบบเทคโนโลยีสารสนเทศ
- ☐ การกระทำความผิดในแง่ของโอกาสที่จะเกิดขึ้นกับการให้บริการอินเตอร์เน็ต

3.3.1 ช่องโหว่หรือข้อบกพร่องของระบบคอมพิวเตอร์และเครือข่ายปัจจุบัน

โครงสร้างระบบคอมพิวเตอร์และเครือข่ายปัจจุบัน มีช่องโหว่หรือข้อบกพร่องหลายประการ ที่อาจส่งผลทำให้องค์กรขาดประสิทธิภาพในการดำเนินงาน ระบบหยุดชะงักไม่สามารถดำเนินงานได้อย่างต่อเนื่อง และเกิดความเสี่ยงต่อการบุกรุกจากผู้ไม่ประสงค์ดี ซึ่งทางผู้จัดทำได้สรุปเป็นประเด็นต่างๆ ในตารางที่ 3.7

ตารางที่ 3.7 ช่องโหว่หรือข้อบกพร่องของระบบคอมพิวเตอร์และเครือข่ายปัจจุบัน

NO.	ช่องโหว่หรือข้อบกพร่อง	รายละเอียด
1	อุปกรณ์เครือข่าย	ปัญหาทางด้านการใช้งานอุปกรณ์เครือข่าย ซึ่ง Access Switch ที่ใช้งานเชื่อมต่อกับผู้ใช้งาน เกิดปัญหาค้างหรือแฮงค์บ่อย เพราะมีอายุการใช้งานที่นานแล้ว ทำให้พนักงานใน

		โซนที่อุปกรณ์ค้างที่มีปัญหา ไม่สามารถใช้งานระบบเครือข่ายได้ ต้องทำการปิดและเปิดอุปกรณ์ใหม่ จึงจะสามารถใช้งานได้
2	ผู้ให้บริการอินเตอร์เน็ต ISP	การใช้บริการอินเตอร์เน็ตทั้ง 3 สัญญาณ จากผู้ให้บริการอินเตอร์เน็ต ISP มีเพียงรายเดียวเท่านั้น คือ TOT ไม่มีการสำรองจากผู้ให้บริการอินเตอร์เน็ต ISP รายอื่นๆ หากเกิดกรณีที่อุปกรณ์มีปัญหาหรือสัญญาณอินเตอร์เน็ตหลักขัดข้อง จะส่งผลทำให้องค์กรไม่สามารถใช้งานอินเตอร์เน็ตได้
3	การติดไวรัส	ปัญหาการติดไวรัสภายในเครือข่าย เนื่องจากองค์กรมีการใช้ Antivirus แบบ Freeware ทำให้ลำบากในการ Update และติดตั้ง Antivirus เพราะไม่สามารถจัดการจากส่วนกลาง (Centralize) ได้ ทำให้มีไวรัสแพร่กระจายในระบบเครือข่ายและเครื่องคอมพิวเตอร์ติดไวรัส ทำให้ทำงานช้าหรือข้อมูลสำคัญสูญหาย
4	Backup & Restore VMware	ไม่มีซอร์ฟแวร์ที่ใช้ในการ Backup สำหรับเครื่องเซิร์ฟเวอร์และเครื่อง VMware ในกรณีที่เครื่องเหล่านี้ใช้งานไม่ได้หรือระบบล้ม จึงทำให้ไม่สามารถ Restore ข้อมูลให้กลับมาใช้งานได้
5	จัดแบ่ง VLAN	เนื่องจากเครือข่ายปัจจุบันยังไม่มีการจัดแบ่ง VLAN สำหรับแต่ละแผนก ทำให้เครื่องคอมพิวเตอร์สามารถเชื่อมต่อถึงกันได้หมด อาจทำให้เกิดความเสี่ยงในการบุกรุกจากผู้ไม่ประสงค์ดี หรืออาจเกิดการแพร่กระจายของไวรัสไปยังทุกเครื่องในองค์กรได้
6	Network Monitoring	ปัญหาการขาดซอฟต์แวร์ในการมอนิเตอร์ตรวจสอบดูการทำงานของระบบเครือข่ายและอุปกรณ์เครือข่าย ซึ่งหากเกิดกรณีที่อุปกรณ์มีปัญหาหรือหยุดทำงาน ทำให้ต้องใช้เวลานานในการหาสาเหตุและอุปกรณ์ที่ชำรุด
7	ไอพีชนกัน	เนื่องจากระบบเครือข่ายขององค์กร มีการกำหนดหมายเลขไอพีแบบสแตติก (Static) สำหรับเครื่องคอมพิวเตอร์โดยแบ่งแยกตามแต่ละแผนก ซึ่งเกิดปัญหาเกี่ยวกับการกำหนด

		ไอพีชนกัน ส่งผลทำให้เครื่องที่ไอพีชนกัน ไม่สามารถใช้งานระบบสารสนเทศและอินเตอร์เน็ตได้ และเป็นการยากหากมีเครื่องคอมพิวเตอร์เพิ่มขึ้นจำนวนมาก
8	การจัดสาย UTP	ปัญหาด้านการจัดสาย UTP ที่เชื่อมต่อไปยัง Outlet LAN ตามห้องประชุมหรือห้องสัมมนาภายในอาคาร ไม่มีการทำเครื่องหมายหรือติดหมายเลขกำกับไว้ ว่าสายเส้นไหนเชื่อมต่อไปที่ใด ทำให้ไม่ทราบว่าสายสัญญาณเส้นดังกล่าวนั้นมาจากไหน เมื่อเกิดปัญหาทางสายสัญญาณขึ้นจะไม่สามารถแก้ไขปัญหาได้อย่างทันท่วงที
9	การเข้าใช้งานเครือข่าย	ขาดการป้องกันทางด้านการเข้าใช้งานเครือข่าย เพราะคอมพิวเตอร์หลายเครื่องเป็นระบบ Work Group ไม่สามารถยืนยันตัวผู้ใช้งานและบริหารจัดการผู้ใช้งานจากส่วนกลาง (Centralize Management) ได้ และอีกทั้งยังสามารถเชื่อมต่อกับเข้าระบบและกำหนด IP Address และสามารถใช้งานอินเตอร์เน็ตได้ทันที โดยไม่ต้องทำการยืนยันตัวตน
10	การลักลอบใช้งานระบบเครือข่าย	การนำคอมพิวเตอร์ส่วนตัวมาใช้งานโดยไม่ได้รับอนุญาติ โดยการเชื่อมต่อเข้าระบบกับเครือข่าย โดยใช้สายแลนที่ว่างหรือนำสายสัญญาณมาเสียบเข้ากับสวิตซ์ หรือ Outlet LAN ซึ่งอาจจะทำให้เกิดความเสี่ยงในกรณีที่ผู้ใช้งาน นำไปใช้ในทางที่ผิดกฎหมายและผิดพรบ.ว่าด้วยการกระทำผิดทางคอมพิวเตอร์ และอาจทำให้เกิดความเสี่ยงต่อระบบเครือข่าย
11	การกำหนดรหัสผ่านอุปกรณ์เครือข่าย	เนื่องจากอุปกรณ์ Access Switch และ Access Point ทุกตัวไม่มีการตั้งค่าความปลอดภัยไว้ โดยไม่มีการกำหนดรหัสผ่านหรือใช้ Username และ Password ที่เป็น Default อาจเกิดความเสี่ยงจากผู้ไม่หวังดี สามารถเข้ามาแก้ไขการตั้งค่าต่างๆ หรือกลั่นแกล้งในระบบเครือข่ายได้
12	Unmanaged Access Switch	ปัญหาจากการอุปกรณ์แอสเซสสวิตซ์ (Access Switch) หลายจุดเชื่อมต่อ ไม่ใช่แบบ Managed ทำให้ไม่สามารถเข้าไปตั้งค่าการใช้งานในส่วนต่างๆ ได้ เช่น การจัดแบ่ง VLAN, หรือการบล๊อกพอร์ตเชื่อมต่อไปยังอุปกรณปลายทาง

13	Backup & Restore Configuration	อุปกรณ์เครือข่าย อาทิ Firewall, Access Switch, Router, Access Point หรืออุปกรณ์อื่นๆ ไม่มีการ Backup Configuration สำหรับการ Restore Configuration ในกรณีที่เกิดความผิดพลาดจากการทำงานของอุปกรณ์ หรือมีการเปลี่ยนแปลงค่า Configuration โดยไม่ได้ตั้งใจหรือจากการโจมตีระบบเครือข่ายจากผู้ไม่หวังดี
14	เครื่องสำรองไฟ UPS	ปัญหาอุปกรณ์แอสเซสสวิตซ์ (Access Switch) แต่ละจุดเชื่อมต่อ ยังไม่มีเครื่องสำรองไฟ UPS ในกรณีที่ไฟฟ้าของอาคารดับหรือตกบ่อย อาจทำอุปกรณ์แอสเซสสวิตซ์หยุดทำงาน และส่งผลทำให้เครือข่ายคอมพิวเตอร์ใช้งานไม่ได้
15	Port Security	Outlet LAN ตามห้องประชุมหรือห้องสัมมนาต่างๆ ในอาคาร ไม่มีการ Disable Port การใช้งานที่อุปกรณ์แอสเซสวิตซ์ ส่งผลส่งผลทำให้บุคคลที่ไม่หวังดีสามารถนำอุปกรณ์เข้ามาเชื่อมต่อกับระบบเครือข่ายภายในได้ เพื่อหาช่องโหว่ในการโจมตี
16	การควบคุมการเข้าออกห้อง Server	ห้อง Server ของระบบคอมพิวเตอร์และเครือข่าย เป็นห้องเดียวกันกับห้องระบบโทรศัพท์ บุคคลที่ไม่มีความเกี่ยวข้องในการปฏิบัติงานสามารถเข้าถึงได้ ซึ่งไม่มีการบันทึกข้อมูลการเข้าออกห้อง Server และไม่มีขั้นตอนการขอเข้าใช้งาน

3.3.2 ความเสี่ยงในการเข้าถึงระบบเทคโนโลยีสารสนเทศ

จากการสำรวจความเสี่ยงในการเข้าถึงระบบสารสนเทศของพนักงาน ที่อาจส่งผลกระทบต่อความไม่ความปลอดภัยต่อผู้ใช้งานและระบบเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่าย ซึ่งทางผู้จัดทำได้สรุปเป็นประเด็นความเสี่ยงต่างๆ ในตารางที่ 3.8

ตารางที่ 3.8 ความเสี่ยงในการเข้าถึงระบบเทคโนโลยีสารสนเทศ

NO.	ความเสี่ยงในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศ	มาตรฐาน ISO/IEC 27001
1	พนักงานเข้าถึงระบบงานของเครือข่ายภายในจากระยะไกลได้โดยไม่มีสิทธิ์เข้าถึง	A.6.2.2 การปฏิบัติงานจากระยะไกล
2	พนักงานไม่มีการลงทะเบียนผู้ใช้งานระบบสารสนเทศ	A9.1.1 นโยบายควบคุมการเข้าถึง
3	ไม่มีการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ	A9.1.1 นโยบายควบคุมการเข้าถึง
4	เครื่องจากภายนอกสามารถเข้าถึงเครือข่ายได้ด้วยระบบ Wi-Fi เมื่อเข้ามาแล้วสามารถใช้เครือข่ายเดียวกัน	A9.1.2 การเข้าถึงเครือข่ายและการบริการเครือข่าย
5	พนักงานใหม่ ใช้ Username และ Password ของพนักงานเก่าในการเข้าใช้งานระบบสารสนเทศ	A9.2.1 การลงทะเบียนและถอดถอนสิทธิ์ผู้ใช้งาน
6	เมื่อมีพนักงานออกแล้ว ไม่ถอดถอนสิทธิ์ในการเข้าถึงระบบทันที แต่ยังสามารถเข้าระบบได้อยู่	A9.2.1 การลงทะเบียนและถอดถอนสิทธิ์ผู้ใช้งาน
7	พนักงานขอเข้าใช้งานสิทธิ์ที่ไม่มีสิทธิ์ โดยที่ไม่มีการอนุมัติจากหัวหน้างาน	A9.2.2 การจัดการสิทธิ์การเข้าถึงของผู้ใช้งาน
8	อุปกรณ์ถูกเข้าถึงโดยผู้ไม่มีสิทธิ์ หรือผู้ไม่หวังดี เพราะอุปกรณ์ถูกติดตั้งไว้ด้านนอก	A9.2.2 การจัดการสิทธิ์การเข้าถึงของผู้ใช้งาน
9	ผู้ดูแลระบบมีการใช้งาน Account ที่ใช้เป็น Admin ร่วมกัน	A9.2.3 การบริหารจัดการสิทธิ์การเข้าถึงตามระดับสิทธิ์
10	ระบบสารสนเทศถูกเข้าถึงโดยมีสิทธิ์การใช้งานเกินความจำเป็น	A9.2.3 การบริหารจัดการสิทธิ์การเข้าถึงตามระดับสิทธิ์
11	พนักงานที่ออกไปแล้วยังมีสิทธิ์ค้างอยู่ในระบบสารสนเทศ	A9.2.5 การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน

12	มีบางโฟลเดอร์ในดาต้าเซ็นเตอร์ สามารถเข้าถึงได้ Everyone โดยไม่ป้องกันการเข้าถึงสำหรับแต่ละแผนก	9.4.1 การจำกัดการเข้าถึงสารสนเทศ
13	ไม่มีการป้องกันการ Login ผิดบ่อยๆ โดยการล็อก User ใช้งาน	A9.4.2 ขั้นตอนปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย
14	คอมพิวเตอร์สามารถเข้าถึงได้ง่าย โดยไม่มีการ Login เข้าใช้งาน	A9.4.2 ขั้นตอนปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย
15	ผู้ใช้งานไม่ได้ Log out ออกจาก windows หลังจากใช้งานเสร็จแล้ว	A9.4.2 ขั้นตอนปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย
16	รหัสผ่านเข้าสู่ระบบคอมพิวเตอร์ง่ายเกินไปหรือไม่เป็นความลับ	A9.4.3 ระบบบริหารจัดการรหัสผ่าน
17	โปรแกรมไม่มีลิขสิทธิ์ ทำให้มีช่องโหว่	A9.4.4 การใช้โปรแกรมอรรถประโยชน์
18	ห้องเซิร์ฟเวอร์ไม่มีการบันทึกการเข้าออกของผู้ใช้งาน	A11.1.2 การควบคุมการเข้าออกทางกายภาพ
19	ตู้แร็ค Switch ตามแต่ละชั้นไม่มีการล็อคหรือมีกุญแจคาไว้	A11.2.1 การจัดตั้งและป้องกันอุปกรณ์
20	อุปกรณ์หยุดหรือไม่สามารถทำงานได้เต็มประสิทธิภาพ เนื่องจากถูกเข้าถึงและเปลี่ยนแปลงการตั้งค่าจากผู้ไม่มีสิทธิ์	A11.2.1 การจัดตั้งและป้องกันอุปกรณ์
21	พนักงานติดรหัสผ่านของระบบสารสนเทศไว้ที่หน้าจอคอมพิวเตอร์หรือติดไว้บนโต๊ะทำงาน	A11.2.9 นโยบายโต๊ะทำงานปลอดเอกสารสำคัญ และนโยบายการป้องกันหน้าจอคอมพิวเตอร์
22	ความผิดพลาดของการ Config อุปกรณ์เครือข่าย ทำให้ระบบทำงานผิดพลาดหรือหยุดให้บริการ	A.12.1.2 การบริหารจัดการการเปลี่ยนแปลง
23	การติดไวรัสและสแปมที่เครื่องเซิร์ฟเวอร์และเครื่องพนักงาน	A12.2.1 มาตรการป้องกันโปรแกรมไม่ประสงค์ดี
24	ไม่สามารถตรวจสอบได้ว่าผู้ดูแลระบบมีกิจกรรมอะไรบ้าง	A12.4.3 ข้อมูลล็อกกิจกรรมของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการระบบ

25	ไม่มีการอัพ Patch Windows ของเครื่องพนักงาน	A12.6.1 การบริหารจัดการช่องโหว่ทางเทคนิค
26	การเข้าถึงและโดนโจมตีจากเครือข่ายภายนอก	A13.1.2 ความมั่นคงปลอดภัยสำหรับบริการเครือข่าย
27	พนักงานสามารถเข้าใช้ระบบงานหรือข้อมูลของคนอื่นได้	A18.1.4 ความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคล

3.3.3 การกระทำความผิดในแง่ของโอกาสที่จะเกิดขึ้นกับการให้บริการอินเตอร์เน็ต

การให้บริการอินเตอร์เน็ตของโรงแรม ปัจจุบันมีขั้นตอนการให้บริการที่อาจสุ่มเสี่ยงต่อการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ที่ไม่สามารถติดตามหรือระบุตัวตนผู้ใช้งานได้ เพราะหน้าที่ของผู้ให้บริการจะต้องเก็บข้อมูลการใช้งานคอมพิวเตอร์และอินเตอร์เน็ต ซึ่งทางผู้จัดทำได้สรุปเป็นประเด็นความผิดต่างๆ ในตารางที่ 3.9

ตารางที่ 3.9 การกระทำความผิดในแง่ของโอกาสที่จะเกิดขึ้นกับการให้บริการอินเตอร์เน็ต

ความผิด	รายละเอียดการกระทำความผิด
1	การ Login เข้าใช้บริการอินเตอร์เน็ตสำหรับลูกค้าของโรงแรม จะใช้งานโดยการระบุ Email Address เพื่อรับ Username และ Password ทำให้ไม่สามารถติดตามหรือระบุตัวตนผู้ใช้งานได้
2	การใช้บริการอินเตอร์เน็ตสำหรับลูกค้าแบบ Group Tour ของโรงแรม จะให้ Username และ Password เดียว ตามจำนวนของผู้ใช้งาน ทำให้ไม่สามารถติดตามหรือระบุตัวตนผู้ใช้งานได้
3	การให้บริการอินเตอร์เน็ตสำหรับห้องประชุมห้องสัมมนา จะใช้วิธีการแจก 1 คูปองเดียว ให้ใช้งานได้หลายๆ คน ทำให้ไม่สามารถติดตามหรือระบุตัวตนผู้ใช้งานได้
4	ในกรณีที่ลูกค้าไม่มี Email Address ทางโรงแรมจะให้ Username และ Password ที่จัดเตรียมไว้ให้กับลูกค้า โดยไม่มีการลงชื่อรับ สำหรับ Login เข้าใช้บริการอินเตอร์เน็ต ทำให้ไม่สามารถติดตามหรือระบุตัวตนผู้ใช้งานได้
5	ลูกค้าห้องอาหารหรือห้องจัดเลี้ยง Login เข้าใช้บริการอินเตอร์เน็ต โดยการระบุ Email Address เพื่อรับ Username และ Password ซึ่งทางโรงแรมไม่ทราบว่าเป็นลูกค้าท่านใด ทำให้ไม่สามารถติดตามหรือระบุตัวตนผู้ใช้งานได้

6	การ Login เข้าใช้บริการอินเตอร์เน็ต ระบุ Email Address ผิดหรือระบุอะไรก็ได้ ก็สามารถรับ Username และ Password ได้เช่นกัน ทำให้ไม่สามารถติดตามหรือระบุตัวตนผู้ใช้งานได้
7	พนักงานในบริษัทสามารถ Login เข้าใช้บริการอินเตอร์เน็ตได้ โดยการใช้ Username และ Password แบบ Share Key เดียวกัน ทำให้ไม่สามารถติดตามหรือระบุตัวตนผู้ใช้งานได้

3.4 การวิเคราะห์ช่องว่าง (Gap Analysis)

การวิเคราะห์ช่องว่าง (Gap Analysis) เพื่อระบุถึงความแตกต่างระหว่างระบบคอมพิวเตอร์และเครือข่าย ปัจจุบันและระบบใหม่ที่ออกแบบไว้ โดยช่องว่างนี้จะถูกนำมาปรับใช้กับการออกแบบแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์และเครือข่าย ซึ่งวิธีการนี้ช่วยให้สามารถปรับปรุงประสิทธิภาพของระบบเครือข่ายโดยรวมให้ดีขึ้นและมีความมั่นคงปลอดภัยมากขึ้น โดยจะแบ่งการวิเคราะห์ช่องว่าง (Gap Analysis) ออกเป็น 3 ส่วน ดังนี้

- การวิเคราะห์ช่องว่างโครงสร้างระบบคอมพิวเตอร์และเครือข่าย
- การวิเคราะห์ช่องว่างการเข้าถึงระบบเทคโนโลยีสารสนเทศ
- การวิเคราะห์ช่องว่างการให้บริการอินเตอร์เน็ตของโรงแรม

3.4.1 การวิเคราะห์ช่องว่างโครงสร้างระบบคอมพิวเตอร์และเครือข่าย

ตารางที่ 3.10 การวิเคราะห์ช่องว่างโครงสร้างระบบคอมพิวเตอร์และเครือข่าย

Network System	Function	มี/ไม่มี	Acting	Action Plan
Network Structure	Core Switch	มี	Use	- เปลี่ยน Access Switch เนื่องจากสวิตซ์มีกันหลายรุ่นหลายยี่ห้อและหลายจุดเชื่อมต่อไม่ใช่แบบ Managed - นำเครื่องเซิฟเวอร์ของแต่ละแผนกมาจัดวางใหม่ที่ DMZ Zone
	Access Switch	มี	Modify	
	สาย UTP	มี	Modify	
	DMZ Zone	ไม่มี	New	
	Switch Server	ไม่มี	New	
	Strong password	ไม่มี	Modify	
	Port Security	ไม่มี	New	
	Disabling ports	ไม่มี	New	

	VLAN	มี	Modify	- ติดตั้งสัญญาณอินเตอร์เน็ต (Internet ADSL) จากผู้ให้บริการ ISP 2 ราย - นำระบบ VLAN เข้ามาใช้งาน โดยจัดแบ่ง VLAN ตามแต่ละฝ่าย
	Inter VLAN Routing	ไม่มี	New	
	Internet ADSL	มี	Modify	
Wi-Fi Hotspot	Wi-Fi Hotspot	มี	Use	- จัดทำระบบ Authentication สำหรับ Wireless Office โดยเชื่อมกับระบบ Radius - จัดทำระบบ Access Point Controller เพื่อควบคุมและตรวจสอบการทำงานของอุปกรณ์ Access Point
	Wireless Office	มี	Modify	
	Access Point Controller	ไม่มี	New	
Firewall	Security Profiles	ไม่มี	New	- กรองข้อมูลการใช้งานอินเตอร์ โดยการเปิดใช้งานฟังก์ชั่น Security Profiles อาทิ Web Filter, Application Control, Intrusion Protection (IPS) - จัดทำ Load balance เป็นแบบ SD WAN - จัดทำ VLAN สำหรับแต่ละแผนก
	VPN	มี	Modify	
	Policy-based routing	ไม่มี	New	
	Port forwarding	มี	Use	
	VLAN	ไม่มี	New	
	Inter VLAN Routing	ไม่มี	New	
	Limiting bandwidth	ไม่มี	Use	
	DHCP Server	มี	Modify	
	Load balance	ไม่มี	New	
Active Directory (AD)	Management Application	มี	Modify	- จัดการการเข้าถึง Application และทรัพยากรตามสิทธิ์ที่ควรจะได้หรือตามแต่ละแผนก - การเข้าใช้งานอินเตอร์เน็ต โดยเชื่อมกับระบบ Radius
	Driver Maps	มี	Modify	
	Policy	มี	Modify	
	Radius	ไม่มี	New	

	Additional Domain Controller	ไม่มี	New	
DHCP Server	DHCP Server	ไม่มี	New	จัดทำระบบ DHCP Server สำหรับกำหนดหมายเลขไอพีตามแต่ละแผนก เพื่อให้มีหมายเลขไม่ซ้ำกัน
File Share	File Share	มี	Modify	จัดการการเข้าถึง File Share ตามสิทธิ์ของแต่ละแผนก โดยเชื่อมกับระบบ Map Network Drive เพื่ออ่านข้อมูลผู้ใช้งานในระบบ Active Directory
	Permissions	มี	Modify	
	Map Network Drive	ไม่มี	New	
Nas Storage	Schedule Automatic Backup	มี	Use	ใช้ระบบปัจจุบันที่มีอยู่
	Backup File Share	มี	Use	
	File Storage	มี	Use	
Antivirus	Computer Protection	มี	Modify	ติดตั้งระบบ ESET Security Management Center เพื่อช่วยจัดการ ESET บนเวิร์กสเตชัน เซิร์ฟเวอร์ ในสภาพแวดล้อมการทำงานของเครือข่ายจากจุดศูนย์กลางจุดเดียว
	Network Protection	มี	Modify	
	Web and Email	มี	Modify	
	Protection	มี	Modify	
	Policy	ไม่มี	New	
Antimalware	Scanner	ไม่มี	New	ติดตั้งโปรแกรม MalwareBytes ป้องกันไวรัส ประเภท Spyware (สปายแวร์) และ Malware (มัลแวร์)
	Detection History	ไม่มี	New	
	Web Protection	ไม่มี	New	
	Malware Protection	ไม่มี	New	
	Exploit Protection	ไม่มี	New	
System Log	Local Traffic	มี	Modify	ติดตั้งโปรแกรม Softnix Logger เป็นระบบจัดการ LOGS ในระบบคอมพิวเตอร์แบบรวมศูนย์ โดยรองรับระบบคอมพิวเตอร์,
	VPN Traffic	มี	Modify	
	Wi-Fi Log	มี	Modify	

				SERVER หรืออุปกรณ์เครือข่าย เช่น FIREWALL, ROUTER, SWITCH และอื่นๆ โดยจัดเก็บ LOGS เริ่มต้นที่ 90 วันและเก็บได้นานสุดถึง 2 ปี ตามพรบ. คอมพิวเตอร์
Network Monitoring	Network Engineer	ไม่มี	New	ติดตั้งซอฟต์แวร์ประเภท NMS (Network Management System) เพื่อตรวจสอบการทำงานของอุปกรณ์ที่ใช้งานในระบบเครือข่าย และมีฟังก์ชั่นการทำงานที่สามารถแจ้งเตือนเมื่ออุปกรณ์หยุดทำงาน
	Security	ไม่มี	New	
	Network Diagram	ไม่มี	New	
	Event Log	ไม่มี	New	
Backup and Recovery	Backup	ไม่มี	New	ติดตั้งโปรแกรม Veeam Backup & Replication เพื่อสำรองและกู้คืนข้อมูลในระบบเสมือน (Virtualization) เช่น VMware หรือ Microsoft Hyper-V และสามารถทำ Replication ไปยัง Site สำรอง
	Replication	ไม่มี	New	
	Restore	ไม่มี	New	
Intrusion Detection System (IDS)	Packet Decoder	ไม่มี	New	ติดตั้งโปรแกรม Snort เป็นระบบตรวจจับการบุกรุกบนเครือข่ายที่สามารถตรวจจับได้อย่างรวดเร็ว มีการทำงานเป็นแบบ Real Time ตรวจจับการบุกรุกด้วยวิธี Misuse Detection
	Detection Engine	ไม่มี	New	
	Logging/ Alerting Subsystem	ไม่มี	New	

