

การยืนยันตัวบุคคลเพื่อเข้าใช้งานระบบเครือข่ายอินเทอร์เน็ต  
ของสำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช

นายเอกชัย แก้วเรืองฤทธิ์

สำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช  
กรมควบคุมโรค

## บทคัดย่อ

สำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช ได้ดำเนินการตามนโยบายระบบราชการ 4.0 ของรัฐบาล เพื่อให้มีการนำระบบเทคโนโลยีสารสนเทศและการสื่อสาร มาใช้ในการสนับสนุนการปฏิบัติงานให้เป็นไปอย่างเหมาะสม มีประสิทธิภาพ ซึ่งโดยทั่วไปในการปฏิบัติงานบุคลากรมีความจำเป็นต้องใช้เทคโนโลยีสารสนเทศในการวิเคราะห์ ประมวลผลข้อมูลด้านโรคและสุขภาพและได้ทำการจัดเก็บไว้ในเครื่องคอมพิวเตอร์ที่อยู่ในเครือข่ายของหน่วยงาน ส่งผลให้มีความเสี่ยงในการทำงานเทคโนโลยีสารสนเทศ เพื่อให้การเข้าถึงสารสนเทศและการสื่อสารต่าง ๆ รวมทั้งระบบอินเทอร์เน็ตมีความมั่นคงปลอดภัย ป้องกันการรั่วไหลของข้อมูลและเป็นการป้องกันโปรแกรมไม่ประสงค์ดีต่าง ๆ และเป็นการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกระทรวงสาธารณสุข พ.ศ. 2565 จึงได้ได้ตระหนักถึงความสำคัญของการควบคุมการเข้าถึงระบบเครือข่ายเพื่อเป็นการป้องกันปัญหาที่อาจจะเกิดขึ้นจากการให้บริหารเครือข่ายทั้งทางตรงและทางอ้อม จึงต้องมีการควบคุมการเข้าถึงการบริการทางเครือข่ายผู้รับการประเมินในนำหลักงาน PDCA (Plan – Do – Check - Act) มาเป็นแนวทางในการพัฒนาระบบ และได้นำเครื่องมือ VMware ESXi ซึ่งเป็นเครื่องมือในการบริหารจัดการเครื่องคอมพิวเตอร์เสมือนจริงมาใช้ ร่วมกับการใช้ Windows Server 2012 พร้อมทั้งการจัดทำ Active Directory Domain Services และ Watchguard Firebox M4600 ที่ใช้ในการกำหนด Policy เพื่อเป็นการควบคุมการเข้าถึงเครือข่าย หลังจากที่ได้พัฒนาแล้วจึงได้มีการทดสอบจากผู้พัฒนาระบบเพื่อตรวจสอบความถูกต้องของการทำงาน และมีการวางแผนปรับปรุงข้อผิดพลาดที่จะนำไปสู่การพัฒนาระบบให้ดียิ่งขึ้นต่อไป

ดังนั้น จากการพัฒนาระบบงานดังกล่าว สำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช จึงมีระบบการยืนยันตัวบุคคลในการใช้งานอินเทอร์เน็ตเพื่อใช้ในการตรวจสอบกำกับดูแล ผู้ใช้งานให้ใช้ระบบเทคโนโลยีสารสนเทศ และการสื่อสารให้เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง

## กิตติกรรมประกาศ

การจัดทำเอกสารผลงาน เรื่อง “การยืนยันตัวบุคคลเพื่อเข้าใช้งานระบบเครือข่ายอินเทอร์เน็ตของสำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช” ฉบับนี้ สำเร็จลุล่วงได้ด้วยดี ขอขอบพระคุณผู้บริหารทุกท่านที่เล็งเห็นความสำคัญความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศซึ่งควรนำมาใช้ในการดำเนินงานภายในหน่วยงาน และนางสาวกรรณิกา สุวรรณหา หัวหน้ากลุ่มงานยุทธศาสตร์แผนงาน และเครือข่าย เป็นอย่างสูง ที่ให้การสนับสนุนในการพัฒนาระบบเทคโนโลยีสารสนเทศ ขอขอบคุณบุคลากรภายในหน่วยงานทุกท่านที่ให้ความร่วมมือและเห็นความสำคัญของการใช้ระบบเทคโนโลยี และการสื่อสารให้เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยต่อไป

ขอขอบคุณคณาจารย์ทุกท่านที่ถ่ายทอดวิชาความรู้ในด้านต่างๆ ให้สามารถนำทฤษฎีองค์ความรู้ที่ได้เรียนรู้นำมาปรับใช้ในการทำงาน

ขอขอบคุณผู้เขียนบทความ งานวิจัย เอกสารต่างๆ ทั้งในรูปแบบเอกสาร และในรูปแบบออนไลน์ทุกท่านทั้งที่ได้ระบุ และไม่ได้ระบุไว้ในเอกสารผลงานนี้ซึ่งทำให้มีข้อมูลที่ใช้ในการศึกษาค้นคว้า และอ้างอิง หากมีข้อบกพร่องประการใด ผู้ขอรับประเมินขออภัยไว้ และพัฒนาปรับปรุงในโอกาสต่อไป

นายเอกชัย แก้วเรืองฤทธิ์

## สารบัญ

	หน้า
บทคัดย่อ	ก
กิตติกรรมประกาศ	ข
สารบัญ	ค
สารบัญภาพ	จ
สารบัญตาราง	ฉ
<b>บทที่ 1 บทนำ</b>	<b>1</b>
1.1 ความเป็นมา และความสำคัญของผลงาน	1
1.2 วัตถุประสงค์ของการดำเนินการ	2
1.3 กรอบแนวคิด	2
1.4 ประโยชน์ที่คาดว่าจะได้รับ	3
1.5 คำจำกัดความ	3
<b>บทที่ 2 ความรู้ทางวิชาการหรือแนวคิดที่ใช้ในการดำเนินการ</b>	<b>4</b>
2.1 หลักการของวงจรคุณภาพ (PDCA)	4
2.2 การพิสูจน์ตัวตน (Authentication)	7
2.3 องค์ประกอบด้านความมั่นคงปลอดภัยของระบบสารสนเทศ : CIA Triad	8
2.4 เทคโนโลยีที่ใช้ในการปฏิบัติงาน	9
2.5 กฎหมาย นโยบาย มาตรฐาน ที่เกี่ยวข้องกับการปฏิบัติงาน	12
2.6 แนวคิดทฤษฎีเกี่ยวกับการประเมิน	14
2.7 ทฤษฎีการคำนวณหากลุ่มตัวอย่าง	15
<b>บทที่ 3 วิธีการดำเนินการ</b>	<b>16</b>
3.1 เครื่องมือที่ใช้วิจัย	16
3.2 การเก็บรวบรวมข้อมูล	16
3.3 วิเคราะห์ข้อมูล	17
3.4 การดำเนินการวิจัย	18
3.5 การวางแผนพัฒนาตามหลัก PDCA	22

## สารบัญ (ต่อ)

	หน้า
<b>บทที่ 4 ผลการดำเนินการ</b>	<b>24</b>
4.1 ขั้นตอนการวางแผน (Plan)	24
4.2 ดำเนินการตามแผนการพัฒนา (Do)	37
4.3 ผลการตรวจสอบการทำงาน (Check)	68
4.4 ขั้นตอนการดำเนินงานให้เหมาะสม (Act)	83
4.5 การวัดผลการพัฒนาระบบและแบบประเมินประสิทธิภาพ	88
<b>บทที่ 5 บทสรุป และข้อเสนอแนะ</b>	<b>103</b>
5.1 สรุปผล	103
5.2 การนำไปใช้ประโยชน์/ผลกระทบ	104
5.3 ความยุ่งยากและซับซ้อนในการดำเนินงาน	104
5.4 ปัญหาและอุปสรรคในการดำเนินงาน	105
5.5 ข้อเสนอแนะ	105
<b>บรรณานุกรม</b>	<b>106</b>
<b>ภาคผนวก</b>	<b>108</b>
ภาคผนวก ก ประกาศใช้แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	108
ภาคผนวก ข ประกาศการใช้งานระบบพิสูจน์ยืนยันตัวตน	110
ภาคผนวก ค คู่มือการใช้งานบนคอมพิวเตอร์	112
ภาคผนวก ง คู่มือการใช้งานบนมือถือ	116
ภาคผนวก จ คู่มือการเปลี่ยนรหัสผ่าน	122
ภาคผนวก ฉ แบบสอบถาม	128
ภาคผนวก ช ผลการเข้าใช้งานระบบเครือข่ายอินเทอร์เน็ตของบุคลากรในระยะเวลา 90 วัน	131

## สารบัญภาพ

	หน้า
ภาพที่ 1 กรอบแนวคิดการพัฒนาระบบ	2
ภาพที่ 2 หลักการพัฒนา PDCA (Plan – Do – Check - Act)	4
ภาพที่ 3 ตัวอย่างการแบ่ง Organizational Unit	10
ภาพที่ 4 จำลองการทำงานของ Lightweight Directory Access Protocol (LDAP)	11
ภาพที่ 5 แสดงผังงาน (Flowchart) เปรียบเทียบการเข้าถึงเครือข่ายด้วยรูปแบบเดิมเปรียบเทียบกับระบบใหม่โดยสามารถแสดงให้เห็นถึงกระบวนการยืนยันตัวตนบุคคลของระบบใหม่	25
ภาพที่ 6 แสดงลำดับกระบวนการทำงานของระบบในภาพรวม	26
ภาพที่ 7 แสดงลำดับกระบวนการทำงานของระบบในภาพรวม (User)	27
ภาพที่ 8 แสดงลำดับกระบวนการทำงานของระบบในภาพรวม (Administrator)	28
ภาพที่ 9 แสดงขั้นตอนการเข้าสู่ระบบ และการขอสิทธิ์การใช้งาน	30
ภาพที่ 10 แสดงขั้นตอนการเปลี่ยนรหัสผ่าน	31
ภาพที่ 11 แสดงขั้นตอนการรับข้อมูลจากงานการเจ้าหน้าที่ เพื่อทำการลงทะเบียนเพิ่ม/ลบ สิทธิ์การใช้งาน	32
ภาพที่ 12 แสดงผังงานการทำงานของระบบรายงานข้อมูลจราจรคอมพิวเตอร์	33
ภาพที่ 13 แสดงตัวอย่างข้อมูลที่ได้ทำการวิเคราะห์แล้วก่อนบันทึกลงระบบ Active Directory	35
ภาพที่ 14 แสดงขั้นตอนการร้องขอตรวจสอบประวัติการใช้งานระบบเครือข่ายอินเทอร์เน็ต โดยข้อมูลจราจรทางคอมพิวเตอร์	36
ภาพที่ 15 แสดงหน้าต่างการเข้าใช้งานโปรแกรม VMware vSphere Client	37
ภาพที่ 16 แสดงหน้าต่างการกำหนด CPUs cores ของเครื่องเสมือนจริง	38
ภาพที่ 17 แสดงหน้าต่างการกำหนด Memory ของเครื่องเสมือนจริง	39
ภาพที่ 18 แสดงหน้าต่างการกำหนด Disk size ของเครื่องเสมือนจริง	40
ภาพที่ 19 แสดงหน้าต่างรายละเอียดการตั้งค่าทั้งหมดของเครื่องเสมือนจริงตามที่ได้กำหนดไว้	41
ภาพที่ 20 แสดงการเลือก ISO Files ของ Windows ที่จะทำการติดตั้ง	42
ภาพที่ 21 แสดงการกำหนด IP address ของเครื่อง Server	43
ภาพที่ 22 แสดงหน้าต่างการติดตั้ง Roles and Features	44
ภาพที่ 23 ทำการเลือกเซิร์ฟเวอร์ที่จะทำการติดตั้ง Roles	45

## สารบัญภาพ (ต่อ)

	หน้า
ภาพที่ 24 แสดงหน้าต่างการเลือก Roles ที่จะทำการติดตั้ง	46
ภาพที่ 25 แสดงหน้าต่างสรุปการตั้งค่า Roles ที่ได้ทำการเลือกติดตั้ง	47
ภาพที่ 26 แสดงหน้าต่างการกำหนด domain name	48
ภาพที่ 27 แสดงหน้าต่างรายละเอียดการตั้งค่า domain controller และปุ่ม Install	49
ภาพที่ 28 แสดงหน้าต่าง Server Manager ผลการติดตั้ง Roles ของ Server หลังจาก Install เสร็จแล้ว	50
ภาพที่ 29 แสดงหน้าต่างการเปิดใช้งาน Network Policy Server	51
ภาพที่ 30 แสดงผลของการกำหนด Password Policy	52
ภาพที่ 31 การสร้าง organization unit (OU) เพื่อกำหนดชื่อตามกลุ่มงาน	53
ภาพที่ 32 แสดงหน้าต่างรายละเอียดข้อมูล New User	54
ภาพที่ 33 แสดงหน้าต่างการกำหนด Password New User	55
ภาพที่ 34 แสดงหน้าต่างสรุปผลการสร้าง User	55
ภาพที่ 35 แสดงตัวอย่างการคลิกขวาที่ New User แล้วเลือกเมนู Add to a group	56
ภาพที่ 36 แสดงหน้าต่างการ Select Groups หลังจากที่ได้ทำการ Check Names	56
ภาพที่ 37 แสดงจำนวนรูปแบบการเชื่อมต่อที่สามารถเชื่อมต่อได้บน Firewall	57
ภาพที่ 38 แสดงวิธีการกำหนด Domain Name	58
ภาพที่ 39 แสดงการกำหนด session Authentication โดยกำหนดค่าการใช้งาน	59
ภาพที่ 40 แสดงหน้าต่าง Firewall Policies > ADD Policy	60
ภาพที่ 41 แสดงหน้าต่างการ ADD Member type เป็น group ที่ได้กำหนดไว้ใน ADDS	60
ภาพที่ 42 แสดงผลการ configure firewall policy ที่ได้กำหนดให้ User จาก group ODPC11 สามารถเข้าถึงเครือข่าย	61
ภาพที่ 43 แสดงหน้าต่างการเลือก Windows 10 ISO Files สำหรับติดตั้ง	62
ภาพที่ 44 แสดงหน้าต่างการกำหนด IP Address	63
ภาพที่ 45 แสดงหน้าต่างการติดตั้ง Watchguard System manager	64
ภาพที่ 46 แสดงหน้าต่างการกำหนดการเชื่อมต่อ WatchGuard System Manager	65
ภาพที่ 47 แสดงรายการ Device ของ Firebox ที่ได้ทำการเชื่อมต่อไว้	66

## สารบัญภาพ (ต่อ)

	หน้า
ภาพที่ 48 แสดงหน้าต่างการกำหนดการตั้งค่าการ์ดเก็บ Log Files	67
ภาพที่ 49 แสดงหน้าต่าง Firewall Management เมนู TEST CONNECTION FOR LDAP AND ACTIVE DIRECTORY	68
ภาพที่ 50 แสดงหน้าต่างการทดสอบด้วย Username และ Password ที่ถูกต้อง	69
ภาพที่ 51 แสดงหน้าต่างการทดสอบด้วย Username และ Password ที่ถูกต้อง	69
ภาพที่ 52 หน้าต่างแสดงผลการเข้าสู่ระบบสำเร็จ	71
ภาพที่ 53 แสดงหน้าต่างการแจ้งเตือนเข้าใช้งานไม่สำเร็จ	71
ภาพที่ 54 แสดงหน้าต่างการเข้าสู่โปรแกรมจัดเก็บ Log Files	72
ภาพที่ 55 แสดงหน้าต่างการเข้าสู่โปรแกรมจัดเก็บ Log Files	72
ภาพที่ 56 แสดงหน้าต่าง Dash board ของการจัดเก็บ Log Files	73
ภาพที่ 57 แสดงหน้าต่างโปรแกรม PuTTY สำหรับเชื่อมต่อไปยัง Firewall	73
ภาพที่ 58 แสดงหน้าต่างโปรแกรม PuTTY สำหรับ login ใช้งาน	74
ภาพที่ 59 แสดงการใช้คำสั่ง show log-setting watchguard-log-server เพื่อดูปลายทางในการจัดเก็บ Log ของ Firewall	74
ภาพที่ 60 แสดงผลการทดสอบหลังใช้งานระบบ Authentication	76
ภาพที่ 61 แสดงผลการตรวจสอบผู้ใช้งานระบบเครือข่ายก่อนการใช้งาน ระบบ Authentication	77
ภาพที่ 62 แสดงผลการตรวจสอบผู้ใช้งานระบบเครือข่ายหลังการใช้งาน ระบบ Authentication	77
ภาพที่ 63 แสดงระบุระยะเวลาในการค้นหาข้อมูล Log ย้อนหลัง	80
ภาพที่ 64 แสดงผลการตรวจสอบการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log Files)	81
ภาพที่ 65 แสดงตัวอย่างข้อมูลการค้นหา Log Files	82
ภาพที่ 66 แสดงผลปรับปรุงขนาดของพื้นที่ในการจัดเก็บเพิ่มจากเดิม 100 GB เป็น 300 GB	83
ภาพที่ 67 แสดงการจัดลำดับ Policy บน Firewall	85
ภาพที่ 68 แสดงผลการค้นหาประวัติการใช้งานอินเทอร์เน็ตตามข้อมูลที่ได้รับร้องขอ	86
ภาพที่ 69 แสดงการ Export ข้อมูลให้อยู่ในรูปแบบ CSV เพื่อส่งมอบให้แก่ผู้ร้องขอ	87
ภาพที่ 70 ประกาศใช้แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	109
ภาพที่ 71 ประกาศการใช้งานระบบพิสูจน์ยืนยันตัวตน	111



## สารบัญภาพ (ต่อ)

	หน้า
ภาพที่ 72 หน้าต่างการเข้าสู่ระบบ	113
ภาพที่ 73 หน้าต่างแจ้งเตือนการเชื่อมต่อเครือข่าย	113
ภาพที่ 74 หน้าต่างการระบบ URL	114
ภาพที่ 75 หน้าต่างการอนุญาตการเข้าถึง	114
ภาพที่ 76 หน้าต่างการเข้าสู่ระบบ	115
ภาพที่ 77 หน้าเว็บไซต์ Google	115
ภาพที่ 78 หน้าต่างการเข้าสู่ระบบสำเร็จ	115
ภาพที่ 79 หน้าต่างการเชื่อมต่อ Wireless	117
ภาพที่ 80 หน้าต่างการลิ้ม Wireless	118
ภาพที่ 81 หน้าต่างการยืนยันการลิ้ม Wireless	119
ภาพที่ 82 หน้าต่างการเชื่อมต่อ Wireless ใหม่อีกครั้ง	120
ภาพที่ 83 หน้าต่างการเข้าสู่ระบบ Authentication	121
ภาพที่ 84 ตัวอย่าง User และ Password ที่ได้รับ	123
ภาพที่ 85 QR code เข้าสู่เว็บไซต์เปลี่ยนรหัสผ่าน	123
ภาพที่ 86 เว็บไซต์ ให้กดปุ่ม Advanced หรือขั้นสูง	124
ภาพที่ 87 หน้าต่างการ Proceed to unsafe	124
ภาพที่ 88 หน้าต่างการเปลี่ยนรหัสผ่าน	125
ภาพที่ 89 หน้าต่างการเปลี่ยนรหัสผ่าน	126
ภาพที่ 90 หน้าต่างการเปลี่ยนรหัสผ่าน	126
ภาพที่ 91 แบบฟอร์มการแจ้งลิ้มชื่อผู้ใช้หรือรหัสผ่าน	127

## สารบัญตาราง

	หน้า
ตารางที่ 1 โครงสร้างตารางข้อมูล	16
ตารางที่ 2 ประเด็นและรายละเอียดเกณฑ์การให้คะแนน	21
ตารางที่ 3 แสดงผลการเปรียบเทียบทรัพยากรของหน่วยงาน	24
ตารางที่ 4 แสดงตารางโครงสร้างการจัดเก็บข้อมูล	35
ตารางที่ 5 แสดงผลการทดสอบระบบ	70
ตารางที่ 6 แสดงผลการตรวจสอบการทำงาน	71
ตารางที่ 7 การตรวจสอบคุณลักษณะเครื่องเซิร์ฟเวอร์	75
ตารางที่ 8 การตรวจสอบคุณลักษณะเฉพาะเครื่องคอมพิวเตอร์ log files	75
ตารางที่ 9 แสดงผลการเปรียบเทียบการทดสอบการใช้งานก่อนและหลังติดตั้งระบบ	76
ตารางที่ 10 เปรียบเทียบการทำงานก่อนและหลังการใช้งานระบบ	78
ตารางที่ 11 สรุปผลการเข้าใช้งานระบบเครือข่ายอินเทอร์เน็ตของบุคลากรในระยะเวลา 90 วัน	78
ตารางที่ 12 แสดงความหมายของข้อมูลที่จัดเก็บเป็น Log Files	80
ตารางที่ 13 แสดงตารางการบำรุงรักษาเครื่อง Server	84
ตารางที่ 14 แสดงสถิติการใช้งานระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log Files) ของสำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช จำนวน 90 วัน ระหว่างวันที่ 24 กันยายน พ.ศ. 2566 ถึงวันที่ 22 ธันวาคม พ.ศ. 2566	88
ตารางที่ 15 ผลการประเมิน	92
ตารางที่ 16 ผลการศึกษาปัจจัยส่วนบุคคล แยกตามช่วงอายุ	94
ตารางที่ 17 ผลการศึกษาปัจจัยส่วนบุคคล ด้านกลุ่มที่ปฏิบัติงาน	94
ตารางที่ 18 ผลการศึกษาปัจจัยด้านระดับการปฏิบัติงาน	95
ตารางที่ 19 แสดงผลการประเมินความสำเร็จของระบบด้านประสิทธิภาพของระบบ ของผู้บริหารและหัวหน้ากลุ่ม	97
ตารางที่ 20 แสดงผลการประเมินความสำเร็จของระบบด้านประสิทธิภาพของระบบของผู้ปฏิบัติงาน	97
ตารางที่ 21 แสดงผลการประเมินความสำเร็จของระบบด้านประสิทธิภาพของระบบ	97
ตารางที่ 22 แสดงผลการประเมินความสำเร็จของระบบด้านความสำคัญของการป้องกันระบบ ของผู้บริหารและหัวหน้ากลุ่ม	98

## สารบัญตาราง (ต่อ)

	หน้า
ตารางที่ 23 การประเมินความสำเร็จของระบบด้านความสำคัญของการป้องกันระบบของผู้ปฏิบัติงาน	99
ตารางที่ 24 แสดงผลการประเมินความสำเร็จของระบบด้านความสำคัญของการป้องกันระบบ	99
ตารางที่ 25 แสดงผลการประเมินความสำเร็จของระบบด้านความน่าเชื่อถือของระบบ ของผู้บริหารและหัวหน้ากลุ่ม	100
ตารางที่ 26 แสดงผลการประเมินความสำเร็จของระบบด้านความน่าเชื่อถือของระบบของผู้ปฏิบัติงาน	100
ตารางที่ 27 แสดงผลการประเมินความสำเร็จของระบบด้านความน่าเชื่อถือของระบบ	100
ตารางที่ 28 แสดงผลการประเมินความสำเร็จของระบบด้านคุณภาพการให้บริการ ของผู้บริหารและหัวหน้ากลุ่ม	101
ตารางที่ 29 แสดงผลการประเมินความสำเร็จของระบบด้านคุณภาพการให้บริการของผู้ปฏิบัติงาน	102
ตารางที่ 30 แสดงผลการประเมินความสำเร็จของระบบด้านคุณภาพการให้บริการ	102
ตารางที่ 31 ผลของการตรวจสอบการใช้งานระบบการยืนยันตัวตนบุคคลเพื่อเข้าใช้งาน ระบบเครือข่ายอินเทอร์เน็ต	103
ตารางที่ 32 แสดงผลการประเมินความสำเร็จของระบบในการใช้งานระบบใน 4 ปีจ้าย	104

# บทที่ 1

## บทนำ

### 1.1 ความเป็นมาและความสำคัญของการดำเนินงาน

สำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช สังกัดกรมควบคุมโรค เป็นหน่วยงานวิชาการ ด้านป้องกันควบคุมโรค มีบทบาทหน้าที่ในการเฝ้าระวัง ติดตาม นิเทศ ถ่ายทอดองค์ความรู้ด้านการป้องกัน ควบคุมโรคแก่หน่วยงานเครือข่าย โดยทั่วไปการปฏิบัติงานของบุคลากรมีความจำเป็นต้องใช้เทคโนโลยี สารสนเทศในการวิเคราะห์ ประมวลผลข้อมูลด้านโรคและสุขภาพ ซึ่งได้จัดเก็บไว้ในเครื่องคอมพิวเตอร์ที่อยู่ใน เครือข่ายของหน่วยงาน ส่งผลให้มีความเสี่ยงในงานเทคโนโลยีสารสนเทศ

สำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช ได้ดำเนินการตามนโยบายระบบราชการ 4.0 ของรัฐบาล เพื่อให้มีการนำระบบเทคโนโลยีสารสนเทศและการสื่อสาร มาใช้ในการสนับสนุนการ ปฏิบัติงานให้เป็นไปอย่างเหมาะสม มีประสิทธิภาพ แม้การนำเทคโนโลยีสารสนเทศและการสื่อสารมาใช้ใน หน่วยงานจะช่วยให้การดำเนินงานมีประสิทธิภาพมากยิ่งขึ้น แต่ส่งผลให้มีความเสี่ยงต่อความมั่นคง ปลอดภัยของข้อมูล การใช้งานระบบอินเทอร์เน็ต และการป้องกันโปรแกรมไม่ประสงค์ดี เพื่อให้การเข้าถึง สารสนเทศและการสื่อสารต่าง ๆ รวมทั้งระบบอินเทอร์เน็ตมีความมั่นคงปลอดภัย ป้องกันการรั่วไหลของ ข้อมูล รวมทั้งเป็นการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกระทรวงสาธารณสุข พ.ศ. 2565

หน่วยงานได้ตระหนักถึงความสำคัญของการควบคุมการเข้าถึงระบบเครือข่ายเพื่อเป็นการป้องกัน ปัญหาที่อาจเกิดขึ้นจากการให้บริการเครือข่ายทั้งทางตรงและทางอ้อม จึงดำเนินการควบคุมการเข้าถึง การบริการทางเครือข่าย โดยต้องกำหนดสิทธิ์ในการเข้าถึงเครือข่าย ผู้ที่จะเข้าใช้งานต้องลงบันทึกเข้าใช้ งาน (Login) ซึ่งจะแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใส่รหัสผ่านก่อนเข้าใช้งาน และกำหนดระยะเวลาเชื่อมต่อระบบสารสนเทศเพื่อให้การใช้งานระบบ เครือข่ายและอินเทอร์เน็ตของหน่วยงานมีความมั่นคงปลอดภัยสามารถควบคุมการเข้าถึงโดยไม่สามารถ อนุญาตจากบุคคลภายนอกได้

ดังนั้นการยืนยันตัวบุคคลเพื่อการเข้าใช้งานระบบเครือข่ายอินเทอร์เน็ตของสำนักงานป้องกันควบคุม โรคที่ 11 จังหวัดนครศรีธรรมราช จึงเป็นไปตามนโยบายและแนวปฏิบัติ ทำให้มีการพัฒนาระบบการยืนยัน ตัวบุคคลที่เข้าใช้งานระบบเครือข่ายอินเทอร์เน็ต เพื่อทำการจัดเก็บข้อมูลบุคลากรของหน่วยงานที่มีสิทธิ์ ใช้งาน และเป็นการจัดเก็บข้อมูลการจราจรทางคอมพิวเตอร์ซึ่งเป็นไปตามพระราชบัญญัติว่าด้วยการ

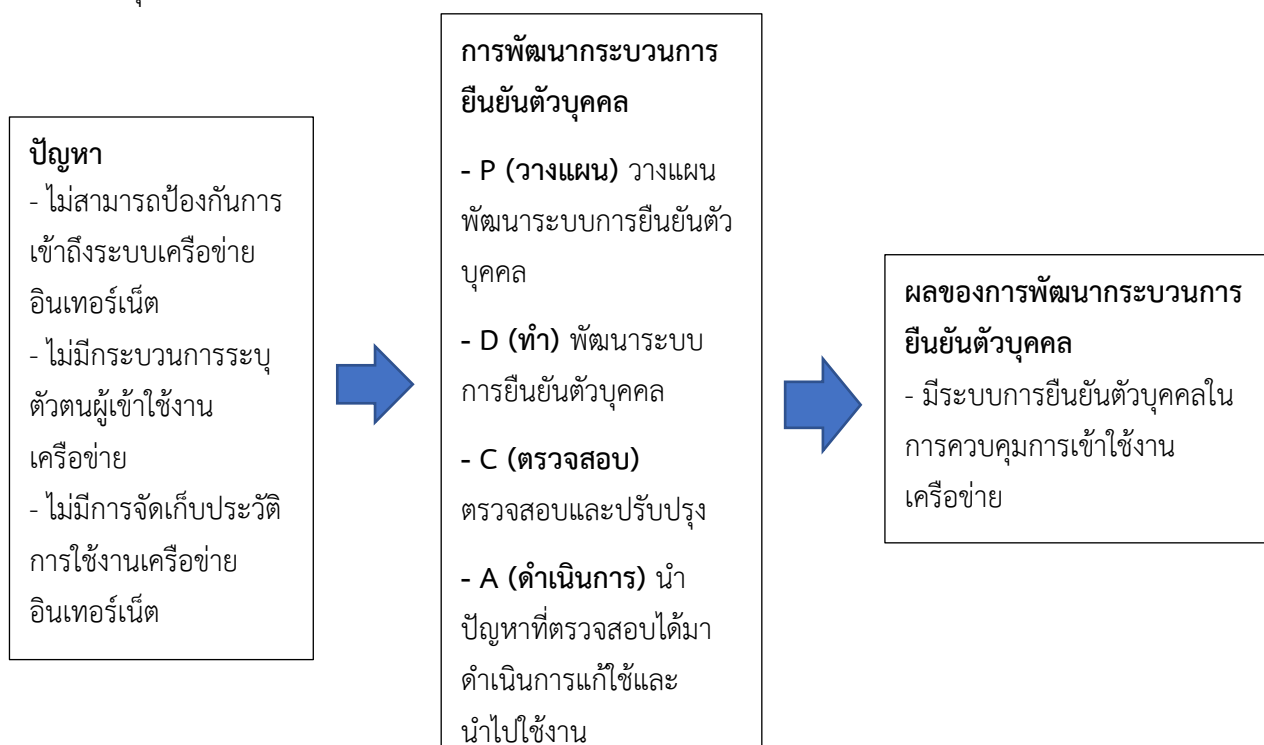
กระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 ฉบับที่ 2 รวมทั้งเป็นการสร้างความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน

## 1.2 วัตถุประสงค์ของการดำเนินการ

1. เพื่อให้สามารถควบคุมการเข้าถึงการใช้งานระบบเครือข่ายอินเทอร์เน็ตของสำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช
2. เพื่อให้สามารถยืนยันตัวตนบุคคลที่ใช้งานระบบเครือข่ายอินเทอร์เน็ตของสำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช
3. เพื่อให้สามารถสืบค้นข้อมูลการจราจรทางคอมพิวเตอร์ (Log File) ย้อนหลังได้ไม่น้อยกว่าเก้าสิบวัน เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 มาตราที่ 26

## 1.3 กรอบแนวคิด

การดำเนินงานในครั้งนี้ เป็นการพัฒนาระบบยืนยันตัวตนบุคคลที่ใช้งานระบบเครือข่ายอินเทอร์เน็ตของสำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกที่ไม่ได้รับอนุญาตเข้าถึงระบบสารสนเทศของหน่วยงาน ซึ่งเน้นที่กระบวนการพิสูจน์ตัวตน (Identification and Authentication) ของผู้ใช้บริการ โดยใช้หลักการ PDCA (Plan – Do – Check - Act) ซึ่งเป็นเครื่องมือที่ใช้เพื่อปรับปรุงกระบวนการทำงานอย่างเป็นระบบ นำมาใช้เป็นแนวคิดหลักในการพัฒนาระบบสารสนเทศ



ภาพที่ 1 กรอบแนวคิดการพัฒนาระบบ

## 1.4 ประโยชน์ที่คาดว่าจะได้รับ

1. สำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช ได้ปฏิบัติตามแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ทำให้หน่วยงานมีความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ป้องกันการเข้าถึงระบบเครือข่ายจากบุคคลภายนอกที่ไม่ได้รับอนุญาต
2. สำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช มีระบบที่สามารถยืนยันตัวตนบุคคลที่ใช้งานระบบเครือข่ายอินเทอร์เน็ตโดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใส่รหัสผ่านก่อนเข้าใช้งานซึ่งเป็นการควบคุมการเข้าถึงเครือข่าย
3. สำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช มีระบบที่สามารถจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ไว้นานอย่างน้อยเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ ตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 ฉบับที่ 2 ทำให้สามารถดูข้อมูลประวัติการใช้งานอินเทอร์เน็ตได้ย้อนหลังได้

## 1.5 คำจำกัดความ

1. Active Directory (AD) เป็นโครงสร้างระบบจัดการผู้ใช้และความปลอดภัยของ Windows Server
2. Active Directory Domain Service (AD DS) เป็นบริการไต่แรกทอรีของ Windows Server ช่วยให้ผู้ใช้ดูแลระบบสามารถจัดการและกำหนดสิทธิ์การเข้าถึงทรัพยากรต่างๆ
3. Authentication หมายถึง กระบวนการระบุตัวตนและกระบวนการพิสูจน์ตัวตนว่าบุคคลนั้นเป็นผู้มีสิทธิ์เข้าใช้งานระบบเครือข่ายอินเทอร์เน็ตของหน่วยงาน
4. User หมายถึง ผู้ใช้งานระบบซึ่งเป็นบุคลากรภายใต้สำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช
5. ระบบการยืนยันตัวตนบุคคล หรือระบบ Authentication หมายถึง ระบบยืนยันตัวตนบุคคลเพื่อเข้าใช้งานระบบเครือข่ายอินเทอร์เน็ตของสำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช
6. Log Files คือ ข้อมูลการจราจรทางคอมพิวเตอร์ที่เกิดขึ้นจากการใช้งานระบบเครือข่ายอินเทอร์เน็ต
7. หน่วยงาน หมายถึง สำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช

## บทที่ 2

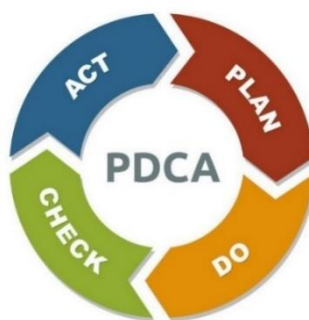
### ความรู้ทางวิชาการหรือแนวคิดที่ใช้ในการดำเนินการ

การศึกษาเรื่องการยืนยันตัวตนบุคคลเพื่อเข้าใช้งานระบบเครือข่ายอินเทอร์เน็ตของสำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช ผู้ศึกษาได้ทบทวนวรรณกรรมที่เกี่ยวข้องเพื่อกำหนดกรอบการศึกษา ดังนี้

- 2.1 ระบบวงจรคุณภาพ PDCA
- 2.2 การพิสูจน์ตัวตน (Authentication)
- 2.3 องค์ประกอบด้านความมั่นคงปลอดภัยของระบบสารสนเทศ : CIA Triad
- 2.4 เทคโนโลยีที่ใช้ในการปฏิบัติงาน
- 2.5 กฎหมาย นโยบาย มาตรฐาน ที่เกี่ยวข้องกับการปฏิบัติงาน
- 2.6 แนวคิดทฤษฎีเกี่ยวกับการประเมิน
- 2.7 ทฤษฎีการคำนวณหากลุ่มตัวอย่าง Taro Yamane

#### 2.1 หลักการของวงจรคุณภาพ (PDCA) [1]

PDCA หรือวงจรเดมมิง (Deming Cycle) หรือวงจรชูฮาร์ต (Shewhart Cycle) คือ วงจรบริหารงานคุณภาพ ประกอบไปด้วย 4 ขั้นตอน Plan – Do – Check - Act เป็นกระบวนการที่ใช้ปรับปรุงการทำงานขององค์กรอย่างเป็นระบบ โดยมีเป้าหมายเพื่อแก้ปัญหาและเกิดการพัฒนาอย่างต่อเนื่อง (Continuous improvement)



ภาพที่ 2 หลักการพัฒนา PDCA (Plan – Do – Check - Act)

โครงสร้าง PDCA ประกอบด้วย 4 ขั้นตอน ดังนี้

- |           |                             |
|-----------|-----------------------------|
| P – Plan  | คือ การวางแผน               |
| D – DO    | คือ การปฏิบัติตามแผน        |
| C – Check | คือ การตรวจสอบ              |
| A – Act   | คือ การปรับปรุงการดำเนินการ |

### 2.1.1 P – Plan ระบุและวิเคราะห์ปัญหา

เริ่มต้นการวางแผนจะต้องมีเป้าหมายที่ชัดเจนเสียก่อน โดยขั้นตอนนี้ต้องกำหนดให้ครอบคลุมทั้งกระบวนการตั้งแต่เริ่มไปจนถึงสิ้นสุด

การค้นหาปัญหาขององค์กร (Problem Recognition) คือ การกำหนดเป้าหมายที่ชัดเจนในการปรับปรุงโดยใช้ระบบเข้ามาช่วยนำข้อมูลปัญหาที่ได้มาจำแนกจัดกลุ่มและจัดลำดับความสำคัญเพื่อใช้คัดเลือกโครงการที่เหมาะสมที่สุดมาพัฒนา โดยโครงการที่จะทำการพัฒนาต้องสามารถแก้ปัญหาที่มีในองค์กรและให้ประโยชน์กับองค์กรมากที่สุด

Action Plan [2] คือ แผนปฏิบัติการทำงาน ที่ผ่านการคิดและการวางแผนมาอย่างละเอียดแล้ว เพื่อเป็นตัวกำหนดแผนการดำเนินงานทั้งหมดให้บรรลุวัตถุประสงค์ หรือกล่าวง่าย ๆ คือ ถูกสร้างมาให้เป็นแบบแผนในการปฏิบัติงาน โดยจะระบุรายละเอียดในแต่ละช่วงของการปฏิบัติงานว่า มีกิจกรรมอะไรบ้าง หรือมีการปฏิบัติงานกันอย่างไร ซึ่ง Action Plan นี้จะช่วยตรวจสอบการทำงานในแต่ละขั้นตอนของแผนปฏิบัติการทำงาน ให้สำเร็จลุล่วงตามเป้าหมาย

นอกจากนี้การใช้ Action Plan ยังสามารถบ่งบอกได้ถึงความสำเร็จของแต่ละงานได้ด้วย ช่วยให้ทุกคนที่มีความเกี่ยวข้องกับงาน มีแนวโน้มเข้าใจและปฏิบัติไปในทิศทางเดียวกัน ซึ่งก็จะช่วยให้การทำงานสำเร็จได้อย่างราบรื่น เร็ว และง่ายขึ้น

องค์ประกอบของ Action Plan มีดังนี้

- ชื่อแผนงาน (Name) ในการทำงานแต่ละชิ้นจำเป็นจะต้องระบุชื่อแผนงานให้ชัดเจน เพราะจะช่วยให้คนในทีม หรือคนที่เกี่ยวข้องกับชิ้นงานสามารถปฏิบัติตามได้อย่างถูกต้อง และไม่สับสน
- กระบวนการทำงาน (Process) โดยจะต้องระบุขั้นตอนหลัก ๆ ไว้ตั้งแต่ขั้นตอนแรกจนถึงขั้นตอนสุดท้าย
- กิจกรรมการทำงาน (Activity) คือสิ่งที่เอาไว้ระบุสิ่งที่ต้องทำในแต่ละขั้นตอนของการทำงาน เพื่อกำหนดให้ทีมหรือผู้ที่เกี่ยวข้องปฏิบัติงานไปในทิศทางเดียวกัน
- กำหนดช่วงระยะเวลา (Deadline) โดยจะต้องระบุช่วงระยะเวลาของแต่ละกิจกรรม และขั้นตอนทั้งหมดของกระบวนการทำงานว่าเริ่มและสิ้นสุดเมื่อใด เพื่อตรวจสอบความสำเร็จในแต่ละขั้นตอน
- แผนสำรอง (Backup plan) ควรมีไว้ในกรณีแผนที่ตั้งไว้เกิดมีปัญหาหรืออุปสรรค ดังนั้นจึงควรมีแผนสำรองเพื่อให้งานสำเร็จลุล่วงตามเป้าหมาย
- ประเมินความเสี่ยง (Risk) ที่อาจเกิดขึ้นในแผนการทำงานทั้งหมด รวมถึงในแต่ละกิจกรรมด้วย



- ผู้รับผิดชอบ (Owner) ในแผนการทำงานทั้งหมด จะต้องเป็นผู้รับผิดชอบเพื่อคอยตรวจสอบและติดตามงานทั้งกระบวนการ เพื่อให้งานสำเร็จตามแผนที่วางไว้

- งบประมาณ (Budget) ขั้นตอนใด ๆ ที่กำหนดไว้จะต้องคำนึงถึงงบประมาณที่ตั้งเอาไว้ด้วย เพื่อลดความเสียหายที่อาจเกิดขึ้นได้

### 2.1.2 D – DO พัฒนาทางออกและดำเนินการตามแผน

หลังจากกำหนดแผนแล้วก็ถึงเวลาที่จะลงมือทำ เพราะจะต้องนำแผนดังกล่าวมาใช้จริง ดำเนินการจริง เพื่อให้เห็นผลลัพธ์จริง

ในขั้นตอนนี้ต้องระลึกไว้เสมอว่า การดำเนินการจะเกิดปัญหาอื่นตามมาเสมอ จึงเป็นเหตุผลว่าควรใช้แผนดังกล่าวกับทีมงานหรือไม่ก็คนหรือเป็นโปรเจกต์เล็ก ๆ เสียก่อน เพราะสภาพแวดล้อมที่ควบคุมได้ จะป้องกันความเสียหายที่เกิดขึ้นไม่ให้ส่งผลกระทบต่อทั้งบริษัท

### 2.1.3 C – Check ประเมินและสรุปผล

เมื่อดำเนินการมาถึงจุดหนึ่งแล้ว จะต้องตรวจสอบให้ได้ว่า แผนดังกล่าวมีผลลัพธ์เป็นไปตามตัวชี้วัดที่ต้องการหรือไม่

ถ้าประสบความสำเร็จตามตัวชี้วัด ก็สามารถดำเนินการไปสู่ขั้นตอนสุดท้ายได้เลย แต่ถ้าไม่ประสบความสำเร็จ ก็ควรนำข้อมูลที่ได้มาวิเคราะห์หาสาเหตุของปัญหา แล้วดำเนินการขั้นตอนที่ 1 – 3 ใหม่จนกว่าจะประสบความสำเร็จหรือผ่านตัวชี้วัดที่กำหนดไว้

### 2.1.4 A – Act ปรับปรุงแก้ไขและวางแผนใหม่ต่อไป

ถ้าการปฏิบัติแผนดังกล่าวประสบความสำเร็จเป็นอย่างดี ก็ถึงเวลานำแผนนั้นมาประยุกต์ใช้กับทุกคน องค์กร ผ่านการประกาศ ประชุม อีเมล หรือการจัดการอบรมภายในบริษัท เพื่อสร้างการเปลี่ยนแปลงจนเกิดตามมาตรฐานใหม่

## 2.2 การพิสูจน์ตัวตน (Authentication) [3]

การระบุตัวตนการพิสูจน์ตัวตน และการให้สิทธิ์ เป็นกระบวนการที่นำเทคโนโลยีมาใช้ควบคู่กับทรัพยากรคนและกระบวนการ เพื่อเป็นการเพิ่มประสิทธิภาพและศักยภาพในการรักษาความลับ (Confidentiality) ความถูกต้อง (Integrity) และความพร้อมใช้ของข้อมูล (Availability) รวมถึงเพื่อไม่ให้เกิดการถูกคุกคามโดยผู้ไม่ประสงค์ดีหรือจากโปรแกรมบางประเภทได้เพิ่มมากขึ้น หากเกิดการคุกคามหรือถูกบุกรุกขึ้นอาจนำมาซึ่งความเสียหายอย่างมากมาต่อองค์กร ในการดำเนินการนี้จะช่วยให้รูปแบบการรักษาความปลอดภัยของข้อมูลเป็นไปอย่างเหมาะสม และช่วยลดความเสี่ยงจากการปลอมแปลงตัวบุคคลที่เกิดมาจากการทำธุรกรรมต่าง ๆ โดยรูปแบบของกระบวนการเหล่านี้ถือว่าเป็นองค์ประกอบที่สำคัญ เนื่องจากจำเป็นต้องอาศัยเทคโนโลยี และความรู้เฉพาะทางเพื่อที่จะใช้ในการควบคุมข้อมูลต่าง ๆ ซึ่งสามารถแบ่งออกเป็น 3 ขั้นตอนดังนี้

### 2.2.1 การระบุตัวตน (Identification)

การระบุตัวตน เป็นการค้นหาและเปรียบเทียบตัวบุคคลโดยดึงข้อมูลจากระบบที่เป็นฐานข้อมูลของผู้ใช้งาน ซึ่งเป็นขั้นตอนที่ผู้ใช้งานจำเป็นต้องแสดงตัวตน เช่น การกรอกชื่อผู้ใช้งาน (Username) หรือรหัสผู้ใช้งาน (User ID) เพื่อเข้าใช้งานในระบบ หรือการใช้บัตรประจำตัวประชาชนในการระบุตัวตนของแต่ละบุคคล ทั้งนี้ในปัจจุบันชื่อผู้ใช้งาน และรหัสผู้ใช้งาน อาจจะไม่เพียงพอที่จะใช้ในการระบุตัวตนของผู้ใช้งานจริง ดังนั้นจำเป็นต้องเก็บข้อมูลอย่างอื่น เพื่อนำมาประกอบในการตรวจสอบความน่าเชื่อถือของผู้ใช้งาน เช่น ชื่อผู้ใช้งาน (Username/User ID) รหัสผ่าน (Password) ข้อมูลส่วนบุคคล (Data Privacy) สิทธิ์ในการเข้าใช้งาน (Access Right) เป็นต้น

### 2.2.2 การยืนยันพิสูจน์ตัวตน (Authentication)

การพิสูจน์ตัวตน เป็นการตรวจสอบที่ช่วยสร้างความมั่นใจ และเป็นเครื่องยืนยันว่าเป็นบุคคลนั้นจริง ขั้นตอนการพิสูจน์ตัวตนสามารถใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ในการพิสูจน์ตัวตน โดยการพิสูจน์ตัวตนผ่านชื่อผู้ใช้งาน และรหัสผ่าน เป็นวิธีการที่พบเจอได้มากที่สุด อย่างไรก็ตามกลไกของการพิสูจน์ตัวตน (Authentication mechanisms) ที่นำมาช่วยในการสร้างความปลอดภัย สามารถแบ่งได้ 3 คุณลักษณะดังนี้

1. Knowledge factor คือ สิ่งที่คุณรู้ (Something You Know) ข้อมูลที่เจ้าของข้อมูลรู้เพียงคนเดียว เช่น รหัสผ่าน (password) หรือการใช้พิน (PINs) เป็นต้น

2. Possession factor คือ สิ่งที่คุณมี (Something You Have) ข้อมูลที่สามารถยืนยันว่าเป็นตัวเจ้าของจริง เช่น พาสปอร์ต บัตรประจำตัวประชาชน กุญแจหรือคีย์การ์ด เป็นต้น

3. Biometric factor คือ สิ่งที่คุณเป็น (Something You Are) ข้อมูลที่ไม่สามารถเปลี่ยนแปลงได้ เช่น ลายนิ้วมือ ม่านตา โครงหน้า เสียง เป็นต้น

### 2.2.3 การให้สิทธิ์ (Authorization)

การให้สิทธิ์ เป็นลักษณะหนึ่งของการควบคุมความมั่นคงปลอดภัย (Security Controls) โดยเป็นการเข้าถึงหรือสิทธิ์ของผู้ใช้งานที่จะเข้ามาใช้งานในระบบต่าง ๆ โดยการพิสูจน์ตัวตน (Authentication) ต้องทำควบคู่กับการให้สิทธิ์ (Authorization) ซึ่งไม่สามารถตัดกระบวนการใดกระบวนการหนึ่งออกไปได้ อันดับแรกให้ดำเนินการกระบวนการพิสูจน์ตัวตนก่อน เพื่อแสดงให้เห็นว่าเป็นบุคคลดังกล่าวจริง คือผู้เข้าใช้ระบบต้องถูกยอมรับจากระบบว่าสามารถเข้าสู่ระบบได้ และลำดับถัดมาเป็นการให้สิทธิ์ คือข้อจำกัดของบุคคลที่เข้ามาในระบบ ว่าบุคคลนั้นสามารถทำอะไรกับระบบได้บ้าง ดังนั้นการให้สิทธิ์จึงสามารถแบ่งออกเป็น 3 รูปแบบดังนี้

1. การให้สิทธิ์เป็นรายบุคคล ใช้สำหรับพิสูจน์ตัวตน และอนุญาตให้เข้าถึงตามสิทธิ์ที่กำหนดไว้
2. การให้สิทธิ์เป็นรายกลุ่ม ใช้สำหรับการกำหนดสิทธิ์ให้แต่ละกลุ่มรูปแบบนี้จะใช้ทรัพยากรน้อย และนิยมใช้กันอย่างแพร่หลาย
3. การให้สิทธิ์หลายระบบ เป็นกระบวนการที่พิสูจน์ตัวตน และอนุญาตให้เข้าใช้งานต่าง ๆ ได้ โดยที่รูปแบบนี้เป็นที่นิยม เนื่องจากชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) สามารถรองรับการให้ผู้ใช้งานลงชื่อเข้าใช้งานระบบ (Login) เพียงครั้งเดียว แต่สามารถเข้าหลายระบบได้โดยไม่ต้องลงชื่อเข้าใช้งานซ้ำ

## 2.3 องค์ประกอบด้านความมั่นคงปลอดภัยของระบบสารสนเทศ : CIA Triad [4]

The CIA Triad เป็นแนวคิดที่สำคัญในด้านการรักษาความปลอดภัยของข้อมูล ช่วยให้มั่นใจได้ในเรื่องของการปกป้องข้อมูลที่ละเอียดอ่อนจากการเข้าถึง การตัดแปลง หรือการทำลายโดยไม่ได้รับอนุญาต นอกจากนี้ยังเป็น Framework ที่มีประโยชน์สำหรับการประเมินการรักษาความปลอดภัยโดยรวมขององค์กร

The CIA Triad ประกอบไปด้วยตัวอักษรทั้งหมด 3 ตัว คือ

1. Confidentiality (การรักษาความลับ) การปกป้องข้อมูลจากการเข้าถึงหรือการเปิดเผยโดยไม่ได้รับอนุญาต ซึ่งหมายความว่าเฉพาะบุคคลที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงหรือดูข้อมูลที่ละเอียดอ่อนได้ การรักษาความลับสามารถทำได้ด้วยวิธีต่างๆ เช่น การเข้ารหัส (Encryption), การควบคุมการเข้าถึง (Access Controls) และการรับรองความถูกต้องของผู้ใช้ (User Authentication)
2. Integrity (ความสมบูรณ์) การรักษาความถูกต้องและความสอดคล้องของข้อมูล ซึ่งหมายความว่าไม่ควรมีการแก้ไขหรือทำลายข้อมูลในลักษณะที่ไม่ได้รับอนุญาต เพื่อให้มั่นใจถึงความสมบูรณ์ สามารถทำ

ได้ด้วยวิธีต่างๆ เช่น การสำรองและกู้คืนข้อมูล (Data backup and Recovery), อัลกอริทึมการตรวจสอบ (Checksum Algorithms) และลายเซ็นดิจิทัล (Digital Signatures)

3. Availability (ความพร้อมใช้งาน) ระบบและเครือข่ายต้องพร้อมใช้งานและทำงานอย่างถูกต้อง เพื่อให้สามารถเข้าถึงข้อมูลได้ สามารถใช้วิธีต่างๆ เช่น ความซ้ำซ้อน (Redundancy), ระบบเฟลโอเวอร์ (Failover systems) และโหลดบาลานซ์ (Load Balancing) เพื่อให้แน่ใจว่ามีความพร้อมใช้งาน

## 2.4 เทคโนโลยีที่ใช้ในการปฏิบัติงาน

### 2.4.1 Domain Controller

Domain Controller เป็นชื่อเรียกแทนเครื่อง Server ที่ใช้ทำหน้าที่เป็น Active Directory Domain Service ซึ่งจะทำหน้าที่จัดเก็บฐานข้อมูลของโดเมน (Domain database) และจัดการการสื่อสารระหว่างผู้ใช้งานกับโดเมน รวมถึงยังทำหน้าที่ให้บริการตรวจสอบการลงชื่อเข้าใช้ (Logon Authentication) การเข้าโดเมนของเครื่องคอมพิวเตอร์ลูกข่าย (Client computer) และผู้ใช้ (User)

### 2.4.2 Active Directory [5]

Active Directory เป็นเทคโนโลยี หรือการบริการที่เรียกว่า Directory Services ที่นำมาใช้เป็นศูนย์กลางในการบริหารจัดการทรัพยากรในระบบ ทั้งการจัดเก็บข้อมูลในรูปของ Object การคอนฟิกและการควบคุมการให้บริการ ซึ่ง Object ใน Active Directory เป็น Key หลักของข้อมูลใน AD Database เนื่องจากสามารถนำมาบริหารจัดการที่เกี่ยวข้องกับความปลอดภัย ใช้พิสูจน์ตัวตน ซึ่ง Object ใน AD จะมี Security ID ไม่ซ้ำกันเลย โดย SID จะถูก Random ผ่านทาง RID Master Role แต่ละ Object ที่ถูกสร้างขึ้น จะมี SID ที่ใช้แทนชื่อเรียกของแต่ละ Object จึงทำให้แต่ผู้ใช้งานจะเห็นเป็นชื่อ Object ที่แตกต่างกันกับระบบภายใน

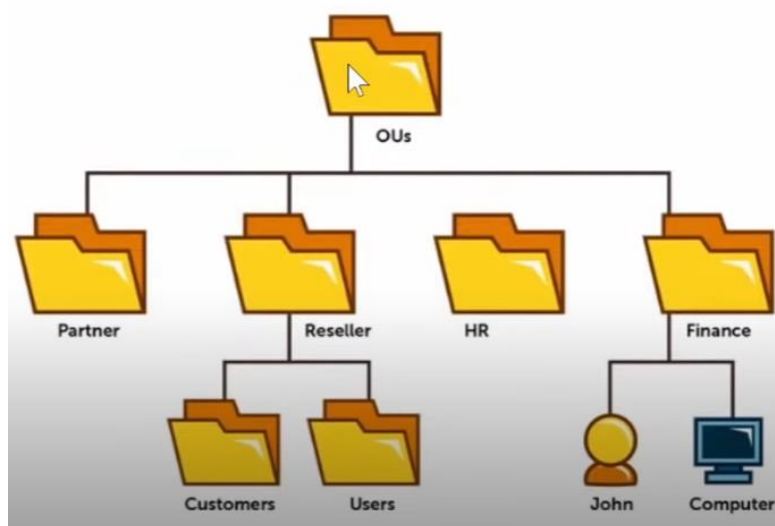
### 2.4.3 Group Policy [6]

Group Policy เป็นการออกแบบที่จะเพื่อนำมาช่วยให้สามารถจัดการเครื่องคอมพิวเตอร์ และผู้ใช้งานในเครือข่ายได้ง่ายขึ้น โดยอาศัยช่องทางของ Active Directory ซึ่งสามารถกำหนด Policy ที่ต้องการบังคับใช้จากเครื่องที่ทำหน้าที่เป็น Domain Controller โดย Policy เหล่านี้จะถูกส่งต่อไปยังเครื่องและผู้ใช้งานในองค์กรที่ระบุไว้โดยอัตโนมัติ

### 2.4.4 Organizational Unit

Organizational Unit คือ วิธีการจัดเก็บ Active Directory Object ซึ่งเป็นการแบ่งแยก Object เชิง Logical เพื่อให้เหมาะสมกับการรวมกลุ่มในการบริหารจัดการ หลังจากสร้าง OU เสร็จแล้ว

จึงจะสามารถนำสมาชิก เช่น Users / Groups / Computers / Printer นำเข้าไปใส่ OU เพื่อให้สามารถแบ่งแยกการจัดการเป็นกลุ่ม ๆ ต่อไป



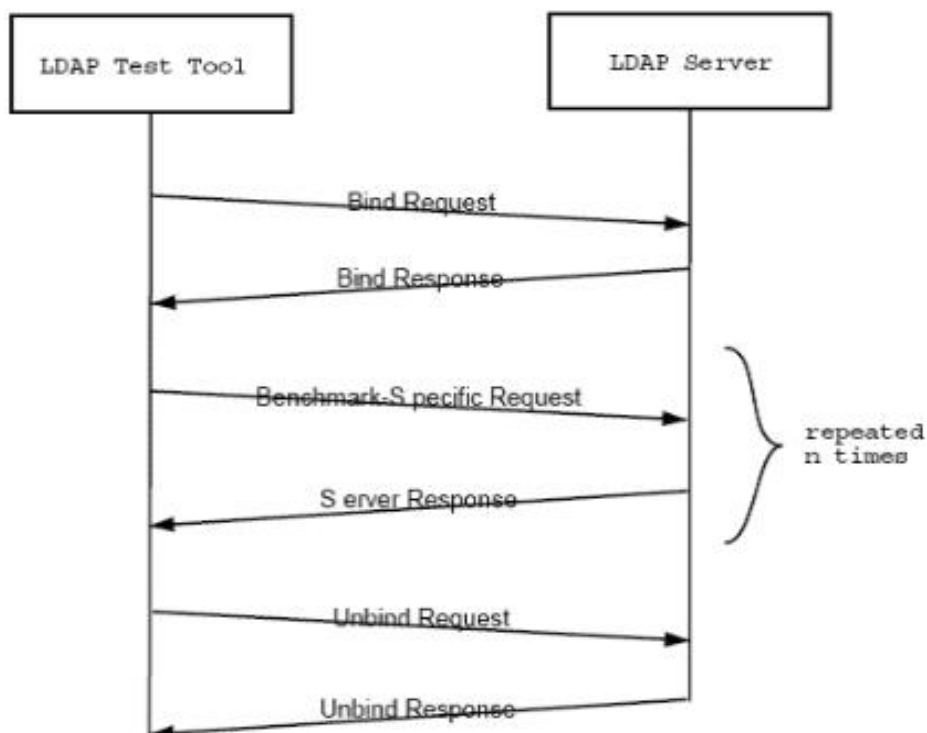
ภาพที่ 3 ตัวอย่างการแบ่ง Organizational Unit

#### 2.4.5 Lightweight Directory Access Protocol (LDAP) [7]

Lightweight Directory Access Protocol (LDAP) เป็น Protocol ที่ใช้สำหรับค้นหาข้อมูลในฐานข้อมูล ก่อนที่จะลงลึกว่า LDAP คืออะไร มาดูที่มาก่อน Directory Access Protocol (DAP) คือมาตรฐาน X.500 ของ Directory ในระบบ Network ซึ่ง LDAP เป็น “lightweight” นั้น หมายถึง มีขนาดเล็ก เพราะ Version เริ่มต้นไม่ได้มีระบบ Security มาด้วย ส่วนใหญ่จะนำมาใช้กับข้อมูลจำพวกรายละเอียดของพนักงาน เช่น ชื่อ, นามสกุล, ตำแหน่ง, ที่อยู่ เป็นต้น

กระบวนการทำงานของ Protocol LDAP

เมื่อ Client ได้ทำการเชื่อมต่อ LDAP session เข้ากับ LDAP server จะเรียกว่า Directory System Agent (DSA) ซึ่งปกติจะใช้ TCP port 389 สำหรับ LDAP over SSL ซึ่งจะเป็น port 636 โดยทาง Client จะส่ง Request มาที่ Server และทาง Server ก็จะตอบ Response กลับไป โดยไม่จำเป็นที่ Client ต้องรอ Response กลับมาก่อนที่จะส่ง Request อันต่อไป รวมถึง Server เองก็ไม่ต้องส่ง Response เรียกตามลำดับด้วย เพราะข้อมูลทั้งหมดจะถูกส่งโดยใช้ Basic Encoding Rules (BER)



ภาพที่ 4 จำลองการทำงานของ Lightweight Directory Access Protocol (LDAP)

#### 2.4.6 WatchGuard Log Server [10]

WatchGuard Log Server เป็นส่วนหนึ่งของ WatchGuard Server Center เป็นฐานข้อมูลที่สามารถเก็บรวบรวมข้อมูลข้อความบันทึกจาก Watchguard Firebox ที่เชื่อมต่อกับระบบสามารถติดตั้ง WatchGuard Log Server ได้ทั้งบนคอมพิวเตอร์ที่ใช้สำหรับการจัดการหรือบนคอมพิวเตอร์อื่น ๆ และยังสามารถเพิ่มเซิร์ฟเวอร์บันทึกเพิ่มเติม เพื่อการสำรองข้อมูลและการขยายขนาดได้อีกด้วยในการทำเช่นนี้ การจะใช้โปรแกรมติดตั้ง WatchGuard System Manager (WSM) และเลือกติดตั้งเฉพาะส่วนประกอบของ Log Server เท่านั้น โดย Log Server บันทึกข้อมูลรับข้อมูลผ่านพอร์ต TCP 4107 และ 4115 Watchguard Firebox ทุกเครื่องที่เชื่อมต่อกับ Log Server จะบันทึกข้อมูลจะส่งชื่อเครื่องหมายเลขซีเรียล ไซนเวลา ข้อมูลบันทึกเรื่องการจราจรของตัวเองมายัง Log Server

## 2.5 กฎหมาย นโยบาย มาตรฐาน ที่เกี่ยวข้องกับการปฏิบัติงาน

### 2.5.1 นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงสาธารณสุข พ.ศ. 2565 [9]

กระทรวงสาธารณสุขได้ประกาศใช้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ ของกระทรวงสาธารณสุข พ.ศ. 2565 เมื่อวันที่ 23 มีนาคม 2565 ตามแนวทางพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 สำนักงานปลัดกระทรวงสาธารณสุข ได้ระบุไว้ดังนี้ ข้อ 5. นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงสาธารณสุข กำหนดประเด็นสำคัญดังต่อไปนี้

#### 5.1 การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

ข้อ 5.1.1 การเข้าถึงระบบสารสนเทศ ต้องควบคุมการเข้าถึงข้อมูล และอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งาน และความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศกำหนดกฎเกณฑ์ที่เกี่ยวข้อง การอนุญาตให้เข้าถึงกำหนดสิทธิ์ เพื่อให้ผู้ใช้งานในทุกระดับได้รับรู้เข้าใจ และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

ข้อ 5.1.2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงระบบสารสนเทศและป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ต้องกำหนดให้มีการลงทะเบียนผู้ใช้งาน ตรวจสอบบัญชีผู้ใช้งาน อนุมัติและกำหนดรหัสผ่านการลงทะเบียนผู้ใช้งาน เพื่อให้ผู้ใช้งานที่มีสิทธิ์เท่านั้นที่สามารถเข้าใช้ระบบสารสนเทศได้ และต้องเก็บบันทึกข้อมูลการเข้าถึงและข้อมูลจราจรทางคอมพิวเตอร์ ตลอดจนบริหารจัดการสิทธิ์การเข้าถึงข้อมูลให้เหมาะสมตามระดับชั้นความลับของผู้ใช้งาน ต้องมีการทบทวนสิทธิ์การใช้งานและตรวจสอบการละเมิดความปลอดภัยเสมอ

ข้อ 5.1.3 การควบคุมการเข้าถึงเครือข่าย เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ต้องกำหนดสิทธิ์ในการเข้าถึงเครือข่ายให้ผู้ที่ จะเข้าใช้งานต้องลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการเข้ารหัสผ่านก่อนการเข้าใช้งาน ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์สำหรับใช้งานอินเทอร์เน็ต โดยผ่านระบบรักษาความปลอดภัยตามที่กระทรวงสาธารณสุขจัดสรรไว้ และมีการออกแบบระบบเครือข่ายโดยแบ่งเขต (Zone) การใช้งาน เพื่อให้การควบคุมและป้องกันภัยคุกคามได้อย่างเป็นระบบและมีประสิทธิภาพ

ข้อ 5.1.4 การควบคุมการเข้าถึงโปรแกรมประยุกต์และแอปพลิเคชัน ต้องกำหนดสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศที่สำคัญ โปรแกรมประยุกต์หรือแอปพลิเคชันต่าง ๆ รวมถึง จดหมายอิเล็กทรอนิกส์(E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) และระบบงานต่าง ๆ โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจาก

หัวหน้าหน่วยงานเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิที่ตั้งกล่าวอย่างสม่ำเสมอ จึงขอให้หน่วยงานในสังกัดกระทรวงสาธารณสุขทุกแห่งถือปฏิบัติตามประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ พ.ศ. 2565 โดยเคร่งครัด

### 2.5.2 พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 [10]

พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 ได้ประกาศลงในราชกิจจานุเบกษาแล้ว เมื่อวันที่ 23 มกราคม พ.ศ.2560 และมีผลใช้บังคับตั้งแต่วันที่ 24 มกราคม พ.ศ. 2560 เป็นต้นไป พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 ได้ระบุไว้ดังนี้

มาตรา 18 เพื่อประโยชน์ในการสืบสวนและสอบสวนในกรณีที่มีเหตุอันควรเชื่อได้ว่ากระทำความผิดตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่ที่มีอำนาจอย่างหนึ่งอย่างใด ดังต่อไปนี้ เฉพาะที่จำเป็นเพื่อประโยชน์ในการใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด

(2) เรียกข้อมูลจากรางคอมพิวเตอร์จากผู้ให้บริการที่เกี่ยวข้องกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือจากบุคคลที่เกี่ยวข้อง

มาตรา 26 ผู้ให้บริการต้องเก็บรักษาข้อมูลจากรางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็นพนักงานเจ้าหน้าที่จะสั่งให้ผู้บริการผู้ใดเก็บรักษาข้อมูลจากรางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินหนึ่งปีเป็นกรณีพิเศษ

### 2.5.3 พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 [11]

หลังจากที่ PDPA หรือ พ.ร.บ คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ถูกประกาศใช้แล้ว “ข้อมูลส่วนตัว” ถือว่าต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อน องค์กรหรือนิติบุคคลจึงจะนำข้อมูลไปใช้ประโยชน์อื่นได้ ดังนั้นพนักงานก็มีสิทธิที่จะรู้ว่าข้อมูลส่วนตัวนำไปใช้ทำอะไรบ้าง และนอกจากมีสิทธิรู้แล้วยังมีสิทธิอีกมากมาย ดังนี้

- สิทธิได้รับการแจ้งให้ทราบ (Right to be informed)

ผู้มีส่วนเกี่ยวข้องทั้งหมด ไม่ว่าจะเป็น HR ฝ่าย IT ต้องแจ้งเจ้าของข้อมูลให้ทราบถึงวัตถุประสงค์ที่จะนำข้อมูลไปใช้ รวมถึงช่องทางในการติดต่อผู้ควบคุมข้อมูล นอกจากนี้ยังต้องบอกระยะเวลาใช้งานข้อมูลอย่างชัดเจน

- สิทธิขอเข้าถึงข้อมูลส่วนบุคคล (Right of access)

พนักงานมีสิทธิเข้าถึงข้อมูลที่เกี่ยวข้องกับตนเองและขอสำเนาข้อมูลจากผู้ควบคุมข้อมูล ทั้งยังขอทราบข้อมูลที่ได้มาโดยไม่ได้ออกญาแต่อีกด้วย (โดยองค์กร-บริษัทควรจัดทำเอกสารเพื่อให้พนักงานเซ็นยินยอมการเข้าถึงข้อมูล)



- สิทธิในการขอให้โอนข้อมูลส่วนบุคคล (Right to data portability)

หากพนักงานเคยให้ข้อมูลกับผู้ควบคุมรายหนึ่งไว้ แล้วจะไปใช้กับอีกผู้ควบคุมอีกรายหนึ่ง สามารถให้ผู้ควบคุมข้อมูลรายนั้นส่งหรือโอนข้อมูลให้ได้ หรือจะโอนข้อมูลระหว่างผู้ควบคุมก็ทำได้ ถ้าไม่ติดขัดทางเทคนิคและไม่ได้ละเมิดกฎหมาย

- สิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล (Right to object)

เจ้าของข้อมูลสามารถคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนตัวเมื่อไรก็ได้ หากไม่ประสงค์ให้เก็บข้อมูล

- สิทธิขอให้ลบหรือทำลาย (Right to erasure also known as right to be forgotten)

หากพบว่าผู้ควบคุมข้อมูล นำข้อมูลไปเผยแพร่ในที่สาธารณะหรือเข้าถึงได้ง่าย เจ้าของข้อมูลมีสิทธิขอให้ลบ ทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคล

- สิทธิขอให้ระงับการใช้ข้อมูล (Right to restrict processing)

เมื่อเปลี่ยนใจไม่ให้ข้อมูลแล้ว หรือเปลี่ยนใจระงับการทำลายข้อมูลเมื่อถึงเวลาต้องทำลาย เพราะจะนำข้อมูลนั้นไปใช้ในทางกฎหมาย หรือเรียกร้องสิทธิใดๆ

- สิทธิในการขอให้แก้ไขข้อมูลส่วนบุคคล (Right of rectification)

เจ้าของข้อมูลมีสิทธิขอแก้ไขข้อมูลให้ถูกต้อง และอัปเดตข้อมูลให้ใหม่อยู่เสมอ ไม่ก่อให้เกิดความเข้าใจผิด การแก้ไขข้อมูลต้องสุจริตและเป็นไปตามกฎหมาย

## 2.6 Black Box Testing Technique [12]

เป็นการทดสอบตาม Spec เป็นหลักเรียกว่าเป็น Spec-based คือดูจาก requirements spec ว่ามี feature การทำงานยังงัยบ้างแล้วก็ทำการทดสอบตามนั้น ดังนั้นการทดสอบประเภทนี้จะได้สนใจว่า source code เขียนไว้ยังงัย เหมือนกล่องดำที่ไม่สนใจว่าข้างในมีอะไรให้สนใจเฉพาะ input และ output ที่ได้จากกล่องดำเท่านั้น

## 2.7 ทฤษฎีการคำนวณหากลุ่มตัวอย่าง Taro Yamane

Taro Yamane[13] คือ หนึ่งในสูตรคำนวณขนาดกลุ่มตัวอย่างที่เหมาะสมสำหรับงานวิจัย เพื่อแจกแบบสอบถามโดยใช้สูตร ทาโร่ ยามาเน (Taro Yamane) ในการคำนวณขนาดกลุ่มตัวอย่าง จะทำให้รู้ว่าควรแจกแบบสอบถามให้กับกลุ่มตัวอย่างกี่คน แทนที่จะต้องแจกให้กับกลุ่มตัวอย่างทุกคน สูตร Taro Yamane (ทาโร่ ยามาเน) หรือสูตรอื่นในการคำนวณหาขนาดกลุ่มตัวอย่างที่เหมาะสมเป็นสิ่งจะช่วยให้ผู้วิจัย (สำหรับงานวิจัยเชิงสำรวจ) ไม่ต้องแจกแบบสอบถามให้กับกลุ่มตัวอย่างของงานวิจัยทุกคนที่อาจมีจำนวนหลายพันคน โดยการใช้อนุกรม Taro Yamane คำนวณหาขนาดกลุ่มตัวอย่างที่เหมาะสมในงานวิจัยเชิงสำรวจ (Survey Research) ซึ่งจะช่วยลดจำนวนกลุ่มตัวอย่างที่ต้องแจกแบบสอบถามจากพันหรือหมื่นคน เหลือเพียงหลักร้อยคน

สูตร Taro Yamane (ทาโร่ ยามาเน)

$$n = \frac{N}{1+Ne^2}$$

เมื่อ  $n$  คือ ขนาดกลุ่มตัวอย่าง

$N$  คือ ขนาดประชากร

$e$  คือ ความคลาดเคลื่อนของกลุ่มตัวอย่าง

## บทที่ 3

### วิธีการดำเนินการ

การพัฒนาระบบยืนยันตัวตนบุคคลที่ใช้งานระบบเครือข่ายอินเทอร์เน็ตของสำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช มีจุดมุ่งหมายเพื่อควบคุมและยืนยันการเข้าถึงเครือข่ายอินเทอร์เน็ต เพื่อให้การในระบบเทคโนโลยีสารสนเทศให้เป็นไปอย่างเหมาะสม มีความมั่นคงปลอดภัย

#### 3.1 เครื่องมือที่ใช้วิจัย

1. ระบบยืนยันตัวตนบุคคลที่ใช้งานระบบเครือข่ายอินเทอร์เน็ตที่ผู้วิจัยได้พัฒนาขึ้นใช้สำหรับจัดเก็บข้อมูลสิทธิ์การใช้งานและตรวจสอบสิทธิ์ผู้ใช้งานโดยไฟร์วอลล์
2. ระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์โดยใช้โปรแกรม WatchGuard Server Center ซึ่งเป็นโปรแกรมที่ใช้งานร่วมกับ Firewall WatchGuard M4600 ทำหน้าที่จัดเก็บและแสดงข้อมูลจราจรคอมพิวเตอร์โดยแสดงผลเป็นเว็บอินเทอร์เน็ตเฟสซึ่งสามารถใช้งานได้ง่าย
3. อุปกรณ์ป้องกันเครือข่าย (Firewall) เพื่อใช้เป็นระบบรักษาความปลอดภัยเครือข่าย ทำหน้าที่คอยตรวจจับ ตรวจสอบสิทธิ์ และให้สิทธิ์ในการเข้าถึงเครือข่าย คัดกรองผู้ใช้งานตามนโยบายที่ผู้วิจัยได้กำหนด
4. เครื่องคอมพิวเตอร์สำนักงานใช้สำหรับทดสอบการใช้งาน

#### 3.2 การเก็บรวบรวมข้อมูล

1. กำหนดการเก็บข้อมูลในส่วนของประวัติการเข้าใช้งานโดยกำหนดระยะเวลาเก็บข้อมูลจำนวน 90 วัน โดยอ้างอิงตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 ที่ได้กำหนดหน้าที่ของผู้ให้บริการ ตามมาตรา 26 ให้เก็บข้อมูลการจราจรไม่น้อยกว่า 90 วัน โดยงานวิจัยนี้ได้ดำเนินการเก็บข้อมูลตั้งแต่วันที่ 24 กันยายน พ.ศ. 2566 ถึงวันที่ 22 ธันวาคม พ.ศ. 2566 เพื่อเป็นการตรวจสอบความสามารถในการป้องกันการเข้าถึงเครือข่ายและการระบุตัวตนของผู้ใช้งานเครือข่าย ซึ่งข้อมูลที่จัดเก็บอยู่ใน WatchGuard Server Center จะเป็นรูปแบบตารางเพื่อนำไปวิเคราะห์ต่อไป โดยแสดงตัวอย่างดังตารางที่ 1