3.4.2 การวิเคราะห์ช่องว่างการเข้าถึงระบบเทคโนโลยีสารสนเทศ

ตารางที่ 3.11 การวิเคราะห์ช่องว่างการเข้าถึงระบบเทคโนโลยีสารสนเทศ

ความเสี่ยง	มาตรฐาน ISO 27001	Current Controls	Acting	Action Plan
พนักงานเข้าถึงระบบงานของเครือข่ายภายในจากระยะไกลได้โดยไม่มีสิทธิ์เข้าถึง	A.6.2.2 การปฏิบัติงานจากระยะไกล	ไม่มี	New	ลบโปรแกรม Remote จากระยะไกลทุกชนิดออกจากเครื่องคอมพิวเตอร์ของพนักงาน หากต้องการใช้งานต้องกรอกแบบฟอร์มขอใช้งานโปรแกรม Remote
พนักงานไม่มีการลงทะเบียนผู้ใช้งานระบบสารสนเทศ	A9.1.1 นโยบายควบคุมการเข้าถึง	มี	Modify	การกำหนดให้กรอกแบบฟอร์มเพื่อขอใช้งานระบบสารสนเทศ
ไม่มีการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ	A9.1.1 นโยบายควบคุมการเข้าถึง	มี	Modify	ต้องมีการบริหารจัดการสิทธิ์ผู้ใช้งานในการเข้าถึงสารสนเทศแต่ละชนิด
เครื่องจากภายนอกสามารถเข้าถึงเครือข่ายภายในได้ด้วยระบบ Wi-Fi เมื่อเข้ามาแล้วสามารถใช้เครือข่ายเดียวกัน	A9.1.2 การเข้าถึงเครือข่ายและการบริการเครือข่าย	ไม่มี	New	แยกเครือข่าย Wi-Fi ออกจากเครือข่ายภายใน หรือกำหนดสิทธิ์การเข้าถึงของ Wi-Fi
พนักงานใหม่ ใช้ Username และ Password ของพนักงานเก่าในการเข้าใช้งานระบบสารสนเทศ	A9.2.1 การลงทะเบียนและถอดถอนสิทธิ์ผู้ใช้งาน	มี	Modify	HR ต้องแจ้งข้อมูลพนักงานที่ออกส่งต่อให้ฝ่ายไอทีทำการถอดสิทธิ์ออกจากระบบทันที
เมื่อมีพนักงานออกแล้วไม่ถอดถอนสิทธิ์ในการ	A9.2.1 การลงทะเบียนและ	มี	Modify	HR ต้องแจ้งข้อมูลพนักงานที่ออกส่งต่อให้

เข้าถึงระบบทันที แต่ยังสามารถเข้าระบบได้อยู่	ถอดถอนสิทธิ์ผู้ใช้งาน			ฝ่ายไอทีทำการถอดสิทธิ์ออกจากระบบทันที
พนักงานขอเข้าใช้งานสิทธิ์ที่ไม่มีสิทธิ์ โดยที่ไม่มีการอนุมัติจากหัวหน้างาน	A9.2.2 การจัดการสิทธิ์การเข้าถึงของผู้ใช้งาน	มี	Modify	ผู้ที่จะได้สิทธิ์การเข้าถึงข้อมูลต้องได้รับอนุญาตจากหัวหน้างานเป็นลายลักษณ์อักษร
ผู้ดูแลระบบมีการใช้งาน Account ที่ใช้เป็น Admin ร่วมกัน	A9.2.3 การบริหารจัดการสิทธิ์การเข้าถึงตามระดับสิทธิ์	ไม่มี	New	มีมาตรการไม่ใช้งาน Account ที่ใช้เป็น Admin ร่วมกัน โดยปิดผลึกไว้ นำมาใช้งานเมื่อมีความจำเป็นเท่านั้น และต้องได้รับการอนุมัติจากหัวหน้างานเท่านั้น
ระบบสารสนเทศถูกเข้าถึงโดยมีสิทธิ์การใช้งานเกินความจำเป็น	A9.2.3 การบริหารจัดการสิทธิ์การเข้าถึงตามระดับสิทธิ์	มี	Modify	กำหนด PERMISSION ให้กับพนักงานตรงกับที่หัวหน้างานอนุมัติ
พนักงานที่ออกไปแล้วยังมีสิทธิ์ค้างอยู่ในระบบสารสนเทศ	A9.2.5 การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน	ไม่มี	New	นำสิทธิ์ที่มีอยู่ในระบบมาทบทวนตรวจสอบอย่างไตรมาสละ 1 ครั้ง
มีบางโฟลเดอร์ในดาต้าเซ็นเตอร์ สามารถเข้าถึงได้ Everyone โดยไม่ป้องกันการเข้าถึงสำหรับแต่ละแผนก	9.4.1 การจำกัดการเข้าถึงสารสนเทศ	มี	Modify	กำหนด PERMISSION ของพนักงานให้ตรงตามแต่ละแผนก
ไม่มีการป้องกันการ Login ผิดบ่อยๆ โดยการล็อก User ใช้งาน	A9.4.2 ขั้นตอนปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย	ไม่มี	New	หากมีการล็อคอินผิดเกิน 3 ครั้ง ให้ตั้งระบบให้ทำการรอ 15 นาที หรือต้องแจ้งการปลดล็อคจาก admin เท่านั้น

คอมพิวเตอร์สามารถเข้าถึงได้ง่าย โดยไม่มีการ Login เข้าใช้งาน	A9.4.2 ขั้นตอนปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย	มี	Modify	นำคอมพิวเตอร์ทุกเครื่องเชื่อมต่อกับระบบ Active Directory
ผู้ใช้งานไม่ได้ Log out ออกจาก windows หลังจากใช้งานเสร็จแล้ว	A9.4.2 ขั้นตอนปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย	มี	Modify	ตั้งระบบ Log out อัตโนมัติ หลังจากไม่มีการใช้งานเกิน 15 นาที
รหัสผ่านเข้าสู่ระบบคอมพิวเตอร์ง่ายเกินไปหรือไม่เป็นความลับ	A9.4.3 ระบบบริหารจัดการรหัสผ่าน	ไม่มี	New	มีระบบบริหารจัดการรหัสผ่านอย่างรัดกุม โดยกำหนดเงื่อนไขการตั้งรหัสผ่าน และเวลาการเปลี่ยนรหัสผ่านอัตโนมัติ
ห้องเซิร์ฟเวอร์ไม่มีการบันทึกการเข้าออกของผู้ใช้งาน	A11.1.2 การควบคุมการเข้าออกทางกายภาพ	ไม่มี	New	ติดตั้งเครื่องสแกนนิ้ว กล้องวงจรปิด และบันทึกการเข้าออกห้องเซิร์ฟเวอร์
ตู้แร็ค Switch ตามแต่ละชั้นไม่มีการล็อคหรือมีกุญแจคาไว้	A11.2.1 การจัดตั้งและป้องกันอุปกรณ์	มี	Modify	ล็อคตู้แร็ค Switch ทุกๆ ชั้น
อุปกรณ์หยุดหรือไม่สามารถทำงานได้เต็มประสิทธิภาพ เนื่องจากถูกเข้าถึงและเปลี่ยนแปลงการตั้งค่าจากผู้ไม่มีสิทธิ์	A11.2.1 การจัดตั้งและป้องกันอุปกรณ์	ไม่มี	New	ป้องกันการเข้าถึงอุปกรณ์ โดยการกำหนด Password ที่คาดเดาได้ยาก หรือควบคุมการเข้าถึงอุปกรณ์ผ่าน Controller
พนักงานติดรหัสผ่านของระบบสารสนเทศ	A11.2.9 นโยบายโต๊ะทำงานปลอด	ไม่มี	New	กำหนดนโยบายในการตั้งรหัสผ่าน และทำ

ไว้ที่หน้าจอคอมพิวเตอร์หรือติดไว้บนโต๊ะทำงาน	เอกสารสำคัญและนโยบายการป้องกันหน้าจอคอมพิวเตอร์			ประกาศถึงภัยอันตรายของการโดนโจมตีรหัสผ่านจากบุคคลอื่น
ความผิดพลาดของการ Config อุปกรณ์เครือข่าย ทำให้ระบบทำงานผิดพลาดหรือหยุดให้บริการ	A.12.1.2 การบริหารจัดการการเปลี่ยนแปลง	ไม่มี	New	การสำรอง Config ของอุปกรณ์เครือข่ายไว้ โดยต้องสามารถทำการ Restore Configuration กลับคืนได้
การติดไวรัสและสแปมที่เครื่องเซิร์ฟเวอร์และเครื่องพนักงาน	A12.2.1 มาตรการป้องกันโปรแกรมไม่ประสงค์ดี	มี	Modify	ติดตั้งโปรแกรม Antivirus และ Antimalware และตรวจสอบให้มีการ Update อยู่เสมอ
ไม่มีการอัพ Patch Windows ของเครื่องพนักงาน	A12.6.1 การบริหารจัดการช่องโหว่ทางเทคนิค	มี	Modify	ตั้ง AUTO UPDATE PATCH WINDOWS
การเข้าถึงและโดนโจมตีจากเครือข่ายภายนอก	A13.1.2 ความมั่นคงปลอดภัยสำหรับบริการเครือข่าย	มี	Modify	ติดตั้งระบบ Firewall โดยมีการตั้งค่า Policy ความปลอดภัยของเครือข่ายภายใน
พนักงานสามารถเข้าใช้ระบบงานหรือข้อมูลของคนอื่นได้	A18.1.4 ความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคล	มี	Modify	มีนโยบายในการเข้ารหัสข้อมูลที่สำคัญ

3.4.3 การวิเคราะห์ช่องว่างการให้บริการอินเตอร์เน็ตของโรงแรม

ตารางที่ 3.12 การวิเคราะห์ช่องว่างการให้บริการอินเตอร์เน็ตของโรงแรม

System	Function	มี/ไม่มี	Acting	Action Plan
การให้บริการอินเตอร์เน็ตสำหรับลูกค้า In-House Guest	Authentication	มี	Modify	- นำระบบ Interface เข้ามาช่วยในการเชื่อมต่อฐานข้อมูลของลูกค้าในระบบจองห้องพัก Epitome กับระบบ Wi-Fi Hotspot - ระบุ Room Number, Last Name สำหรับเข้าใช้บริการอินเตอร์เน็ต
	Interface	ไม่มี	New	
	System Log	มี	Modify	
การให้บริการอินเตอร์เน็ตสำหรับลูกค้า Visitors	Authentication	มี	Modify	- การแจกคูปอง โดยให้มีการลงชื่อลูกค้าและแสดงบัตรประจำตัวประชาชน - ระบุ Access Code, First Name, Last Name เพื่อเข้าใช้บริการอินเตอร์เน็ต - Login เข้าใช้บริการผ่าน Facebook
	Access Code	ไม่มี	New	
	Facebook	ไม่มี	New	
	System Log	มี	Modify	
การให้บริการอินเตอร์เน็ตสำหรับพนักงานของโรงแรม	Authentication	ไม่มี	New	- เชื่อมต่อกับระบบ Radius เพื่อให้ผู้ใช้งานทำการยืนยันตัวตนผ่านหน้า Login ก่อนเข้าใช้งานอินเตอร์เน็ต - ให้พนักงานกรอกแบบฟอร์มขอใช้บริการอินเตอร์เน็ต - ระบุ Username และ Password เพื่อเข้าใช้บริการอินเตอร์เน็ต
	Radius	ไม่มี	New	
	แบบฟอร์มขอใช้บริการอินเตอร์เน็ต	ไม่มี	New	
	Login Page	ไม่มี	New	
	System Log	ไม่มี	New	

สำหรับขั้นตอนการออกแบบแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์และเครือข่าย จะขอกล่าวถึงใน **บทที่ 4 ผลการดำเนินการ**

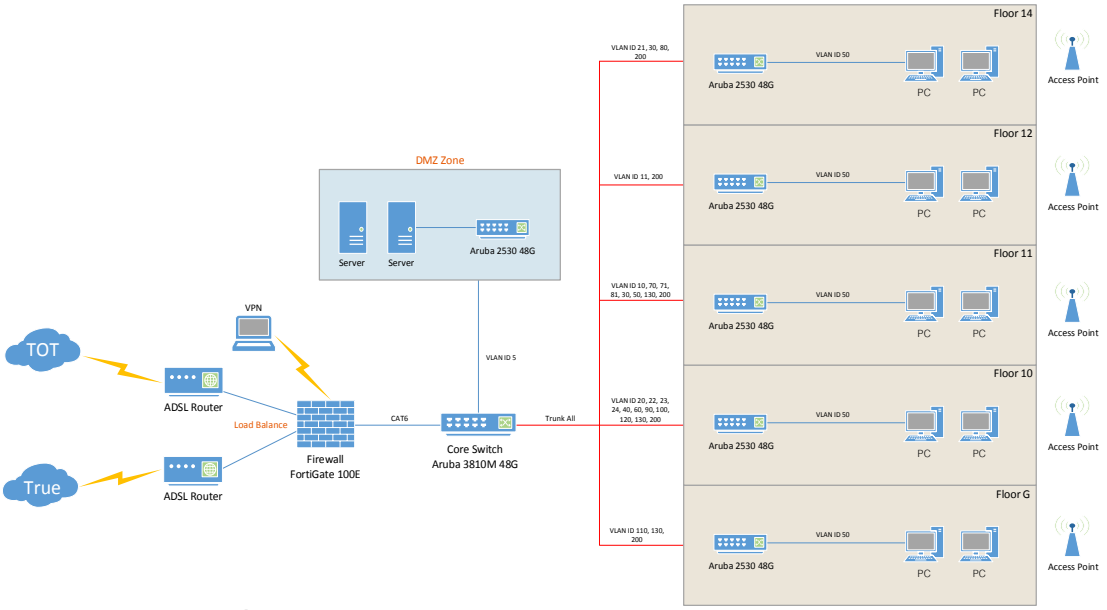
บทที่ 4
ผลการดำเนินงาน

หลังจากทำการวิเคราะห์ระบบคอมพิวเตอร์และเครือข่ายปัจจุบัน และวิเคราะห์ช่องว่าง (Gap Analysis) เสร็จแล้ว ทางผู้จัดทำได้นำข้อมูลดังกล่าวมาออกแบบเป็นแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์และเครือข่าย โดยแบ่งออกเป็น 3 ส่วน ดังนี้

- การออกแบบโครงสร้างความมั่นคงปลอดภัยระบบคอมพิวเตอร์และเครือข่ายใหม่
- แนวทางปฏิบัติในการเข้าถึงระบบเทคโนโลยีสารสนเทศ ภายใต้มาตรฐาน ISO/IEC 27001
- แนวทางปฏิบัติในการให้บริการอินเตอร์เน็ตตามแนวทางพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

4.1 การออกแบบโครงสร้างความมั่นคงปลอดภัยระบบคอมพิวเตอร์และเครือข่ายใหม่

โดยการนำข้อมูลจากการวิเคราะห์โครงสร้างเครือข่าย ช่องโหว่หรือข้อบกพร่องของระบบคอมพิวเตอร์และเครือข่ายปัจจุบัน และการวิเคราะห์ช่องว่าง (Gap Analysis) มาปรับใช้กับการออกแบบโครงสร้างระบบเครือข่ายใหม่ โดยมีการปรับปรุงโครงสร้างอุปกรณ์และเครือข่าย ปรับปรุงการตั้งค่าการทำงานของระบบคอมพิวเตอร์และเครือข่ายให้มีความปลอดภัย พร้อมทั้งแนะนำโปรแกรมหรือระบบรักษาความปลอดภัยบนระบบคอมพิวเตอร์และเครือข่าย ดังต่อไปนี้



รูปที่ 4.1 แสดงผังการออกแบบผังโครงสร้างระบบเครือข่ายใหม่

4.1.1 การปรับปรุงโครงสร้างอุปกรณ์และเครือข่าย

การปรับปรุงโครงสร้างอุปกรณ์และเครือข่าย ให้มีประสิทธิภาพที่สามารถรองรับการใช้งานเครือข่ายภายในองค์กรณ์ และมีระบบรักษาความปลอดภัยที่เพิ่มขึ้น โดยมีรายละเอียดดังต่อไปนี้

4.1.1.1 การเปลี่ยนสวิตซ์หลัก (Core Switch) โดยจัดหาซื้ออุปกรณ์สวิตซ์ Layer 3 มาทำการเปลี่ยนแทน จากเดิมที่ใช้อุปกรณ์สวิตซ์ Extreme X-350-48T (Layer 2) เป็นอุปกรณ์สวิตซ์ยี่ห้อ Aruba 3810M 48G (Layer 3) เพื่อเป็นตัวควบคุมการทำงาน และยังสามารถกำหนดค่าความปลอดภัยในเครือข่ายทั้งหมดได้

รูปที่ 4.2 ตัวอย่างอุปกรณ์ Core Switch ยี่ห้อ Aruba 3810M 48G

4.1.1.2 การเปลี่ยนสวิตซ์ในส่วนที่เชื่อมต่อกับผู้ใช้งานในแต่ละชั้น (Access Switch) เป็นรุ่น Aruba 2530 48G เนื่องจากสวิตซ์มีกันหลายรุ่นหลายยี่ห้อและหลายจุดเชื่อมต่อไม่ใช่แบบ Managed เพื่อรองรับการใช้งานเครือข่าย แอพพลิเคชั่น และเซิฟเวอร์ได้อย่างมีประสิทธิภาพมากขึ้น และกำหนดค่าการเชื่อมต่อไปยังสวิตซ์หลัก โดยใช้

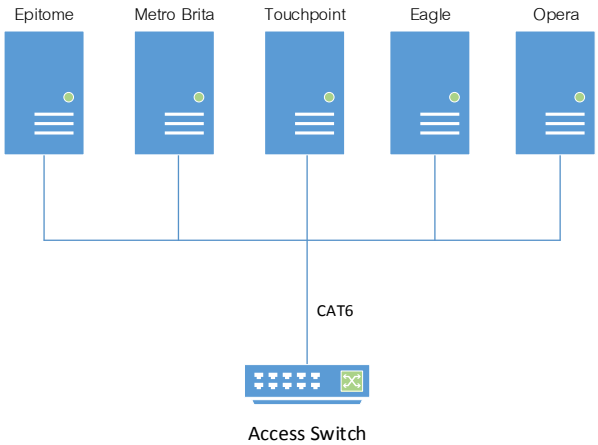
สายสัญญาณไฟเบอร์ออฟติก (Fiber Optic) เชื่อมต่อกัน เพื่อให้รองรับแบนวิดธ์ (Bandwidth) ได้ปริมาณมากในการรับส่งข้อมูล

รูปที่ 4.3 ตัวอย่างอุปกรณ์ Access Switch ยี่ห้อ รุ่น Aruba 2530 48G

4.1.1.3 การเปลี่ยนสาย UTP จาก CAT5 เป็น CAT6 ทั้งหมด เพื่อเพิ่มประสิทธิภาพในการรับส่งข้อมูลระหว่างอุปกรณ์และผู้ใช้งาน เพื่อรองรับปริมาณ Application และปริมาณผู้ใช้งานที่จะเพิ่มขึ้นในอนาคต

รูปที่ 4.4 ตัวอย่างสาย UTP แบบ CAT6

4.1.1.4 การนำเครื่องเซิร์ฟเวอร์ของแต่ละแผนกมาจัดวางใหม่ที่ DMZ Zone ภายใต้ Firewall เพื่อความปลอดภัยจากการโจมตีจากภายนอก และลดการกระจายโหลดไปยังแต่ละ VLAN

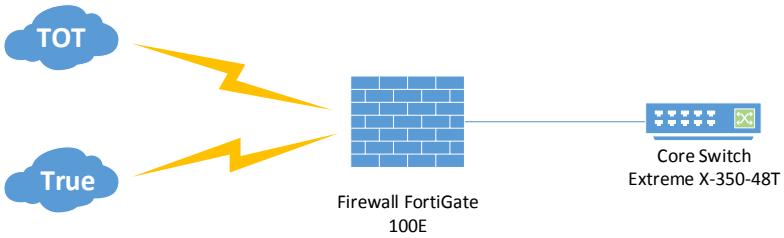


รูปที่ 4.5 ตัวอย่างการนำเครื่องเซิร์ฟเวอร์ของแต่ละแผนกมาจัดวางใหม่ที่ DMZ Zone

4.1.1.5 การติดตั้งสวิตช์เซิร์ฟเวอร์ เพื่อทำเป็นสวิตช์สำหรับเชื่อมต่อกับเครื่องเซิร์ฟเวอร์ โดยเครื่องเซิร์ฟเวอร์แต่ละตัวจะใช้สาย UTP แบบ CAT6 ในการเชื่อมต่อกับสวิตช์

รูปที่ 4.6 ตัวอย่างการติดตั้งสวิตช์สำหรับเครื่องเซิร์ฟเวอร์

4.1.1.6 การติดตั้งสัญญาณอินเตอร์เน็ต (Internet ADSL) จากผู้ให้บริการ ISP อย่างน้อยต้องมีผู้ให้บริการ 2 ราย เพื่อป้องกันกรณีที่อุปกรณ์มีปัญหาหรือสัญญาณอินเตอร์เน็ตหลักขัดข้อง สัญญาณอินเตอร์เน็ตสำรองก็สามารถทำงานต่อได้ ไม่ส่งผลกระทบต่อการใช้งานอินเตอร์เน็ตขององค์กร

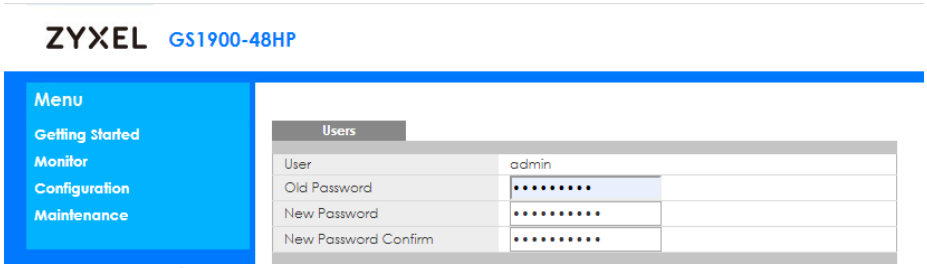


รูปที่ 4.7 การติดตั้งสัญญาณอินเตอร์เน็ต (Internet ADSL) จากผู้ให้บริการ ISP 2 ราย

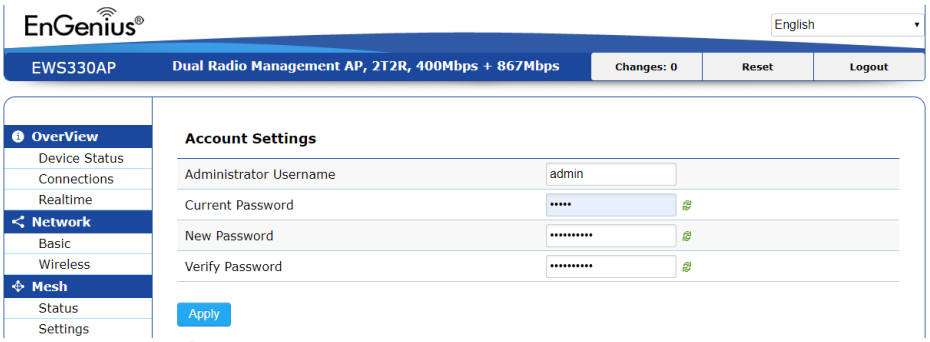
4.1.1.7 การป้องกันการเข้าถึงอุปกรณ์ Access Switch และ Access point โดยการกำหนด Password ที่คาดเดาได้ยาก เพื่อลดความเสี่ยงจากผู้ไม่หวังดี ที่สามารถเข้ามาแก้ไขการตั้งค่าต่างๆ ของอุปกรณ์ได้ (รหัสผ่านควรมีความยาวอย่างน้อย 8 ตัวอักษร ประกอบด้วยตัวพิมพ์ใหญ่อย่างน้อย 1 ตัว และเครื่องหมายหรืออักขระพิเศษอย่างน้อย 1 ตัว)

ตารางที่ 4.1 แสดงการกำหนด Username และ Password ที่อุปกรณ์ Access Switch

Floor Switch	Brand/Model	IP Address	Username	Password
FL.1 (Front Office)	Extreme X-350-48T	192.168.111.21	admin	KKnjnw279
FL.11 (Sale Room)	Extreme X-350-48T	192.168.111.11	admin	KKnjnw279
FL.10 (Core-Switch)	Aruba 3810M 48G	192.168.111.2	admin	bkl@dm1n
FL.10 (Account)	Cisco GS 200	192.168.111.22	admin	KKnjnw279
FL.10 (Engineer)	Extreme X-150-48T	192.168.111.26	admin	KKnjnw279
FL.10 (Kitchen)	Extreme X-350-24T	192.168.111.27	admin	KKnjnw279
FL.11 (F&B Room)	Cisco GS 200	192.168.111.23	admin	KKnjnw279
FL.12 (IT-Room)	Aruba 2530 24G	192.168.111.12	admin	bkl@dm1n
FL.14 (Reservation)	Cisco GS 200	192.168.111.14	admin	KKnjnw279



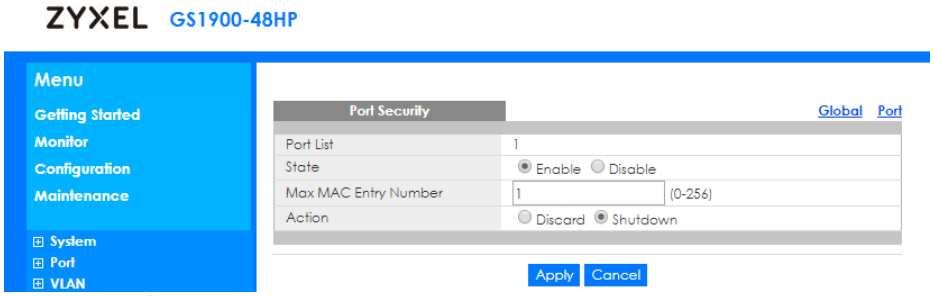
รูปที่ 4.8 การกำหนดรหัสผ่านเข้าถึงอุปกรณ์ Access Switch



รูปที่ 4.9 การกำหนดรหัสผ่านเข้าถึงอุปกรณ์ Access Point

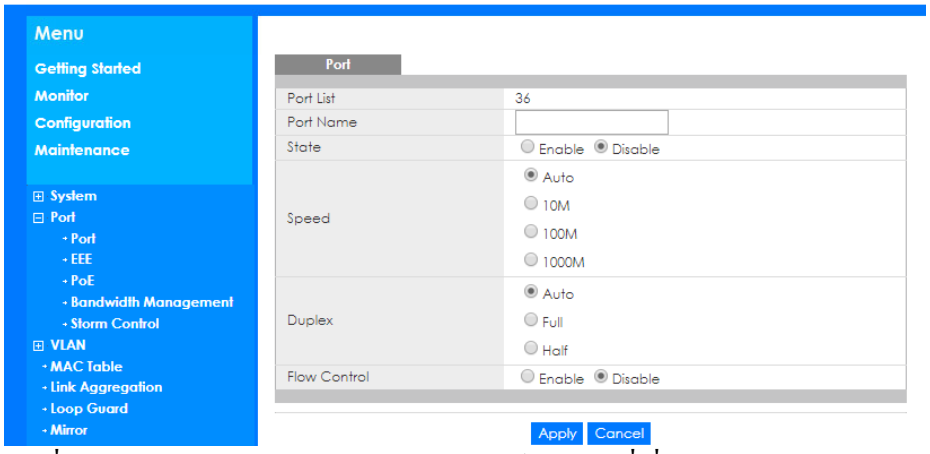
4.1.1.8 การใช้งาน Port Security จะทำให้สามารถจำกัดจำนวนหมายเลขของ Mac Address ที่ได้รับอนุญาตให้ใช้งานในแต่ละ Port ได้ หากพบว่า Mac Address ที่เข้ามาทาง

port นั้น ไม่ตรงกับรายการที่มีอยู่ จะไม่อนุญาตให้ส่งต่อข้อมูลจากต้นทาง Mac Address นั้นได้ หรือทำการ Shutdown Port นั้นไปเลย



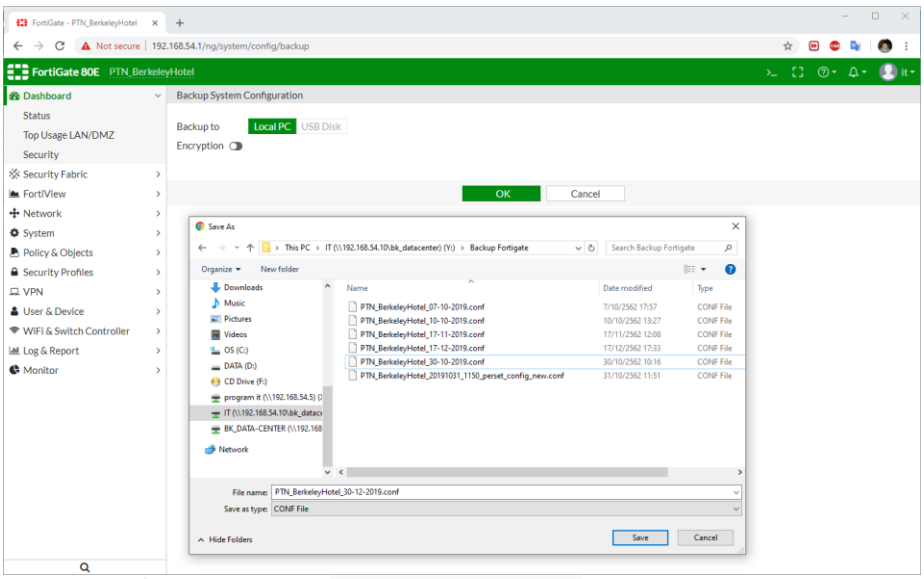
รูปที่ 4.10 แสดงการทำ Port Security ของอุปกรณ์ Access Switch

4.1.1.9 การทำ Disable Port ของอุปกรณ์ Switch ที่เชื่อมต่อไปยัง Outlet Lan ตามห้องประชุมหรือห้องสัมมนาภายในอาคาร ไว้ก่อนชั่วคราว เพื่อป้องกันการโจมตีหรือก่อกวนระบบเครือข่ายจากบุคคลภายนอก โดยการนำเอาอุปกรณ์มาเชื่อมต่อ Outlet Lan



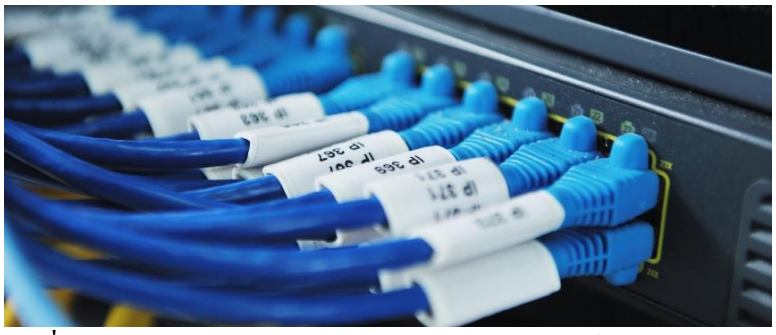
รูปที่ 4.11 แสดงการ Disable Port ของอุปกรณ์ Switch ที่เชื่อมต่อไปยัง Outlet Lan

4.1.1.10 การทำ Backup & Restore Configuration โดยการ Backup เก็บค่า Config หรือข้อมูลต่างๆ ที่ได้ทำการตั้งค่าไว้บนตัวอุปกรณ์เครือข่าย อาทิ Firewall, Switch, Router, Access Point หรืออุปกรณ์อื่นๆ เพื่อสำรองการตั้งค่าเก็บไว้ ในกรณีที่อุปกรณ์นั้นอาจจะเกิดปัญหาหรือเกิดการเปลี่ยนแปลงค่า Config ที่ผิดพลาด ดังนั้นเมื่อ Backup Configuration ได้แล้ว ต้องสามารถทำการ Restore Configuration กลับคืนได้



รูปที่ 4.11 แสดงการ Backup เก็บค่า Config ของอุปกรณ์ Firewall

4.1.1.11 การทำเครื่องหมายหรือติดหมายเลขกำกับไว้ที่สายแลนที่เชื่อมต่อกับ Access Switch เพื่อให้ทราบว่าสายแลนเส้นไหนเชื่อมต่อไปยังจุดปลายทางที่ใด หรือเชื่อมต่อมาจาก Outlet Lan ที่ไหน



รูปที่ 4.12 ตัวอย่างการกำหนดรหัสผ่านเข้าถึงอุปกรณ์ Access Switch

4.1.1.12 การนำระบบ VLAN เข้ามาใช้งาน ในการออกแบบนั้น ทางผู้จัดทำได้แนะนำให้เปลี่ยนระบบเครือข่ายปัจจุบันที่เป็นแบบไอพีแอดเดรสภายใต้ซับเน็ตเดียว เป็นการจัดแบ่ง VLAN ของแต่ละฝ่าย โดยแต่ละ VLAN จะไม่สามารถเชื่อมต่อเพื่อแลกเปลี่ยนข้อมูลกันได้ เพื่อป้องกันการแพร่กระจายไวรัสหรือมัลแวร์ภายในเครือข่าย ซึ่งทางองค์กรมีจำนวนฝ่ายทั้งหมด 20 ฝ่าย พร้อมทั้ง VLAN ของเครือข่ายวงดีเอ็มแซด (DMZ) ซึ่งเป็นโซนของเครื่องเซิฟเวอร์ที่ทุก VLAN จะสามารถเชื่อมต่อเข้ามาใช้งานได้

ตารางที่ 4.2 แสดงตัวอย่างการออกแบบ VLAN ของระบบเครือข่ายใหม่

แผนก	ฝ่าย	VLAN ID	IP Address	Subnet Mark
Administration	Executive	10	192.168.10.1	255.255.255.0
	Information Technology	11	192.168.11.1	255.255.255.0
Finance & Accounting	Finance & Accounting	20	192.168.20.1	255.255.255.0
	Account Receivable	21	192.168.21.1	255.255.255.0
	Cost	22	192.168.22.1	255.255.255.0
	Receiving	23	192.168.23.1	255.255.255.0
	Purchasing	24	192.168.24.1	255.255.255.0
	Reservation	30	192.168.30.1	255.255.255.0
	Human Resource	40	192.168.40.1	255.255.255.0
	Food & Beverage	50	192.168.50.1	255.255.255.0
	Housekeeping	60	192.168.60.1	255.255.255.0
Catering & Sales	Catering	70	192.168.70.1	255.255.255.0
	Sales	71	192.168.71.1	255.255.255.0
Business Development	Business Development	80	192.168.80.1	255.255.255.0
	Graphic	81	192.168.81.1	255.255.255.0
	Engineer	90	192.168.90.1	255.255.255.0
	Security	100	192.168.100.1	255.255.255.0
	Front Office	110	192.168.110.1	255.255.255.0
	Kitchen	120	192.168.120.1	255.255.255.0
System		**VLAN**	**IP Address**	**Subnet Mark**
POS		130	192.168.130.1	255.255.255.0
DMZ		5	192.168.5.1	255.255.255.0
Wireless Office		200	172.16.0.1	255.255.254.0
Wi-FI Hotspot		300	10.10.0.1	255.255.248.0
VLAN Management		111	192.168.111.1	255.255.255.0

4.1.1.13 การทำ Inter VLAN Routing เพื่อการติดต่อสื่อสารกันระหว่าง VLAN เพื่อให้แต่ละแผนกที่ทำงานใน Operation เดียวกัน สามารถติดต่อหรือแลกเปลี่ยนข้อมูลกันได้ แต่จะไม่กวนกัน หรือ Broadcast ถึงกัน โดยการใช้อุปกรณ์ Core Switch Layer 3 เป็นตัวเชื่อมหรือเป็น Gateway เช่น คอมพิวเตอร์ของฝ่าย Finance & Accounting ที่อยู่ใน VLAN ID 20 สามารถติดต่อกับคอมพิวเตอร์ของฝ่าย Cost ที่อยู่ใน VLAN ID 22 และยังสามารถติดต่อกับเซิร์ฟเวอร์ Epitome ที่อยู่ใน VLAN ID 5 ได้อย่างปกติ

ตารางที่ 4.3 แสดงตัวอย่างการทำ Inter VLAN Routing ของแต่ละแผนกที่ทำงานใน Operation เดียวกัน

ฝ่าย	VLAN ID	IP Address / Subnet Mark	Gateway	Inter VLAN Routing	Routing to DMZ
Executive	10	192.168.10.0/24	192.168.10.1	Inter VLAN Routing	DMZ
Information Technology	11	192.168.11.0/24	192.168.11.1		
Catering	70	192.168.70.0/24	192.168.70.1	Inter VLAN Routing	DMZ
Sales	71	192.168.71.0/24	192.168.71.1		
Business Development	80	192.168.80.0/24	192.168.80.1	Inter VLAN Routing	DMZ
Graphic	81	192.168.81.0/24	192.168.81.1		

4.1.1.14 การควบคุมการเข้าออกห้อง Server เพื่อให้การใช้งานห้อง Server มีความปลอดภัยต่ออุปกรณ์เครือข่ายและข้อมูลที่อยู่ในห้อง Server จะต้องมีระบบรักษาความปลอดภัย สำหรับแนวทางการปฏิบัติในการเข้าใช้งานห้อง Server ดังต่อไปนี้

- ติดตั้งเครื่อง Finger Scan ที่หน้าห้อง Server เพื่อบันทึกข้อมูลวันเวลาเข้าออกห้อง Server
- ติดตั้งกล้องวงจรปิดในห้อง Server เพื่อบันทึกเหตุการณ์ต่างๆ ในห้อง Server
- ต้องแจ้งเจ้าหน้าที่ผู้ดูแลห้อง Server ก่อนเข้าใช้งานอย่างน้อย 1 ชั่วโมง

- ต้องทำการบันทึกรายละเอียดการปฏิบัติและลงลายมือชื่อในบันทึกการเข้าใช้งานห้อง Server
- หากบุคคลภายนอกต้องการเข้าห้อง Server ต้องมีเจ้าหน้าที่ไอทีเข้าไปด้วยทุกครั้ง

รูปที่ 4.13 ตัวอย่างแสดงการติดตั้ง Finger Scan และกล้องวงจรปิด CCTV

4.1.2 ออกแบบระบบสนับสนุนความปลอดภัยของระบบคอมพิวเตอร์และเครือข่าย

จากการออกแบบโครงสร้างของระบบคอมพิวเตอร์และเครือข่ายใหม่แล้ว จึงได้มีการปรับปรุงการตั้งค่าการทำงานของระบบสนับสนุนความปลอดภัย และแนะนำโปรแกรมหรือระบบรักษาความปลอดภัย สำหรับระบบคอมพิวเตอร์และเครือข่าย ดังนี้

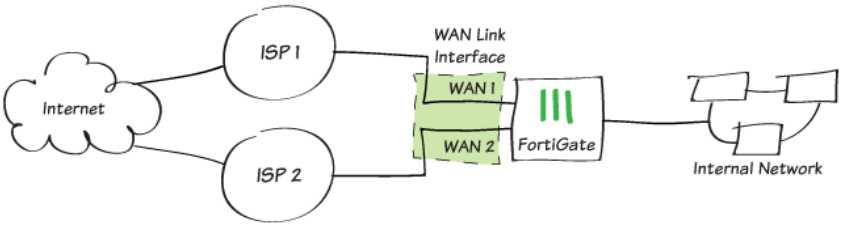
4.1.2.1 การปรับปรุงการตั้งค่าการทำงานของระบบความปลอดภัยคอมพิวเตอร์และเครือข่าย

ระบบ Firewall

โดยแนะนำการปรับปรุงการตั้งค่าการทำงานของระบบ Firewall เพื่อให้มีความปลอดภัยมากยิ่งขึ้น ดังต่อไปนี้

- **Redundant internet connections**

เป็นการสร้างอินเตอร์เฟสในการเชื่อมต่อ WAN กับอินเทอร์เน็ตจากผู้ให้บริการ (ISP) 2 ราย โดยการรวมเอาอินเตอร์เฟสการเชื่อมต่อ 2 WAN รวมไว้ในอินเตอร์เฟส โดยให้ ISP ที่ใช้สำหรับการเชื่อมต่ออินเทอร์เน็ตหลัก เชื่อมต่อกับ WAN1 และ ISP ที่ใช้สำหรับการเชื่อมต่ออินเทอร์เน็ตสำรอง เชื่อมต่อกับ WAN2

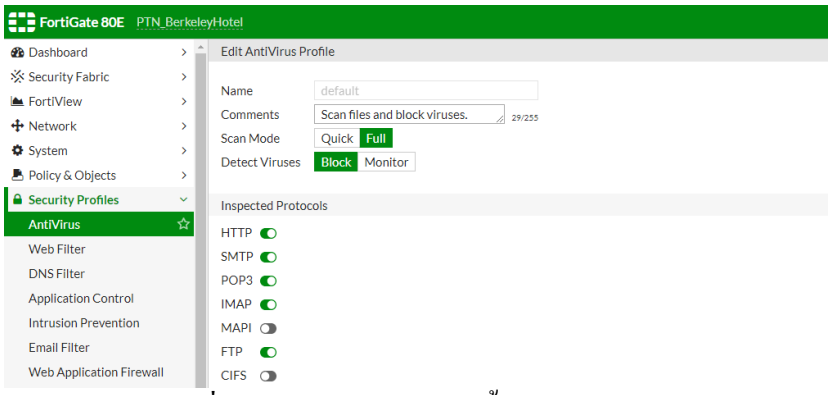


รูปที่ 4.14 ตัวอย่างแสดง Redundant internet connections

☐ Security Profiles

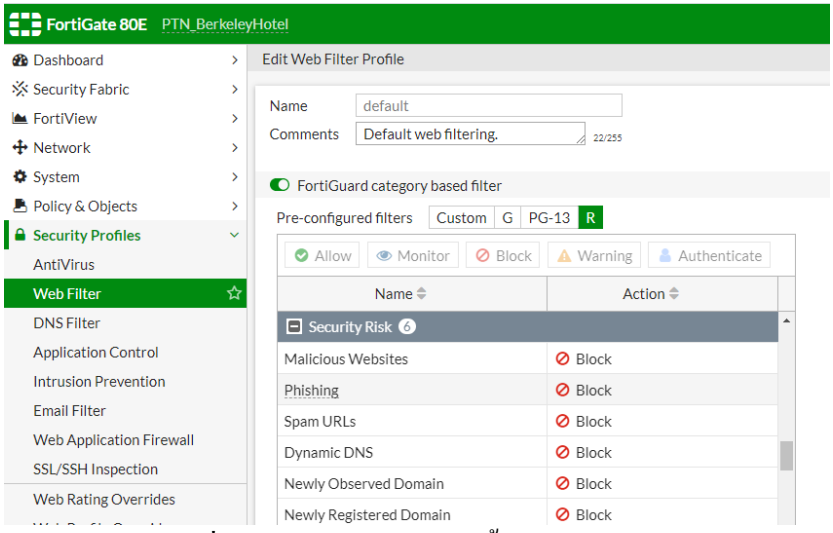
โดยการกำหนดหรือสร้าง Security Profiles ของแต่ละหมวด ดังต่อไปนี้

- Anti-Virus



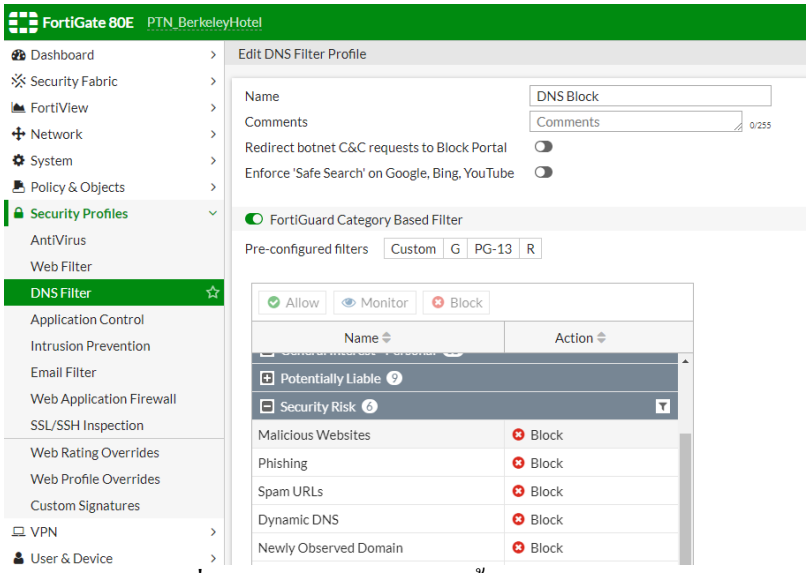
รูปที่ 4.15 ตัวอย่างแสดงการตั้งค่า Anti-Virus

- Web Filter



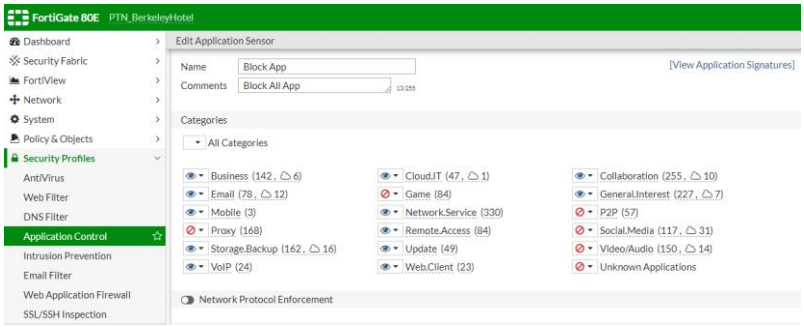
รูปที่ 4.16 ตัวอย่างแสดงการตั้งค่า Web Filter

- DNS Filter



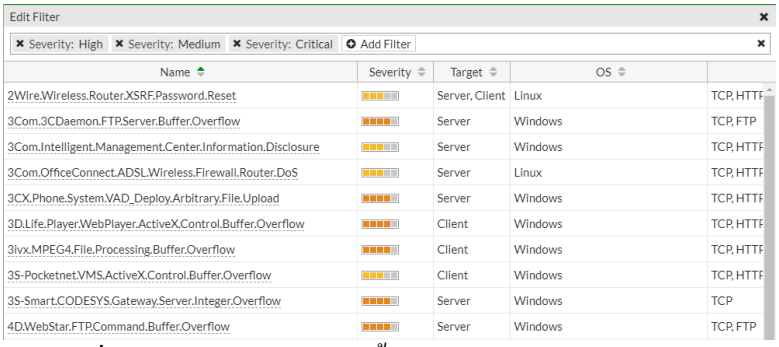
รูปที่ 4.17 ตัวอย่างแสดงการตั้งค่า DNS Filter

- Application Control



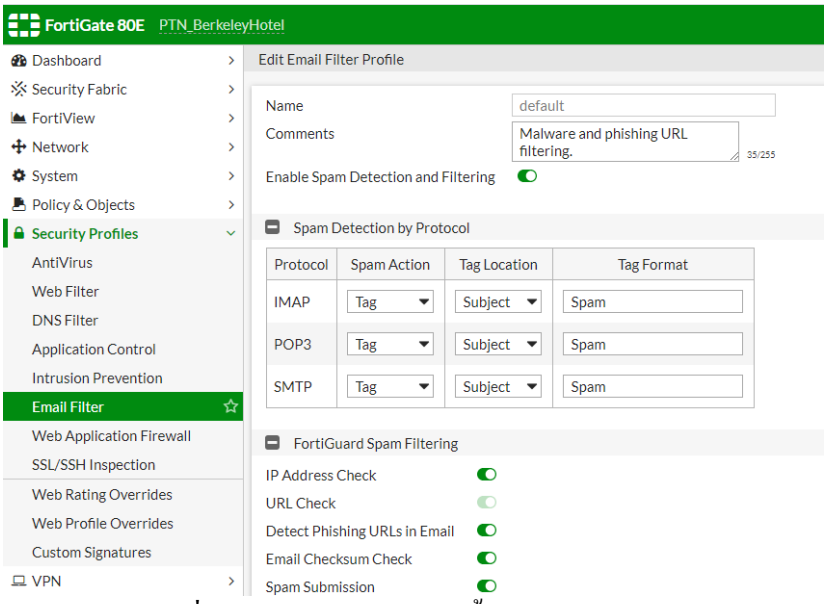
รูปที่ 4.18 ตัวอย่างแสดงการตั้งค่า Application Control

- Intrusion Protection (IPS)



รูปที่ 4.19 ตัวอย่างแสดงการตั้งค่า Intrusion Protection (IPS)

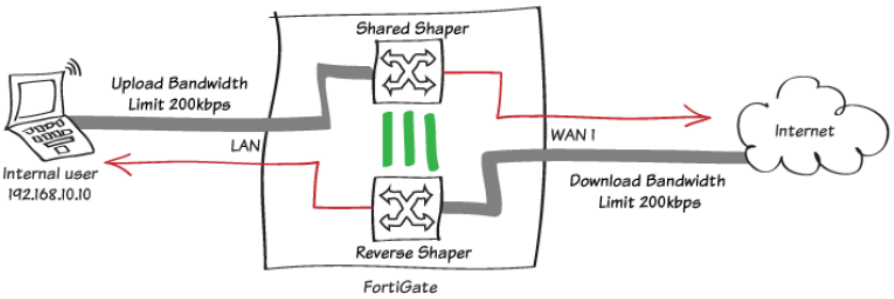
- Email Filter



รูปที่ 4.20 ตัวอย่างแสดงการตั้งค่า Email Filter

☐ **Limiting bandwidth with traffic shaping**

เป็นการควบคุมให้อินเตอร์เน็ตวิ่งในระดับ Bandwidth ที่กำหนด เพื่อทำให้การใช้งานอินเตอร์เน็ตมีความ Smooth เช่น ทำงานไม่ช้า เพราะ Speed Internet มีจำนวนการใช้งานอย่างจำกัด ถ้าระบบหนึ่งระบบใดมีการใช้งานอินเตอร์เน็ตมากเกินกว่าปกติ ระบบอื่นๆ จะมีปัญหาทันที

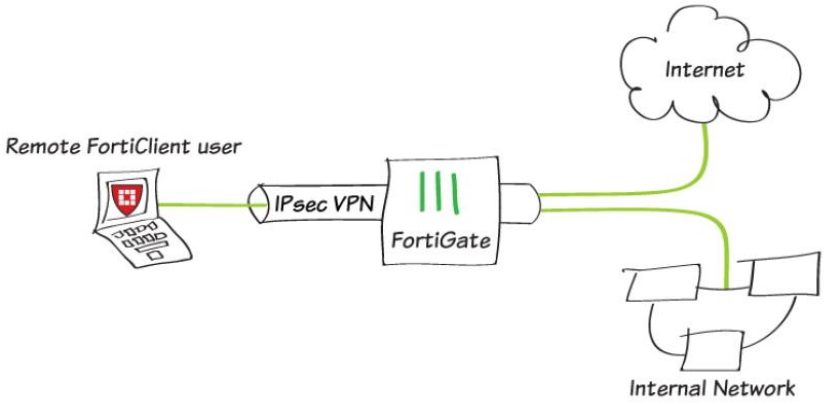


รูปที่ 4.21 ตัวอย่างแสดง Limiting bandwidth with traffic shaping

☐ **IPsec VPN with FortiClient**

เป็นชุดของโปรโตคอลที่ใช้ในการรักษาความปลอดภัยของข้อมูล มีการตรวจสอบความถูกต้องในการรับ - ส่งข้อมูล, มีการพิสูจน์ตัวตน, การเข้ารหัส

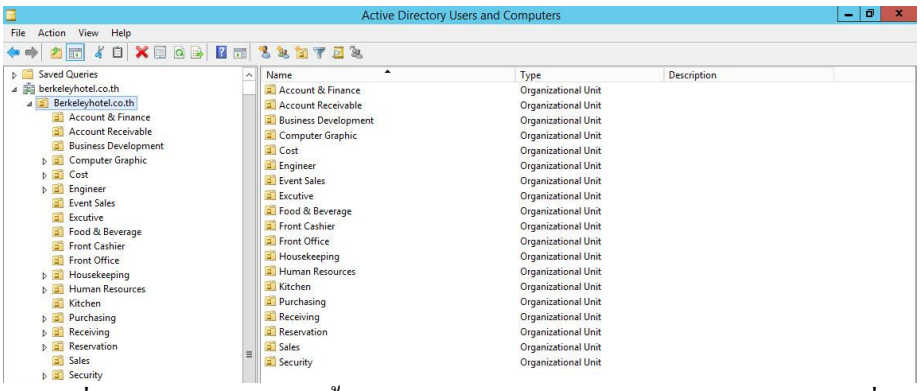
ข้อมูล เป็นต้น ทำงานในระดับ Network Layer โดยจะทำการเข้ารหัสและสร้าง Header ขึ้นมาใหม่ไปใช้แทน Header เดิมที่ถูกเข้ารหัสเอาไว้



รูปที่ 4.22 ตัวอย่างแสดง IPsec VPN with FortiClient

ระบบ Active Directory

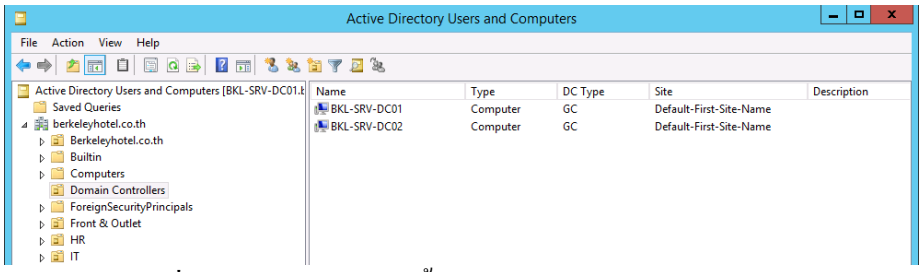
☐ **การออกแบบระบบ Active Directory (AD)** เพื่อให้ผู้ใช้งานทำการยืนยันตัวตนก่อนเข้าใช้งานเครื่องคอมพิวเตอร์ขององค์กร โดยทำการสร้างออบเจ็กต์ของ Organization Unit (OU) ในระบบ AD ตามฝ่ายในองค์กร เพื่อง่ายในการดูแลจัดการ User Account ของผู้ใช้งานในแผนก



รูปที่ 4.23 ตัวอย่างการติดตั้งโครงสร้างออบเจ็คในระบบแอคทีฟไดเรกเทอรี่

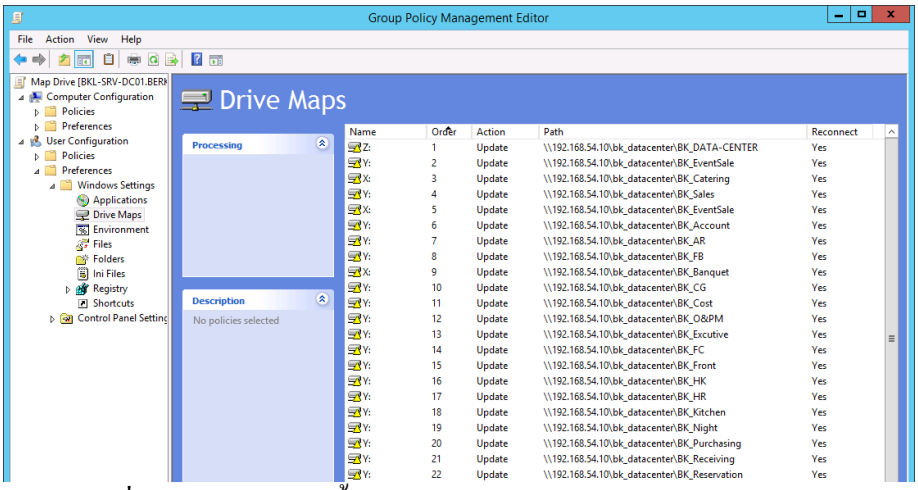
☐ **การติดตั้ง Additional Domain Controller** เป็นการเพิ่ม Domain Controller เข้าไปใน Domain ที่มีอยู่แล้ว เพื่อแบ่งเบาภาระการทำงานของ Domain Controller เครื่องหลัก และเพื่อ Backup การทำงานในกรณีที่ Domain Controller เครื่องหลัก อาจไม่สามารถทำงานได้ชั่วคราว (เรียกการทำงานแบบนี้ว่า Multi–Master) คือสามารถทำงาน