ตารางที่ 1 โครงสร้างตารางข้อมูล

User	IP Address	Login Time	Logout Time	Duration	Method	Status
-	-	-	-	-	-	-

โดยข้อมูลนี้สามารถแสดงให้เห็นว่าใคร (User) ใช้งานจากที่ใด (IP Address) เริ่มต้นการใช้งานเมื่อไหร่ (Login Time) สิ้นสุดการใช้งานเมื่อไหร่ (Logout Time) ระยะเวลาการใช้งานรวมเท่าไร (Duration) วิธีการเข้าใช้งานอนุญาตผ่านช่องทางใด (Method) และสถานการณ์ใช้งานเป็นอย่างไร (Status) ซึ่งสถานะการใช้งานจะแสดงถึงว่าผู้ใช้งานผู้นั้นสามารถเข้าถึงระบบได้หรือไม่ เพื่อนำข้อมูลดังกล่าวไปวิเคราะห์ศักยภาพในการให้บริการระบบเครือข่าย และระดับความสามารถในการป้องกัน ควบคุม ระบุตัวตน ผู้ใช้งานเครือข่าย

2. ผู้วิจัยได้เก็บรวบรวมข้อมูล โดยออกแบบสอบถามสร้างในรูปแบบออนไลน์ให้บุคลากรในสำนักงาน ป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช และ ศตม.11.2 นครศรีธรรมราช ตอบแบบสอบถามเอง (Self-Administration) โดยมีแบบประเมินความสำเร็จของระบบใน 4 ปัจจัยดังนี้

1. ด้านประสิทธิภาพของระบบ
2. ด้านความสำคัญของการป้องกันระบบ
3. ด้านความน่าเชื่อถือ
4. ด้านคุณภาพการให้บริการ

### 3.3 วิเคราะห์ข้อมูล

1. วิเคราะห์ความสามารถในการป้องกันการเข้าใช้งานเครือข่าย ผู้วิจัยได้นำข้อมูลที่ได้มาทำการวิเคราะห์ข้อมูลพร้อมทั้งเขียนรายงานผลในรูปแบบตาราง เพื่อสรุปผลให้เข้าใจง่าย การวิเคราะห์ข้อมูลโดยใช้สถิติพรรณนา ได้แก่ ค่าต่ำสุด ค่าสูงสุด ร้อยละ ส่วนเบี่ยงเบนมาตรฐาน และค่าเฉลี่ย

2. วิเคราะห์ความสามารถในการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ โดยทำการค้นหาข้อมูลประวัติการใช้งานเครือข่าย เพื่อดูความครบถ้วน ถูกต้องของข้อมูล

3. วิเคราะห์ความสามารถในการจัดเก็บข้อมูลตามข้อกำหนด โดยการเปรียบเทียบระยะเวลาในการจัดเก็บที่ผ่านมากับระยะเวลาในการจัดเก็บตามเป้าหมาย เพื่อดูขนาดพื้นที่ความจุว่าเพียงพอหรือไม่

4. วิเคราะห์ความสามารถในการปฏิบัติตามมาตรการที่ได้กำหนดไว้ โดยเปรียบเทียบความสามารถในการทำงานของระบบกับแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงสาธารณสุข พ.ศ. 2565 และพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560

5. จากการเก็บข้อมูลแบบสอบถาม ผู้วิจัยได้นำข้อมูลที่ได้มาทำการวิเคราะห์และแปลผลข้อมูลพร้อมทั้งเขียนรายงานผลในรูปแบบตาราง เพื่อสรุปข้อมูลให้เข้าใจได้ง่าย ซึ่งสถิติที่ใช้ ได้แก่ ค่าเฉลี่ย และส่วนเบี่ยงเบนมาตรฐาน (S.D.) ดังนี้

การหาค่าเฉลี่ย  $\bar{x} = \frac{\sum fx}{n}$

การหาส่วนเบี่ยงเบนมาตรฐาน S. D. =  $\sqrt{\frac{n \sum fx^2 - (\sum x)^2}{n(n-1)}}$

### 3.4 การดำเนินการวิจัย

#### 3.4.1 กำหนดกลุ่มเป้าหมายและวิธีสุ่มตัวอย่าง

การสุ่มตัวอย่างข้อมูลแบ่งได้เป็น 2 ส่วน ดังนี้

1. บุคลากรที่ใช้ในการวิจัยสำหรับใช้ตอบแบบสอบถาม ได้แก่ บุคลากรในสำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช และ ศตม.11.2 นครศรีธรรมราช ที่มีสิทธิ์เข้าใช้งานเครือข่ายอินเทอร์เน็ตของหน่วยงานจำนวน 160 คน ผู้วิจัยได้ทำการสุ่มตัวอย่างของบุคลากรจำนวน 114 คน โดยได้จากการคำนวณของสูตรของ ทาโร่ ยามาเน่ ในการกำหนดตัวอย่างโดยเลือกระดับความเชื่อมั่น 95% ค่าระดับความคลาดเคลื่อนยอมรับได้ไม่เกิน 5% หรือ 0.05 ของระดับนัยสำคัญ

การสุ่มตัวอย่างดังกล่าวของบุคลากรในสำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช และ ศตม.11.2 นครศรีธรรมราช ที่มีสิทธิ์เข้าใช้งานเครือข่ายอินเทอร์เน็ตได้ดังนี้

ตามวิธีของ ยามาเน่ (Taro Yamane)

$$n = \frac{N}{1 + Ne^2}$$

เมื่อ n คือ ขนาดกลุ่มตัวอย่าง

N คือ ขนาดประชากร

e คือ ความคลาดเคลื่อนของกลุ่มตัวอย่าง

$$\begin{aligned} \text{แทนค่าได้เท่ากับ} &= \frac{160}{1 + (160(0.0025))} \\ &= \frac{160}{1.40} \\ &= 114.2 \text{ จำนวนสุ่มตัวอย่าง} \end{aligned}$$

2. การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ภายในสำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช โดยกำหนดเป็นจำนวนผู้ใช้งานทั้งหมดที่ได้ลงทะเบียนขอรับสิทธิ์การใช้งานเครือข่ายอินเทอร์เน็ตคือ 160 คน แบ่งออกเป็นเจ้าหน้าที่ที่ปฏิบัติงานที่สำนักงาน จำนวน 120 คน และเจ้าหน้าที่ที่ปฏิบัติงานที่ภายนอกสำนักงาน จำนวน 40 คน กำหนดการเก็บข้อมูลในส่วนของประวัติการเข้าใช้งานโดยกำหนดระยะเวลาเก็บข้อมูลจำนวน 90 วัน ตั้งแต่วันที่ 24 กันยายน พ.ศ. 2566 ถึงวันที่ 22 ธันวาคม พ.ศ. 2566

### 3.4.2 การชี้วัดความสำเร็จ

ความสำเร็จของการพัฒนาระบบในครั้งนี้ สามารถแบ่งการชี้วัดความสำเร็จได้เป็น 2 ส่วน ดังนี้

1. ส่วนของการให้บริการระบบ วัดผลโดยใช้แบบสอบถามความคิดเห็นเกี่ยวกับความสำเร็จของระบบ ด้วยเทคนิค Black Box Testing Technique ใน 4 ปัจจัย คือ ด้านประสิทธิภาพของระบบ ด้านความสำคัญของการป้องกันระบบ ความน่าเชื่อถือของระบบ และคุณภาพการให้บริการ ซึ่งเป็นแบบสอบถามมาตราส่วนประมาณค่าคะแนน มี 5 ระดับ คือ มากที่สุด มาก ปานกลาง น้อย น้อยที่สุด เป็นแบบมาตรวัดประมาณค่าต่อเนื่อง Likert Scale 5 ระดับ ตั้งแต่

มากที่สุด ( 5 คะแนน)	มาก (4 คะแนน)	ปานกลาง (3 คะแนน)	น้อย (2 คะแนน)	น้อยที่สุด (1 คะแนน)
-------------------------	------------------	----------------------	-------------------	-------------------------

เกณฑ์การประเมินในภาพรวมกำหนด 5 ระดับโดยใช้สูตรการคำนวณความกว้างของแต่ละอันตรภาคชั้น ดังนี้

โดยใช้ค่าคะแนนนำมาคำนวณความกว้างแต่ละอันตรภาคชั้นใช้สูตร

$$\frac{\text{คะแนนสูงสุด} - \text{คะแนนต่ำสุด}}{5} = \text{ค่าคะแนนความกว้างอันตรภาคชั้น}$$

5

$$\frac{5-1}{5} = 0.80$$

5

หลังจากได้ค่าที่มาจาก การคำนวณช่วงระดับคะแนนดังกล่าวแล้วนำค่าที่ได้นั้นมาแบ่งเป็นระดับคะแนนความสำเร็จของระบบ 5 ระดับ ดังนี้

คะแนนเฉลี่ย 4.21–5.00 หมายถึง มากที่สุด

คะแนนเฉลี่ย 3.41–4.20 หมายถึง มาก

คะแนนเฉลี่ย 2.61–3.40 หมายถึง ปานกลาง

คะแนนเฉลี่ย 1.81–2.60 หมายถึง น้อย

คะแนนเฉลี่ย 1.00–1.80 หมายถึง น้อยที่สุด

2. การชี้วัดความสามารถการทำงานของระบบโดยอ้างอิงตามวัตถุประสงค์ของการพัฒนาระบบ เพื่อให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงสาธารณสุข พ.ศ. 2565 และพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 ฉบับที่ 2 โดยมีประเด็นที่จะนำมาใช้ชี้วัด ดังต่อไปนี้

2.1 นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงสาธารณสุข พ.ศ. 2565

1) ข้อ 5.1.1 การเข้าถึงระบบสารสนเทศ ต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง กำหนดสิทธิ์ เพื่อให้ผู้ใช้งานในทุกระดับได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

2) ข้อ 5.1.2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงระบบสารสนเทศและป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาตต้องกำหนดให้มีการลงทะเบียนผู้ใช้งาน ตรวจสอบบัญชีผู้ใช้งาน อนุมัติและกำหนดรหัสผ่านการลงทะเบียนผู้ใช้งาน เพื่อให้ผู้ใช้งานที่มีสิทธิ์เท่านั้นที่สามารถเข้าใช้ระบบสารสนเทศได้ และต้องเก็บบันทึกข้อมูลการเข้าถึงรวมถึงข้อมูลจราจรทางคอมพิวเตอร์ตลอดจนบริหารจัดการสิทธิ์การเข้าถึงข้อมูลให้เหมาะสมตามระดับชั้นความลับของผู้ใช้งานต้องมีการทบทวนสิทธิ์การใช้งาน และตรวจสอบการละเมิดความปลอดภัยเสมอ

3) ข้อ 5.1.3 การควบคุมการเข้าถึงเครือข่าย เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ต้องกำหนดสิทธิ์ในการเข้าถึงเครือข่ายให้ผู้ที่ จะเข้าใช้งานต้องลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่านก่อนการเข้าใช้งาน ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์สำหรับใช้งานอินเทอร์เน็ตให้ผ่านระบบรักษาความปลอดภัยตามที่กระทรวงสาธารณสุขจัดสรรไว้ และมีการออกแบบระบบเครือข่ายโดยแบ่งเขต (Zone) การใช้งาน เพื่อทำให้การควบคุมและป้องกันภัยคุกคามได้อย่างเป็นระบบและมีประสิทธิภาพ

4) ข้อ 5.1.4 การควบคุมการเข้าถึงโปรแกรมประยุกต์และแอปพลิเคชัน ต้องกำหนดสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศที่สำคัญ โปรแกรมประยุกต์หรือแอปพลิเคชันต่าง ๆ รวมถึงจดหมายอิเล็กทรอนิกส์(E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) และระบบงานต่าง ๆ โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

## 2.2 พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 ฉบับที่ 2

1) “มาตรา 26 ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็น พนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินสองปีเป็นกรณีพิเศษเฉพาะราย และเฉพาะคราวก็ได้”

2.3 การชี้วัดความสามารถของการควบคุมการเข้าถึงเครือข่ายโดยใช้สถิติการเข้าใช้งานระบบยืนยันตัวตนบุคคลเพื่อเข้าใช้งานระบบเครือข่ายอินเทอร์เน็ตของสำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช จำนวน 90 วัน

จากนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงสาธารณสุข พ.ศ. 2565 และพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2560 ดังข้างต้น ทำให้สามารถนำประเด็นดังกล่าวมาใช้เป็นเกณฑ์ชี้วัด ดังนี้

ตารางที่ 2 ประเด็นและรายละเอียดเกณฑ์การให้คะแนน

รายละเอียดการวัดผล	คะแนนเต็ม
<b>1. การควบคุมการเข้าถึงและการทำงานของระบบสารสนเทศ</b>	
1.1 มีการควบคุมการเข้าถึงเครือข่าย	0.25
1.2 มีการควบคุมการเข้าถึงอุปกรณ์	0.25
1.3 มีการกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตการเข้าถึง	0.25
1.4 มีการกำหนดนโยบายเพื่อให้บุคลากรสามารถปฏิบัติตามแนวทางได้	0.25
<b>2. มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน</b>	
2.1 มีการกำหนดให้มีการลงทะเบียนผู้ใช้งาน	0.5
2.2 มีการบริหารจัดการสิทธิ์การเข้าถึงข้อมูล	0.5
<b>3. สามารถควบคุมการเข้าถึงเครือข่าย</b>	
3.1 มีการกำหนดให้ใช้การลงชื่อเข้าใช้ (Login) เพื่อแสดงตัวตนผู้ใช้งาน	0.33
3.2 มีการกำหนดให้ต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยรหัสผ่าน	0.33
3.3 มีการออกแบบเครือข่ายโดยแบ่งเขตการใช้งาน	0.33
<b>4. มีการควบคุมการเข้าถึงระบบปฏิบัติการและโปรแกรมประยุกต์</b>	
4.1 มีการป้องกันการเข้าถึงระบบปฏิบัติการด้วยการลงชื่อเข้าใช้งานด้วยรหัสผ่าน	0.5
4.2 มีการควบคุมการเข้าถึงโปรแกรมประยุกต์และแอปพลิเคชัน	0.5
<b>5.สามารถเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์</b>	1
รวม	5



### 3.5 การวางแผนพัฒนาตามหลัก PDCA

#### ขั้นตอนการวางแผน (Plan)

1. การวางแผนเพื่อระบุปัญหาและกำหนดเป้าหมาย
2. สํารวจทรัพยากรด้านเทคโนโลยีสารสนเทศที่ใช้งานอยู่ในปัจจุบัน
3. สํารวจข้อมูลกระบวนการเข้าถึงเครือข่ายที่ใช้งานอยู่ในปัจจุบัน
4. ออกแบบการเชื่อมต่อและการทำงานของกระบวนการเข้าถึงเครือข่าย
5. ออกแบบการเชื่อมต่อและการทำงานของกระบวนการเข้าถึงเครือข่าย
6. นำข้อมูลบุคลากรของหน่วยงานมาวิเคราะห์เพื่อกำหนดชื่อผู้ใช้ รหัสผ่าน และข้อมูลพื้นฐานที่จำเป็น

#### ในการระบุตัวตน

7. ศึกษาวางแผนกระบวนการตรวจสอบประวัติการใช้งานจากข้อมูลจราจรคอมพิวเตอร์

#### ขั้นตอนการปฏิบัติ (Do)

1. ดำเนินการตามขั้นตอนการปฏิบัติตามแผนที่วางไว้ ดังต่อไปนี้
  - 1.1 ดำเนินการสร้างเครื่องเซิร์ฟเวอร์ และคอมพิวเตอร์เสมือนจริง
  - 1.2 ติดตั้ง Windows Server 2012 บน Server และดำเนินการกำหนดการตั้งค่า
  - 1.3 ติดตั้ง Role And Feature ที่จำเป็นบน Windows Server
  - 1.4 กำหนด Password Policy สำหรับผู้ใช้งาน
  - 1.5 การบันทึกข้อมูลบุคลากรเข้าสู่ Active Directory
  - 1.6 เชื่อมต่อ Active Directory กับ Firewall
  - 1.7 กำหนด Session Authentication บน Firewall
  - 1.8 กำหนด Firewall Policy สำหรับการเปิดการใช้งาน Authentication
  - 1.9 ติดตั้ง Windows 10 บน Log Client และดำเนินการกำหนดการตั้งค่า
  - 1.10 ติดตั้งโปรแกรม Watchguard System manager
  - 1.11 ทำการเชื่อมต่อ Watchguard System manager กับ Firewall
  - 1.12 กำหนดระยะเวลาในการจัดเก็บ Log Files
2. เก็บรวบรวมบันทึกข้อมูลในขั้นตอนการปฏิบัติ เช่น วิธีดำเนินการ ผลของการปฏิบัติงาน

## ขั้นตอนการตรวจสอบ (Check)

1. ตรวจสอบความถูกต้องของการทำงานของระบบ โดยทำการเปรียบเทียบระหว่างขั้นตอนการวางแผน กับผลลัพธ์การดำเนินการเป็นไปตามแผนที่วางไว้หรือไม่ โดยมีขั้นตอนดังนี้

1.1 ทดสอบการเชื่อมต่อระหว่าง Firewall และ Active Directory

1.2 ทดสอบการเข้าใช้งานระบบยืนยันตัวตนบุคคล

1.3 ตรวจสอบการเข้าใช้งานระบบจัดเก็บ Log Files

1.4 ตรวจสอบการทำงานของระบบการเก็บ Log Files

1.5 ตรวจสอบผลการกำหนดความต้องการของระบบ

1.6 ตรวจสอบประสิทธิภาพการทำงานของเครือข่ายอินเทอร์เน็ต

2. ตรวจสอบผลลัพธ์การทำงานของระบบ เพื่อให้เป็นไปตามวัตถุประสงค์ของงานวิจัย โดยมีขั้นตอนดังนี้

2.1 ตรวจสอบความสามารถการควบคุมการเข้าถึงเครือข่ายอินเทอร์เน็ต

2.2 ตรวจสอบผลของการจัดเก็บ Log Files

2.3 ตรวจสอบความสามารถของการระบุตัวตนของผู้ใช้งานเครือข่ายอินเทอร์เน็ต

2.4 ตรวจสอบการทำงานของระบบขอตรวจสอบประวัติการใช้งาน

## ขั้นตอนการดำเนินงานให้เหมาะสม (Act)

หลังจากที่ได้ทำการวางแผน พัฒนา ตรวจสอบความถูกต้องแล้วนั้น ในส่วนของขั้นตอนการดำเนินงานให้เหมาะสมมีขั้นตอนดังนี้

1. การปรับปรุงด้านเทคนิค คือ วางแผน ปรับปรุง พัฒนา ตรวจสอบความถูกต้องของการทำงานของระบบ

2. ผลการบำรุงรักษาระบบ

3. ประกาศการเข้าใช้งานระบบ

4. กำหนดแนวทางในการเพิ่ม ลบ สิทธิ์การใช้งาน แก่งานการเจ้าหน้าที่

5. ขั้นตอนดำเนินงาน ในกรณีของการขอตรวจสอบประวัติการใช้งาน

## บทที่ 4

### ผลการดำเนินงาน

ผลการศึกษาการพัฒนากระบวนการยืนยันตัวบุคคลเพื่อเข้าใช้งานระบบเครือข่ายอินเทอร์เน็ตของสำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช โดยแบ่งผลการศึกษาออกเป็น 2 ส่วน คือ 1) การพัฒนากระบวนการตามหลัก PDCA 2) ผลการประเมินการพัฒนากระบวนการ ได้ดำเนินการดังนี้

#### 4.1 ขั้นตอนการวางแผน (Plan)

##### 4.1.1 ระบุปัญหาและกำหนดวัตถุประสงค์

ประชุมร่วมกับกรรมการบริหารหน่วยงานเพื่อทราบถึงวัตถุประสงค์การบริหารจัดการเครือข่ายที่หน่วยงานต้องการเพื่อนำไปใช้ในการระบุปัญหาและกำหนดเป้าหมาย โดยมีขั้นตอนดังนี้

1. ดำเนินการสำรวจปัญหา และข้อบกพร่องของกระบวนการเข้าถึงระบบเครือข่ายของสำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช กำหนดวัตถุประสงค์พร้อมทั้งทำความเข้าใจในสิ่งที่ต้องการจะแก้ไข ซึ่งสามารถนำผลการสำรวจมาเขียนเป็นผังงานได้ดังภาพที่ 5

2. เก็บรวบรวมข้อมูล และศึกษาความเป็นไปได้ในวิธีการที่ใช้ในการแก้ไขปัญหาจากทรัพยากรที่มีอยู่ โดยได้ทำการวิเคราะห์ความต้องการของระบบ และเปรียบเทียบกับทรัพยากรที่มีอยู่ ดังนี้

##### 4.1.2 ผลการสำรวจทรัพยากรด้านเทคโนโลยีสารสนเทศ

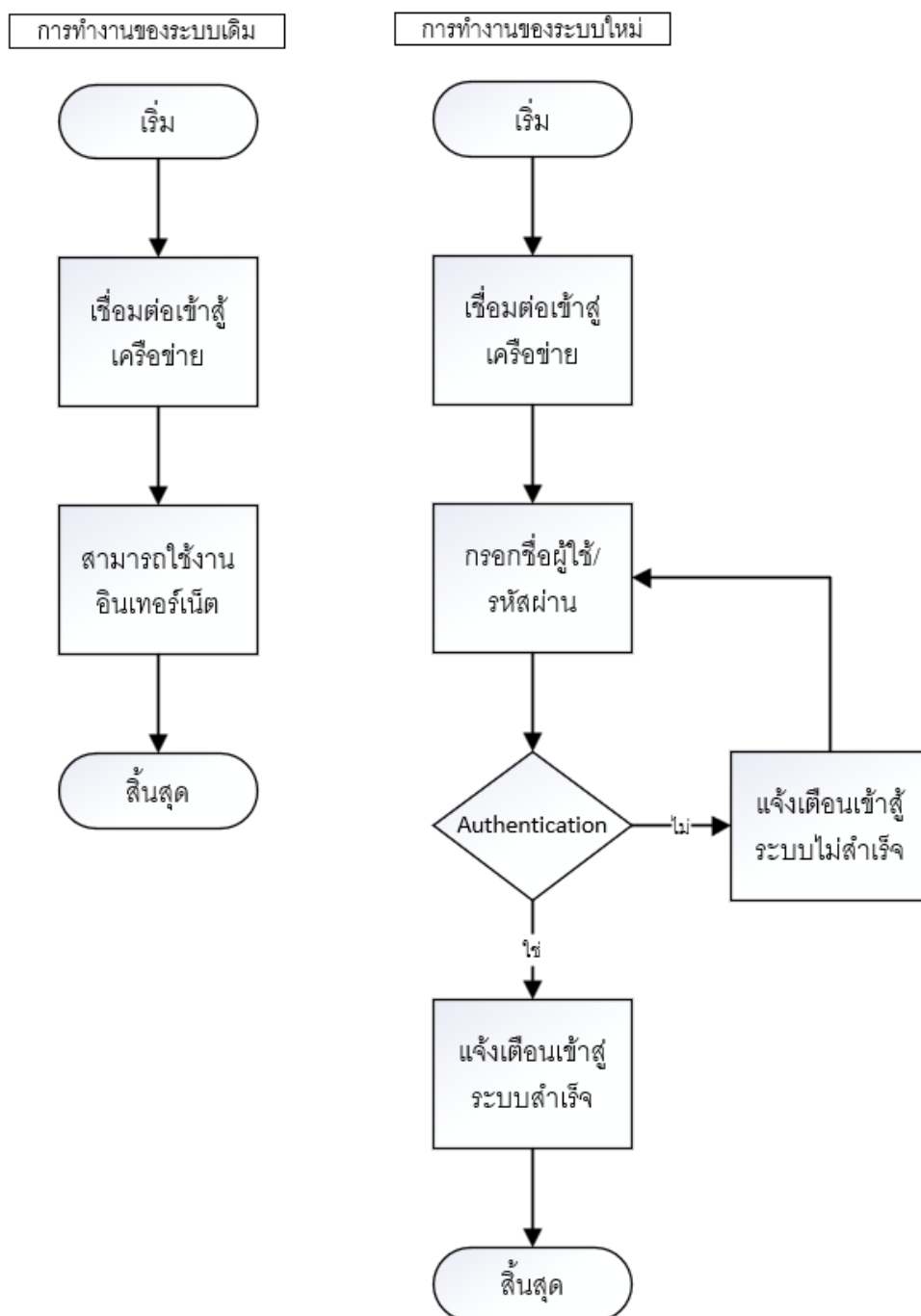
ตารางที่ 3 แสดงผลการเปรียบเทียบทรัพยากรของหน่วยงาน

ทรัพยากรที่จำเป็นต้องใช้	ทรัพยากรที่มีอยู่
Server หรือ Server Virtualization	Server Virtualization (VMware ESXi 6.0)
Firewall	Firewall Watchguard M 4600
ระบบปฏิบัติการ Windows Server	Windows Server 2012

จากตารางที่ 3 แสดงผลการเปรียบเทียบทรัพยากรที่หน่วยงานจำเป็นต้องจัดหากับทรัพยากรที่หน่วยงานมีอยู่ จึงสรุปได้ว่าสามารถดำเนินการได้ให้ระบบสามารถทำงานได้โดยไม่จำเป็นต้องใช้งบประมาณในการดำเนินการเพิ่มเติม และสามารถปรับปรุงเครื่องมือให้ทันสมัยเพิ่มขึ้นได้ในอนาคต

#### 4.1.3 ผลการสำรวจข้อมูลกระบวนการเข้าถึงเครือข่ายที่ใช้งานอยู่ในปัจจุบัน

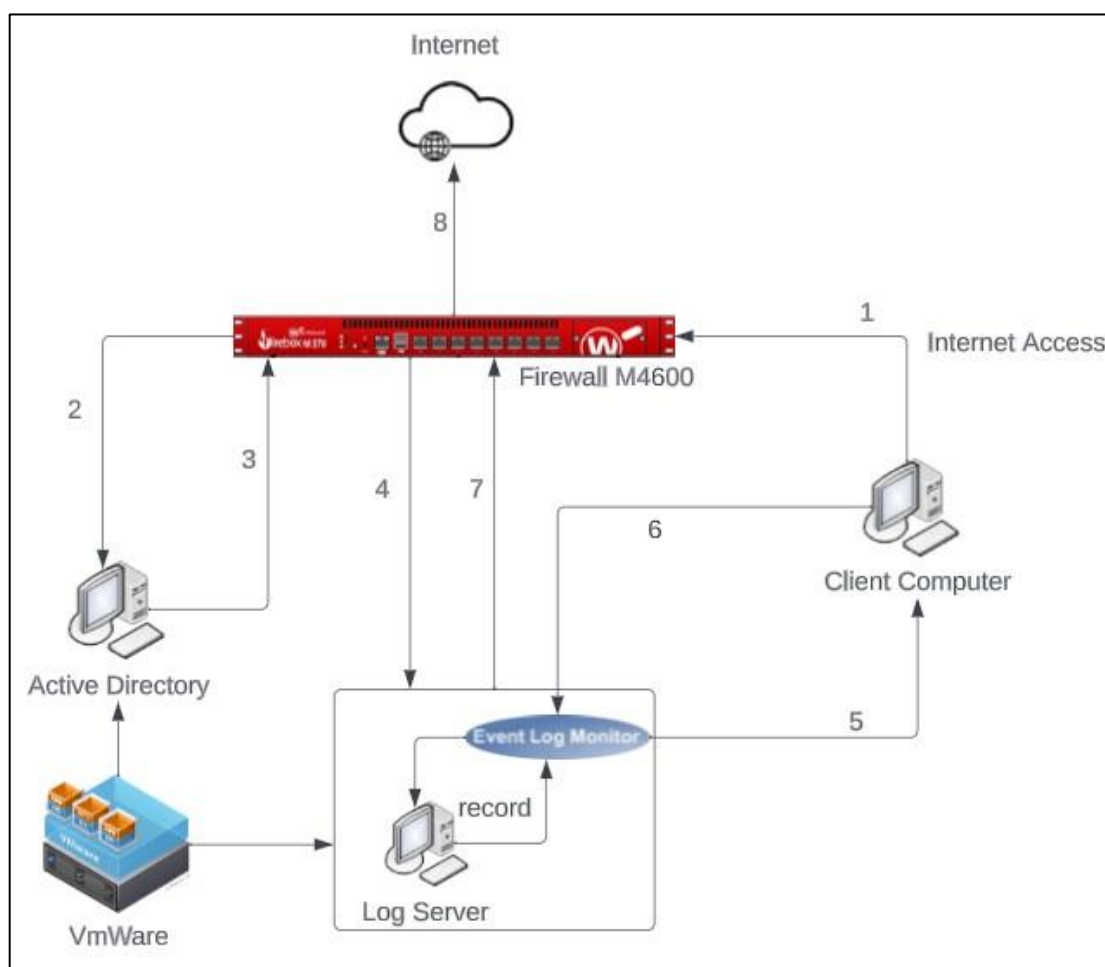
กระบวนการเข้าถึงเครือข่ายที่ใช้งานอยู่ในปัจจุบันมาเขียนเป็นผังการทำงานเพื่อระบุจุดที่ยังไม่มีและกำหนดเป้าหมายที่ต้องพัฒนาเพิ่มได้ดังนี้



ภาพที่ 5 แสดงผังงาน (Flowchart) เปรียบเทียบการเข้าถึงเครือข่ายด้วยรูปแบบเดิมเปรียบเทียบกับระบบใหม่ โดยสามารถแสดงให้เห็นถึงกระบวนการยืนยันตัวบุคคลของระบบใหม่

#### 4.1.4 ผลออกแบบการเชื่อมต่อและการทำงานของกระบวนการเข้าถึงเครือข่ายที่จะพัฒนา

1 กำหนดรูปแบบการทำงานของระบบที่กำลังจะพัฒนา เพื่อให้เห็นการทำงานของระบบภาพรวม ซึ่งสามารถนำมาจำลองเป็นรูปภาพของกระบวนการทำงาน และลำดับของการทำงานได้ดังนี้



ภาพที่ 6 แสดงลำดับกระบวนการทำงานของระบบในภาพรวม

จากภาพที่ 6 แสดงขั้นตอนการทำงานของระบบภาพรวมได้ดังนี้

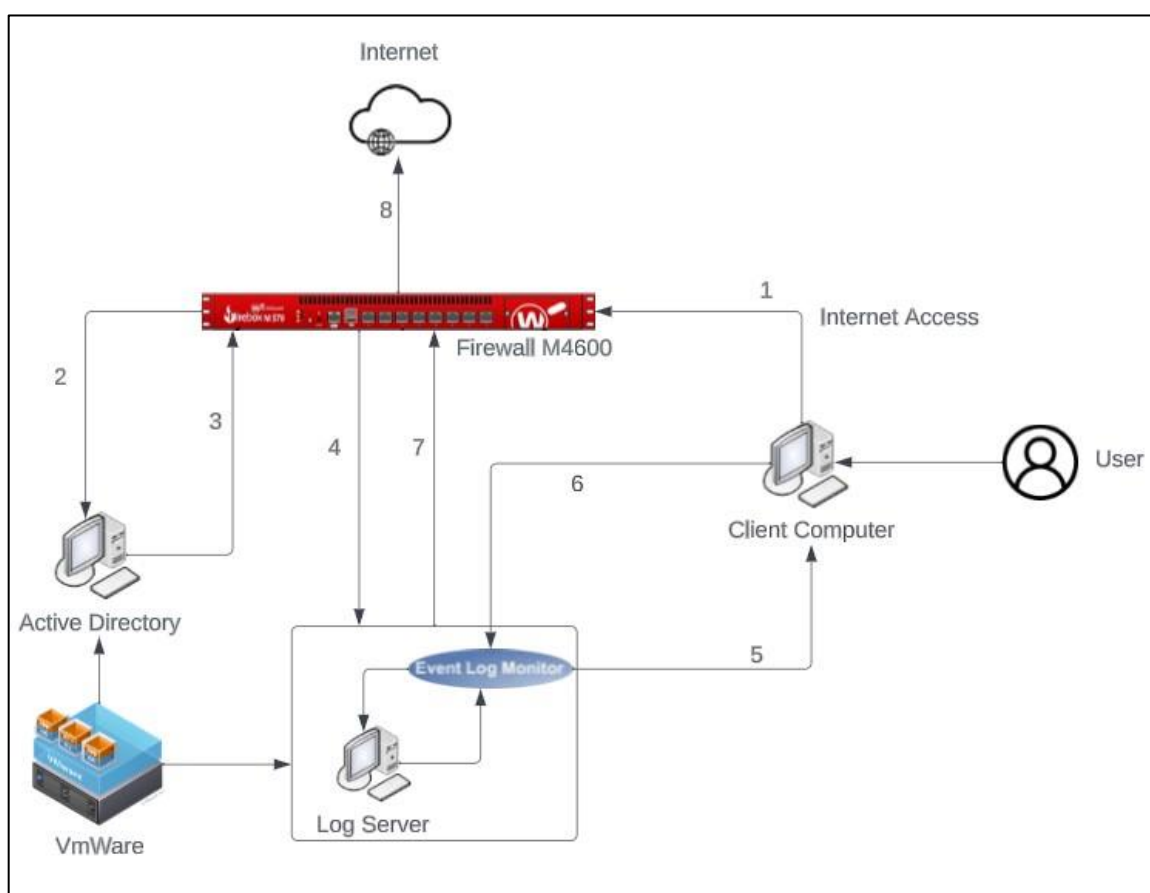
ขั้นตอนที่ 1 การเข้าใช้งานอินเทอร์เน็ตผ่านเครื่องคอมพิวเตอร์ คอมพิวเตอร์โน้ตบุ๊ก คอมพิวเตอร์ แท็บเล็ต หรือ โทรศัพท์มือถือ จะทำการส่งการร้องขอไปที่ Firewall

ขั้นตอนที่ 2 Firewall จะทำการตรวจสอบสิทธิ์ตาม Policy และ สืบค้นข้อมูลผู้ใช้งานบน Active Directory ที่ติดตั้งไว้บน VmWare

ขั้นตอนที่ 3 Active Directory จะทำการส่งกลับข้อมูลผู้ใช้งานที่ได้รับการยืนยันสิทธิ์กลับไปยัง Firewall

ขั้นตอนที่ 4 Firewall จะทำการส่งข้อมูลการใช้งานไปยังเครื่อง Log Server

- ขั้นตอนที่ 5 Log Server ทำการตรวจสอบการใช้งานของเครื่อง Client ผ่าน Event Log Monitor
- ขั้นตอนที่ 6 Log Server ทำการรับผลการใช้งานของเครื่อง Client ผ่าน Event Log Monitor และบันทึกเก็บข้อมูลการใช้งานไว้ใน Log Server
- ขั้นตอนที่ 7 Log Server ตอบกลับการบันทึก Log
- ขั้นตอนที่ 8 Client สามารถเข้าถึงการใช้งาน Internet ได้



ภาพที่ 7 แสดงลำดับกระบวนการทำงานของระบบในภาพรวมโดย (User)

จากภาพที่ 7 แสดงขั้นตอนการทำงานของระบบฝั่งผู้ใช้งานได้ดังนี้

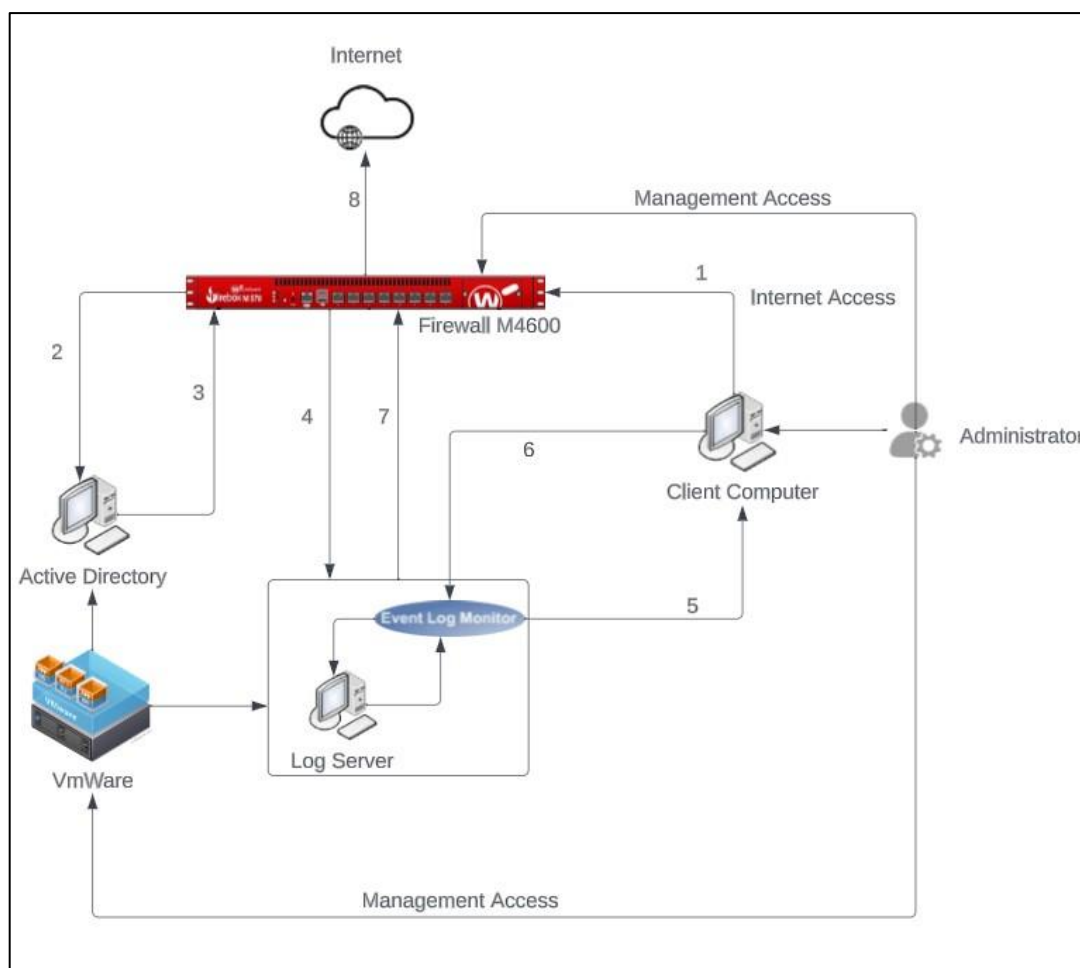
ขั้นตอนที่ 1 User เข้าใช้งานอินเทอร์เน็ตผ่านเครื่องคอมพิวเตอร์ คอมพิวเตอร์โน้ตบุ๊ก คอมพิวเตอร์ แท็บเล็ต หรือ โทรศัพท์มือถือ จะทำการส่งการร้องขอไปที่ Firewall

ขั้นตอนที่ 2 Firewall จะทำการตรวจสอบสิทธิ์ตาม Policy และ สืบค้นข้อมูลผู้ใช้งานบน Active Directory ที่ติดตั้งไว้บน VMware

ขั้นตอนที่ 3 Active Directory จะทำการส่งกลับข้อมูลผู้ใช้งานที่ได้รับการยืนยันสิทธิ์กลับไปยัง Firewall

ขั้นตอนที่ 4 Firewall จะทำการส่งข้อมูลการใช้งานไปยังเครื่อง Log Server

- ขั้นตอนที่ 5 Log Server ทำการตรวจสอบการใช้งานของเครื่อง Client ผ่าน Event Log Monitor
- ขั้นตอนที่ 6 Log Server ทำการรับผลการใช้งานของเครื่อง Client ผ่าน Event Log Monitor และบันทึกเก็บข้อมูลการใช้งานไว้ใน Log Server
- ขั้นตอนที่ 7 Log Server ตอบกลับการบันทึก Log
- ขั้นตอนที่ 8 Client สามารถเข้าถึงการใช้งาน Internet ได้



ภาพที่ 8 แสดงลำดับกระบวนการทำงานของระบบในภาพรวม (Administrator)

จากภาพที่ 8 แสดงขั้นตอนการทำงานของระบบในภาพของผู้ดูแลระบบได้ดังนี้

ขั้นตอนที่ 1 Administrator เข้าใช้งานอินเทอร์เน็ตผ่านเครื่องคอมพิวเตอร์ คอมพิวเตอร์โน้ตบุ๊ก คอมพิวเตอร์แท็บเล็ต หรือ โทรศัพท์มือถือ จะทำการส่งการร้องขอไปที่ Firewall

โดย Administrator สามารถเข้าไปบริหารจัดการ Firewall และ VmWare ได้โดยผ่านช่องทางการบริหารจัดการไม่จำเป็นต้องเข้าถึงอินเทอร์เน็ต

ขั้นตอนที่ 2 Firewall จะทำการตรวจสอบสิทธิ์ตาม Policy และ สืบค้นข้อมูลผู้ใช้งานบน Active Directory ที่ติดตั้งไว้บน VmWare

ขั้นตอนที่ 3 Active Directory จะทำการส่งกลับข้อมูลผู้ใช้งานที่ได้รับการยืนยันสิทธิ์กลับไปยัง Firewall

ขั้นตอนที่ 4 Firewall จะทำการส่งข้อมูลการใช้งานไปยังเครื่อง Log Server

ขั้นตอนที่ 5 Log Server ทำการตรวจสอบการใช้งานของเครื่อง Client ผ่าน Event Log Monitor

ขั้นตอนที่ 6 Log Server ทำการรับผลการใช้งานของเครื่อง Client ผ่าน Event Log Monitor และบันทึกเก็บข้อมูลการใช้งานไว้ใน Log Server

ขั้นตอนที่ 7 Log Server ตอบกลับการบันทึก Log

ขั้นตอนที่ 8 Client สามารถเข้าถึงการใช้งาน Internet ได้

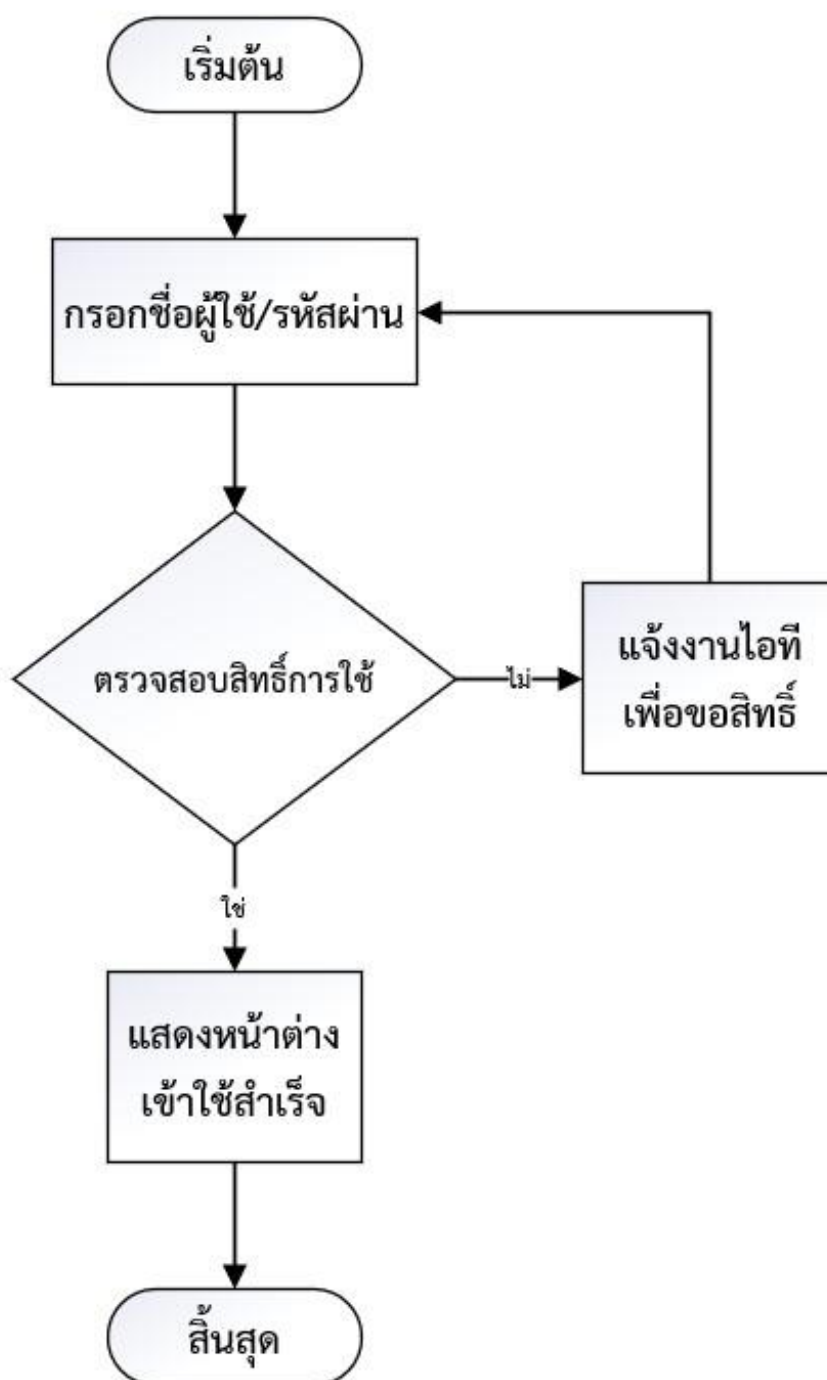
#### 4.1.5 ผลการออกแบบกระบวนการทำงานของขั้นตอนการทำงานของระบบ

ออกแบบการการใช้งานระบบในแต่ละงาน และนำมาเขียนให้อยู่ในรูปแบบของผังงาน (Flowchart) ได้ดังต่อไปนี้

1. ขั้นตอนการเข้าสู่ระบบ และการขอสิทธิ์การใช้งาน
2. ขั้นตอนการเปลี่ยนรหัสผ่าน
3. แสดงขั้นตอนการรับข้อมูลจากงานการเจ้าหน้าที่ เพื่อทำการลงทะเบียนเพิ่ม/ลบ สิทธิ์การใช้งาน
4. นำการทำงานของโปรแกรมจัดเก็บและรายงานข้อมูลจราจรคอมพิวเตอร์มาเขียนให้อยู่ในรูปแบบของผังงาน เพื่อให้เห็นภาพการทำงานของระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์