ทดแทนกันได้ โดยการย้าย Roles ไปยังเครื่อง Backup Domain เนื่องจากว่า Primary และ Additional นั้น มีการ Replicate ข้อมูลกันตลอดเวลา



รูปที่ 4.24 ตัวอย่างการติดตั้ง Additional Domain Controller

☐ **การติดตั้งระบบ File Share Server & Map Network Drive** เพื่อใช้ในการ Sync กับ Fire Server เพื่ออ่านข้อมูลผู้ใช้งานในระบบ Active Directory โดยการเพิ่มหน้าที่ (Role) ในการทำงานเป็น Driver Maps และกำหนดสิทธิ์ในการเข้าถึง File Share ของแต่ละฝ่าย หลังจาก Login เข้าสู่ระบบคอมพิวเตอร์

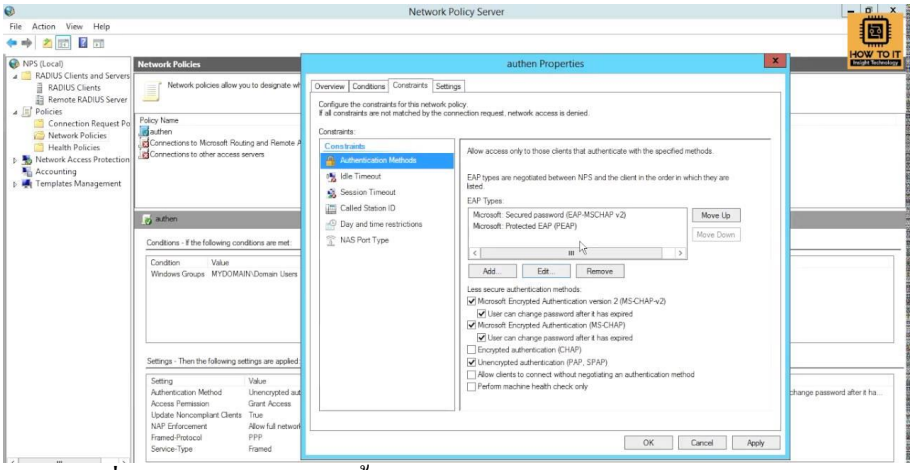


รูปที่ 4.25 ตัวอย่างการตั้งค่า Driver Maps ในระบบ Active directory

ระบบ Radius (Remote Authentication Dial-In User Service)

การติดตั้งระบบ Radius (Remote Authentication Dial-In User Service) ลงบนเซิฟเวอร์ เพื่อใช้ในการ Sync กับ Firewall เพื่ออ่านข้อมูลผู้ใช้งานในระบบ Active Directory เพื่อนำไปให้ผู้ใช้งานทำการยืนยันตัวตนผ่านหน้าเว็บเบราเซอร์ก่อนใช้งานอินเตอร์เน็ตบนระบบ Wireless Office โดยการเพิ่มหน้าที่ (Role) ในการทำงานเป็น Radius Server บนตัวเครื่องเซิฟเวอร์ สำหรับดึงฐานข้อมูลของผู้ใช้งานระหว่างระบบ

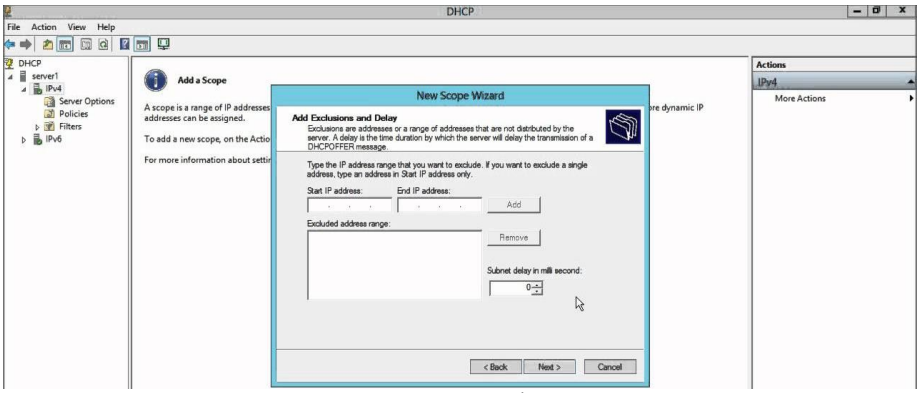
Active Directory และตัวไฟวอล์ เพื่อนำฐานข้อมูลดังกล่าวมาใช้ในการให้ผู้ใช้งานทำการยืนยันตัวตนก่อนเข้าใช้งานระบบเครือข่าย Internet



รูปที่ 4.26 ตัวอย่างการติดตั้ง Radius Server ในระบบ Active directory

ระบบ DHCP Server

เนื่องจากระบบเครือข่ายขององค์กรมีการออกแบบหมายเลขไอพีสำหรับเครื่องคอมพิวเตอร์พนักงานไว้ โดยแยกตามแต่ละแผนก แต่หากผู้ดูแลระบบต้องไปกำหนดหมายเลขไอพีให้ทุกเครื่องก็จะเป็นการยากหากมีเครื่องคอมพิวเตอร์จำนวนมาก การติดตั้งระบบ DHCP Server จึงเป็นสิ่งที่จำเป็น โดยกำหนดหมายเลขไอพีให้แยกตามแผนกในองค์กร แล้วทำการตั้งค่าที่อุปกรณ์สวิตช์ให้ระบุค่าหมายเลขไอพีจากเครื่องเซิร์ฟเวอร์

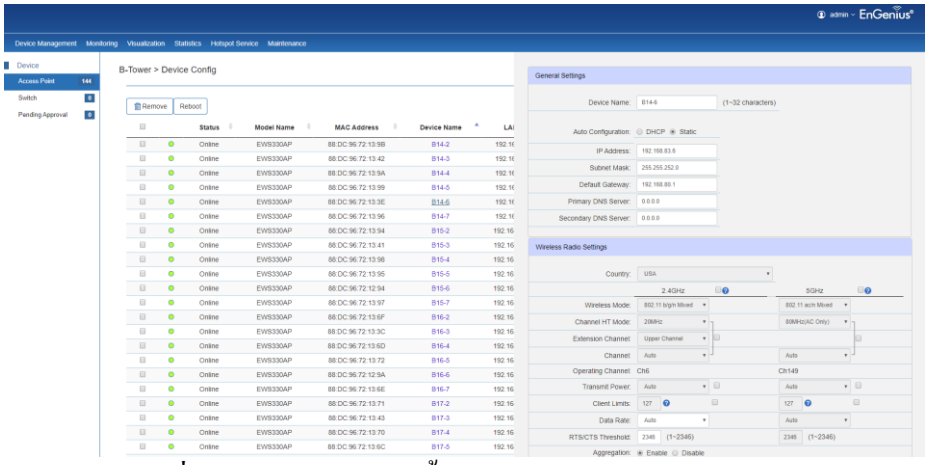


รูปที่ 4.27 ตัวอย่างการติดตั้ง DHCP Server

ระบบ Access Point Controller

เพื่อควบคุมและตรวจสอบการทำงานของอุปกรณ์ Access Point พร้อมทั้งป้องกันการเข้าถึงตัวอุปกรณ์และการโจมตีเครือข่ายจากผู้ไม่หวังดี โดย Access Point

ยี่ห้อ Engenius (ใช้งานภายในองค์กร) มีซอร์ฟแวร์ที่ชื่อว่า ezMaster ที่ช่วยจัดการอุปกรณ์ให้ใช้งานง่าย ตอบโจทย์ผู้ดูแลระบบโดยตรง

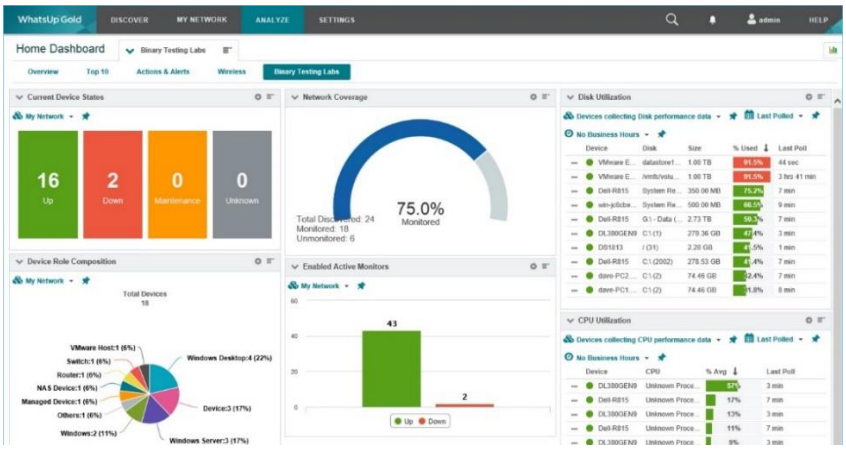


รูปที่ 4.28 ตัวอย่างการติดตั้งระบบ Access Point Controller

4.1.2.2 แนะนำโปรแกรมหรือระบบรักษาความปลอดภัยบนระบบคอมพิวเตอร์และเครือข่าย

ระบบ Network Monitoring

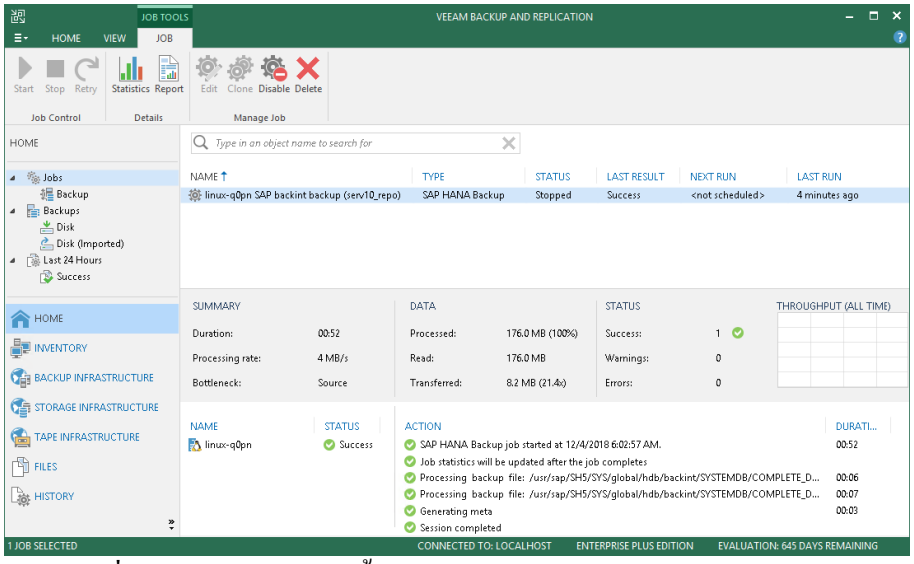
โดยการติดตั้งซอฟต์แวร์ประเภท NMS (Network Management System) ซึ่งสามารถใช้ตรวจสอบการทำงานของอุปกรณ์ที่ใช้งานในระบบเครือข่าย โดยทางองค์กรได้เลือกใช้งานโปรแกรม IPswitch WhatsUp Gold ซึ่งมีการใช้งานที่ง่ายและไม่ซับซ้อน รวมถึงมี Interface ที่ใช้งานง่าย และมีฟังก์ชั่นการทำงานที่หลากหลาย รวมถึงสามารถแจ้งเตือนเมื่ออุปกรณ์หยุดทำงานได้ ไม่ว่าจะทาง Email หรือ SMS ผ่านทางโทรศัพท์มือถือ ทำให้ผู้ดูแลระบบสารสนเทศ หรือเจ้าหน้าที่ IT Support ก็สามารถใช้งานได้อย่างไม่ยาก และสามารถตรวจพบปัญหาได้ง่ายขึ้นอีกด้วย



รูปที่ 4.29 ตัวอย่างระบบมอนิเตอร์อุปกรณ์เครือข่ายด้วยโปรแกรม IPswitch WhatsUp Gold

ระบบ Backup and Recovery

โดยการติดตั้งซอฟต์แวร์ Veeam Backup & Replication เพื่อสำรองและกู้คืนข้อมูลในระบบเสมือน (Virtualization) ได้อย่างรวดเร็วและง่ายดาย โดยรองรับระบบ Virtualization ชั้นนำ เช่น VMWare หรือ Microsoft Hyper-V และสามารถทำ Replication ไปยัง Site สำรองได้อย่างง่ายดาย โดยไม่ต้องซื้อเพิ่ม โดยการ Backup VM-Guests ในลักษณะที่เรียกว่า Incremental Forever คือการสำรองข้อมูลเฉพาะ Block ที่มีการเปลี่ยนแปลงเท่านั้น และรองรับการทำ Reduplication ซึ่งเป็นการเก็บเฉพาะข้อมูลที่ซ้ำซ้อนลงดิสก์เท่านั้น ทำให้ประหยัดเวลาและเนื้อที่ในการจัดเก็บได้อย่างมีประสิทธิ์ภาพมากขึ้น โดยที่การกู้คือ (Recover) ข้อมูลนั้น สามารถกู้คืนได้ ทั้งแบบทั้ง VM หรือบางส่วน (Individual Object) เช่น ไฟล์ หรือ โฟลเดอร์ที่ต้องการ

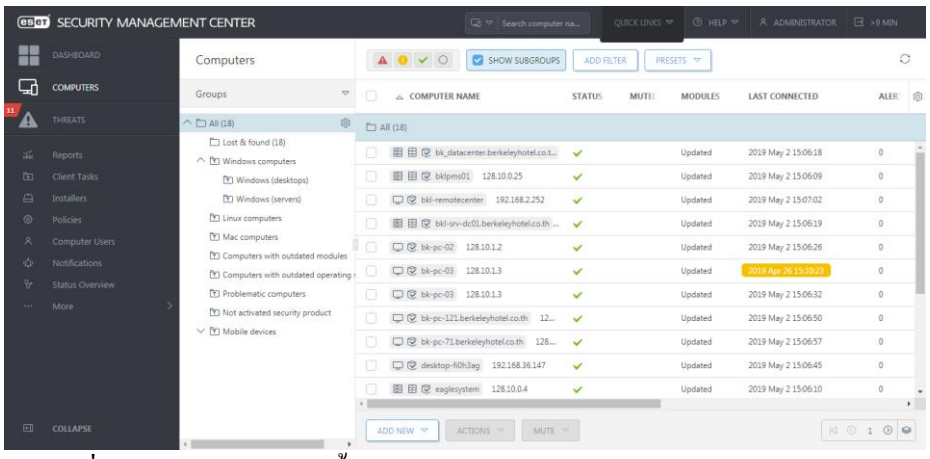


รูปที่ 4.30 ตัวอย่างการติดตั้งโปรแกรม Veeam Backup & Replication

ระบบ Antivirus

โดยการติดตั้งระบบ ESET Security Management Center เพื่อช่วยจัดการโปรแกรม ESET บนเครื่องคอมพิวเตอร์ เซิร์ฟเวอร์ และอุปกรณ์เคลื่อนที่ในเครือข่ายจากจุดศูนย์กลางจุดเดียว โดยการทำงาน ESET Security ประกอบด้วย

- ส่วน คอมพิวเตอร์
- ส่วน การป้องกันเครือข่าย
- ส่วน เว็บและอีเมล



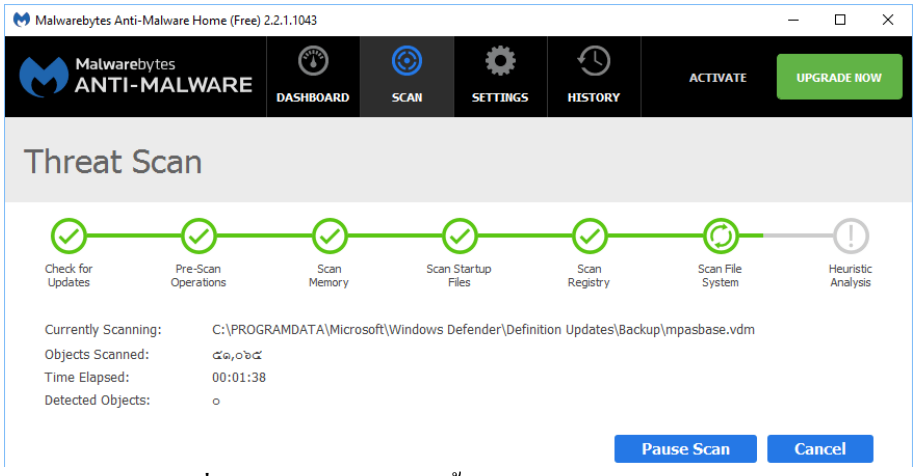
รูปที่ 4.31 ตัวอย่างการติดตั้งโปรแกรม ESET Security Management Center

ระบบ Antimalware

การติดตั้งโปรแกรม MalwareBytes ซึ่งเป็นโปรแกรมป้องกันไวรัส ประเภท Spyware (สปายแวร์) และ Malware (มัลแวร์) โปรแกรมจะทำการสแกนเครื่องคอมพิวเตอร์เพื่อตรวจสอบว่ามีโปรแกรมใดบ้างที่เป็น Spyware / Malware ซึ่งอาจจะถูกติดตั้งในเครื่องโดยที่เราไม่รู้ตัว ซึ่งโปรแกรมนั้นจะมีด้วยกัน 3 โหมด คือ โหมด Threat Scan โหมด Custom Scan และโหมด Hyper Scan

คุณสมบัติของโปรแกรม

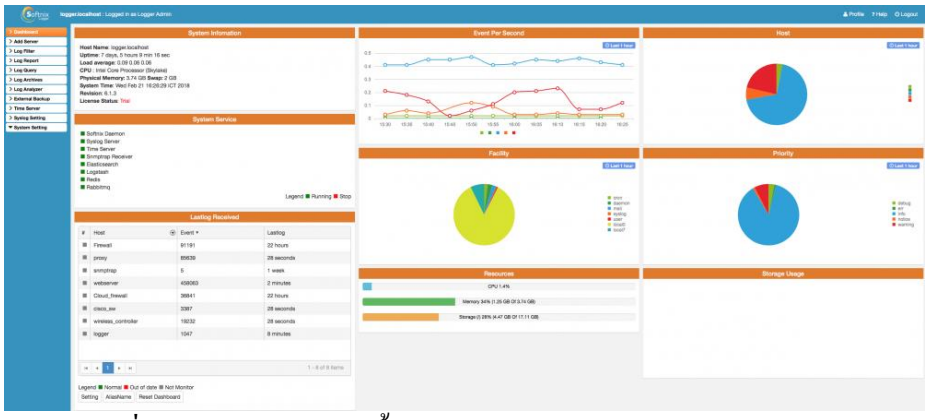
- ตรวจสอบและป้องกันมัลแวร์ ได้ตลอดเวลา โดยไม่รบกวนการใช้งาน
- บล็อคบุคคลที่พยายามแฮ็ค และขโมยข้อมูล (ฟิชชิ่ง)
- กำจัดไวรัสและมัลแวร์ได้อย่างมีประสิทธิภาพ โดยไม่ทำให้ไฟล์เสียหาย
- สามารถกำจัดมัลแวร์ได้หลากหลาย เช่น Worm, Rootkits, Spyware



รูปที่ 4.32 ตัวอย่างการติดตั้งโปรแกรม MalwareBytes

ระบบ System Log

การติดตั้งระบบ Softnix Logger ซึ่งเป็นระบบจัดการ LOGS ในระบบคอมพิวเตอร์แบบรวมศูนย์หรือเรียกว่า CENTRALIZED LOGS MANAGEMENT โดยรองรับการจัดเก็บ LOGS ของระบบคอมพิวเตอร์ SERVER หรืออุปกรณ์เครือข่ายคอมพิวเตอร์อื่นๆ มากมาย โดยรองรับทั้งแบบ AGENT BASED และ AGENT-LESS โดยจัดเก็บ LOGS เริ่มต้นที่ 90 วันและเก็บได้นานสุดถึง 2 ปี ตามพรบ.คอมพิวเตอร์ เพื่อช่วยเหลือผู้ดูแลในการจัดการข้อมูล Log ได้อย่างครอบคลุม ซึ่งการมองเห็นภาพรวมการใช้งานเป็นสิ่งสำคัญ รวมถึงมีเครื่องมือช่วยสามารถค้นหาข้อมูลในเชิงลึกตามความสนใจ



รูปที่ 4.33 ตัวอย่างการติดตั้งโปรแกรม SOFTNIX LOGGER (SLG)

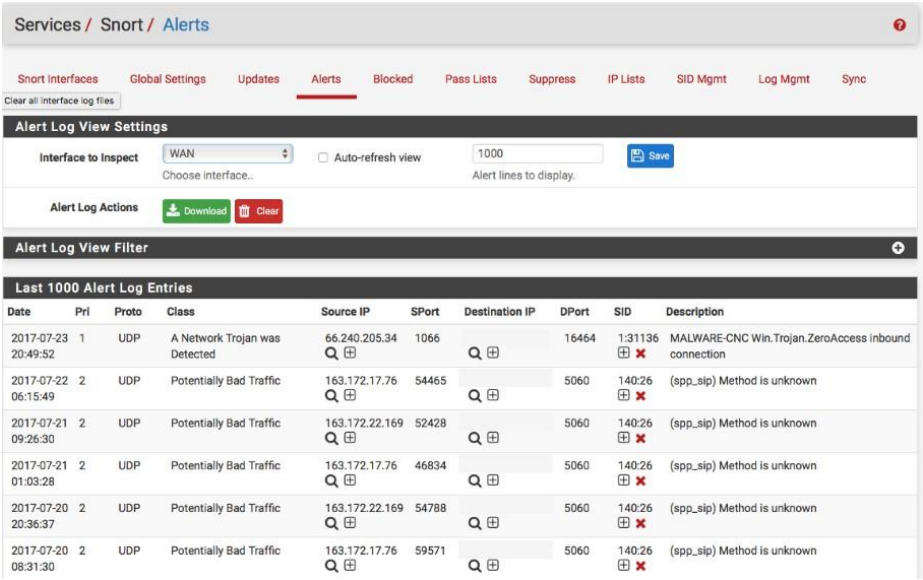
ระบบ Intrusion Detection System (IDS)

การติดตั้งโปรแกรม Snort ซึ่งเป็นโปรแกรมตรวจจับการบุกรุกที่มีขนาดเล็ก มีการใช้ทรัพยากรน้อย ทำให้ไม่สิ้นเปลือง โปรแกรมตรวจจับการบุกรุก Snort จัดเป็นระบบตรวจจับการบุกรุกบนเครือข่ายที่สามารถตรวจจับได้อย่างรวดเร็ว มีการทำงานเป็นแบบ Real Time ตรวจจับการบุกรุกด้วยวิธี Misuse Detection เข้าใจได้ง่ายและมีความยืดหยุ่น เป็นโอเพนซอส (Open Source) ตามข้อตกลงของ General Public License หรือ GNU จึงสามารถนำไปใช้งานได้โดยไม่ต้องเสียค่าใช้จ่ายใดๆ ด้วยคุณสมบัติต่างๆ ทำให้ระบบตรวจจับการบุกรุก Snort จึงกลายเป็นที่นิยมมีการนำไปใช้งานกันอย่างแพร่หลาย

โครงสร้างของระบบตรวจจับการบุกรุก Snort สามารถแบ่งได้เป็น 3 ส่วนด้วยกันคือ

- ส่วนที่ใช้ในการถอดรหัสข้อมูลจากแพ็คเกต (Packet Decoder)
- ส่วนที่ใช้ในการตรวจสอบหาการบุกรุก (Detection Engine)

- ส่วนที่ทำการบันทึกข้อมูลและแจ้งเตือน (Logging/Alerting Subsystem)



รูปที่ 4.34 ตัวอย่างการติดตั้งโปรแกรม Snort

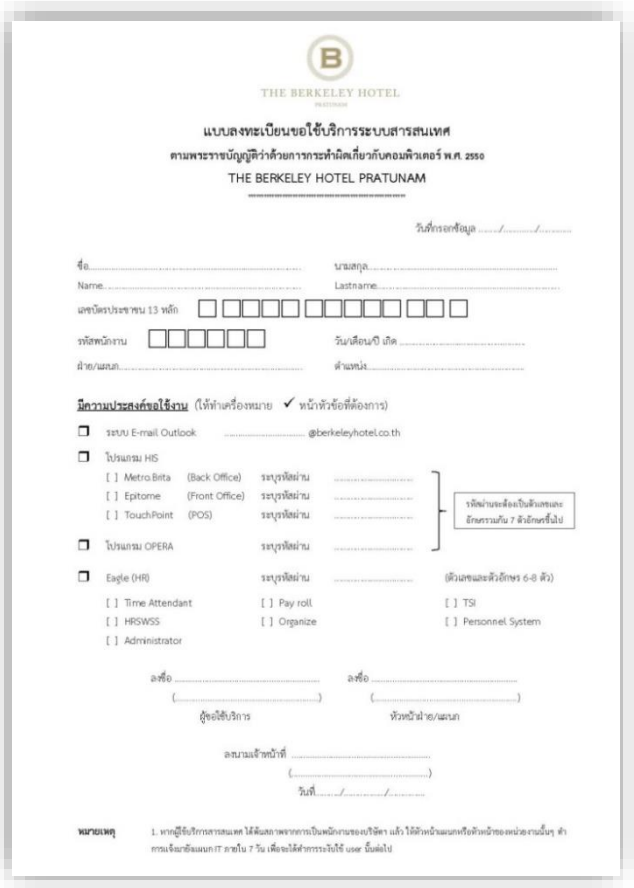
4.2 แนวทางปฏิบัติในการเข้าถึงระบบเทคโนโลยีสารสนเทศ ภายใต้มาตรฐาน ISO/IEC 27001

จากการวิเคราะห์ถึงปัญหาการเข้าถึงระบบเทคโนโลยีสารสนเทศ และได้ทำการวิเคราะห์ช่องว่าง (Gap Analysis) สามารถนำมาจัดทำเป็นแนวทางปฏิบัติในการเข้าใช้งานระบบสารสนเทศเพื่อลดความเสี่ยง โดยมีมาตรการควบคุม แผนปฏิบัติการ ความรับผิดชอบ และการรายงานติดตามผล ดังต่อไปนี้

4.2.1 การลงทะเบียนผู้ใช้งานระบบสารสนเทศ

ความเสี่ยง :	พนักงานไม่มีการลงทะเบียนผู้ใช้งานระบบสารสนเทศ
มาตรการควบคุม :	A9.1.1 นโยบายควบคุมการเข้าถึง
แผนปฏิบัติการ :	การกำหนดให้กรอกแบบฟอร์มเพื่อขอใช้งานระบบสารสนเทศ
ความรับผิดชอบ :	ฝ่ายไอที
รายงานติดตามผล :	ต้องไม่มี User ที่ไม่มีการลงทะเบียนผู้ใช้งาน

แสดงแบบฟอร์มการลงทะเบียนขอใช้บริการระบบสารสนเทศ โดยต้องได้รับการเซ็นต์รับทราบจากหัวหน้าฝ่าย/แผนก และลงนามเจ้าหน้าที่ไอทีที่สร้างบัญชีผู้ใช้งานให้กับพนักงาน



THE BERKELEY HOTEL

แบบลงทะเบียนขอใช้บริการระบบสารสนเทศ

ตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

THE BERKELEY HOTEL PRATUNAM

วันที่กรอกข้อมูล ...../...../.....

ชื่อ..... นามสกุล.....

Name..... Lastname.....

เลขบัตรประชาชน 13 หลัก

รหัสพนักงาน วัน/เดือน/ปี เกิด .....

ฝ่าย/แผนก..... ตำแหน่ง.....

มีความประสงค์ขอใช้งาน (ให้ทำเครื่องหมาย ✓ หน้าหัวข้อที่ต้องการ)

❒ ระบบ E-mail Outlook ..... @berkeleyhotel.co.th

❒ โปรแกรม HIS

[ ] Metro.Brita (Back Office) ระบุรหัสผ่าน .....

[ ] Epitome (Front Office) ระบุรหัสผ่าน .....

[ ] TouchPoint (POS) ระบุรหัสผ่าน .....

รหัสผ่านจะต้องเป็นตัวเลขและอักษรรวมกัน 7 ตัวอักษรขึ้นไป

❒ โปรแกรม OPERA ระบุรหัสผ่าน .....

❒ Eagle (HR) ระบุรหัสผ่าน ..... (ตัวเลขและตัวอักษร 6-8 ตัว)

[ ] Time Attendant [ ] Pay roll [ ] TSI

[ ] HRSWSS [ ] Organize [ ] Personnel System

[ ] Administrator

ลงชื่อ ..... ลงชื่อ .....

(.....) (.....)

ผู้ขอใช้บริการ หัวหน้าฝ่าย/แผนก

ลงนามเจ้าหน้าที่ .....

(.....)

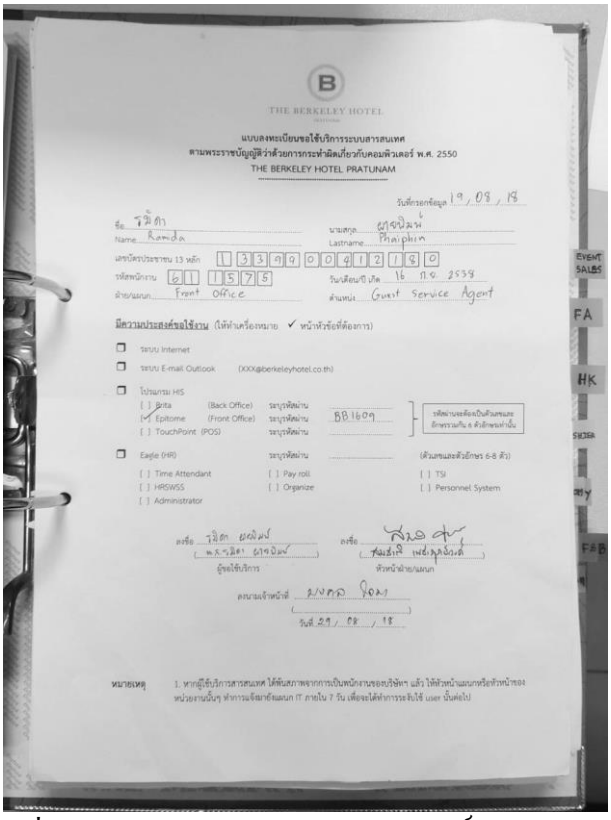
วันที่...../...../.....

หมายเหตุ 1. หากผู้ขอใช้บริการสารสนเทศ ได้พ้นสภาพจากการเป็นพนักงานของบริษัทฯ แล้ว ให้หัวหน้าแผนกหรือหัวหน้าของหน่วยงานนั้นๆ ดำเนินการแจ้งฝ่ายสนเทศ IT ภายใน 7 วัน เพื่อจะได้ดำเนินการระงับใช้ user ชั่วคราวต่อไป

รูปที่ 4.35 แบบฟอร์มลงทะเบียนขอใช้บริการระบบสารสนเทศ

ความเสี่ยง :	- พนักงานขอเข้าใช้งานสิทธิ์ที่ไม่มีสิทธิ์ โดยที่ไม่มีการอนุมัติจากหัวหน้างาน - พนักงานที่ออกไปแล้วยังมีสิทธิ์ค้างอยู่ในระบบสารสนเทศ
มาตรการควบคุม :	A9.2.2 การจัดการสิทธิ์การเข้าถึงของผู้ใช้งาน A9.2.5 การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน
แผนปฏิบัติการ :	- ผู้ที่จะได้สิทธิ์การเข้าถึงระบบต้องได้รับอนุญาตจากหัวหน้างานเป็นลายลักษณ์อักษร - นำสิทธิ์ที่มีอยู่ในระบบมาทบทวนตรวจสอบอย่างไตรมาสละ 1 ครั้ง
ความรับผิดชอบ :	ฝ่ายไอที
รายงานติดตามผล :	- เจ้าหน้าที่ต้องให้สิทธิ์กับพนักงาน เมื่อได้รับเอกสารเป็นลายลักษณ์อักษรเท่านั้น - การทบทวนสิทธิ์ ต้องไม่มีผู้ใช้งานที่ไม่มีสิทธิ์ในการเข้าถึงระบบ และไม่มีพนักงานที่ออกไปแล้ว

แสดงการทบทวนเอกสารสิทธิ์ของพนักงาน โดยต้องได้รับอนุญาตจากหัวหน้างานเป็นลายลักษณ์อักษรเท่านั้น และลงนามเจ้าหน้าที่ไอทีที่สร้างบัญชีผู้ใช้งานให้กับพนักงาน


THE BERKELEY HOTEL

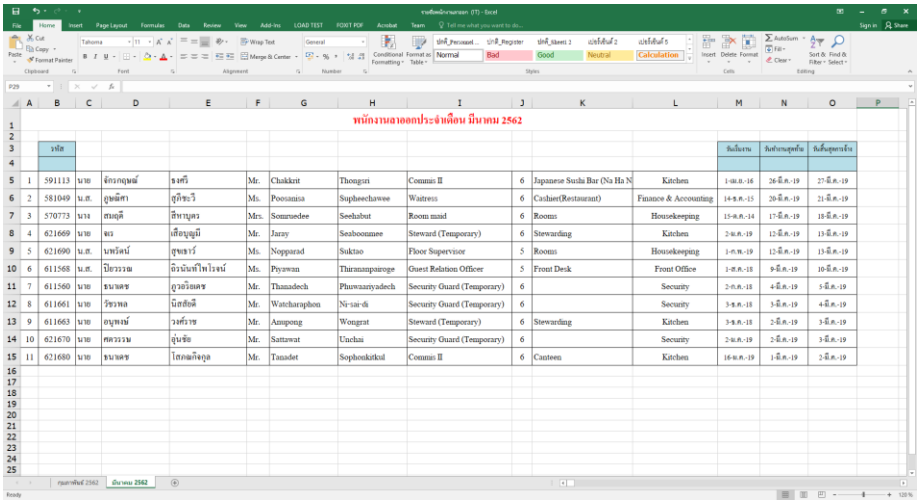
แบบลงทะเบียนขอใช้บริการระบบสารสนเทศ
ตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550
THE BERKELEY HOTEL PRATUNAM

รูปที่ 4.36 ตัวอย่างการทบทวนเอกสารสิทธิ์ของพนักงาน

4.2.2 การถอดถอนสิทธิ์ผู้ใช้งานระบบสารสนเทศ

ความเสี่ยง :	- พนักงานใหม่ ใช้ Username และ Password ของพนักงานเก่าในการเข้าใช้งานระบบสารสนเทศ - เมื่อมีพนักงานออกแล้ว ไม่ถอดถอนสิทธิ์ในการเข้าถึงระบบทันที แต่ยังสามารถเข้าระบบได้อยู่
มาตรการควบคุม :	A9.2.1 การลงทะเบียนและถอดถอนสิทธิ์ A9.2.6 การถอดถอนหรือปรับปรุงสิทธิ์การเข้าถึง
แผนปฏิบัติการ :	HR ต้องแจ้งข้อมูลพนักงานที่ออกส่งต่อให้ฝ่ายไอทีทำการถอดสิทธิ์ออกจากระบบทันที
ความรับผิดชอบ :	ฝ่าย HR และฝ่ายไอที
รายงานติดตามผล :	สุ่มตรวจข้อมูลพนักงานที่ออกแล้ว ต้องไม่มีในระบบต่างๆ ขององค์กร

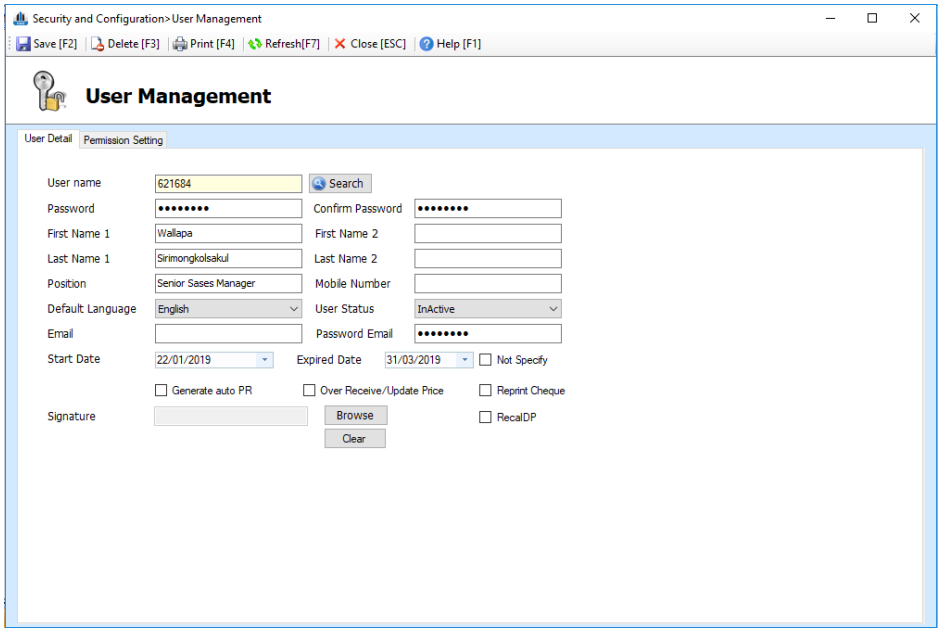
แสดงรายชื่อพนักงานที่ออกแล้วจากฝ่าย HR ที่ส่งให้ฝ่ายไอที เพื่อทำการถอดสิทธิ์ออกจากระบบสารสนเทศ เพื่อให้เห็นถึงพนักงานที่ออกแล้วต้องอยู่ในสถานะ Disable / Inactive ในระบบสารสนเทศ



พนักงานลาออกประจำเดือน มีนาคม 2562

	บริษัท														
1	591113	นาย	จักรกฤษณ์	ธงศรี	Mr.	Chakkrit	Thongsri	Commis II	6	Japanese Sushi Bar (Na Ha N	Kitchen	1-เม.ย.-16	26-มี.ค.-19	27-มี.ค.-19
2	581049	น.ส.	อุษณีศา	สุภีชะวี	Ms.	Poosanisa	Supheechawee	Waitress	6	Cashier(Restaurant)	Finance & Accounting	14-ธ.ค.-15	20-มี.ค.-19	21-มี.ค.-19
3	570773	นาง	สมยุติ	สีหาบุตร	Mrs.	Somruedee	Seehabut	Room maid	6	Rooms	Housekeeping	15-ต.ค.-14	17-มี.ค.-19	18-มี.ค.-19
4	621669	นาย	จะ	เสือบุญมี	Mr.	Jaray	Seaboonmee	Steward (Temporary)	6	Stewarding	Kitchen	2-ม.ค.-19	12-มี.ค.-19	13-มี.ค.-19
5	621690	น.ส.	นพรัตน์	สุขธาร์	Ms.	Nopparad	Suktao	Floor Supervisor	5	Rooms	Housekeeping	1-ก.พ.-19	12-มี.ค.-19	13-มี.ค.-19
6	611568	น.ส.	ปิยวรรณ	ธีรานันทไพโรจน์	Ms.	Piyawan	Thiranunpairoge	Guest Relation Officer	5	Front Desk	Front Office	1-ส.ค.-18	9-มี.ค.-19	10-มี.ค.-19
7	611560	นาย	ธนาเดช	ภูวอัธเดช	Mr.	Thanadech	Phuwaanyadech	Security Guard (Temporary)	6		Security	2-ก.ค.-18	4-มี.ค.-19	5-มี.ค.-19
8	611661	นาย	วัธรพล	นิสสัยดี	Mr.	Watcharaphon	Ni-sai-di	Security Guard (Temporary)	6		Security	3-ธ.ค.-18	3-มี.ค.-19	4-มี.ค.-19
9	611663	นาย	อนุพงษ์	วงศ์วาช	Mr.	Anupong	Wongrat	Steward (Temporary)	6	Stewarding	Kitchen	3-ธ.ค.-18	2-มี.ค.-19	3-มี.ค.-19
10	621670	นาย	ศตวรรษ	อุ่นชัย	Mr.	Sattawat	Unchai	Security Guard (Temporary)	6		Security	2-ม.ค.-19	2-มี.ค.-19	3-มี.ค.-19
11	621680	นาย	ธนาเดช	โสภณกิจกุล	Mr.	Tanadet	Sophonkitkul	Commis II	6	Canteen	Kitchen	16-พ.ค.-19	1-มี.ค.-19	2-มี.ค.-19

รูปที่ 4.37 ตัวอย่างรายชื่อพนักงานที่ออกแล้วที่ฝ่าย HR ส่งให้ฝ่ายไอที

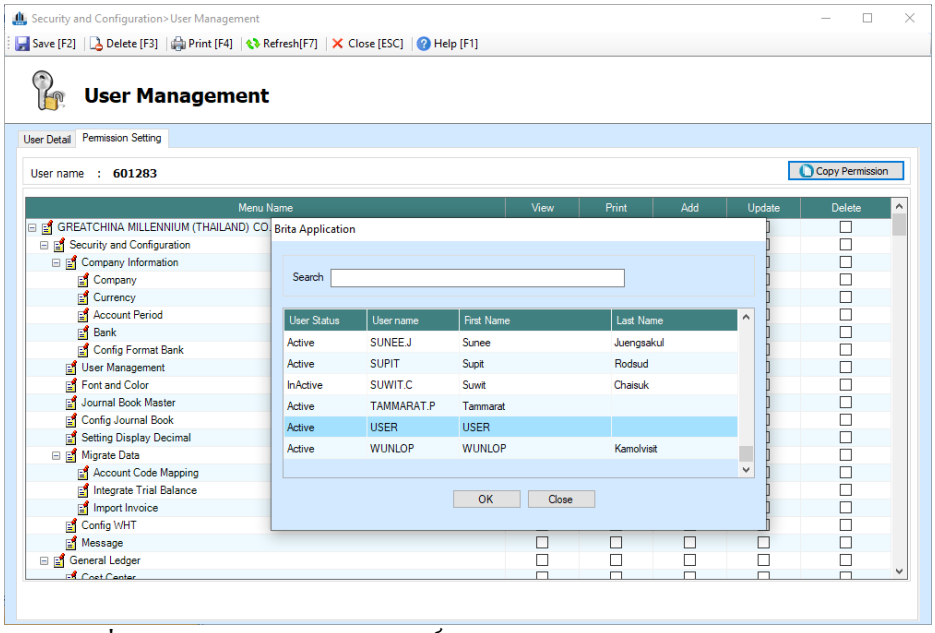


รูปที่ 4.38 ตัวอย่างพนักงานที่ออกแล้วต้องอยู่สถานะ Disable / Inactive

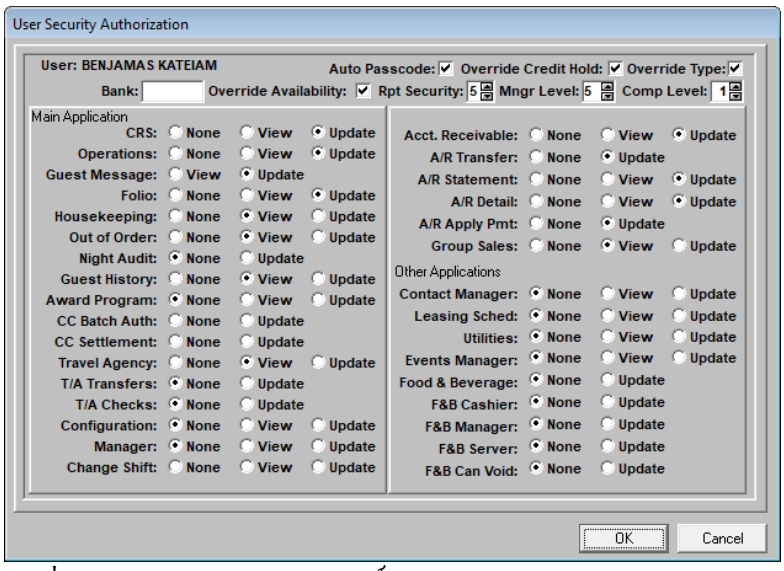
4.2.3 การบริหารจัดการสิทธิ์ในการเข้าถึงระบบสารสนเทศ

ความเสี่ยง :	- ไม่มีการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศแต่ละชนิด - ระบบสารสนเทศถูกเข้าถึงโดยมีสิทธิ์การใช้งานเกินความจำเป็น
มาตรการควบคุม :	A9.1.1 นโยบายควบคุมการเข้าถึง A9.2.3 การบริหารจัดการสิทธิ์การเข้าถึงตามระดับสิทธิ์
แผนปฏิบัติการ :	- การบริหารจัดการสิทธิ์ผู้ใช้งานในการเข้าถึงสารสนเทศแต่ละชนิด โดยการสร้างแบบฟอร์มระดับสิทธิ์ตามตำแหน่งงานของพนักงาน - กำหนด PERMISSION ให้กับพนักงานตรงกับที่หัวหน้างานอนุมัติ
ความรับผิดชอบ :	ฝ่ายไอที
รายงานติดตามผล :	ตรวจสอบสิทธิ์ PERMISSION ผู้ใช้งานในระบบสารสนเทศแต่ละชนิดให้ถูกต้องตรงตามแบบฟอร์มระดับสิทธิ์ตามตำแหน่งงานของพนักงาน

แสดงตัวอย่างการจัดการสิทธิ์ผู้ใช้งานในการเข้าถึงระบบสารสนเทศแต่ละชนิด อาทิ โปรแกรม Metro.Brita และ Epitome โดยการกำหนดระดับสิทธิ์ในการเข้าถึงตามตำแหน่งงานของพนักงาน



รูปที่ 4.39 ตัวอย่างการจัดการสิทธิ์ผู้ใช้งานสำหรับโปรแกรม Metro.Brita

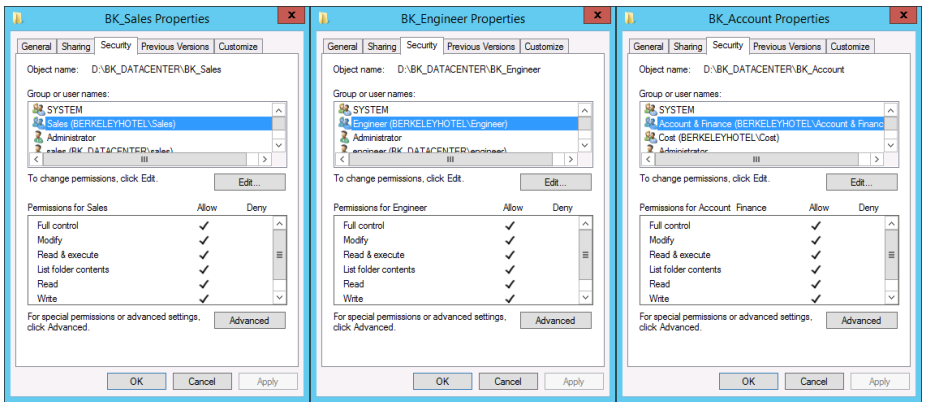


รูปที่ 4.40 ตัวอย่างการจัดการสิทธิ์ผู้ใช้งานสำหรับโปรแกรม Epitome

4.2.4 การบริหารจัดการสิทธิ์ในการเข้าถึงดาต้าเซ็นเตอร์

ความเสี่ยง :	มีบางโฟลเดอร์ในดาต้าเซ็นเตอร์ สามารถเข้าถึงได้ Everyone โดยไม่ป้องกันการเข้าถึงสำหรับแต่ละแผนก
มาตรการควบคุม :	9.4.1 การจำกัดการเข้าถึงสารสนเทศ
แผนปฏิบัติการ :	กำหนด PERMISSION ของโฟลเดอร์ในดาต้าเซ็นเตอร์ ให้ตรงตามแต่ละแผนก
ความรับผิดชอบ :	ฝ่ายไอที
รายงานติดตามผล :	ต้องไม่มีโฟลเดอร์ในดาต้าเซ็นเตอร์ที่มีสิทธิ์ Everyone และ PERMISSION ของโฟลเดอร์ต้องตรงตามแต่ละแผนก

แสดงการกำหนด PERMISSION สำหรับโฟลเดอร์ในดาต้าเซ็นเตอร์สำหรับแต่ละแผนกในองค์กร

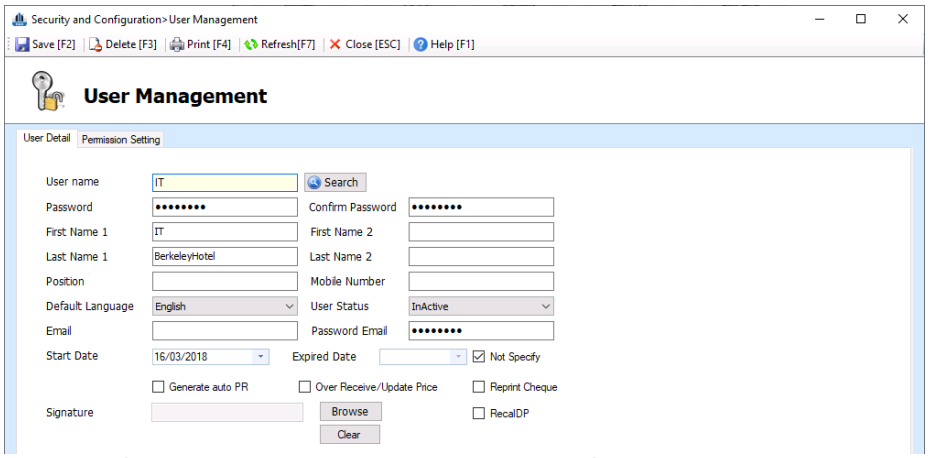


รูปที่ 4.41 ตัวอย่างโฟลเดอร์ในดาต้าเซ็นเตอร์สำหรับแต่ละแผนก

4.2.5 การควบคุมการใช้งานสิทธิ์ Administrator

ความเสี่ยง :	ผู้ดูแลระบบมีการใช้งาน Account ที่ใช้เป็น Admin ร่วมกัน
มาตรการควบคุม :	A9.2.3 การบริหารจัดการสิทธิ์การเข้าถึงตามระดับสิทธิ์
แผนปฏิบัติการ :	มีมาตรการไม่ใช้งาน Account ที่ใช้เป็น Admin ร่วมกัน โดยปิดผลึกไว้ นำมาใช้งานเมื่อมีความจำเป็นเท่านั้น และต้องได้รับการอนุมัติจากหัวหน้างานเท่านั้น
ความรับผิดชอบ :	ฝ่ายไอที
รายงานติดตามผล :	มีการตรวจสอบ Log การใช้งาน Account ที่ใช้เป็น Admin

แสดงสถานะการ InActive ของ Account ที่ใช้เป็น Admin ร่วมกัน ในโปรแกรม Metro.Brita โดยสามารถนำมาใช้งานเมื่อมีความจำเป็น และต้องได้รับการอนุมัติจากหัวหน้างานเท่านั้น

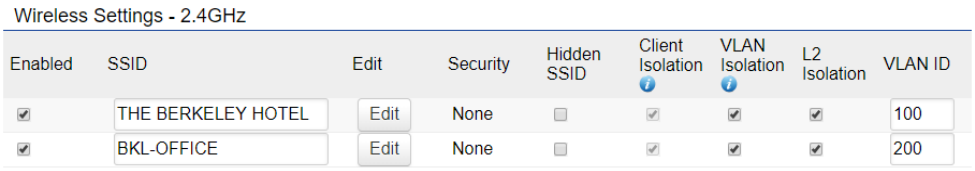


รูปที่ 4.42 แสดงการ InActive ของ Account ที่ใช้เป็น Admin ร่วมกัน

4.2.6 การควบคุมการเข้าถึงเครือข่ายไร้สาย

ความเสี่ยง :	เครื่องจากภายนอกสามารถเข้าถึงเครือข่ายภายในได้ด้วยระบบ Wi-Fi เมื่อเข้ามาแล้วสามารถใช้เครือข่ายเดียวกัน
มาตรการควบคุม :	A9.1.2 การเข้าถึงเครือข่ายและการบริการเครือข่าย
แผนปฏิบัติการ :	แยกเครือข่าย Wi-Fi ออกจากเครือข่ายภายใน หรือกำหนดสิทธิ์การเข้าถึงของ Wi-Fi
ความรับผิดชอบ :	ฝ่ายไอที
รายงานติดตามผล :	การเข้าถึงระบบ Wi-Fi ต้องแบ่งแยกเครือข่ายกับเครือข่ายภายในขององค์กร

แสดงการแบ่งแยกเครือข่ายสำหรับระบบ Wi-Fi โดยการแบ่งแยก SSID เป็นชื่อว่า BKL-OFFICE เพื่อใช้ในการเชื่อมต่อสัญญาณ Wi-Fi จากอุปกรณ์ต่างๆ

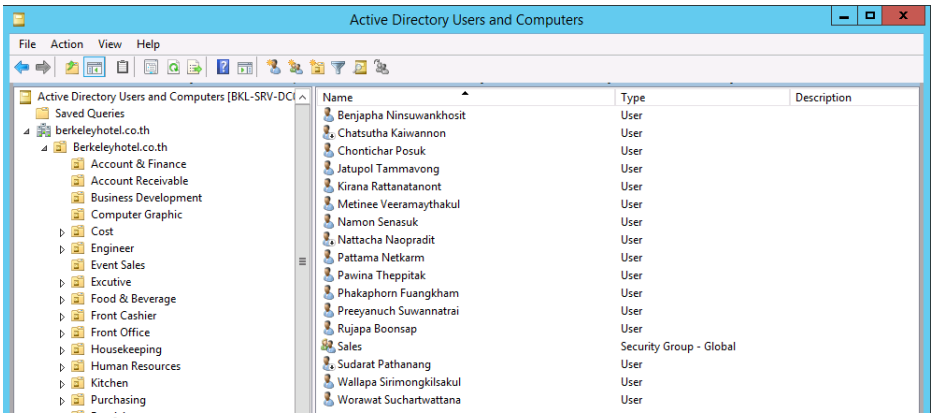


รูปที่ 4.43 ตัวอย่างการแบ่งแยก SSID สำหรับเครือข่ายไร้สาย

4.2.7 การกำหนด Policy ในการเข้าถึงระบบระบบคอมพิวเตอร์

ความเสี่ยง :	คอมพิวเตอร์สามารถเข้าถึงได้ง่าย โดยไม่มีการ Login เข้าใช้งาน
มาตรการควบคุม :	A9.4.2 ขั้นตอนปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย
แผนปฏิบัติการ :	- นำคอมพิวเตอร์ทุกเครื่องเชื่อมต่อกับระบบ Active Directory - กำหนด policy การเข้าถึงระบบเครือข่าย ต้องพิสูจน์ตัวตนก่อนเท่านั้น
ความรับผิดชอบ :	ฝ่ายไอที
รายงานติดตามผล :	- ตรวจสอบคอมพิวเตอร์ทุกเครื่องต้องเชื่อมต่อกับระบบ Active Directory - ตรวจสอบแบบฟอร์มขอใช้งานระบบสารสนเทศ กับ User Account ในระบบ Active Directory เพื่อพิสูจน์ตัวตนก่อนเข้าใช้งานเครื่องคอมพิวเตอร์