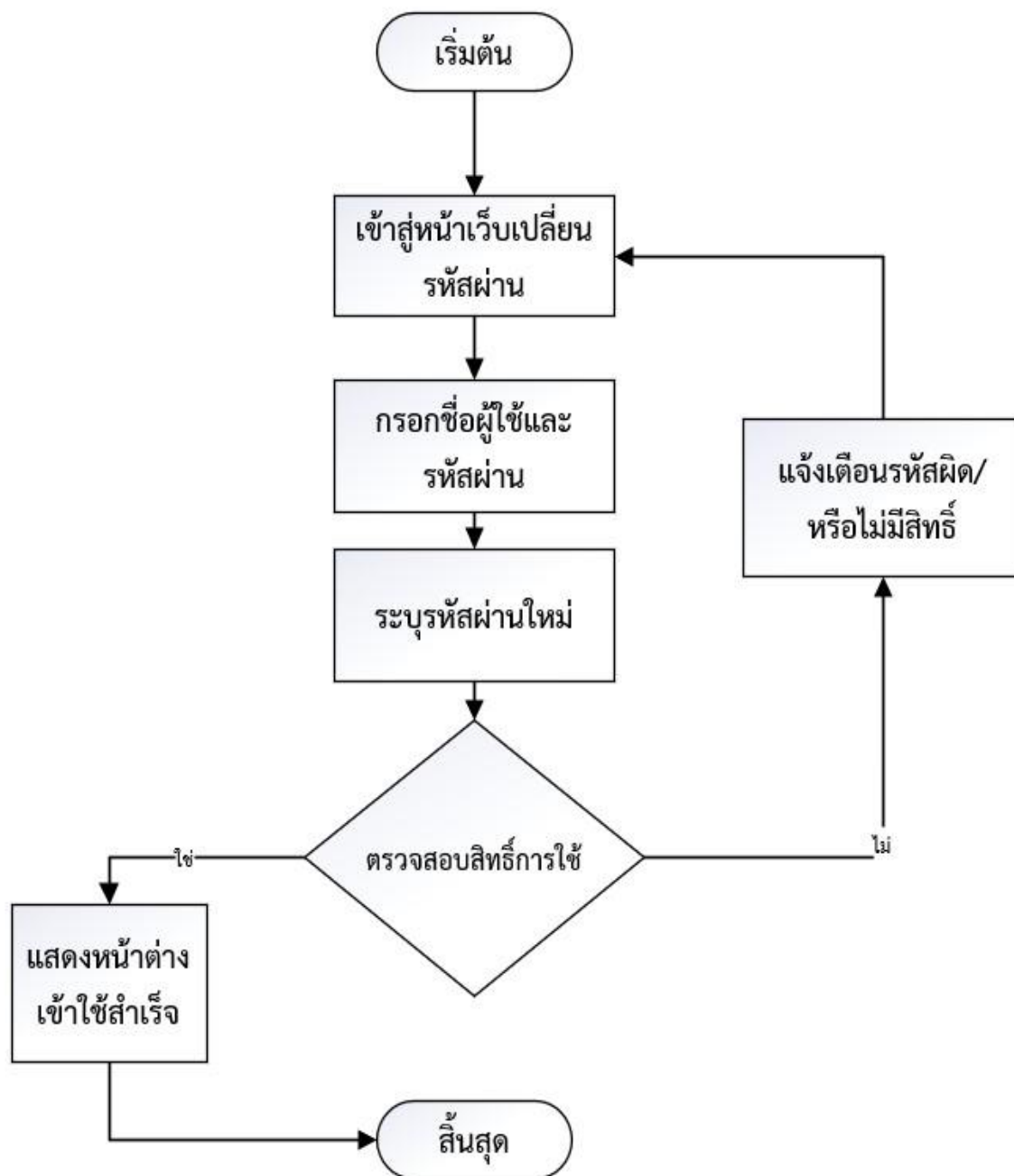


## 1. ขั้นตอนการเข้าสู่ระบบ และการขอสิทธิ์การใช้งาน



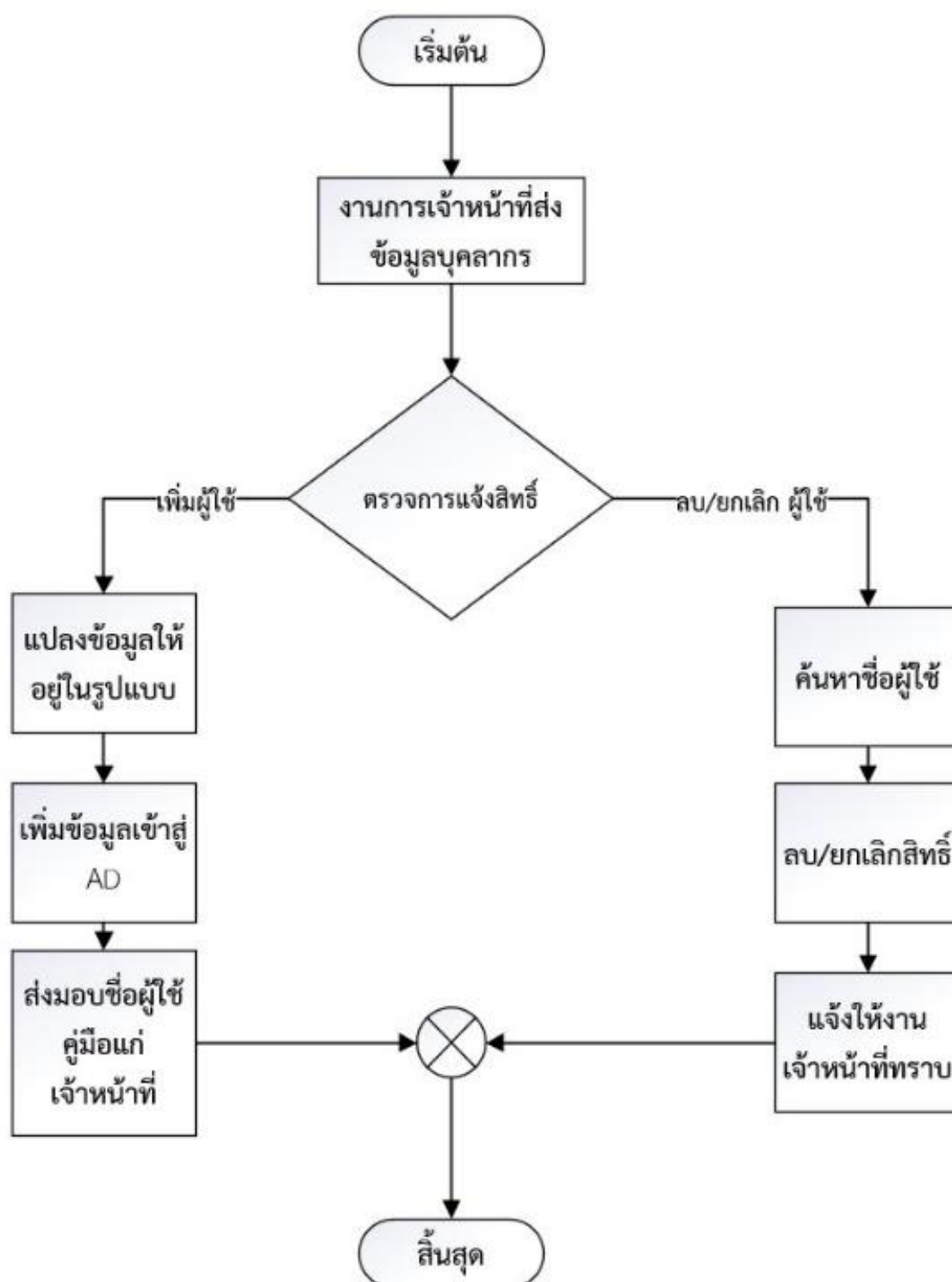
ภาพที่ 9 แสดงขั้นตอนการเข้าสู่ระบบ และการขอสิทธิ์การใช้งาน

## 2. ขั้นตอนการเปลี่ยนรหัสผ่าน



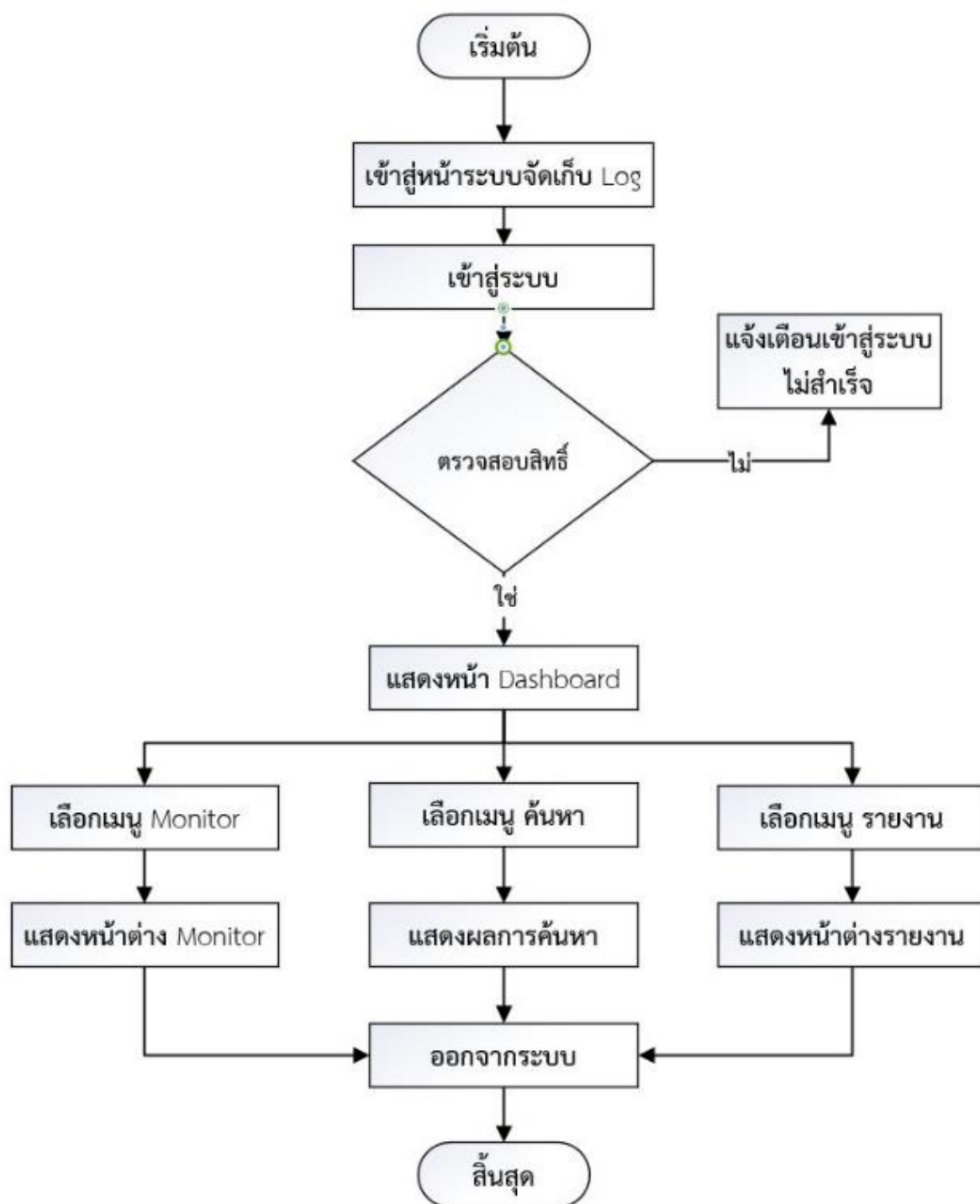
ภาพที่ 10 แสดงขั้นตอนการเปลี่ยนรหัสผ่าน

3. แสดงขั้นตอนการรับข้อมูลจากงานการเจ้าหน้าที่ เพื่อทำการลงทะเบียนเพิ่ม/ลบ สิทธิการใช้งาน



ภาพที่ 11 แสดงขั้นตอนการรับข้อมูลจากงานการเจ้าหน้าที่ เพื่อทำการลงทะเบียนเพิ่ม/ลบ สิทธิการใช้งาน

4. นำการทำงานของโปรแกรมจัดเก็บและรายงานข้อมูลจราจรคอมพิวเตอร์มาเขียนให้อยู่ในรูปของผังงาน เพื่อให้เห็นภาพการทำงานของระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์



ภาพที่ 12 แสดงผังงานการทำงานของระบบรายงานข้อมูลจราจรคอมพิวเตอร์

#### 4.1.6 ผลการนำข้อมูลบุคลากรของหน่วยงานมาวิเคราะห์เพื่อกำหนดชื่อผู้ใช้ รหัสผ่าน และข้อมูลพื้นฐานที่จำเป็นในการระบุตัวตน

##### 1. นำข้อมูลจากงานการเจ้าหน้าที่มาวิเคราะห์

เนื่องจากข้อมูลที่ได้จากงานการเจ้าหน้าที่ มีส่วนของข้อมูลส่วนบุคคลของบุคลากร ซึ่งที่ข้อมูลนำมาใช้กำหนดให้อยู่ในรูปแบบของ Username และ Password จึงจำเป็นต้องตัดข้อมูลที่ไม่จำเป็นต้องเก็บออก และดำเนินการแจ้งให้บุคลากรซึ่งมีสิทธิ์ตามพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ให้ทราบสิทธิ์ดังนี้

- สิทธิได้รับการแจ้งให้ทราบ (Right to be informed)
- สิทธิขอเข้าถึงข้อมูลส่วนบุคคล (Right of access)
- สิทธิในการขอให้โอนข้อมูลส่วนบุคคล (Right to data portability)
- สิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล (Right to object)
- สิทธิขอให้ลบหรือทำลาย (Right to erasure also known as right to be forgotten)
- สิทธิขอให้ระงับการใช้ข้อมูล (Right to restrict processing)
- สิทธิในการขอให้แก้ไขข้อมูลส่วนบุคคล (Right of rectification)

โดยข้อมูลที่ได้รับมาประกอบด้วย ลำดับ ประเภทการจ้าง เลขที่ตำแหน่ง ชื่อ-สกุล ภาษาไทยและภาษาอังกฤษ ตำแหน่ง ระดับ ซึ่งทั้งหมดเป็นข้อมูลพื้นฐาน และข้อมูลส่วนบุคคลประเภททั่วไปไม่มีข้อมูลส่วนบุคคลที่มีความอ่อนไหวภายใต้วัตถุประสงค์ของการใช้ระบบการยืนยันตัวตน เพื่อให้สามารถระบุตัวตนของผู้ใช้งานได้จึงได้กำหนดรูปแบบของการตั้ง Username ไว้ ดังนี้

1.1 ใช้ชื่อภาษาอังกฤษตามด้วย. และตัวอักษรภาษาอังกฤษตัวแรกของนามสกุล

1.2 หากมีชื่อผู้ใช้งานให้ใช้เป็นภาษาอังกฤษตามด้วย ‘.’ ตัวอักษรภาษาอังกฤษสองตัวแรกของนามสกุล และได้ดำเนินการกำหนด Password โดยใช้วิธีการ random password โดยกำหนดความยาวไว้ที่ 8 ตัวอักษร โดยมีโครงสร้างของข้อมูลดังนี้

ตารางที่ 4 แสดงตารางโครงสร้างการจัดเก็บข้อมูล

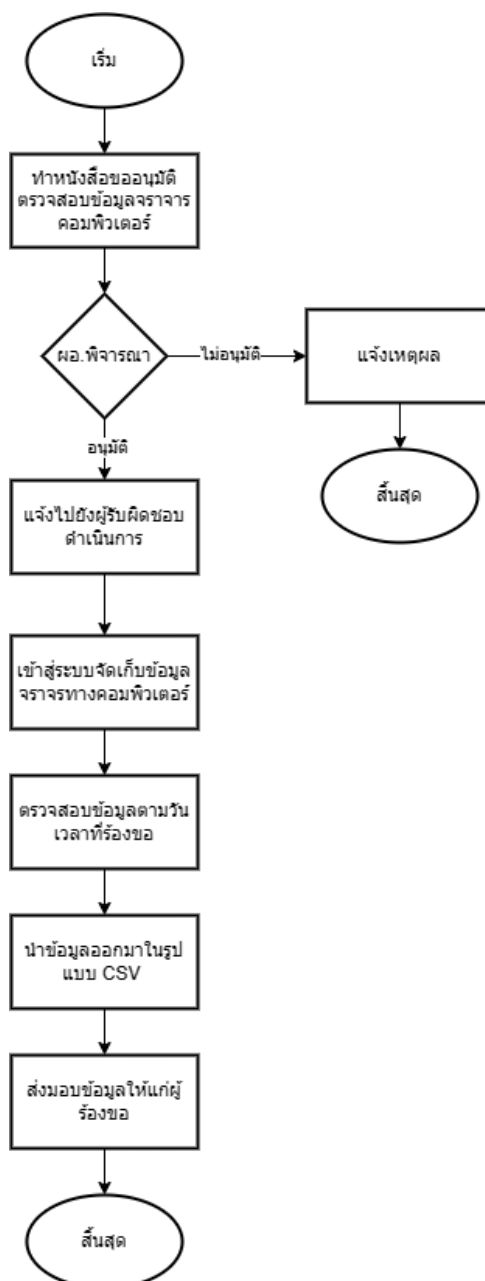
ชื่อตัวแปร	รายละเอียด	ชนิดของข้อมูล
Organization Unit	กลุ่มที่ปฏิบัติงาน	String
Description	ชื่อ-สกุลที่เป็นภาษาไทย เพื่อต่อการค้นหา	String
First Name	ชื่อภาษาอังกฤษเพื่อนำไปใช้ในการสร้าง Username	String
Last Name	นามสกุลภาษาอังกฤษเพื่อนำไปใช้ในการสร้าง Username	String
Username	ชื่อผู้ใช้นั้นชื่อ-สกุลภาษาอังกฤษมาสร้าง	String
Password	ข้อมูล Password ปัจจุบันของผู้ใช้งาน	Binary

A	B	G	H	I	K
Organization Unit	Description	first name	last name	User logon	Password
กลุ่มห้องปฏิบัติการควบคุมโรคและภัยสุขภาพ	นาย			at.k	****
กลุ่มห้องปฏิบัติการควบคุมโรคและภัยสุขภาพ	นางอ			a.p	****
กลุ่มห้องปฏิบัติการควบคุมโรคและภัยสุขภาพ	นางส			a.b	****
กลุ่มห้องปฏิบัติการควบคุมโรคและภัยสุขภาพ	นางส			orn.j	****
กลุ่มห้องปฏิบัติการควบคุมโรคและภัยสุขภาพ	นาย			it.b	****
กลุ่มห้องปฏิบัติการควบคุมโรคและภัยสุขภาพ	นาย			in.c	****
กลุ่มห้องปฏิบัติการควบคุมโรคและภัยสุขภาพ	นางส			van.n	****
กลุ่มห้องปฏิบัติการควบคุมโรคและภัยสุขภาพ	นางส			anok.t	****
กลุ่มห้องปฏิบัติการควบคุมโรคและภัยสุขภาพ	นาย			kham.s	****
กลุ่มห้องปฏิบัติการควบคุมโรคและภัยสุขภาพ	นางส			a.s	****
กลุ่มห้องปฏิบัติการควบคุมโรคและภัยสุขภาพ	นาย			m.k	****
กลุ่มห้องปฏิบัติการควบคุมโรคและภัยสุขภาพ	นางส			on.w	****
กลุ่มห้องปฏิบัติการควบคุมโรคและภัยสุขภาพ	นางส			olt	****

ภาพที่ 13 แสดงตัวอย่างข้อมูลที่ได้ทำการวิเคราะห์แล้วก่อนบันทึกลงระบบ Active Directory

#### 4.1.7 ผลศึกษากระบวนการตรวจสอบประวัติการใช้งาน

1. ขั้นตอนดำเนินงาน ในกรณีของการขอตรวจสอบประวัติการใช้งาน กรณีที่ต้องใช้เป็นหลักฐาน ดำเนินการตามกฎหมาย สามารถเขียนให้อยู่ในรูปผังงานได้ดังนี้



ภาพที่ 14 แสดงขั้นตอนการร้องขอตรวจสอบประวัติการใช้งานระบบเครือข่ายอินเทอร์เน็ต  
โดยข้อมูลจราจรทางคอมพิวเตอร์

## 4.2 ดำเนินการตามแผนการพัฒนา (Do)

### 1. ผลการดำเนินการสร้างเครื่องเซิร์ฟเวอร์ และคอมพิวเตอร์เสมือนจริง

#### 1.1 ดำเนินการสร้างเซิร์ฟเวอร์ และคอมพิวเตอร์เสมือนจริงโดยใช้โปรแกรม VMware vSphere Client

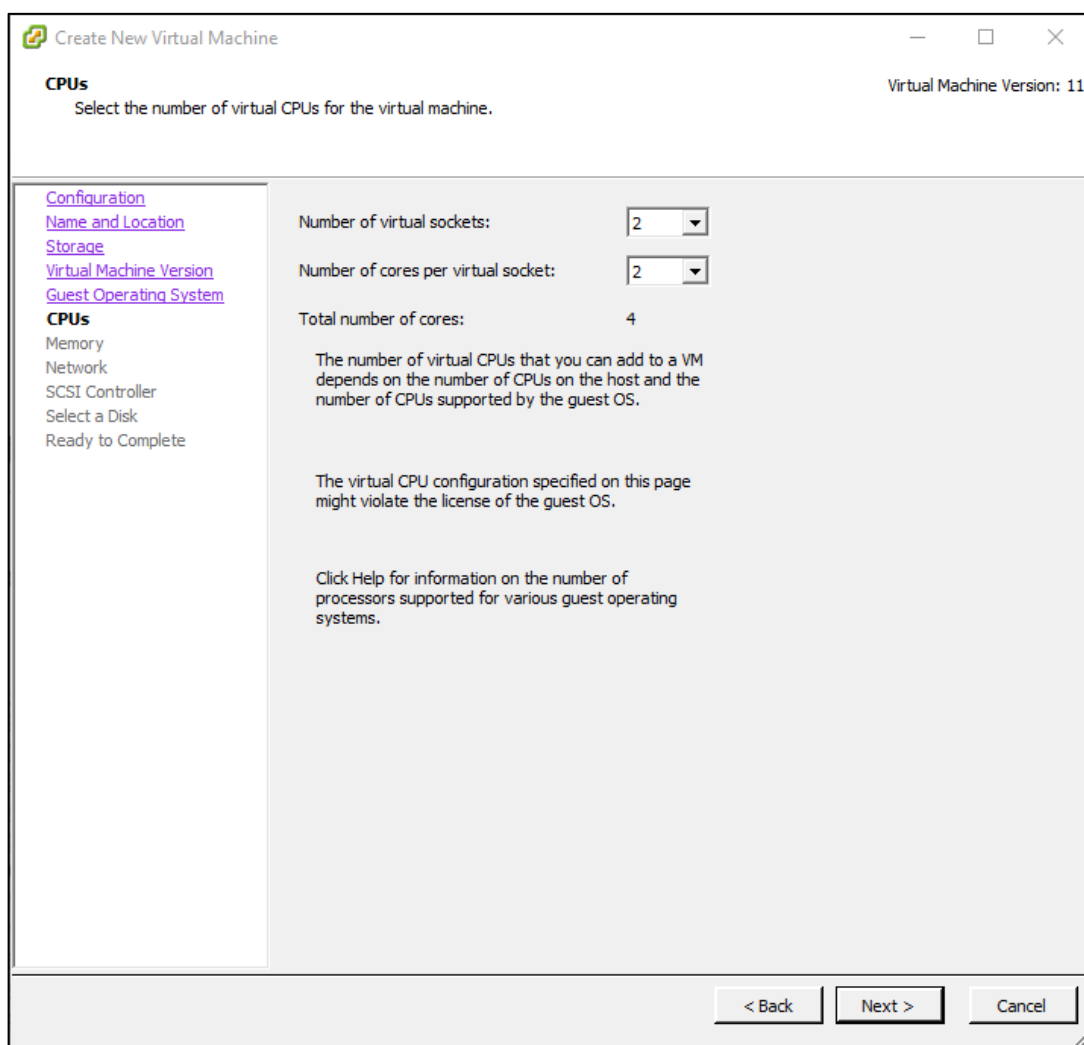


ภาพที่ 15 แสดงหน้าต่างการเข้าใช้งานโปรแกรม VMware vSphere Client

จากภาพแสดงหน้าต่างการเข้าใช้งานโปรแกรม VMware vSphere Client โดยระบุ IP Address ของเครื่องเซิร์ฟเวอร์ที่ติดตั้ง VMware ไว้ และระบุ Username / Password สำหรับเข้าใช้งาน



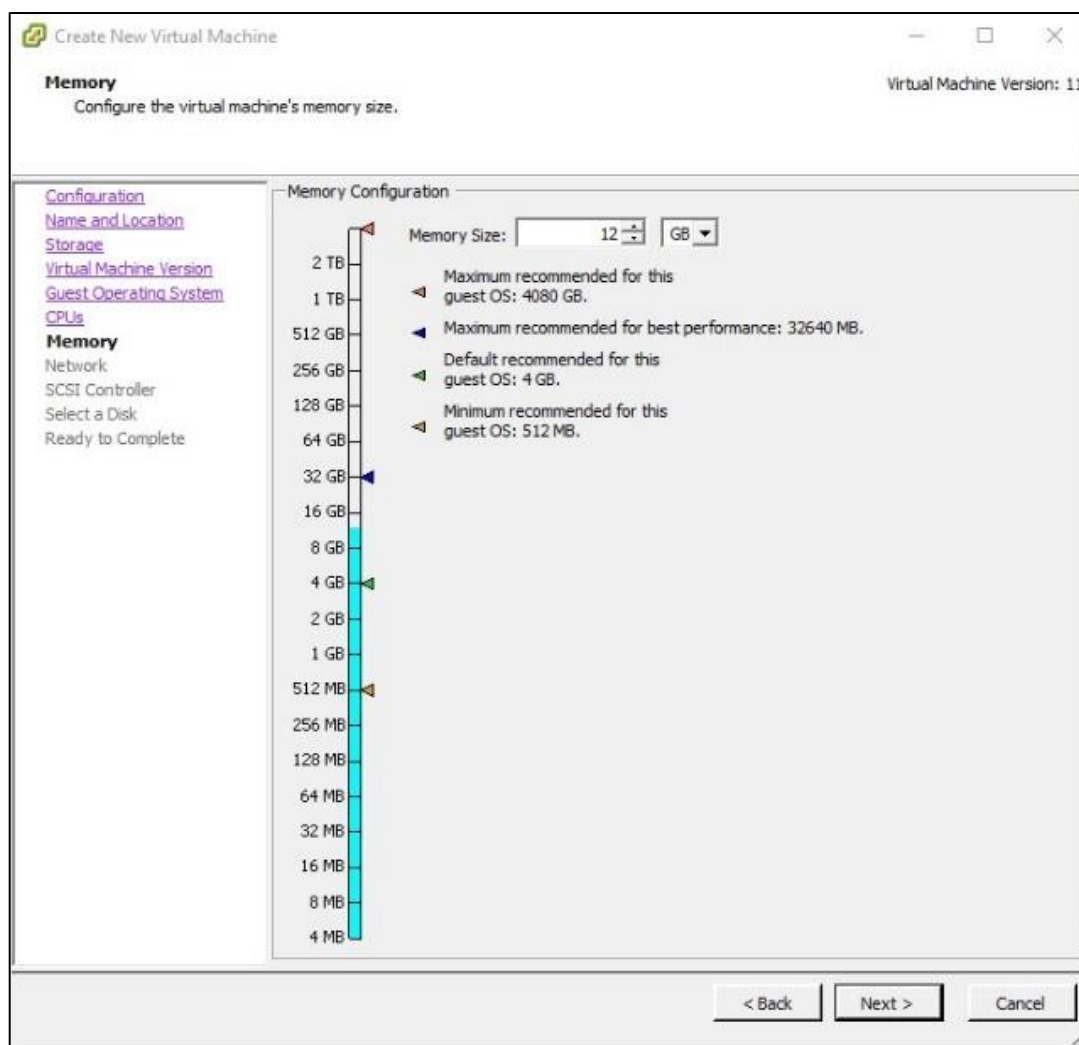
1.2 กดปุ่ม create a new virtual machine แล้ว next ไปยังหน้ากำหนด CPUs ของเครื่อง โดยกำหนดรายละเอียดไว้ดังนี้ socket core และ 2 virtual socket core รวมเป็น 4 cores



ภาพที่ 16 แสดงหน้าต่างการกำหนด CPUs cores ของเครื่องเสมือนจริง

จากภาพแสดงหน้าต่างการกำหนดจำนวน Virtual CPU ให้กับเครื่องเซิร์ฟเวอร์หรือคอมพิวเตอร์เสมือนจริงที่ต้องการสร้าง โดยสามารถเลือกจำนวน CPU ที่ต้องการ และจำนวน Cores ที่ต้องการต่อ CPU ที่กำหนด โดยระบบจะสรุปจำนวน Cores รวมที่ได้กำหนดไว้ที่ด้านล่าง ซึ่งหากจำนวนที่ระบุไว้ไม่เหมาะสมกับการใช้งาน สามารถมาปรับปรุงแก้ไขได้โดยไม่ต้องสร้างใหม่

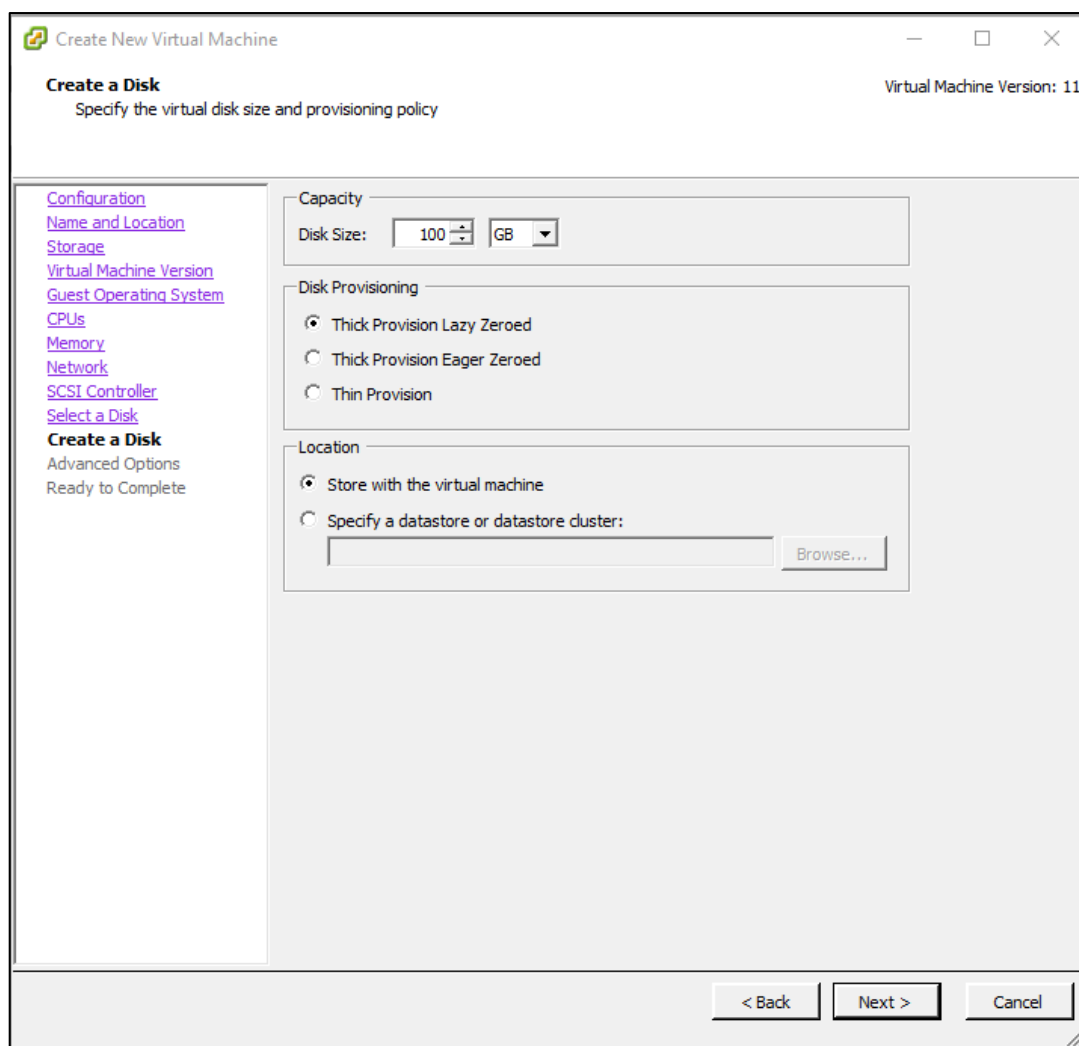
1.3 ต่อไปเป็นหน้าต่างกำหนด Memory ของเครื่อง โดยกำหนดขนาดของ Memory ของเครื่อง เซิร์ฟเวอร์ ไว้ที่ 12 GB และเครื่องคอมพิวเตอร์ Log Files ไว้ที่ 4 GB



ภาพที่ 17 แสดงหน้าต่างการกำหนด Memory ของเครื่องเสมือนจริง

จากภาพแสดงหน้าต่างการกำหนดจำนวนของ Memory ให้กับเครื่องเซิร์ฟเวอร์หรือคอมพิวเตอร์เสมือนจริงที่ต้องการสร้าง โดยสามารถกำหนดขนาดของ Memory ได้ตามความต้องการของระบบที่จะติดตั้งซึ่งหากจำนวนที่ระบุไว้ไม่เหมาะสมกับการใช้งาน สามารถมาปรับปรุงแก้ไขได้โดยไม่จำเป็นต้องสร้างใหม่

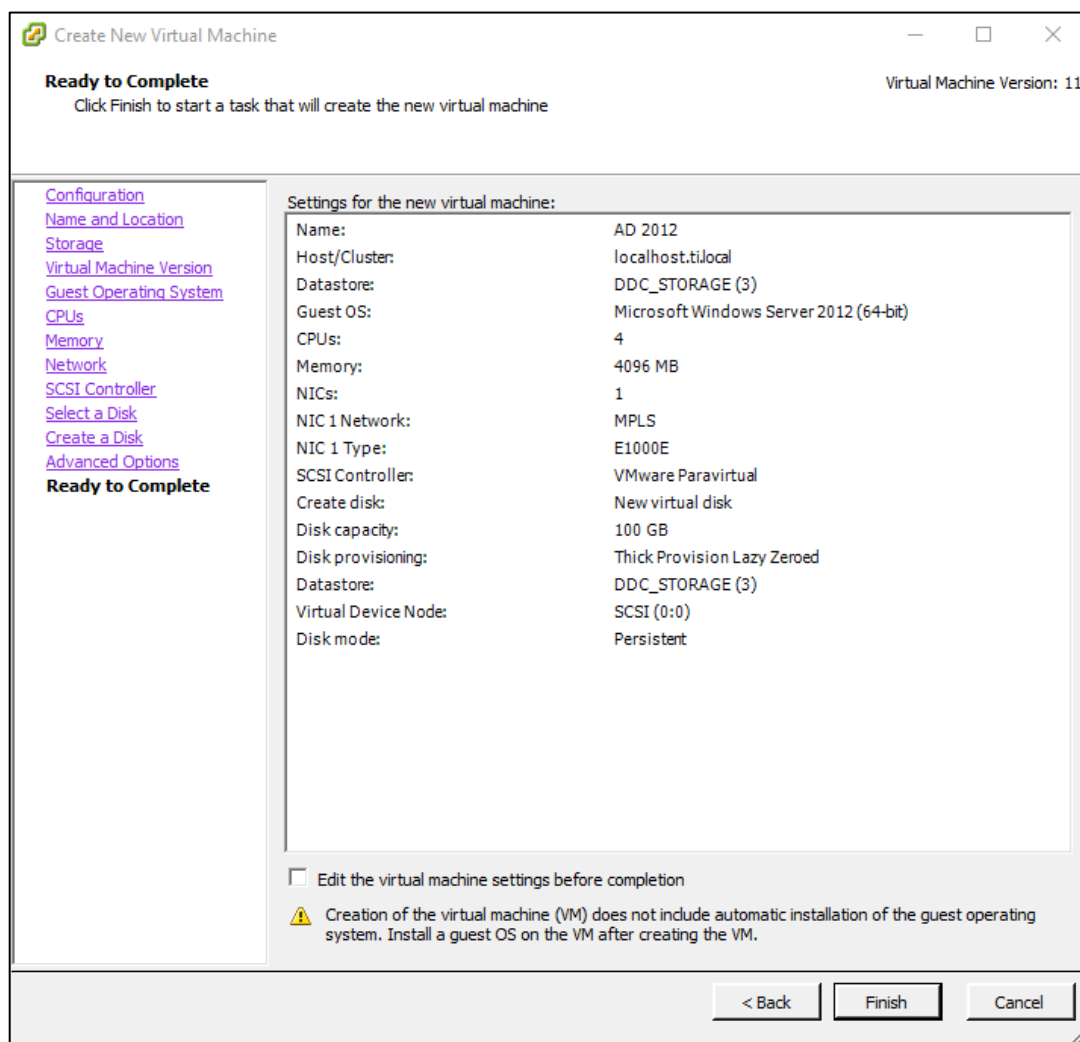
1.4 ต่อไปเป็นหน้าต่างกำหนด Disk ของเครื่อง โดยกำหนดขนาดของ Disk ไว้ที่ 100 GB และกำหนดค่า Disk provisioning ไว้ที่ Thick Provision Lazy Zeroed คือการจองพื้นที่ Disk ให้เท่ากับพื้นที่ที่กำหนดไว้ และกำหนดค่า Location เป็น Default คือ Store with the virtual machine



ภาพที่ 18 แสดงหน้าต่างการกำหนด Disk size ของเครื่องเสมือนจริง

จากภาพแสดงหน้าต่างการกำหนดความจุของพื้นที่จัดเก็บข้อมูล (Disk) ให้กับเครื่องเซิร์ฟเวอร์หรือคอมพิวเตอร์เสมือนจริงที่ต้องการสร้าง โดยสามารถกำหนดความจุของพื้นที่จัดเก็บข้อมูล (Disk) ได้ตามความต้องการของระบบที่จะติดตั้ง ซึ่งหากจำนวนที่ระบุไว้ไม่เหมาะสมกับการใช้งาน สามารถมาปรับปรุงแก้ไขได้โดยไม่ต้องสร้างใหม่

1.5 เมื่อกำหนดรายละเอียดต่าง ๆ เรียบร้อย โปรแกรมจะแสดงหน้าต่างสรุปผลการตั้งค่าให้ตรวจเช็คอีกครั้ง โดยสามารถกด back เพื่อไปทำการแก้ไขรายละเอียดได้ เมื่อตรวจสอบเรียบร้อยแล้วกดปุ่ม Finish

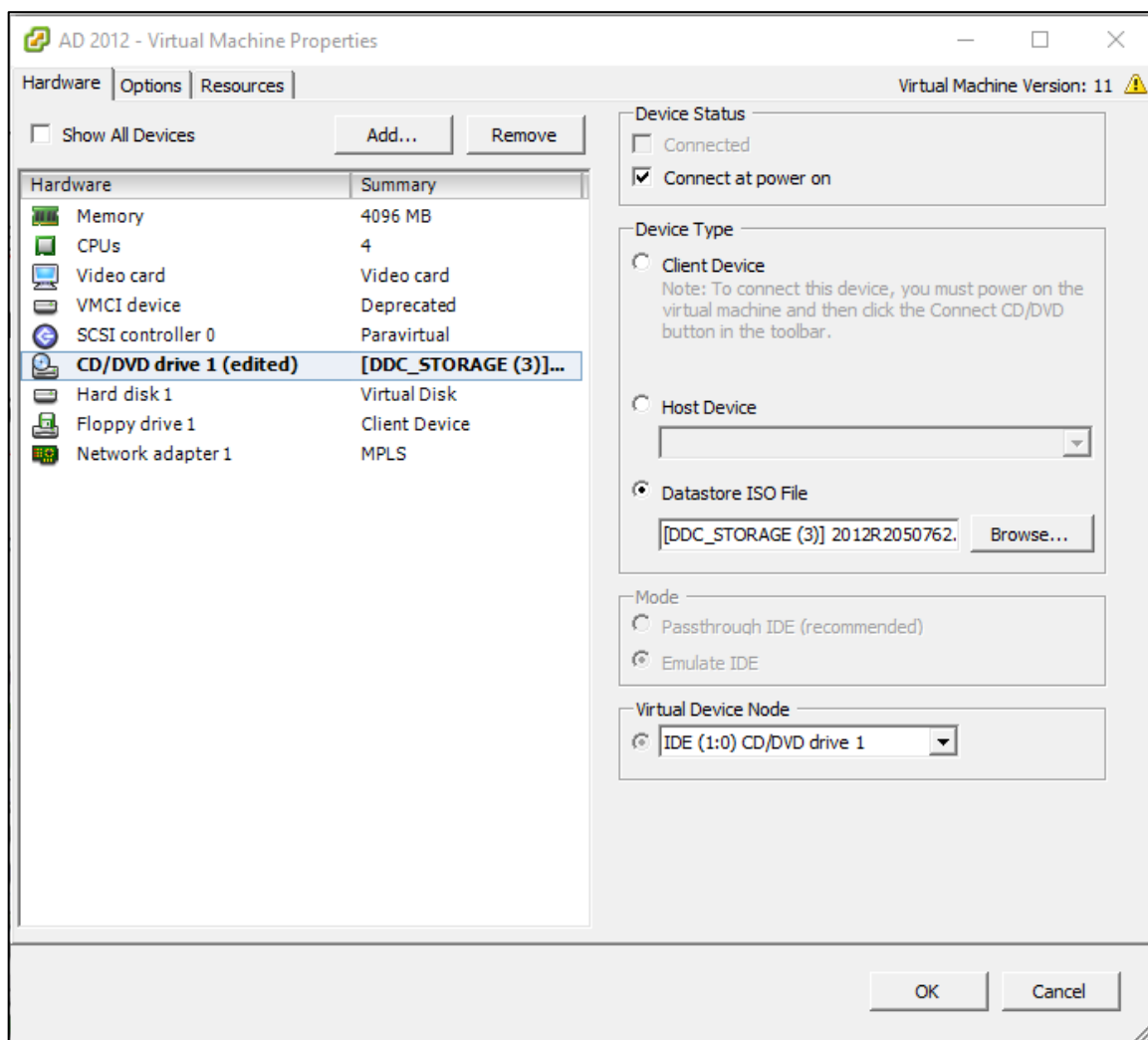


ภาพที่ 19 แสดงหน้าต่างรายละเอียดการตั้งค่าทั้งหมดของเครื่องเสมือนจริงตามที่ได้กำหนดไว้

จากภาพแสดงหน้าต่างรายละเอียดการตั้งค่าที่ได้กำหนดไว้ในขั้นตอนก่อนหน้า โดยจะมีรายละเอียดทั้งหมดของทรัพยากรที่ใช้ในการสร้างคอมพิวเตอร์เสมือนจริงขึ้นมา เพื่อให้สามารถตรวจดูอีกครั้งก่อนกดปุ่ม Finish เพื่อยืนยันการสร้าง

## 2. ติดตั้ง Windows Server 2012 บน Server และดำเนินการกำหนดการตั้งค่า

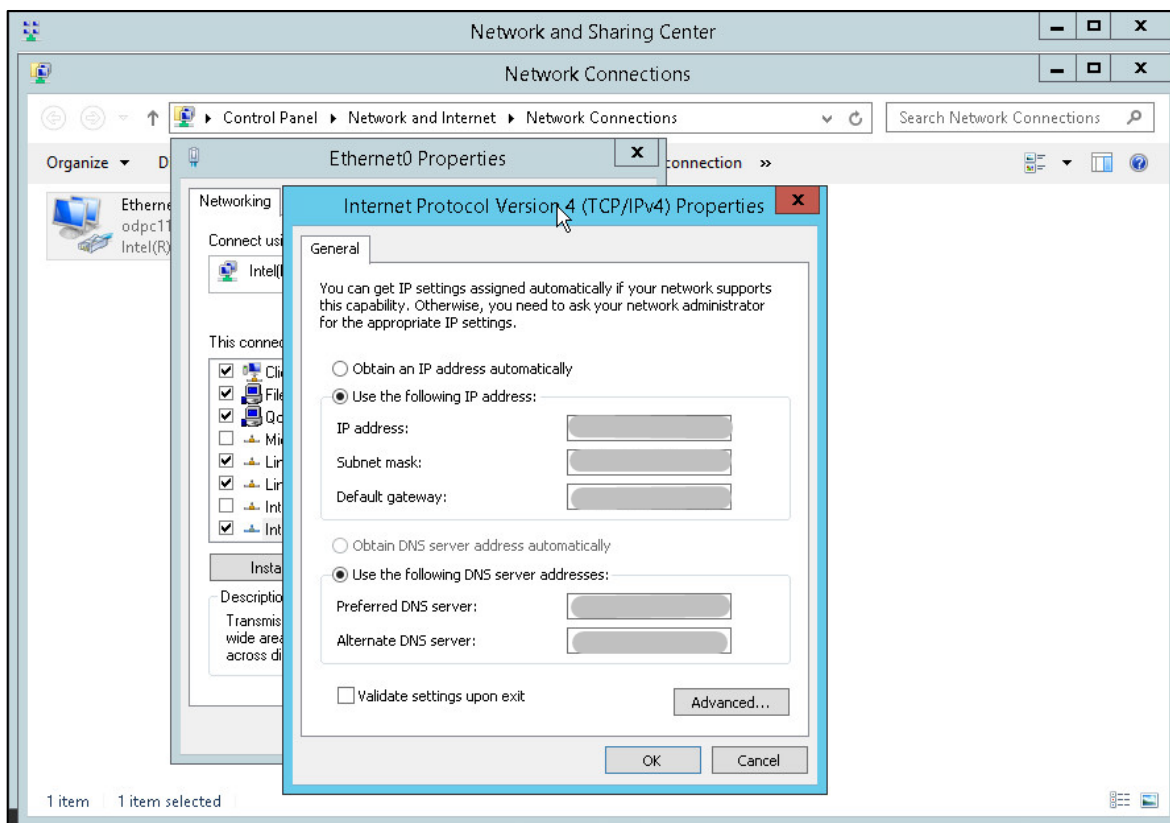
2.1 เมื่อสร้างเครื่องเสมือนจริงเรียบร้อยแล้ว ดำเนินการเลือกไฟล์ ISO windows server 2012 นำมาวางไว้ใน virtual cd/dvd drive เพื่อทำการติดตั้ง windows



ภาพที่ 20 แสดงการเลือก ISO Files ของ Windows ที่จะทำการติดตั้ง

จากภาพแสดงหน้าต่าง Virtual Hardware ที่ได้ทำการสร้างขึ้นมาเป็นเครื่องคอมพิวเตอร์เสมือน โดยหลังจากทำการสร้างเครื่องคอมพิวเตอร์เสร็จเรียบร้อยแล้ว จำเป็นจะต้องติดตั้งระบบปฏิบัติการโดยสามารถดำเนินการได้โดยไปที่ CD/DVD Drive เสมือนจริงที่ได้สร้างไว้ กดเลือก ISO Files ของระบบปฏิบัติการ และติ๊ก Connect at power on เพื่อให้ระบบจำลองการทำงานของ CD/DVD Drive จากนั้นดำเนินการเปิดเครื่องคอมพิวเตอร์เสมือน และติดตั้งระบบปฏิบัติการเหมือนคอมพิวเตอร์ทั่วไปได้เลย

2.2 เมื่อติดตั้ง Windows server 2012 เรียบร้อยแล้ว เข้าสู่การกำหนด IP ให้เครื่อง Server โดยกำหนดให้เป็นแบบ Static เพื่อง่ายต่อการเชื่อมต่อ



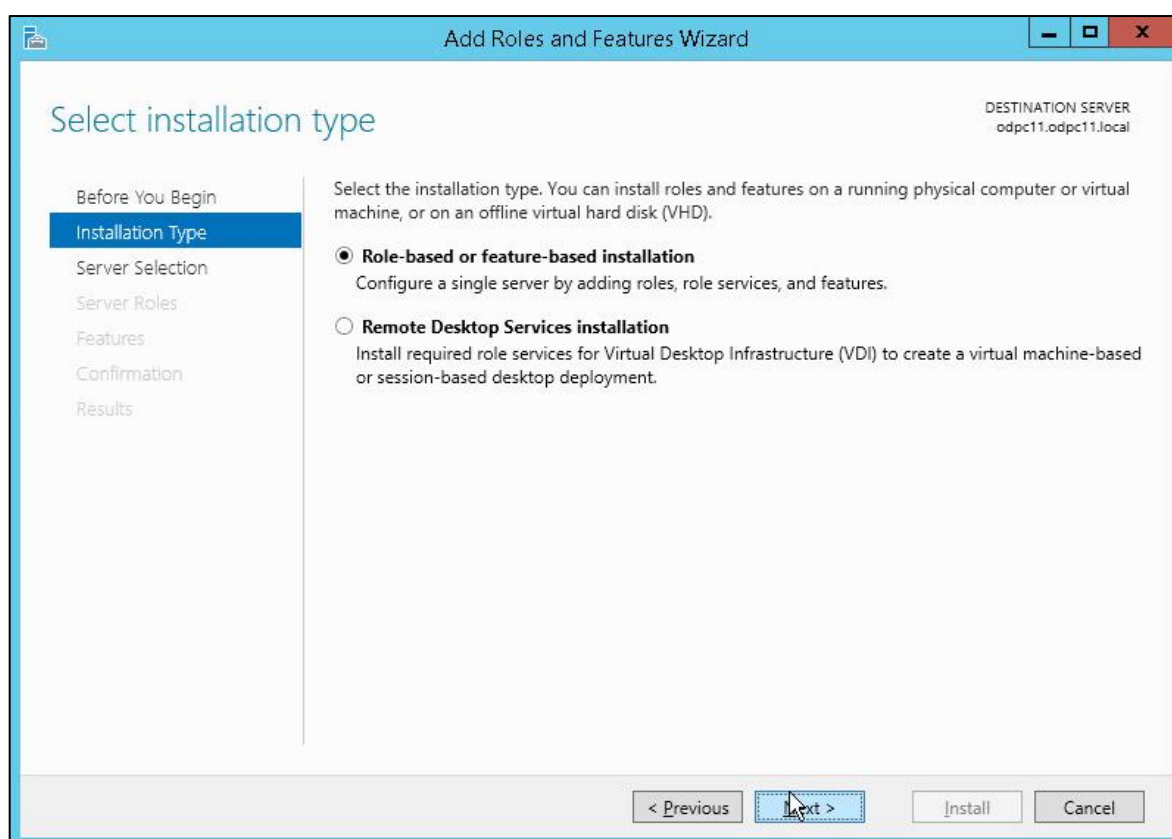
ภาพที่ 21 แสดงการกำหนด IP address ของเครื่อง Server

จากภาพแสดงหน้าต่างการกำหนด IP Address ของเครื่องเซิร์ฟเวอร์หรือคอมพิวเตอร์เสมือนจริง หลังจากที่ได้มีการติดตั้งระบบปฏิบัติการเรียบร้อยแล้ว ขั้นตอนถัดไปคือการกำหนด IP Address ของเครื่อง Server หรือคอมพิวเตอร์เสมือน เพื่อให้เครื่องคอมพิวเตอร์เสมือนที่ได้ทำการสร้างขึ้นมาอยู่ในเครือข่ายเดียวกันกับระบบเครือข่ายที่ต้องการใช้งาน

### 3. ติดตั้ง Role and Feature ที่จำเป็นบน Windows Server

เพื่อเป็นการกำหนดรูปแบบของ server ให้กลายเป็น Active Directory Domain Services จึงต้องมีการติดตั้ง Roles and Features โดยมีขั้นตอนการติดตั้ง ดังนี้