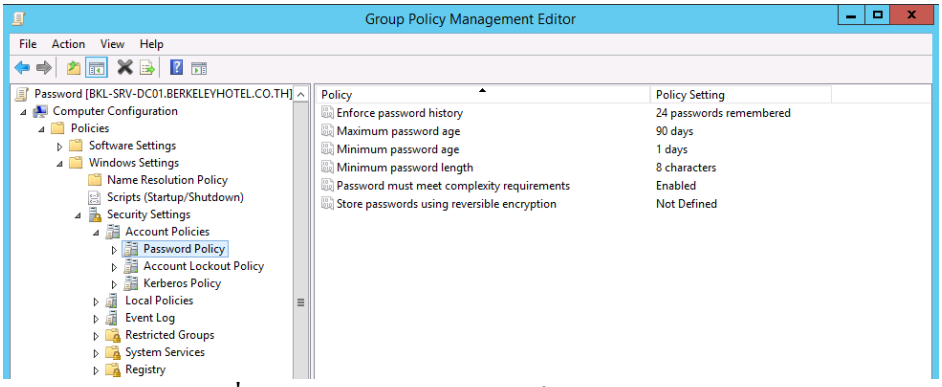
แสดงการจัดการ User Account ของผู้ใช้งานในแต่ละแผนก ในระบบ Active Directory เพื่อพิสูจน์ตัวตนก่อนเข้าใช้งานเครื่องคอมพิวเตอร์ โดยการสร้างออบเจ็กต์ของ Organization Unit (OU) ในระบบ AD ตามแต่ละฝ่ายในองค์กร



รูปที่ 4.44 ตัวอย่างการจัดการ User Account ของผู้ใช้งานในแต่ละแผนก

ความเสี่ยง :	รหัสผ่านเข้าสู่ระบบคอมพิวเตอร์ง่ายเกินไปหรือไม่เป็นความลับ
มาตรการควบคุม :	A9.4.3 ระบบบริหารจัดการรหัสผ่าน
แผนปฏิบัติการ :	มีระบบบริหารจัดการรหัสผ่านอย่างรัดกุม โดยกำหนดเงื่อนไขการตั้งรหัสผ่าน และเวลาการเปลี่ยนรหัสผ่านอัตโนมัติ ทุกๆ 90 วัน
ความรับผิดชอบ :	ฝ่ายไอที
รายงานติดตามผล :	ระบบ Policy ต้องมีการกำหนดเงื่อนไขการตั้งรหัสผ่าน ตามนโยบายบริหารจัดการรหัสผ่าน

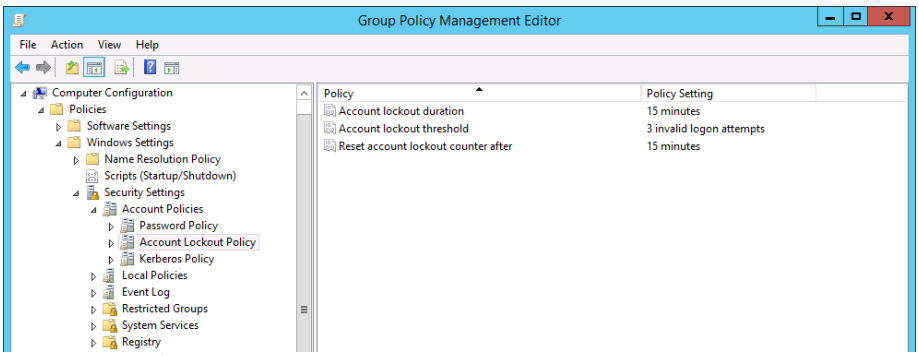
แสดงการกำหนด Policy ใน GPO เพื่อจัดการรหัสผ่านอย่างรัดกุม อาทิ รหัสผ่านควรมีความยาวอย่างน้อย 8 ตัวอักษร ประกอบด้วยตัวพิมพ์ใหญ่อย่างน้อย 1 ตัว และเครื่องหมายหรืออักขระพิเศษอย่างน้อย 1 ตัว และกำหนดระยะเวลาให้เปลี่ยนรหัสผ่านใหม่ทุกๆ 90 วัน



รูปที่ 4.45 ตัวอย่างการกำหนดเป็น Policy ใน GPO

ความเสี่ยง :	ไม่มีการป้องกันการ Login ผิดบ่อยๆ โดยการล็อก User ใช้งาน
มาตรการควบคุม :	A9.4.2 ขั้นตอนปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย
แผนปฏิบัติการ :	หากมีการล็อคอินผิดเกิน 3 ครั้ง ให้ตั้งระบบให้ทำการรอ 15 นาที หรือต้องแจ้งการปลดล็อคจาก admin เท่านั้น
ความรับผิดชอบ :	ฝ่ายไอที
รายงานติดตามผล :	ตรวจสอบระบบ Policy ต้องมีการป้องกันการ BRUTE FORCE

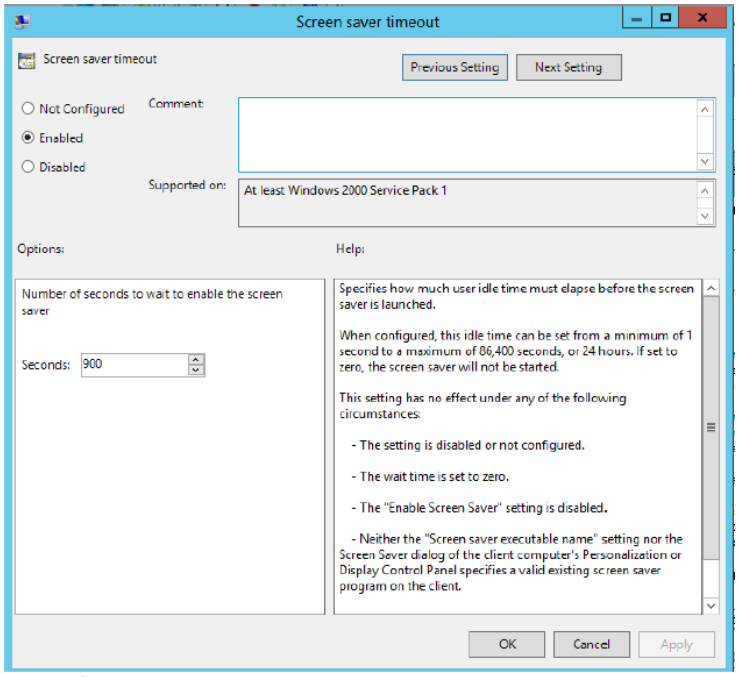
แสดงการกำหนด Policy ป้องกันการ Brute Force ในกรณีที่มีการล็อคอินผิดเกิน 3 ครั้ง โดยตั้งระบบให้ทำการรอ15 นาที หรือต้องแจ้งการปลดล็อคจาก admin เท่านั้น เพื่อป้องกันการเข้าถึงคอมพิวเตอร์จากบุคคลอื่น



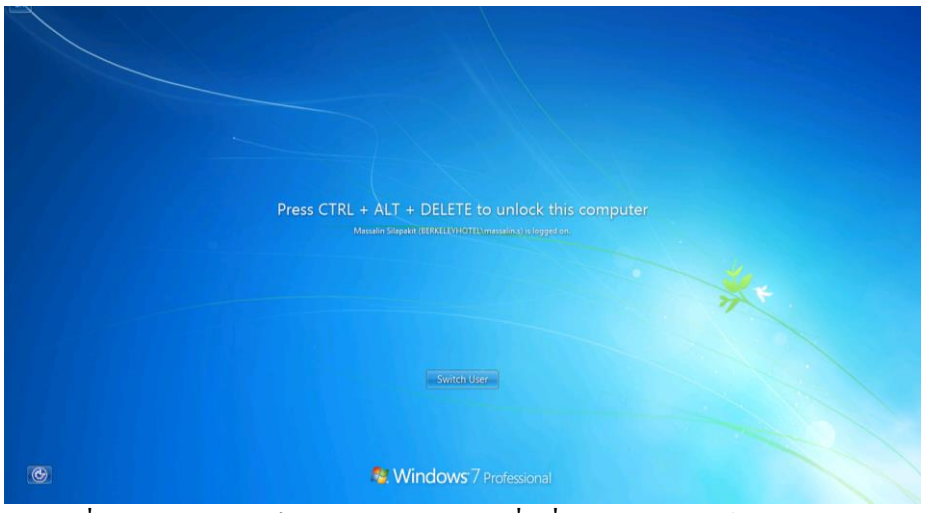
รูปที่ 4.46 ตัวอย่างการกำหนด Policy ป้องกันการ Brute Force

ความเสี่ยง :	ผู้ใช้งานไม่ได้ Log out ออกจาก windows หลังจากใช้งานเสร็จแล้ว
มาตรการควบคุม :	A9.4.2 ขั้นตอนปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย
แผนปฏิบัติการ :	ตั้งระบบ Log out อัตโนมัติ หลังจากไม่มีการใช้งานเกิน 15 นาที
ความรับผิดชอบ :	ฝ่ายไอที
รายงานติดตามผล :	ตรวจสอบระบบ Policy ต้องมีการล็อคหน้าจออัตโนมัติ

แสดงการกำหนด Policy ในการล็อคหน้าจออัตโนมัติ หลังจากไม่มีการใช้งานเกิน 15 นาที เพื่อป้องกันการเข้าใช้งานจากบุคคลอื่น ในกรณีที่ไม่อยู่ที่โต๊ะทำงาน



รูปที่ 4.47 แสดงกำหนด Policy ในการล็อคหน้าจออัตโนมัติ

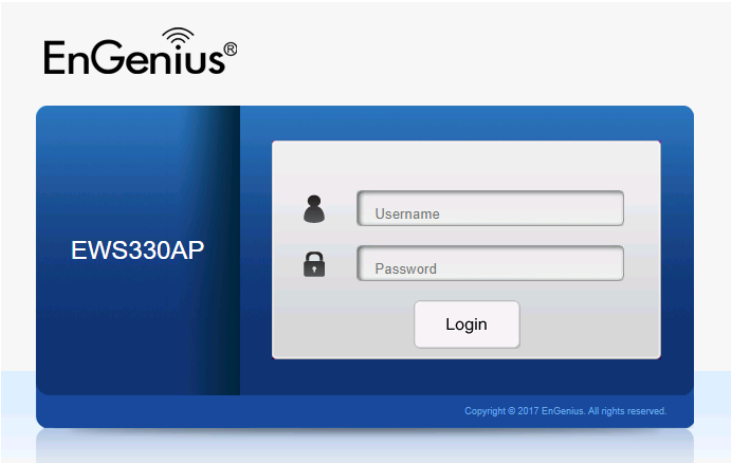


รูปที่ 4.48 แสดงการล็อคหน้าจออัตโนมัติที่เครื่องคอมพิวเตอร์ของพนักงาน

4.2.8 การควบคุมการเข้าถึงอุปกรณ์เครือข่าย

ความเสี่ยง :	อุปกรณ์หยุดหรือไม่สามารถทำงานได้เต็มประสิทธิภาพ เนื่องจากถูกเข้าถึงและเปลี่ยนแปลงการตั้งค่าจากผู้ไม่มีสิทธิ์
มาตรการควบคุม :	A11.2.1 การจัดตั้งและป้องกันอุปกรณ์
แผนปฏิบัติการ :	ป้องกันการเข้าถึงอุปกรณ์ โดยการกำหนด Password ที่คาดเดาได้ยาก หรือควบคุมการเข้าถึงอุปกรณ์ผ่าน Controller
ความรับผิดชอบ :	ฝ่ายไอที
รายงานติดตามผล :	ตรวจสอบ Log และสถานะการทำงานของอุปกรณ์ทุกๆ สัปดาห์

แสดงการกำหนด Password ที่อุปกรณ์ Access Point โดยไม่ใช่ Username และ Password ที่เป็น Default อาจเกิดความเสี่ยงจากผู้ไม่หวังดี ที่สามารถเข้ามาแก้ไขการตั้งค่าต่างๆ ของอุปกรณ์

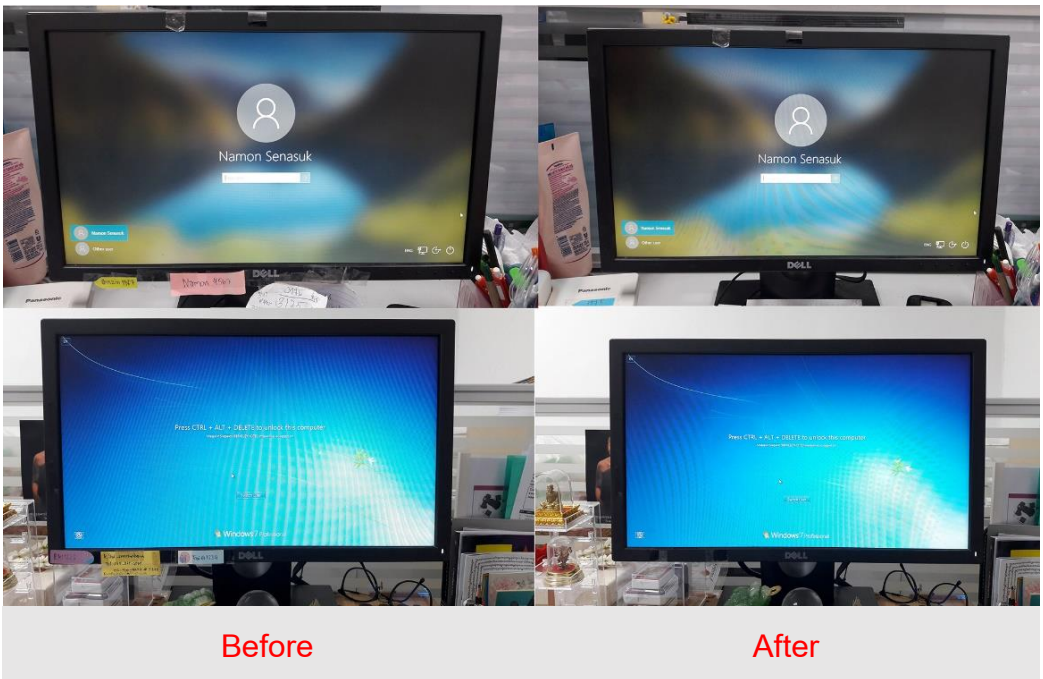


รูปที่ 4.49 แสดงการกำหนด Password ที่อุปกรณ์ Access Point

4.2.9 การควบคุมการติดรหัสผ่านไว้ที่หน้าจอคอมพิวเตอร์หรือบนโต๊ะทำงาน

ความเสี่ยง :	พนักงานติดรหัสผ่านของระบบสารสนเทศไว้ที่หน้าจอคอมพิวเตอร์หรือติดไว้บนโต๊ะทำงาน
มาตรการควบคุม :	A11.2.9 นโยบายโต๊ะทำงานปลอดเอกสารสำคัญ และนโยบายการป้องกันหน้าจอคอมพิวเตอร์
แผนปฏิบัติการ :	กำหนดนโยบายในการตั้งรหัสผ่าน และทำประกาศถึงภัยอันตรายของการโดนโจมตีรหัสผ่านจากบุคคลอื่น
ความรับผิดชอบ :	ฝ่ายไอที
รายงานติดตามผล :	สุ่มตรวจพาสเวิร์ดที่จอคอมพิวเตอร์หรือบนโต๊ะทำงานของพนักงาน 2 คนต่อแผนก หากพบเจอแนะนำให้นำพาสเวิร์ดที่ติดไว้ออกจากจอคอมพิวเตอร์

แสดงตัวอย่างคอมพิวเตอร์ของพนักงานที่ติดพาสเวิร์ดไว้บนจอคอมพิวเตอร์ และหลังจากการนำให้นำพาสเวิร์ดที่ติดไว้ออกจากจอคอมพิวเตอร์แล้ว เพื่อป้องกันการเข้าถึงระบบคอมพิวเตอร์และระบบสารสนเทศต่างๆ จากบุคคลอื่น

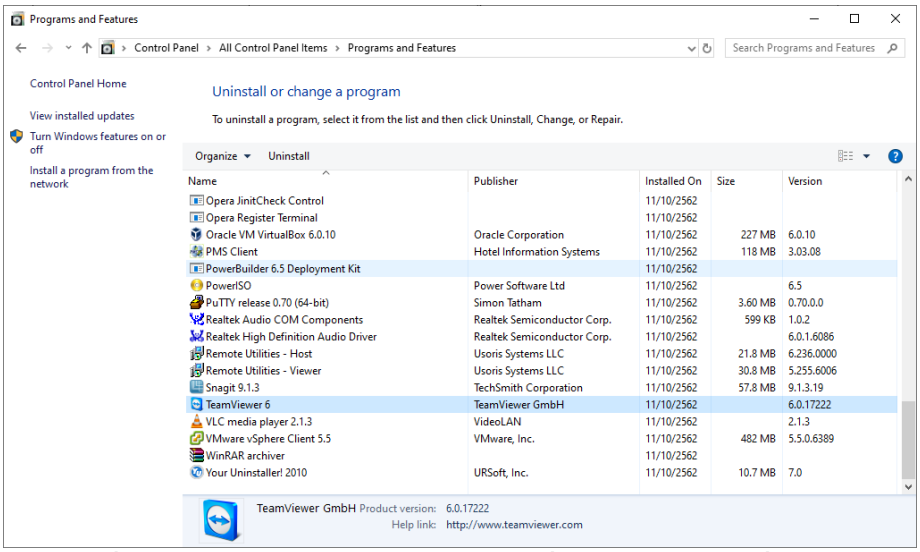


รูปที่ 4.50 ตัวอย่างก่อนติดพาสเวิร์ดและหลังจากนำพาสเวิร์ดที่ติดไว้ออกจากจอคอมพิวเตอร์

4.2.10 การควบคุมการเข้าถึงเครือข่ายภายในจากระยะไกล

ความเสี่ยง :	พนักงานเข้าถึงระบบงานของเครือข่ายภายในจากระยะไกลได้โดยไม่มีสิทธิ์เข้าถึง
มาตรการควบคุม :	A.6.2.2 การปฏิบัติงานจากระยะไกล
แผนปฏิบัติการ :	ลบโปรแกรม Remote จากระยะไกลทุกชนิดออกจากเครื่องคอมพิวเตอร์ของพนักงาน หากต้องการใช้งานต้องกรอกแบบฟอร์มขอใช้งานโปรแกรม Remote หรือติดตั้งระบบ VPN เพื่อเชื่อมต่อกับเครือข่ายภายใน
ความรับผิดชอบ :	ฝ่ายไอที
รายงานติดตามผล :	สุ่มตรวจสอบโปรแกรม Remote จากเครื่องคอมพิวเตอร์ของพนักงาน หากพบเจอ ต้องตรวจสอบกับแบบฟอร์มขอใช้บริการ

แสดงโปรแกรมรีโมทระยะไกลที่ต้องลบออกจากเครื่องคอมพิวเตอร์ของพนักงาน อาทิ โปรแกรม TeamViwer, Anydesk



รูปที่ 4.51 แสดงโปรแกรมรีโมทระยะไกลที่ต้องลบออกจากเครื่องผู้ใช้

4.2.11 การควบคุมการเข้าออกห้องเซิร์ฟเวอร์

ความเสี่ยง :	ห้องเซิร์ฟเวอร์ไม่มีการบันทึกการเข้าออกของผู้ใช้งาน
มาตรการควบคุม :	A11.1.2 การควบคุมการเข้าออกทางกายภาพ
แผนปฏิบัติการ :	ติดตั้งเครื่องสแกนนิ้ว กล้องวงจรปิด และบันทึกการเข้าออกห้องเซิร์ฟเวอร์
ความรับผิดชอบ :	ฝ่ายไอที และฝ่าย Engineer

รายงานติดตามผล :	เครื่องสแกนนิ้วห้องเซิร์ฟเวอร์เข้าได้แต่พนักงานไอที และต้องทำการบันทึกรายละเอียดการปฏิบัติงานและลงลายมือชื่อทุกครั้ง

แสดงตัวอย่างการติดตั้ง Finger Scan หน้าห้องเซิร์ฟเวอร์ เพื่อบันทึกการเข้าออกของผู้ใช้งาน ตัวอย่างการติดตั้งกล้องวงจรปิด CCTV เพื่อบันทึกเหตุการณ์ต่างๆ ในห้องเซิร์ฟเวอร์ และแบบฟอร์มบันทึกการเข้าออกห้องเซิร์ฟเวอร์ โดยต้องทำการบันทึกรายละเอียดการปฏิบัติงานและลงลายมือชื่อทุกครั้ง

รูปที่ 4.52 แสดงการติดตั้ง Finger Scan และกล้องวงจรปิด CCTV

Server Visitor Logbook

Year	
Month	

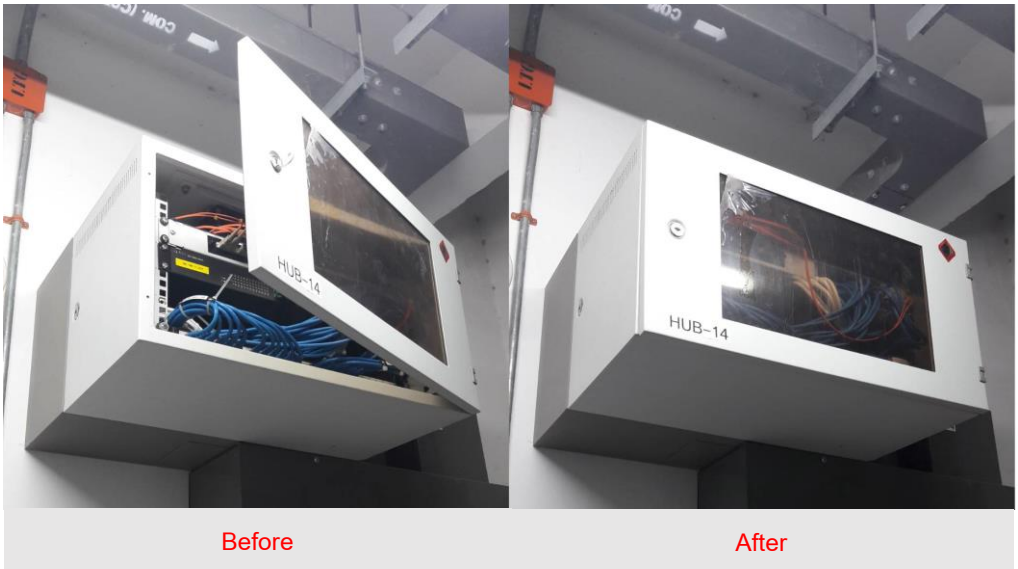
Date	Time	Surname	Lastname	Company	Description

รูปที่ 4.53 แบบฟอร์มบันทึกการเข้าออกห้องเซิร์ฟเวอร์

4.2.12 การควบคุมการเข้าถึงตู้ Switch แต่ละตามชั้น

ความเสี่ยง :	ตู้แร็ค Switch ตามแต่ละชั้นไม่มีการล็อคหรือมีกุญแจคาไว้
มาตรการควบคุม :	A11.2.1 การจัดตั้งและป้องกันอุปกรณ์
แผนปฏิบัติการ :	ล็อคตู้แร็ค Switch ทุกๆ ชั้น
ความรับผิดชอบ :	ฝ่ายไอที
รายงานติดตามผล :	ตรวจสอบการล็อคตู้แร็ค Switch ทุกๆ ชั้น และนำกุญแจมาจัดเก็บไว้

แสดงการล็อคตู้แร็ค Switch ตามชั้นต่างๆ เพื่อป้องกันการเข้าถึงอุปกรณ์ Switch เปลี่ยนแปลงการตั้งค่า และโจมตีระบบเครือข่ายจากผู้ไม่หวังดี

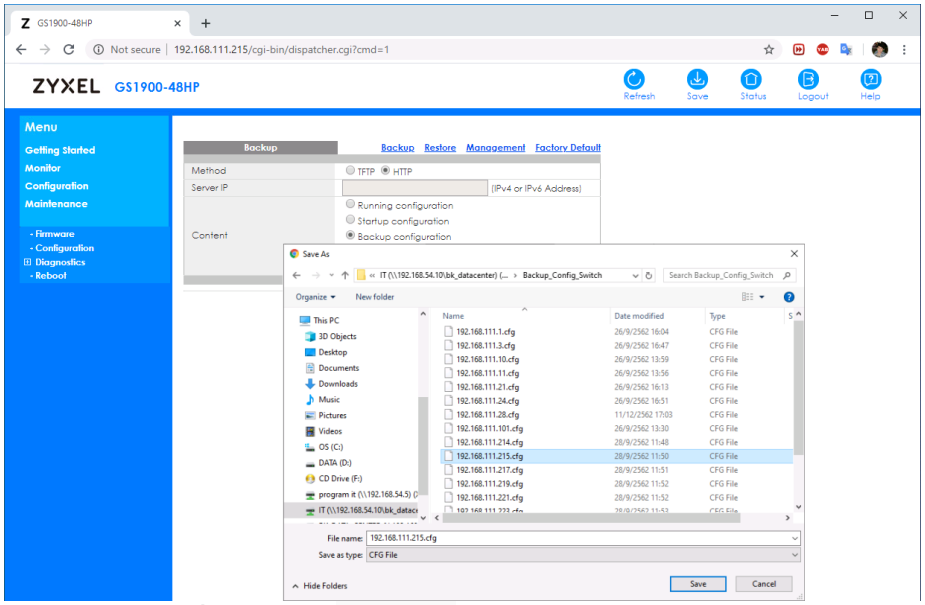


รูปที่ 4.54 แสดงการล็อคตู้แร็ค Switch ตามชั้นต่างๆ

4.2.13 การควบคุมการเปลี่ยนแปลงอุปกรณ์เครือข่าย

ความเสี่ยง :	ความผิดพลาดของการ Config อุปกรณ์เครือข่าย ทำให้ระบบทำงานผิดพลาดหรือหยุดให้บริการ
มาตรการควบคุม :	A.12.1.2 การบริหารจัดการการเปลี่ยนแปลง
แผนปฏิบัติการ :	การสำรอง Config ของอุปกรณ์เครือข่ายไว้ โดยต้องสามารถทำการ Restore Configuration กลับคืนได้
ความรับผิดชอบ :	ฝ่ายไอที
รายงานติดตามผล :	การเปลี่ยนแปลงค่า Config ต้องทำ Change Management ก่อน เพื่อป้องกันความผิดพลาด

แสดงการสำรอง Config ของอุปกรณ์ Switch โดยจัดเก็บเพื่อทำการ Restore Configuration ในกรณีที่มีการเปลี่ยนแปลงค่าที่ผิดพลาดของผู้ดูแลระบบ

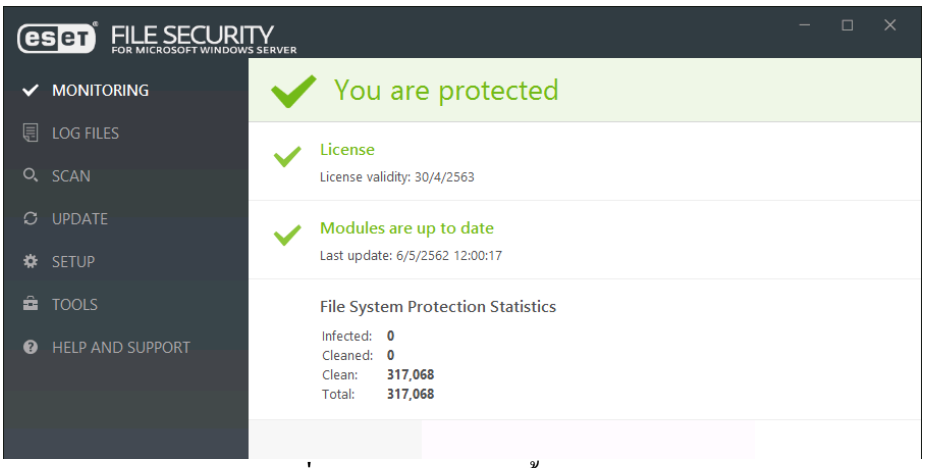


รูปที่ 4.55 แสดงการสำรอง Config ของอุปกรณ์ Switch

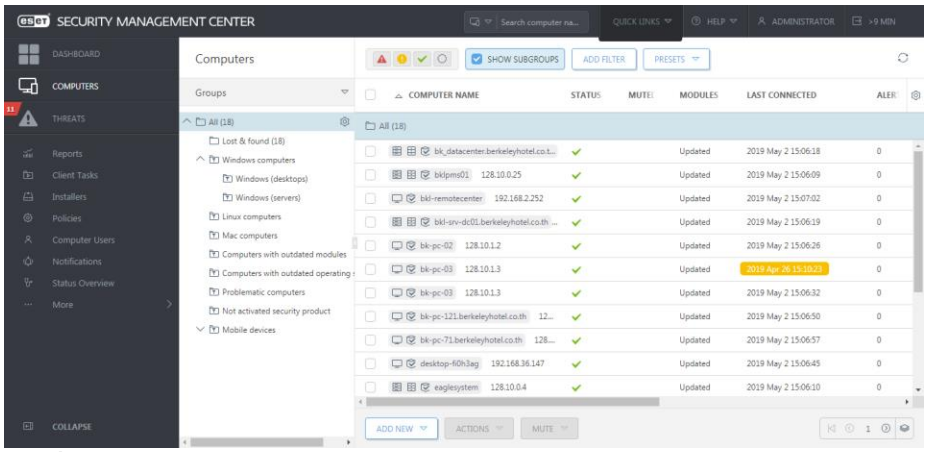
4.2.14 การป้องกันไวรัสและสแปม

ความเสี่ยง :	การติดไวรัสและสแปมที่เครื่องเซิร์ฟเวอร์และเครื่องพนักงาน
มาตรการควบคุม :	A12.2.1 มาตรการป้องกันโปรแกรมไม่ประสงค์ดี
แผนปฏิบัติการ :	ติดตั้งโปรแกรม Antivirus และ Antimalware และตรวจสอบให้มีการ Update อยู่เสมอ
ความรับผิดชอบ :	ฝ่ายไอที
รายงานติดตามผล :	ตรวจการ Update โปรแกรม Antivirus และ Antimalware จากระบบ SECURITY MANAGEMENT CENTER

แสดงการติดตั้งโปรแกรม Antivirus ที่เครื่องเซิร์ฟเวอร์และเครื่องพนักงาน โดยมีการ Update จากระบบ SECURITY MANAGEMENT CENTER



รูปที่ 4.56 แสดงการติดตั้ง Antivirus

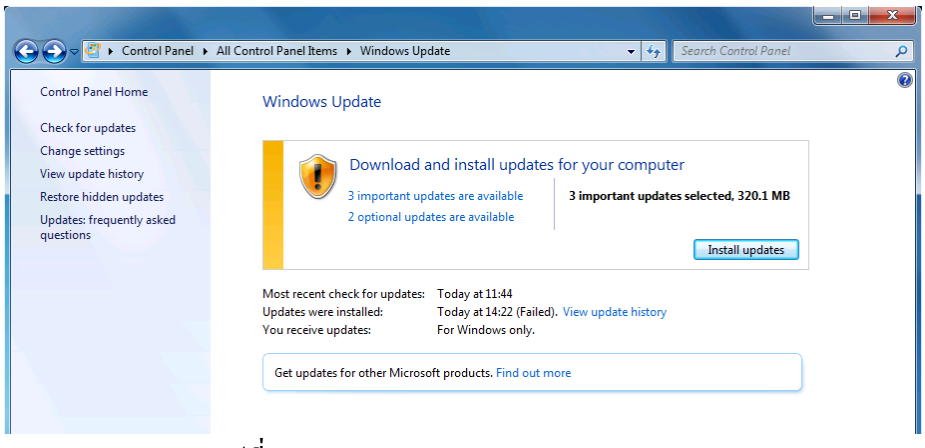


รูปที่ 4.57 แสดงการ Update จากระบบ SECURITY MANAGEMENT CENTER

4.2.15 การจัดการช่องโหว่ของ Windows

ความเสี่ยง :	ไม่มีการอัพ Patch Windows ของเครื่องพนักงาน
มาตรการควบคุม :	A12.6.1 การบริหารจัดการช่องโหว่ทางเทคนิค
แผนปฏิบัติการ :	ตั้ง Auto update patch windows
ความรับผิดชอบ :	ฝ่ายไอที
รายงานติดตามผล :	ตรวจสอบการตั้ง Auto update patch windows ทุกเครื่อง

แสดงตัวอย่างการ Update Patch Windows โดยมีการ Update และ Install ทุกวันอัตโนมัติ

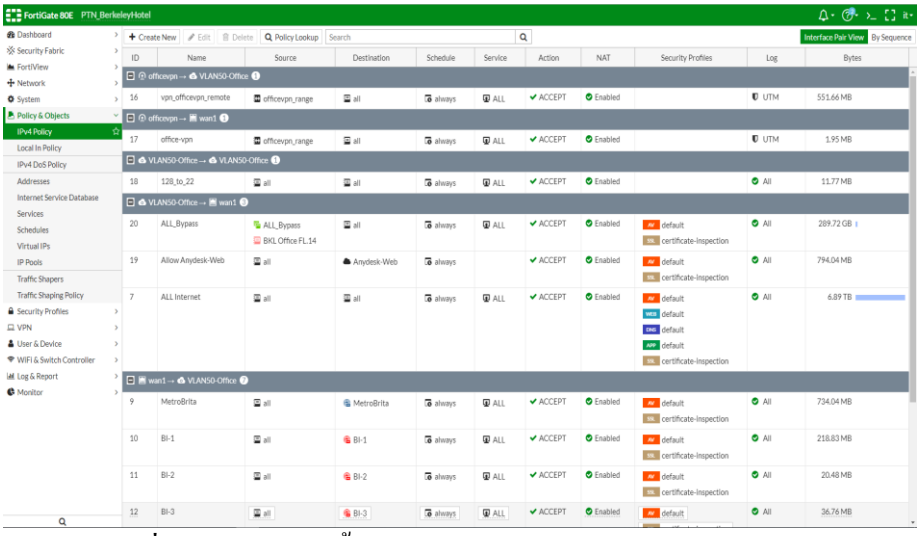


รูปที่ 4.58 แสดงการ Update Patch Windows

4.2.16 การป้องกันการเข้าถึงและโจมตีจากเครือข่ายภายนอก

ความเสี่ยง :	การเข้าถึงและโดนโจมตีจากเครือข่ายภายนอก
มาตรการควบคุม :	A13.1.2 ความมั่นคงปลอดภัยสำหรับบริการเครือข่าย
แผนปฏิบัติการ :	ติดตั้งระบบ Firewall โดยมีการตั้งค่า Policy ความปลอดภัยของเครือข่ายภายใน
ความรับผิดชอบ :	ฝ่ายไอที
รายงานติดตามผล :	ตรวจสอบการตั้งค่า Policy ความปลอดภัยของ Firewall อย่างสม่ำเสมอ

แสดงการตั้งค่า Policy ความปลอดภัยของเครือข่ายภายใน สำหรับอุปกรณ์ Firewall (FortiGate 80E) เพื่อป้องกันการเข้าถึงและการโจมตีจากเครือข่ายภายนอก

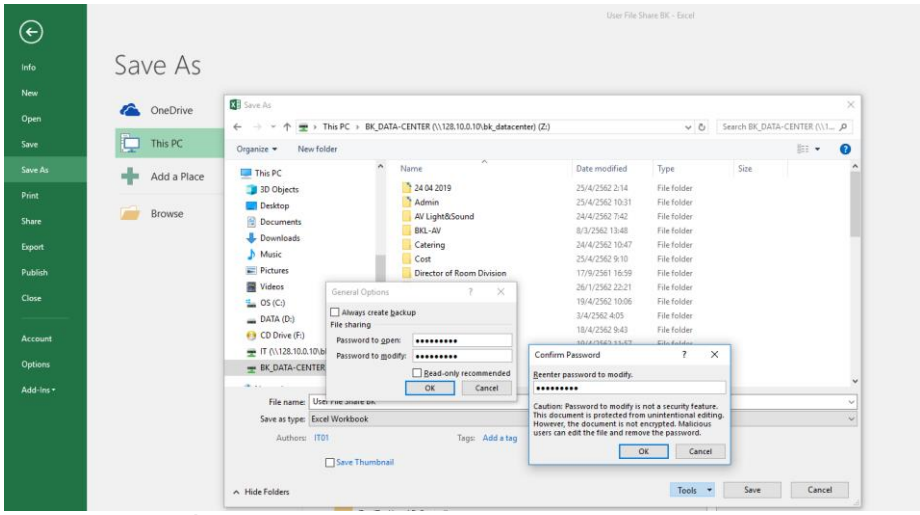


รูปที่ 4.59 แสดงการตั้งค่า Policy ของ Firewall (FortiGate 80E)

4.2.17 การควบคุมการเข้าถึงระบบงานหรือข้อมูลของคนอื่น

ความเสี่ยง :	พนักงานสามารถเข้าใช้ระบบงานหรือข้อมูลของคนอื่นได้
มาตรการควบคุม :	A18.1.4 ความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคล
แผนปฏิบัติการ :	มีนโยบายในการเข้ารหัสข้อมูลที่สำคัญ
ความรับผิดชอบ :	ฝ่ายไอที
รายงานติดตามผล :	มีนโยบายให้ทุกแผนกต้องเข้ารหัสไฟล์เอกสารที่สาคัญ

แสดงตัวอย่างการเข้ารหัสของไฟล์เอกสารสำคัญของพนักงาน อาทิ เอกสารสำคัญจากโปรแกรม Excel



รูปที่ 4.60 แสดงการเข้ารหัสเอกสารจากโปรแกรม Excel

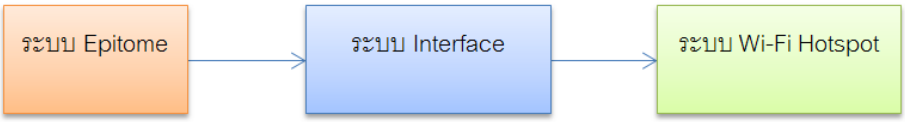
4.3 แนวทางปฏิบัติในการให้บริการอินเตอร์เน็ต ตามแนวทางพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

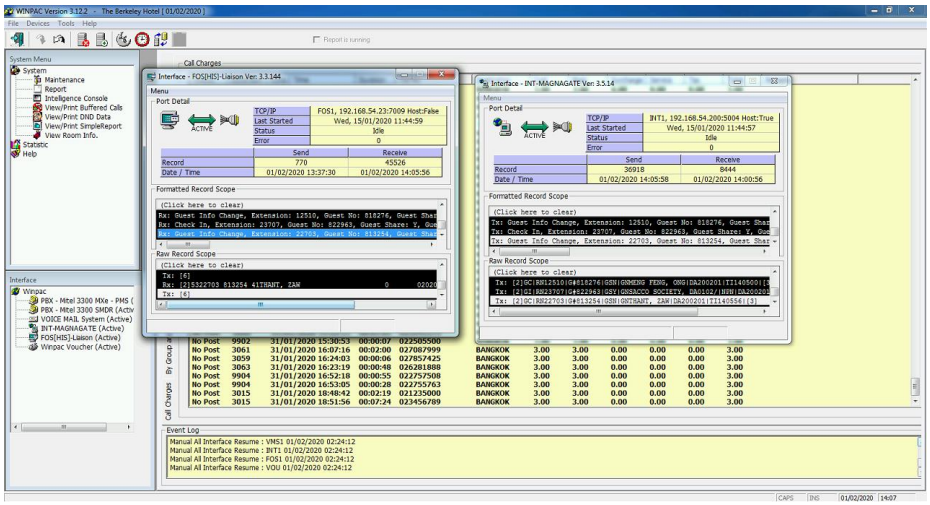
จากการวิเคราะห์ถึงปัญหาเกี่ยวกับการกระทำความผิดในแง่ของโอกาสที่จะเกิดขึ้นกับการให้บริการอินเตอร์เน็ตของโรงแรม ที่มีขั้นตอนการให้บริการที่ไม่สามารถติดตามหรือระบุตัวตนผู้ใช้งานได้ เพราะหน้าที่ของผู้ให้บริการจะต้องเก็บข้อมูลการใช้งานคอมพิวเตอร์และอินเตอร์เน็ต และได้นำมาวิเคราะห์ช่องว่าง (Gap Analysis) สามารถจัดทำเป็นแนวทางปฏิบัติในการให้บริการอินเตอร์เน็ตที่ถูกต้องตามกฎหมาย โดยมีรูปแบบและขั้นตอนการให้บริการ ดังนี้

- การให้บริการอินเตอร์เน็ตสำหรับลูกค้า In-House Guest
- การให้บริการอินเตอร์เน็ตสำหรับลูกค้า Visitors
- การให้บริการอินเตอร์เน็ตสำหรับพนักงานของโรงแรม

4.3.1 การให้บริการอินเตอร์เน็ตสำหรับลูกค้า In-House Guest

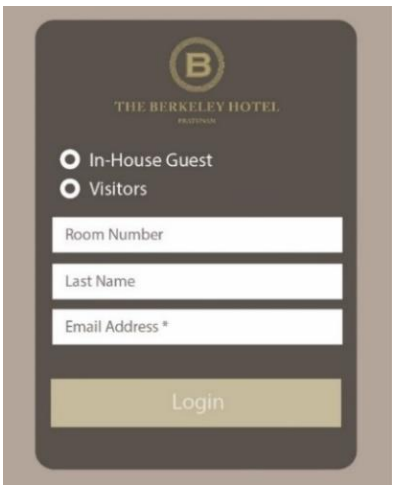
โดยการนำระบบ Interface เข้ามาช่วยในการเชื่อมต่อฐานข้อมูลของลูกค้าในระบบจองห้องพัก Epitome กับระบบ Wi-Fi Hotspot ซึ่งทำให้สามารถติดตามและระบุตัวตนผู้ใช้งานได้





รูปที่ 4.61 แสดงตัวอย่างระบบ Interface ในการเชื่อมต่อฐานข้อมูลของลูกค้า

สำหรับการออกแบบหน้า Login เข้าใช้บริการอินเตอร์เน็ตของลูกค้า In-House Guest จะต้องระบุ Room Number, Last Name และ Email Address ในการเข้าใช้งานได้ (Email Address จะนำมาใช้เพื่อการตลาด สำหรับส่งโปรโมชั่นพิเศษของโรงแรมไปให้ลูกค้าที่เคยเข้ามาพักกับทางโรงแรม)



รูปที่ 4.62 แสดงตัวอย่างหน้า Login เข้าใช้บริการอินเตอร์เน็ต สำหรับลูกค้า In-House Guest

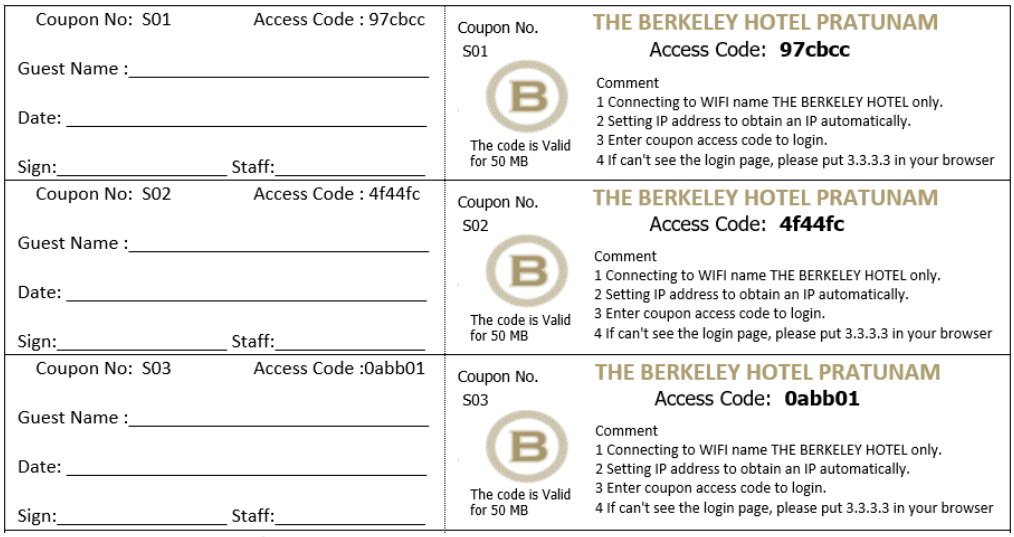
4.3.2 การให้บริการอินเตอร์เน็ตสำหรับลูกค้า Visitors

การให้บริการอินเตอร์เน็ตสำหรับลูกค้า Visitors มีด้วยกัน 3 ประเภท คือ ลูกค้าแบบ Group Tour, ลูกค้าห้องประชุมห้องสัมมนา และลูกค้าทั่วไป ซึ่งการให้บริการอินเตอร์เน็ต จะแบ่งออกเป็น 2 แบบ อาทิ

- ☐ การเข้าใช้บริการอินเตอร์เน็ตจากคูปอง
- ☐ การเข้าใช้บริการอินเตอร์เน็ตผ่าน Facebook

4.3.2.1 การเข้าใช้บริการอินเตอร์เน็ตจากคูปอง

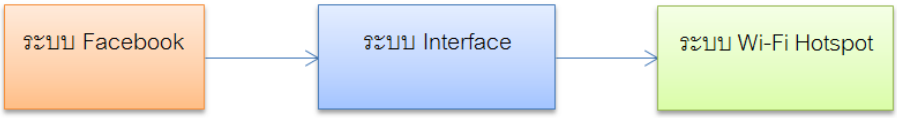
โดยการแจกคูปอง จะให้มีการลงชื่อลูกค้าและแสดงบัตรประจำตัวประชาชนหรือพาสปอร์ตเพื่อขอรับคูปอง พร้อมทั้งลงชื่อพนักงานที่แจกคูปองด้วย คูปองจะประกอบด้วย Access Code, แพ็คเกจอินเตอร์เน็ต และขั้นตอนการเข้าใช้บริการอินเตอร์เน็ต ซึ่งทำให้สามารถติดตามและระบุตัวตนผู้ใช้งานได้ ดังตัวอย่างรูปที่ 4.50



รูปที่ 4.63 แสดงตัวอย่างแบบฟอร์มในการแจกคูปอง

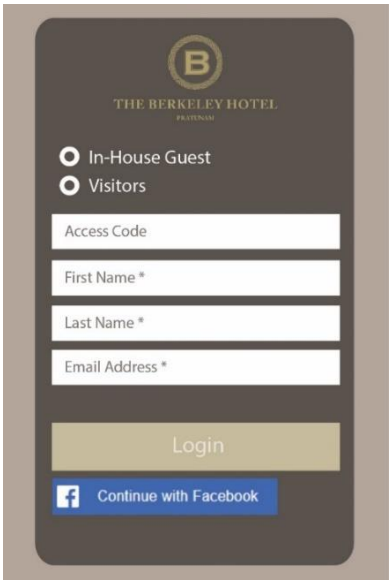
4.3.2.2 การเข้าใช้บริการอินเตอร์เน็ตผ่าน Facebook

เป็นอีกทางเลือกหนึ่งสำหรับลูกค้าทั่วไปของโรงแรม โดยการเข้าใช้บริการอินเตอร์เน็ตผ่าน Facebook ซึ่งต้องติดตั้งแอพพลิเคชั่น Facebook บนโทรศัพท์มือถือเท่านั้น โดยการนำระบบ Interface เข้ามาช่วยในการเชื่อมต่อฐานข้อมูลจาก Facebook กับระบบ Wi-Fi Hotspot ซึ่งทำให้สามารถติดตามและระบุตัวตนผู้ใช้งานได้



รูปที่ 4.64 แสดงตัวอย่างการเข้าใช้บริการอินเตอร์เน็ตผ่าน Facebook

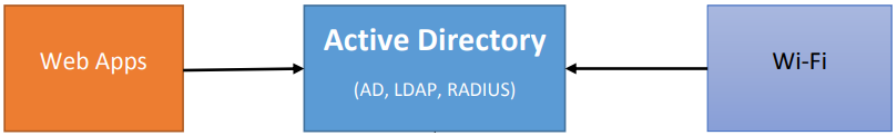
สำหรับการออกแบบหน้า Login เข้าใช้บริการอินเตอร์เน็ตสำหรับลูกค้า Visitors จะต้องระบุ Access Code, First Name, Last Name และ Email Address เพื่อเข้าใช้งานบริการได้ หรือเลือกเข้าใช้บริการอินเตอร์เน็ตผ่าน Facebook



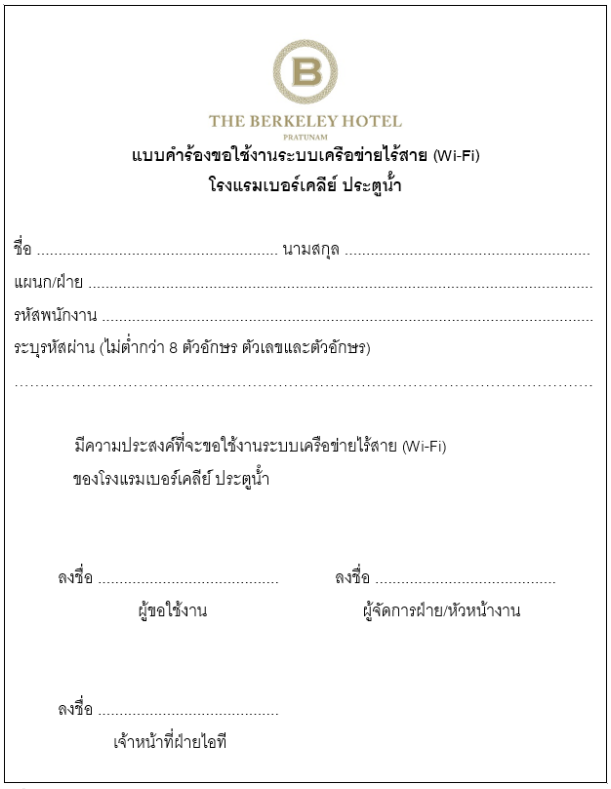
รูปที่ 4.65 แสดงตัวอย่างหน้า Login เข้าใช้บริการอินเตอร์เน็ต

4.3.3 การให้บริการอินเตอร์เน็ตสำหรับพนักงานของโรงแรม

จัดทำระบบ Authentication สำหรับ Wireless Office โดยเชื่อมกับระบบ Radius ซึ่งระบบ Wi-Fi Hotspot จะดึงฐานข้อมูลของผู้ใช้งานระหว่างระบบ Active Directory เพื่อนำไปให้ผู้ใช้งานทำการยืนยันตัวตนผ่านหน้า Login ก่อนเข้าใช้งานอินเตอร์เน็ต



ให้พนักงานกรอกแบบฟอร์มขอใช้บริการอินเตอร์เน็ต โดยการลงชื่อ-นามสกุล แผนก/ฝ่าย รหัสพนักงาน และระบุรหัสผ่าน พร้อมทั้งมีการเซ็นต์อนุมัติจากผู้จัดการฝ่าย/หัวหน้างาน และได้รับการอนุมัติให้ใช้บริการจากเจ้าหน้าที่ฝ่ายไอที ซึ่งทำให้สามารถติดตามและระบุตัวตนผู้ใช้งานได้


THE BERKELEY HOTEL
PRATUNAM

แบบคำร้องขอใช้งานระบบเครือข่ายไร้สาย (Wi-Fi)
โรงแรมเบอร์เคลีย์ ประตูน้ำ

ชื่อ ..... นามสกุล .....
แผนก/ฝ่าย .....
รหัสพนักงาน .....
ระบุรหัสผ่าน (ไม่ต่ำกว่า 8 ตัวอักษร ตัวเลขและตัวอักษร)
.....

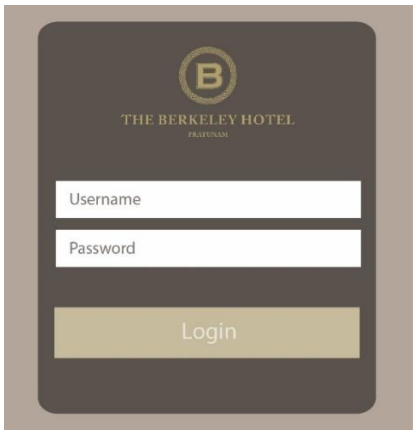
มีความประสงค์ที่จะขอใช้งานระบบเครือข่ายไร้สาย (Wi-Fi)
ของโรงแรมเบอร์เคลีย์ ประตูน้ำ

ลงชื่อ ..... ลงชื่อ .....
ผู้ขอใช้งาน ผู้จัดการฝ่าย/หัวหน้างาน

ลงชื่อ .....
เจ้าหน้าที่ฝ่ายไอที

รูปที่ 4.66 แสดงตัวอย่างแบบฟอร์มขอใช้บริการอินเตอร์เน็ต

สำหรับการออกแบบหน้า Login เข้าใช้บริการอินเตอร์เน็ตสำหรับพนักงานของโรงแรม จะเป็นการแบ่งแยก SSID ชื่อว่า BKL-OFFICE เพื่อใช้ในการเชื่อมต่อสัญญาณ Wi-Fi โดยหน้า Login จะต้องระบุ Username และ Password ในการเข้าใช้บริการอินเตอร์เน็ต



รูปที่ 4.67 แสดงตัวอย่างหน้า Login เข้าใช้บริการอินเตอร์เน็ตสำหรับพนักงาน

บทที่ 5
สรุปผลการดำเนินงาน

5.1 สรุปขั้นตอนการดำเนินงาน

ทางผู้จัดทำได้สรุปขั้นตอนการดำเนินงานสำหรับจัดทำแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์และเครือข่าย และได้แบ่งเป็นหัวข้อดังนี้

<u>ระบบปัจจุบัน</u>

วิเคราะห์โครงสร้างระบบคอมพิวเตอร์และเครือข่ายปัจจุบัน

- โครงสร้างของระบบเครือข่าย และรายละเอียดอุปกรณ์ในระบบเครือข่าย
- รายละเอียดการติดตั้งและการเชื่อมต่อระบบเครือข่าย

วิเคราะห์ระบบสนับสนุนความปลอดภัยระบบคอมพิวเตอร์และเครือข่ายปัจจุบัน

วิเคราะห์ปัญหาในระบบคอมพิวเตอร์และเครือข่ายปัจจุบัน

- ช่องโหว่หรือข้อบกพร่องของระบบคอมพิวเตอร์และเครือข่ายปัจจุบัน
- ความเสี่ยงในการเข้าถึงระบบเทคโนโลยีสารสนเทศ
- การกระทำความผิดในแง่ของโอกาสที่จะเกิดขึ้นกับการให้บริการอินเตอร์เน็ต

<u>Gap Analysis</u>

การวิเคราะห์ช่องว่างโครงสร้างระบบคอมพิวเตอร์และเครือข่าย

การวิเคราะห์ช่องว่างการเข้าถึงระบบเทคโนโลยีสารสนเทศ

การวิเคราะห์ช่องว่างการให้บริการอินเตอร์เน็ตของโรงแรม

<u>ระบบใหม่</u>

ออกแบบโครงสร้างความมั่นคงปลอดภัยระบบคอมพิวเตอร์และเครือข่ายใหม่

ออกแบบระบบสนับสนุนความปลอดภัยของระบบคอมพิวเตอร์และเครือข่าย

- การปรับปรุงการตั้งค่าการทำงานของระบบความปลอดภัยคอมพิวเตอร์และเครือข่าย
- แนะนำโปรแกรมหรือระบบรักษาความปลอดภัยบนระบบคอมพิวเตอร์และเครือข่าย

ออกแบบแนวทางปฏิบัติในการเข้าถึงระบบเทคโนโลยีสารสนเทศ ภายใต้มาตรฐาน ISO/IEC 27001

ออกแบบแนวทางปฏิบัติในการให้บริการอินเตอร์เน็ต ตามแนวทางพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

- การให้บริการอินเตอร์เน็ตสำหรับลูกค้า In-House Guest
- การให้บริการอินเตอร์เน็ตสำหรับลูกค้า Visitors
- การให้บริการอินเตอร์เน็ตสำหรับพนักงานของโรงแรม

5.2 สรุปผลการดำเนินงาน

จากวัตถุประสงค์ในการออกแบบแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์และเครือข่าย พอจะสรุปผลการดำเนินงานได้เป็น 3 ส่วน ดังนี้

1. การออกแบบโครงสร้างความมั่นคงปลอดภัยระบบคอมพิวเตอร์และเครือข่ายใหม่ โดยมีการปรับปรุงการตั้งค่าการทำงานของอุปกรณ์ ปรับปรุงระบบโครงสร้างเครือข่าย และแนะนำโปรแกรมหรือระบบรักษาความปลอดภัยต่อระบบคอมพิวเตอร์และเครือข่ายให้มีความมั่นคงปลอดภัยมากขึ้น เพื่อให้องค์กรมั่นใจได้ว่าการดำเนินงานทางธุรกิจสามารถดำเนินไปได้อย่างต่อเนื่อง
2. แนวทางปฏิบัติในการเข้าถึงระบบเทคโนโลยีสารสนเทศ สามารถนำมาจัดทำเป็นบรรทัดฐานในการทำงานของพนักงานและผู้ดูแลระบบภายในองค์กร โดยมีมาตรการควบคุม แผนปฏิบัติการ และการรายงานติดตามผล เพื่อลดความเสี่ยงและป้องกันการเข้าถึงระบบเทคโนโลยีสารสนเทศจากบุคคลอื่น
3. แนวทางปฏิบัติในการให้บริการอินเตอร์เน็ตของโรงแรม มีรูปแบบและขั้นตอนการให้บริการที่สามารถติดตามหรือระบุตัวตนผู้ใช้งานได้ ตามหน้าที่ของผู้ให้บริการที่จะต้องเก็บข้อมูลการใช้งานคอมพิวเตอร์และอินเตอร์เน็ต

5.3 ปัญหาและอุปสรรค

1. การออกแบบโครงสร้างความมั่นคงปลอดภัยระบบคอมพิวเตอร์และเครือข่ายใหม่
   - การออกแบบโครงสร้างเครือข่ายบางส่วนอยู่นอกเหนือการควบคุมของทางผู้จัดทำ เช่น การเปลี่ยนอุปกรณ์สวิตซ์ การปรับเปลี่ยนโครงสร้างเครือข่ายใหม่ หรือการสั่งซื้อโปรแกรมรักษาความปลอดภัย เพราะถูกจำกัดด้วยงบประมาณจากผู้บริหาร
   - การปรับเปลี่ยนโครงสร้างเครือข่ายในแต่ละส่วน ค่อนข้างใช้เวลานาน อาจทำให้ระบบส่วนอื่นหยุดทำงานไปด้วย เนื่องจากระบบทุกส่วนเชื่อมต่อถึงกัน
2. แนวทางปฏิบัติในการเข้าถึงระบบเทคโนโลยีสารสนเทศ ภายใต้มาตรฐาน ISO/IEC 27001
   - เนื่องจากมีการติดตั้งระบบควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศเพิ่มเติม อาทิ ระบบ Active Directory, การกำหนด Policy ใน GPO อาจทำให้ต้องมีการเข้าไปตั้งค่าที่เครื่องของพนักงานทุกเครื่อง ทำให้เสียเวลาค่อนข้างมาก
   - การติดตั้งเครื่องสแกนนิ้ว กล้องวงจรปิด และโปรแกรม Antivirus และ Antimalware อาจทำให้เสียค่าใช้จ่ายเพิ่มเติมในการสั่งซื้ออุปกรณ์ และ license software
3. แนวทางปฏิบัติในการให้บริการอินเตอร์เน็ต ตามแนวทางพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550
   - การติดตั้งระบบ Interface สำหรับเชื่อมต่อฐานข้อมูลของลูกค้า มีการเชื่อมต่อเข้าด้วยกัน 3 ส่วน ทำให้ผู้ดูแลระบบต้องทำการประสานงานกับเจ้าของระบบ เพื่อดำเนินการติดตั้ง
   - การติดตั้งระบบ Interface สำหรับเชื่อมต่อฐานข้อมูลของลูกค้า และ Interface สำหรับเชื่อมต่อฐานข้อมูลจาก Facebook ต้องมีการเสนองบประมาณเพื่อขอการอนุมัติจากผู้บริหารก่อน
   - ในกรณีที่เป็นการจองห้องพักแบบ Group Tour อาจทำให้ลูกค้าเข้าใจที่ต้องใช้ Room Number, Last Name ของตนเอง โดยไม่ได้มาจากผู้ที่ทำการ Check in หรือ Booking
   - ในกรณีที่เป็นลูกค้าห้องประชุมห้องสัมมนา หากมีจำนวนมาก อาจทำให้พนักงานของโรงแรมเสียเวลาในการแจกคูปองและเก็บข้อมูลจากลูกค้า

5.4 ข้อเสนอแนะ

ทางผู้จัดทำมุ่งหวังที่จะออกแบบแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยของเครือข่ายคอมพิวเตอร์และอินเตอร์เน็ตต่อไปอีกในอนาคต และต้องการจะปรังปรุงระบบให้มีประสิทธิภาพและมั่นคงปลอดภัยมากขึ้น พร้อมทั้งนำเอามาตรฐานความมั่นคงปลอดภัยมาประยุกต์ใช้งานภายในองค์กรให้สอดคล้องกับการทำงาน และรองรับการใช้งานในอนาคตต่อไป โดยมีข้อเสนอแนะ ดังนี้

- การพัฒนาระบบรักษาความมั่นคงปลอดภัยควรคำนึงถึงการประเมินความเสี่ยง การกำหนดนโยบาย การออกแบบและติดตั้งระบบ การรายงานติดตามผล และการฝึกอบรมพนักงาน
- ผู้ดูแลระบบควรจะติดตามหาข้อมูลการตั้งค่าโปรแกรมสนับสนุนความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และเครือข่าย หรืออัพเดทเวอร์ชั่นของโปรแกรม เพราะการอัพเดทสิ่งใหม่ๆ จะทำให้ช่วยลดช่องโหว่ต่างๆ ได้
- หากมีการปรับเปลี่ยนอุปกรณ์ใหม่ในระบบเครือข่าย ต้องมีการพิจารณาฟังค์ชั่นการใช้งานให้เหมาะสม เพราะหากไม่เหมาะสมแล้วจะทำให้มีผลต่อประสิทธิภาพการทำงานในระบบเครือข่าย
- การเลือกใช้เทคโนโลยีต่างๆ ต้องตรวจสอบการใช้งานให้แน่ใจว่าเข้ากันได้กับระบบที่จัดทำขึ้นหรือไม่
- หมั่นจัดทำนโยบายใหม่ๆ ให้สอดคล้องกับในยุคปัจจุบันมากที่สุดเพื่อสร้างความมั่นคงปลอดภัยให้กับองค์กร
- จัดอบรมให้พนักงานเกิดความตระหนักด้านความปลอดภัยในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศ และหลีกเลี่ยงการละเมิดข้อกำหนดทางกฎหมายในการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

บรรณานุกรม

กฤษฎา กลั่นเกิด. 2557. **การออกแบบและพัฒนาระบบเครือข่าย กรณีศึกษาบริษัทอิทธิพรอิมปอร์ต จำกัด.** ภาคนิพนธ์คณะวิทยาการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีมหานคร.

เกษม เบ็ญร่าหีม. 2556. **การออกแบบและพัฒนาระบบเครือข่ายและความปลอดภัย กรณีศึกษากรมการท่องเที่ยว**. ภาคนิพนธ์คณะวิทยาการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีมหานคร.

ศราวุฒิ จันทะคัด. 2554. **การจัดการความปลอดภัยภายในเครือข่ายคอมพิวเตอร์ กรณีศึกษาบริษัทแซนด์แอนด์ซอยล์ อุตสาหกรรม จำกัด.** ภาคนิพนธ์คณะวิทยาการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีมหานคร.

ณัทรัฏฐ์ มณีรัสยากร. 2559. **การพัฒนานโยบายด้านความมั่นคงปลอดภัย ภายใต้มาตรฐาน ISO27001 ขององค์กรกรณีศึกษา บจก. เซ็กโก้ เอ็นจิเนียริ่ง แอนด์ คอนสตรัคชั่น.** ภาคนิพนธ์คณะวิทยาการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีมหานคร.

เอกวิทย์ พิทักษ์คชวงษ์. 2557. **การสร้างความมั่นคงปลอดภัยให้กับระบบเทคโนโลยีสารสารสนเทศภายใต้มาตรฐาน ISO 27001:2013 กรณีศึกษาบริษัท ทีวีไดเร็ค จากัด มหาชน.** ภาคนิพนธ์คณะวิทยาการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีมหานคร.

ขนิษฐา พิมพ์ประชา. 2557. **การจัดการระบบสารสนเทศภายในองค์กร ตามแนวทาง ISO 27001:2013 กรณีศึกษาบริษัทเอ็นทีที คอมมิวนิเคชั่นส์ (ประเทศไทย) จากัด.** ภาคนิพนธ์คณะวิทยาการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีมหานคร.

สำนักกำกับการใช้เทคโนโลยีสารสนเทศ. 2551. **คู่มือการปฏิบัติและแนวทางการป้องกัน เพื่อหลีกเลี่ยงการกระทำความผิดเกี่ยวกับคอมพิวเตอร์.** กรุงเทพฯ: กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร.

นาวาโท กรกช วิไลลักษณ์. 2556. **ความมั่นคงปลอดภัยระบบคอมพิวเตอร์**. ค้นวันที่ 15/10/2562 จาก https://www.stou.ac.th/Schools/sst/main/Subject96101/96101-14.pdf

ภาคผนวก

ภาคผนวก ก

DOMAIN INTERNATIONAL STANDARD ISO/IEC 27001

Domain	ลำดับ	เนื้อหา
A5. นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy)		
A5.1 นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy)	1	A5.1.1 นโยบายสำหรับความมั่นคงปลอดภัยสารสนเทศ (Policies for information security)
	2	A5.1.2 การทบทวนนโยบายสำหรับการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Review of the policies for Information security)
A6. โครงสร้างความมั่นคงปลอดภัยสารสนเทศ (Organization of Information Security)		
A6.1 โครงสร้างภายในองค์กร (Internal organization)	3	A6.1.1 บทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ (Information security roles and responsibilities)
	4	A6.1.2 การแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of duties)
	5	A6.1.3 การติดต่อกับองค์กรผู้มีอำนาจ (Contact with authorities)
	6	A6.1.4 การติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน (Contact with special interest groups)
	7	A6.1.5 ความมั่นคงปลอดภัยสารสนเทศกับการบริหารจัดการโครงการ (Information security in project management)
A6.2 อุปกรณ์คอมพิวเตอร์แบบพกพาและการปฏิบัติงานจากระยะไกล (Mobile device Policy)	8	A6.2.1 นโยบายสำหรับอุปกรณ์คอมพิวเตอร์แบบพกพา (Mobile device Policy)
	9	A6.2.2 การปฏิบัติงานจากระยะไกล (Teleworking)
A7. ความมั่นคงปลอดภัยสำหรับบุคลากร (Human Resource Security)		

A7.1 ก่อนการจ้างงาน (Prior to employment)	10	A7.1.1 การคัดเลือก (Screening)
	11	A7.1.2 ข้อตกลงและเงื่อนไขการจ้างงาน (Terms and conditions of employment)
A7.2 ระหว่างจ้างงาน (During employment)	12	A7.2.1 หน้าที่ความรับผิดชอบของผู้บริหาร (Management responsibilities)
	13	A7.2.2 การสร้างความตระหนัก การให้ความรู้ และการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ (Information security awareness, education and training)
	14	A7.2.3 กระบวนการทางวินัย (Disciplinary process)
	15	A7.3.1 การสิ้นสุดหรือการเปลี่ยนหน้าที่ความรับผิดชอบของการจ้างงาน (Termination or change of employment responsibilities)
A8. การบริหารจัดการทรัพย์สิน (Asset Management)		
A8.1 หน้าที่ความรับผิดชอบต่อทรัพย์สิน (Responsibility for assets)	16	A8.1.1 บัญชีทรัพย์สิน (Inventory of asset)
	17	A8.1.2 ผู้ถือครองทรัพย์สิน (Ownership of asset)
	18	A8.1.3 การใช้ทรัพย์สินอย่างเหมาะสม (Acceptable use of assets)
	19	A8.1.4 การคืนทรัพย์สิน (Return of asset)
A8.2 การจัดชั้นความลับของสารสนเทศ (Information classification)	20	A8.2.1 ชั้นความลับของสารสนเทศ (Classification of information)
	21	A8.2.2 การบ่งชี้สารสนเทศ (Labeling of information)
	22	A8.2.3 การจัดการทรัพย์สิน (Handing of assets)
A8.3 การจัดการสื่อบันทึกข้อมูล (Media Handling)	23	A8.3.1 การบริหารจัดการสื่อบันทึกข้อมูลที่ถอดแยกได้ (Management of removable media)
	24	A8.3.2 การทำลายสื่อบันทึกข้อมูล (Disposal of media)
	25	A8.3.3 การขนย้ายสื่อบันทึกข้อมูล (Physical media transfer)
A.9 การควบคุมการเข้าถึง (Access Control)		
A9.1 ความต้องการทำงธุรกิจสำหรับการ ควบคุมการเข้าถึง (Business requirement of access control)	26	A9.1.1 นโยบายควบคุมการเข้าถึง (Access control policy)
	27	A9.1.2 การเข้าถึงเครือข่ายและการบริการเครือข่าย (Access to networks and network services)
A9.2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน	28	A9.2.1 การลงทะเบียนและถอดถอนสิทธิ์ผู้ใช้งาน (User registration and deregistration)

(User access management)	29	A9.2.2 การจัดการสิทธิ์การเข้าถึงของผู้ใช้งาน (User access provisioning)
	30	A9.2.3 การบริหารจัดการสิทธิ์การเข้าถึงตามระดับสิทธิ์ (Management of privileged access right)
	31	A9.2.4 การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน (Management of secret authentication information of users)
	32	A9.2.5 การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of user access rights)
	33	A9.2.6 การถอดถอนหรือปรับปรุงสิทธิ์การเข้าถึง (Removal or adjustment of access rights)
A9.3 หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)	34	A9.3.1 การใช้ข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ (User of secret authentication information)
A9.4 การควบคุมการเข้าถึงระบบ (System and application access control)	35	A9.4.1 การจำกัดการเข้าถึงสารสนเทศ (Information access restriction)
	36	A9.4.2 ขั้นตอนปฏิบัติสำหรับการล็อกอินเข้าระบบที่มีความมั่นคงปลอดภัย (Secure log-on procedures)
	37	A9.4.3 ระบบบริหารจัดการรหัสผ่าน (Password management system)
	38	A9.4.4 การใช้โปรแกรมอรรถประโยชน์ (Use of privileged utility programs)
	39	A9.4.5 การควบคุมการเข้าถึงซอร์สโค้ดของโปรแกรม (Access control to program source code)
A10. การเข้ารหัสข้อมูล (Cryptography)		
A10.1 มาตรการเข้ารหัสข้อมูล (Cryptographic controls)	40	A10.1.1 นโยบายการใช้มาตรการเข้ารหัสข้อมูล (Policy on the use of cryptographic controls)
	41	A10.1.2 การบริหารจัดการกุญแจ (Key management)
A11. ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม (Physical and environmental Security)		
A11.1 พื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Secure areas)	42	A11.1.1 ขอบเขตหรือบริเวณโดยรอบทางกายภาพ (Physical security perimeter)
	43	A11.1.2 การควบคุมการเข้าออกทางกายภาพ (Physical entry controls)

	44	A11.1.3 การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงานและอุปกรณ์ (Securing office, room and facilities)
	45	A11.1.4 การป้องกันภัยคุกคามจากภายนอก และ สภาพแวดล้อม (Protecting against external and
	46	A11.1.5 การปฏิบัติงานในพื้นที่ที่ต้องการการรักษาความมั่นคงปลอดภัย (Working in secure areas)
	47	A11.1.6 พื้นที่สำหรับรับส่งสิ่งของ (Delivery and loading areas)
A11.2 อุปกรณ์ (Equipment)	48	A11.2.1 การจัดตั้งและป้องกันอุปกรณ์ (Equipment sitting and protection)
	49	A11.2.2 ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting utilities)
	50	A11.2.3 ความมั่นคงปลอดภัยของการเดินสายสัญญาณและสายสื่อสาร (Cabling security)
	51	A11.2.4 การบำรุงรักษาอุปกรณ์ (Equipment maintenance)
	52	AA11.2.5 การนำทรัพย์สินขององค์กรออกจากสำนักงาน (Removal of assets)
	53	A11.2.6 ความมั่นคงปลอดภัยของอุปกรณ์และทรัพย์สินที่ใช้งานอยู่ภายนอกสำนักงาน (Secure of equipment and assets off-premises)
	54	A11.2.7 ความมั่นคงปลอดภัยสำหรับการกำจัดหรือทำลายอุปกรณ์ หรือการนำอุปกรณ์ไปใช้งานอย่างอื่น (Secure disposal or re-use of equipment)
	55	A11.2.8 อุปกรณ์ของผู้ใช้งานที่ทิ้งไว้โดยไม่มีผู้ดูแล (Unattended user equipment)
	56	A11.2.9 นโยบายโต๊ะทำงานปลอดเอกสารสำคัญ และ นโยบายการป้องกันหน้าจอคอมพิวเตอร์ (Clear desk and clear screen policy)
A12. ความมั่นคงปลอดภัยสำหรับการดำเนินการ (Operations Security)		
A12.1 ขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ (Operational Procedures and Responsibilities)	57	A12.1.1 ขั้นตอนการปฏิบัติงานที่เป็นลายอักษร (Documented operating procedures)
	58	A12.1.2 การบริหารจัดการการเปลี่ยนแปลง (Change management)

	59	A12.1.3 การบริหารจัดการขีดความสามารถของระบบ (Capacity management)
	60	A12.1.4 การแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบและการให้บริการออกจากกัน (Separation of development, testing and operational environments)
A12.2 การป้องกันโปรแกรมไม่ประสงค์ดี (Protection from Malware)	61	A12.2.1 มาตรการป้องกันโปรแกรมไม่ประสงค์ดี (control against malware)
A12.3 การสำรองข้อมูล (Backup)	62	A12.3.1 การสำรองข้อมูล (Information backup)
A12.4 การบันทึกข้อมูลล็อกและการเฝ้าระวัง (Logging and Monitoring)	63	A12.4.1 การบันทึกข้อมูลล็อคแสดงเหตุการณ์ (Event Logging)
	64	A12.4.2 การป้องกันข้อมูลล็อก (Protection of log information)
	65	A12.4.3 ข้อมูลล็อกกิจกรรมของผู้ดูและระบบและเจ้าหน้าที่ปฏิบัติการระบบ (Administrator and operator logs)
	66	A12.4.4 การตั้งนาฬิกาให้ถูกต้อง (Clock Synchronization)
A12.5 การควบคุมการติดตั้งซอฟต์แวร์ (Control of operational software)	67	A12.5.1 การติดตั้งซอฟต์แวร์บนระบบให้บริการ (Installation of software on operational systems)
	68	A12.6.1 การบริหารจัดการช่องโหว่ทางเทคนิค (Management of technical vulnerabilities)
	69	A12.6.2 การจัดการการติดตั้งซอฟต์แวร์ (Restrictions on software installation)
A12.7 สิ่งที่ต้องพิจารณาในการตรวจประเมินระบบ (Information Systems Audit	70	A12.7.1 มาตรการการตรวจประเมินระบบ (Information System audit controls)
A13. ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications security)		
A13.1 การบริหารจัดการความมั่นคงปลอดภัยของเครือข่าย (Communications security)	71	A13.1.1 มาตรการเครือข่าย (Network controls)
	72	A13.1.2 ความมั่นคงปลอดภัยสำหรับบริการเครือข่าย (Security of network services)
	73	A13.1.3 การแบ่งแยกเครือข่าย (Segregation in networks)
A13.2 การถ่ายโอนสารสนเทศ (Information transfer)	74	A13.2.1 นโยบายและขั้นตอนปฏิบัติสำหรับการถ่ายโอนสารสนเทศ (Information transfer policies and procedures)
	75	A13.2.2 ข้อตกลงสำหรับการถ่ายโอนสารสนเทศ

		(Agreements on information transfer)
	76	A13.2.3 การส่งข้อความทางอิเล็กทรอนิกส์ (Electronic messaging)
	77	A13.2.4 ข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ (Confidentiality or non-disclosure agreements)
A14. การจัดหา การพัฒนา และการบำรุงรักษาระบบ (System acquisition, development and maintenance)		
A14.1 ความต้องการด้านความมั่นคงปลอดภัยของระบบ (Security requirements of information systems)	78	A14.1.1 การวิเคราะห์และกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ (Information security requirements analysis and specification)
	79	A14.1.2 ความมั่นคงปลอดภัยขอบริการสารสนเทศบนเครือข่ายสาธารณะ (Securing application services on public networks)
	80	A14.1.3 การป้องกันธุรกรรมของบริการสารสนเทศ (Protecting application services transactions)
A14.2 ความมั่นคงปลอดภัยสำหรับกระบวนการพัฒนาและสนับสนุน (Security in development and support processes)	81	A14.2.1 นโยบายการพัฒนาระบบให้มีความมั่นคงปลอดภัย (Secure development policy)
	82	A14.2.2 ขั้นตอนการปฏิบัติสำหรับควบคุมการเปลี่ยนแปลงระบบ (System Change control procedures)
	83	A14.2.3 การทบทวนทางเทคนิคต่อระบบหลังจากเปลี่ยนแปลงโครงสร้างพื้นฐานของระบบ (Technical review of applications after operating platform changes).
	84	A14.2.4 การจำกัดการเปลี่ยนแปลงซอฟต์แวร์สาเร็จรูป (Restrictions on changes to software packages)
	85	A14.2.5 หลักการวิศวะกรรมระบบด้านความมั่นคงปลอดภัย (Secure system 85. engineering principles)
	86	A14.2.6 สภาพแวดล้อมของการพัฒนาระบบที่มีความมั่นคงปลอดภัย (Secure development environment)
	87	A14.2.7 การจ้างองค์กรภายนอกพัฒนาระบบ (Outsourced development)
	88	A14.2.8 การทดสอบด้านความมั่นคงปลอดภัยของระบบ (System security testing)
	89	A14.2.9 การทดสอบเพื่อรับรองระบบ (System acceptance testing)

	90	A14.3.1 การป้องกันข้อมูลสำหรับการทดสอบ (Protection of test data)
A15. ความสัมพันธ์กับผู้ขาย ผู้ให้บริการภายนอก (Supplier relationships)		
A15.1 ความมั่นคงปลอดภัยสารสนเทศกับความสัมพันธ์กับผู้ให้บริการภายนอก (Information security in supplier relationship)	91	A15.1.1 นโยบายความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก (Information security policy for supplier relationships)
	92	A15.1.2 การระบุความมั่นคงปลอดภัยในข้อตกลงการให้บริการของผู้ให้บริการภายนอก (Addressing security within supplier agreements)
	93	A15.1.3 ห่วงโซ่การให้บริการเทคโนโลยีสารสนเทศและการสื่อสารโดยผู้ให้บริการภายนอก (Information and communication technology supply chain)
A15.2 การบริหารจัดการการให้บริการโดยผู้ให้บริการภายนอก (Supplier service delivery management)	94	A15.2.1 การติดตามและทบทวนบริการของผู้ให้บริการภายนอก (monitoring and review of supplier services)
	95	A15.2.2 การบริหารจัดการเปลี่ยนแปลงบริการของผู้ให้บริการภายนอก (managing changes to supplier services)
A16. การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)		
A16.1 การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศและการปรับปรุง (Management of information security incidents and improvements)	96	A16.1.1 หน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติ (Responsibilities and procedures)
	97	A16.1.2 การรายงานสถาณการณ์ความมั่นคงปลอดภัยสารสนเทศ (Reporting information security events)
	98	A16.1.3 การรายงานจุดอ่อนทางความมั่นคงสารสนเทศ (Reporting information security weaknesses)
	99	A16.1.4 การประเมินและตัดสินใจต่อสถาณการณ์ความมั่นคงปลอกภัยสารสนเทศ (Assessment of and decision on information security events)
	100	A16.1.5 การตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Response to information security incidents)
	101	A16.1.6 การเรียนรู้จากเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Learning form information security incidents)
	102	A16.1.7 การเก็บรวบรวมหลักฐาน (Collection of evidence)

A17. ประเด็นด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ (Information security aspects of business continuity management)		
A17.1 ความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Information security continuity)	103	A17.1.1 การวางแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Planning information 103. security continuity)
	104	A17.1.2 การปฏิบัติเพื่อเตรียมการสร้างความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Implementing information security continuity)
	105	A17.1.3 การตรวจสอบ การทบทวน และการประเมินความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Verify, review and evaluate information security continuity)
	106	A17.2.1 สภาพความพร้อมใช้ของอุปกรณ์ประมวลผลสารสนเทศ (Availability of information processing facilities)
A18. ความสอดคล้อง (Compliance)		
A18.1 ความสอดคล้องกับความต้องการด้านกฎหมายและในสัญญาจ้าง (compliance with legal and contractual requirements)	107	A18.1.1 การระบุกฎหมายและความต้องการในสัญญาจ้างที่เกี่ยวข้อง (Identification of applicable legislation and contractual requirements)
	108	A18.1.2 สิทธิ์ในทรัพย์สินทางปัญญา (Intellectual property rights)
	109	A18.1.3 การป้องกันข้อมูล (Protection of records)
	110	A18.1.4 ความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคล (Privacy and protection of personal identifiable information)
	111	A18.1.5 ระเบียบข้อบังคับสำหรับมาตรการเข้ารหัสข้อมูล (Reflation of cryptographic controls)
A18.2 การทบทวนความมั่นคงปลอดภัยสารสนเทศ (Information security reviews)	112	A18.2.1 การทบทวนอย่างอิสระด้านความมั่นคงปลอดภัยสารสนเทศ (Independent review of information security)
	113	A18.2.2 ความสอดคล้องกับนโยบายและมาตรฐานด้านความมั่นคงปลอดภัย (Compliance with security policies and standards)
	114	A18.2.3 การทบทวนความสอดคล้องทางเทคนิค (Technical compliance review)

ประวัติผู้เขียน

ชื่อ นามสกุล	นายมงคล ใจมา
ประวัติการศึกษา	บริหารธุรกิจบัณฑิต (เทคโนโลยีสารสนเทศทางธุรกิจ)
ประสบการณ์ทำงาน	IT Support ณ โรงแรมเบอร์เคลีย์ ประตูน้ำ