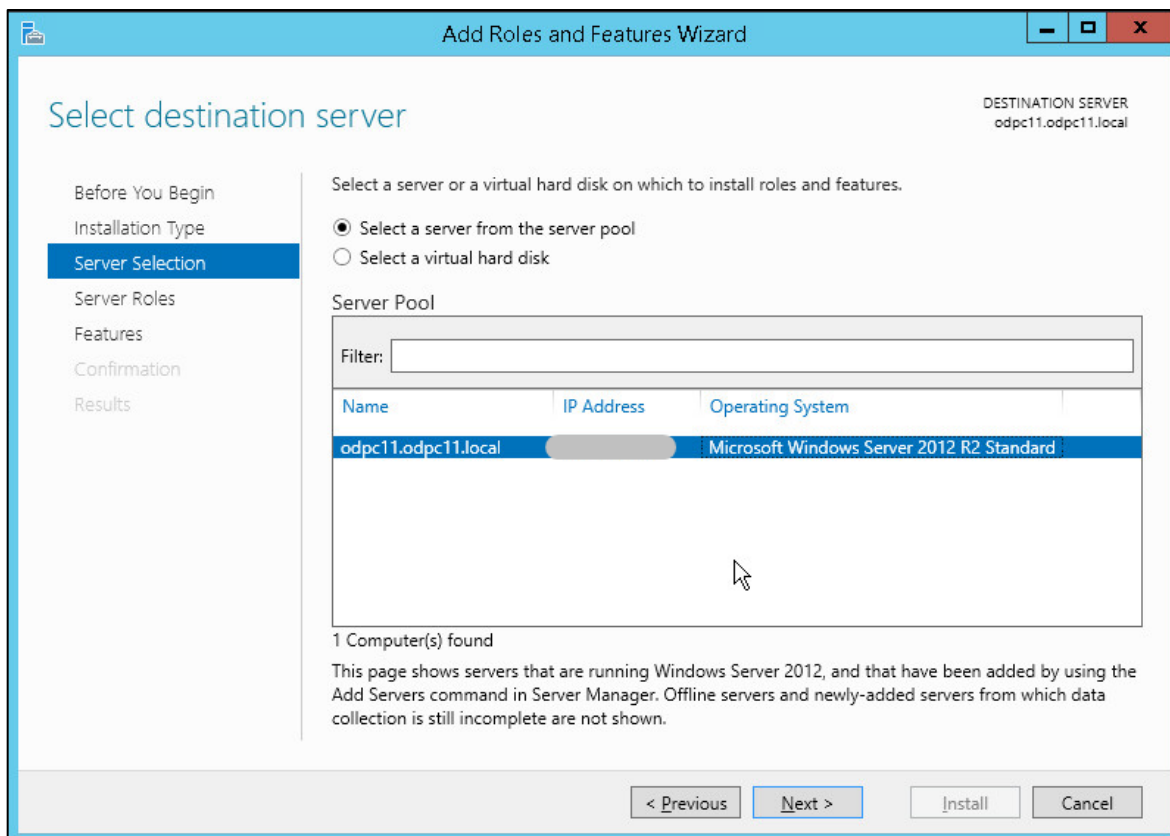
3.1 เปิดโปรแกรม Server Manager ขึ้นมาแล้วเลือก Add roles and features เพื่อเปิดใช้งาน features active directory domain services



ภาพที่ 22 แสดงหน้าต่างการติดตั้ง Roles and Features

จากภาพแสดงหน้าต่างการติดตั้ง Roles and Features ของเครื่องเซิร์ฟเวอร์ การกำหนด Roles and Features ของเครื่องคอมพิวเตอร์เซิร์ฟเวอร์ เพื่อกำหนดหน้าที่ของเครื่องเซิร์ฟเวอร์ที่สร้างขึ้นว่าให้มีความสามารถในการทำอะไรได้บ้าง เพื่อเป็นการประหยัดทรัพยากรในการประมวลผลและให้เซิร์ฟเวอร์ทำงานที่กำหนดไว้อย่างมีประสิทธิภาพ โดยการเลือกที่หัวข้อ Role-Based or Features-Based installation

3.2 กด Next นำไปสู่ขั้นตอนการเลือกเซิร์ฟเวอร์ปลายทางในการติดตั้ง ซึ่งจะเป็นเซิร์ฟเวอร์ปัจจุบันที่ดำเนินการติดตั้ง Roles อยู่

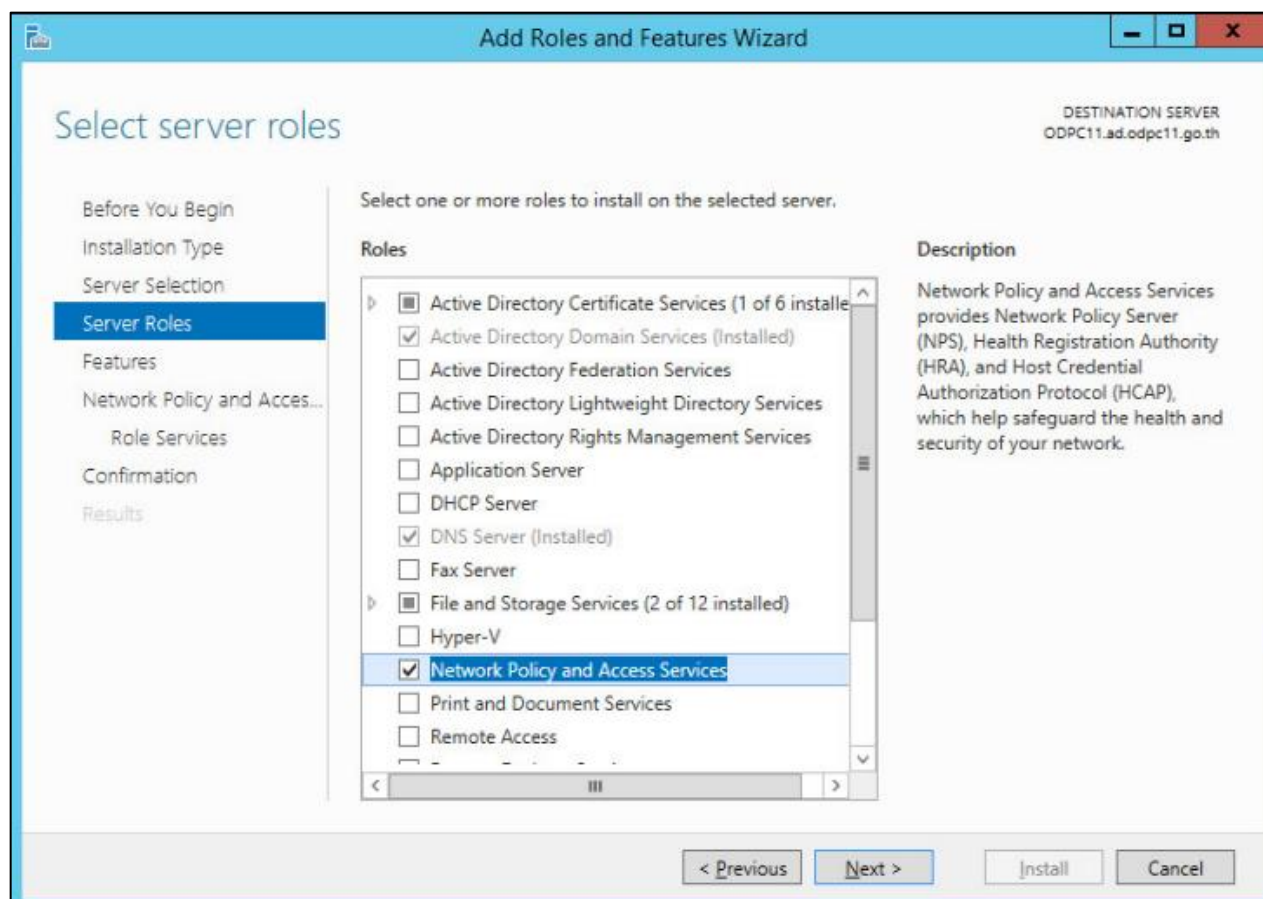


ภาพที่ 23 ทำการเลือกเซิร์ฟเวอร์ที่จะทำการติดตั้ง Roles

จากภาพแสดงหน้าต่างการเลือกเซิร์ฟเวอร์ปลายทางสำหรับติดตั้ง ติดตั้ง Roles and Features โดยหัวข้อนี้มีไว้สำหรับในกรณีที่ทำการบริหารจัดการเซิร์ฟเวอร์หลายตัวพร้อม ๆ กัน เพื่อประหยัดเวลา ในกรณีของผู้วิจัยมีเครื่องเซิร์ฟเวอร์ปลายทางตัวเดียวจึงมีแค่หนึ่งตัวเลือก จากนั้นกดเลือกและกด Next เพื่อไปยังหน้าต่างถัดไป



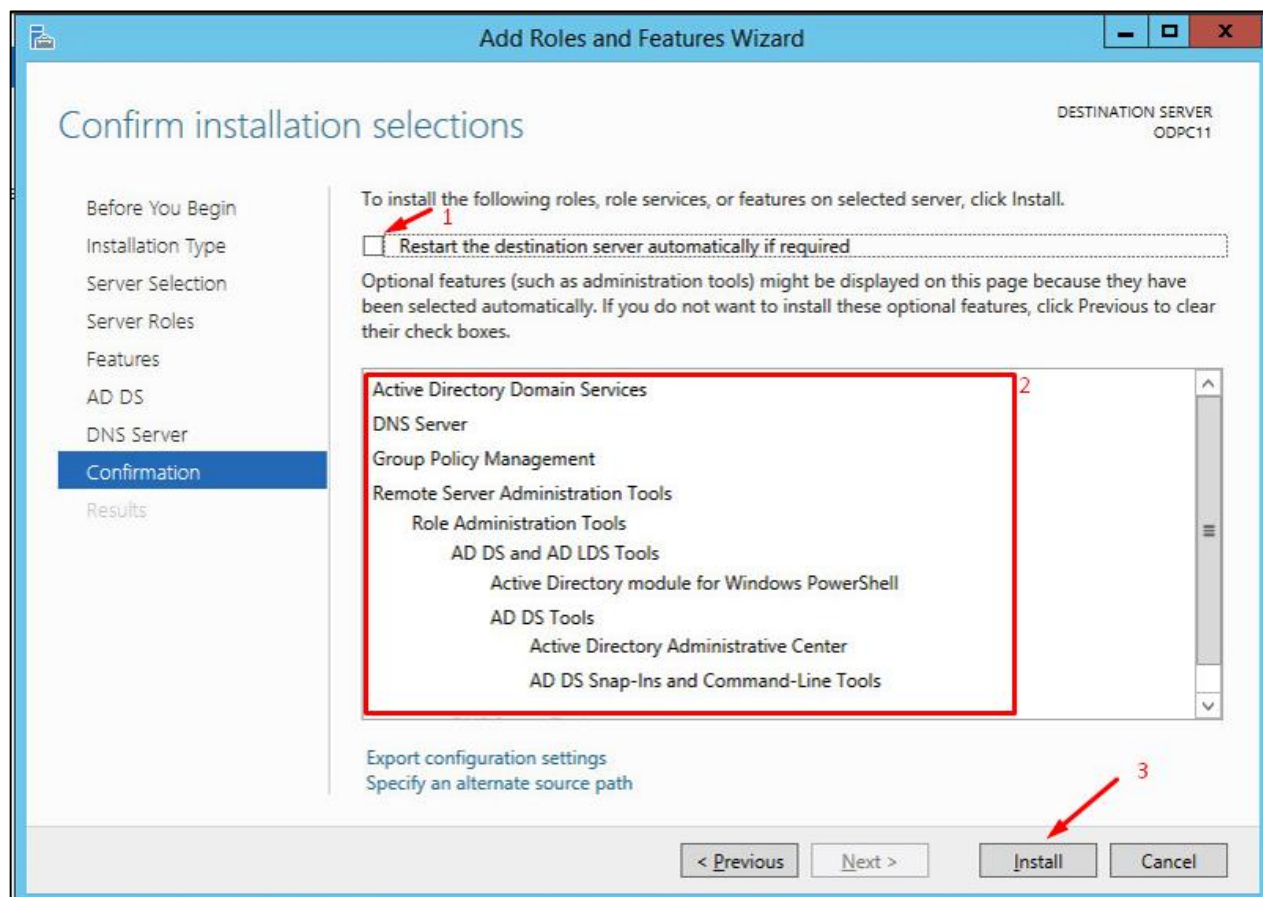
3.3 กด Next นำไปสู่หน้าต่างการเลือก Roles ที่จะติดตั้ง โดยทำการเลือก Roles ดังนี้  
Active directory domain services (AD DS), DNS Server และ Network policy and Access Services



ภาพที่ 24 แสดงหน้าต่างการเลือก Roles ที่จะทำการติดตั้ง

จากภาพแสดงหน้าต่างการเลือก Roles ที่ต้องการติดตั้ง สำหรับกำหนดการทำงานของเครื่องเซิร์ฟเวอร์ โดยทำการเลือก Active Directory Certificate Services , Active Directory Domain Services, DNS Server และ Network Policy and Access Services

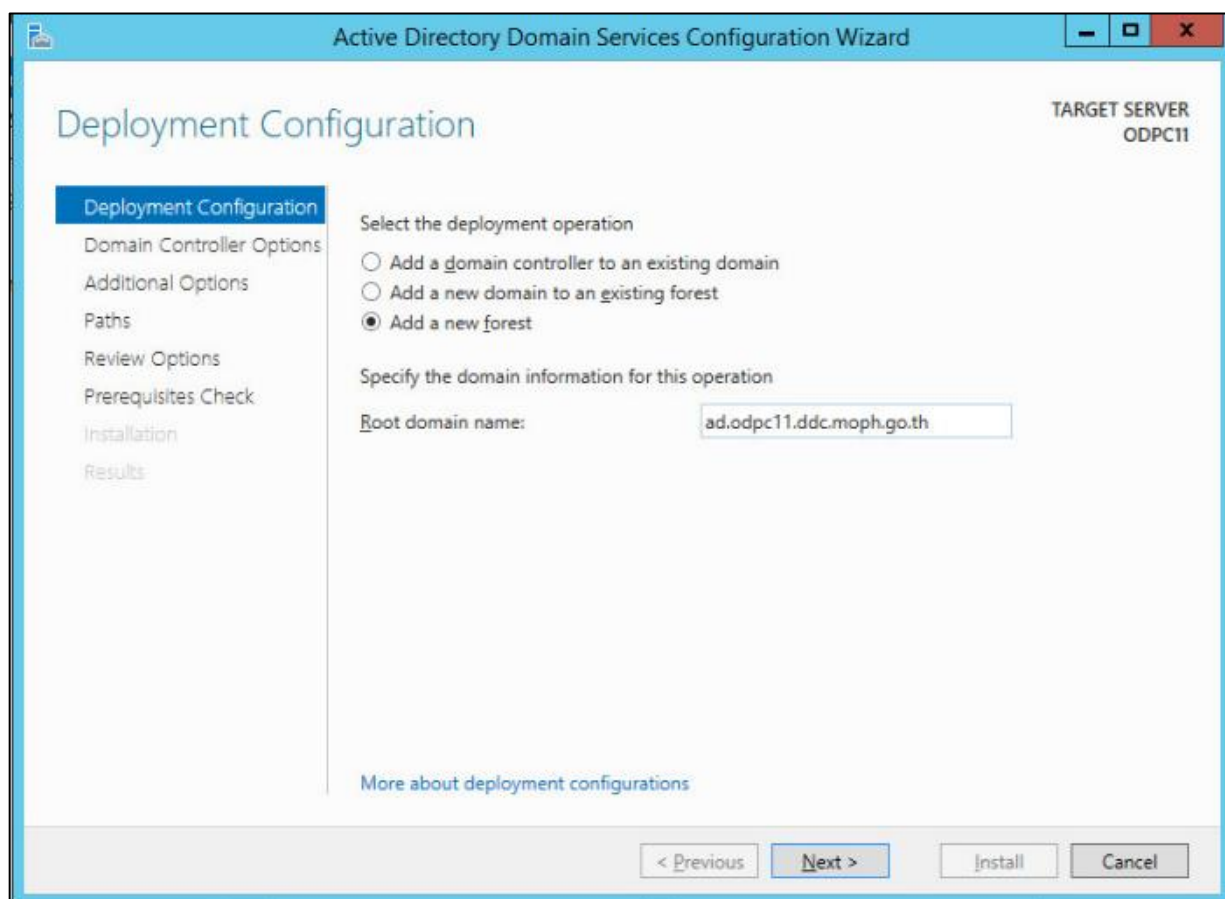
3.4 กด Next นำไปสู่หน้าต่าง Confirm installation เพื่อยืนยันการเพิ่ม Roles โดยมีรายละเอียด Roles ที่ได้เลือกไว้ หลังจากตรวจสอบเรียบร้อยแล้ว โดยให้เลือกในช่องรีสตาร์ทเซิร์ฟเวอร์อัตโนมัติเพื่อเป็นการกำหนดค่าเริ่มต้นของเซิร์ฟเวอร์ใหม่ จากนั้นกดปุ่ม Install



ภาพที่ 25 แสดงหน้าต่างสรุปการตั้งค่า Roles ที่ได้ทำการเลือกติดตั้ง

จากภาพแสดงหน้าต่าง Confirm Installation selections คือ แสดงสรุปรายการ Roles and Features ทั้งหมดที่ได้ทำการเลือกไว้ เพื่อเป็นการยืนยันการติดตั้ง จากนั้นให้ติ๊กถูกที่ช่อง Restart the destination server automatically if required เพื่อให้เครื่องเซิร์ฟเวอร์รีสตาร์ท จากมีความจำเป็นในขั้นตอนของการติดตั้ง Roles and Features จากนั้นกดปุ่ม Install

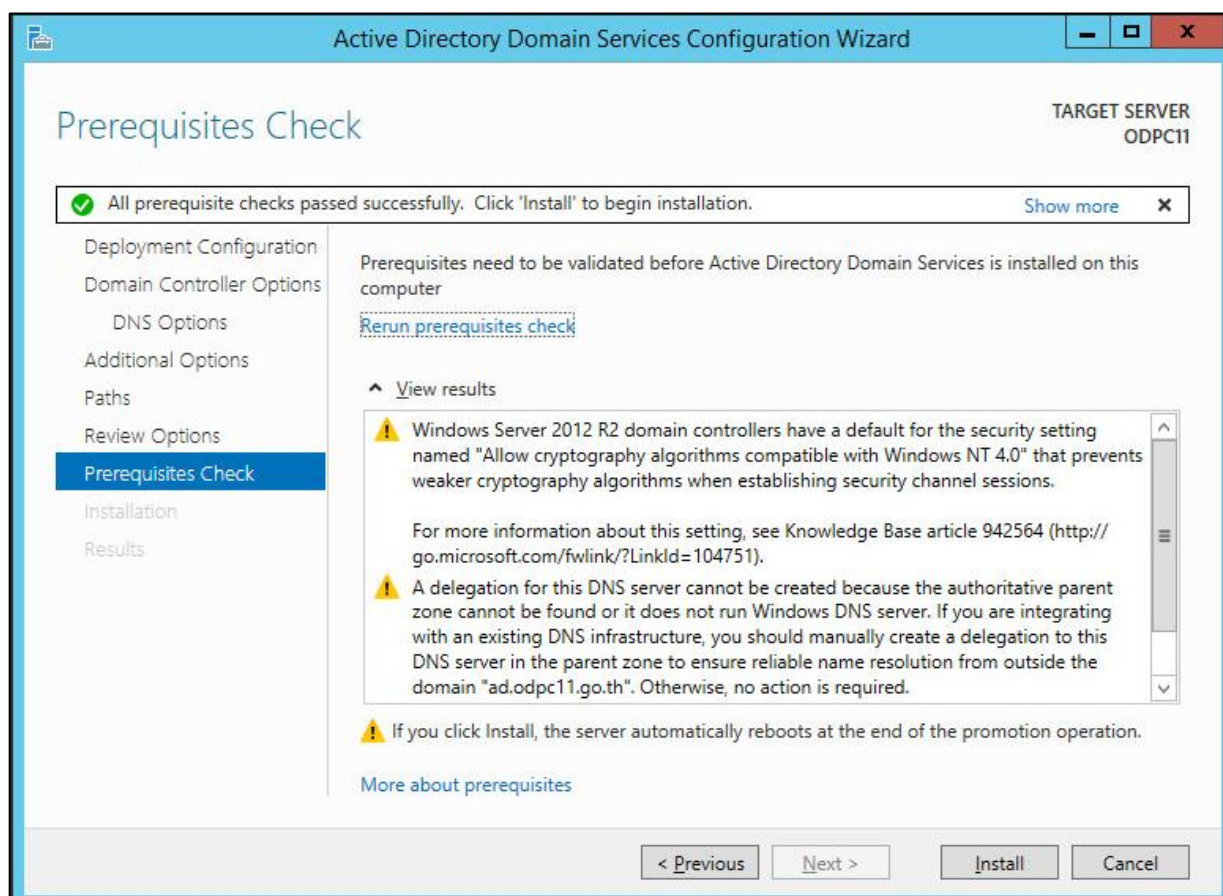
3.5 เมื่อติดตั้งเรียบร้อยแล้วเซิร์ฟเวอร์จะทำการรีสตาร์ทอัตโนมัติ เพื่อเป็นการกำหนดค่าเริ่มต้นใหม่ จากนั้นไปที่ server manager อีกครั้ง กด Promote this server to a domain controller เพื่อเป็นการกำหนด domain name ของเครื่องเซิร์ฟเวอร์



ภาพที่ 26 แสดงหน้าต่างการกำหนด domain name

จากภาพแสดงหน้าต่าง Deployment Configuration เป็นการกำหนดการทำงานของ Active directory domain services ให้เป็น Forest ซึ่งเป็นจุดสูงสุด โดยสามารถแก้ไขชื่อของ Root Domain name ได้ หากไม่ต้องการชื่อที่ระบบกำหนดมาให้ซึ่ง Root Domain name จะเป็น Domain ที่ใช้ในการอ้างอิงถึงเซิร์ฟเวอร์

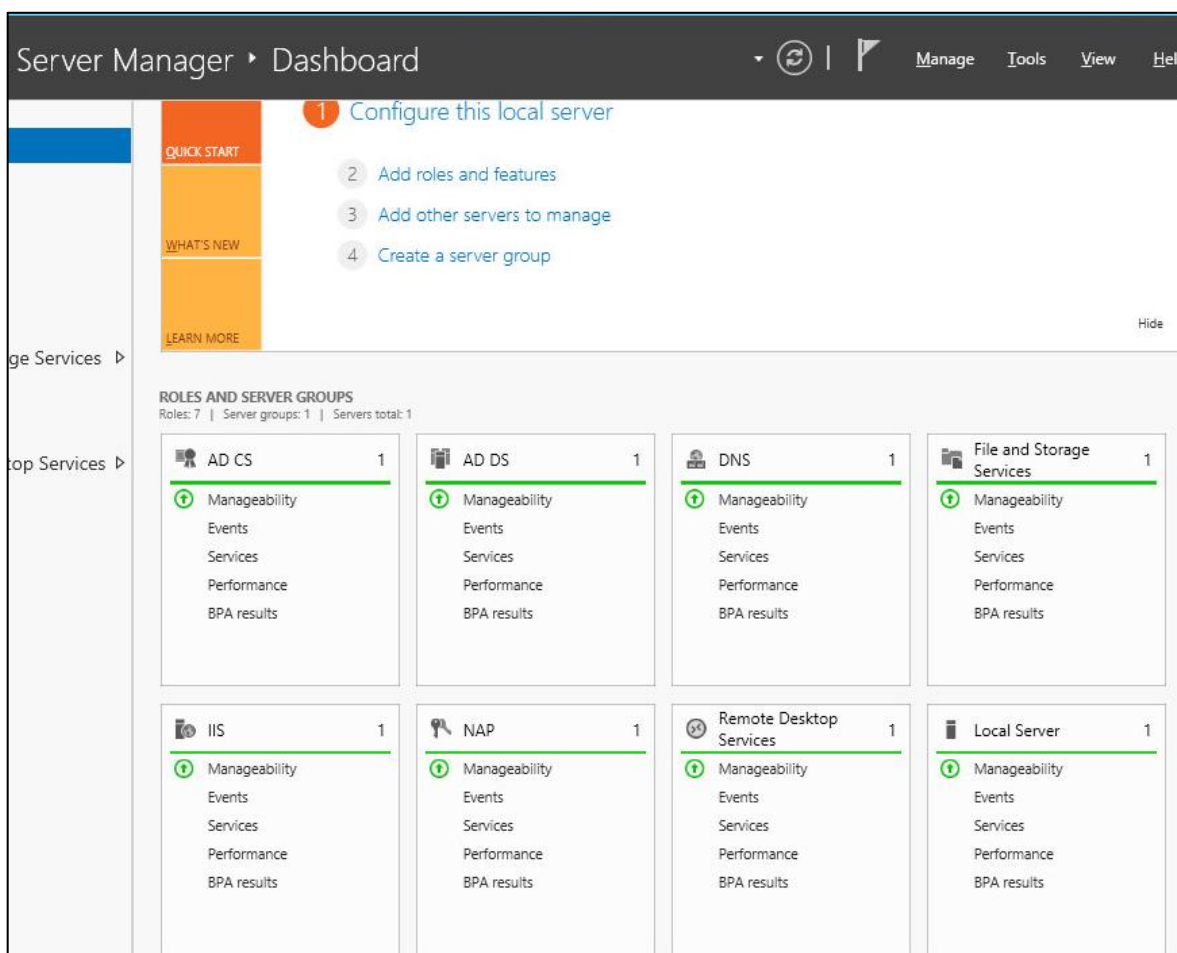
3.6 หลังจากนั้น จะเป็นหน้าต่างการตั้งค่าพื้นฐาน กำหนด Password และแสดงรายละเอียดต่างๆ โดยเลือกค่าทั้งหมดเป็นค่าเริ่มต้นจนไปถึงหน้าสรุปผลการตั้งค่า หลังจากตรวจเช็ครายละเอียดเรียบร้อยแล้ว กดปุ่ม Install ก็จะเสร็จในการตั้งค่า Active Directory Domain Services



ภาพที่ 27 แสดงหน้าต่างรายละเอียดการตั้งค่า domain controller และปุ่ม Install

จากภาพแสดงหน้าต่างการตรวจสอบข้อกำหนดเบื้องต้นที่ได้กำหนดไว้ เพื่อให้ตรวจสอบข้อกำหนดที่กำหนดไว้อีกครั้ง ก่อนทำการกดปุ่ม Install เพื่อ Deployment Configuration สู่เครื่องเซิร์ฟเวอร์

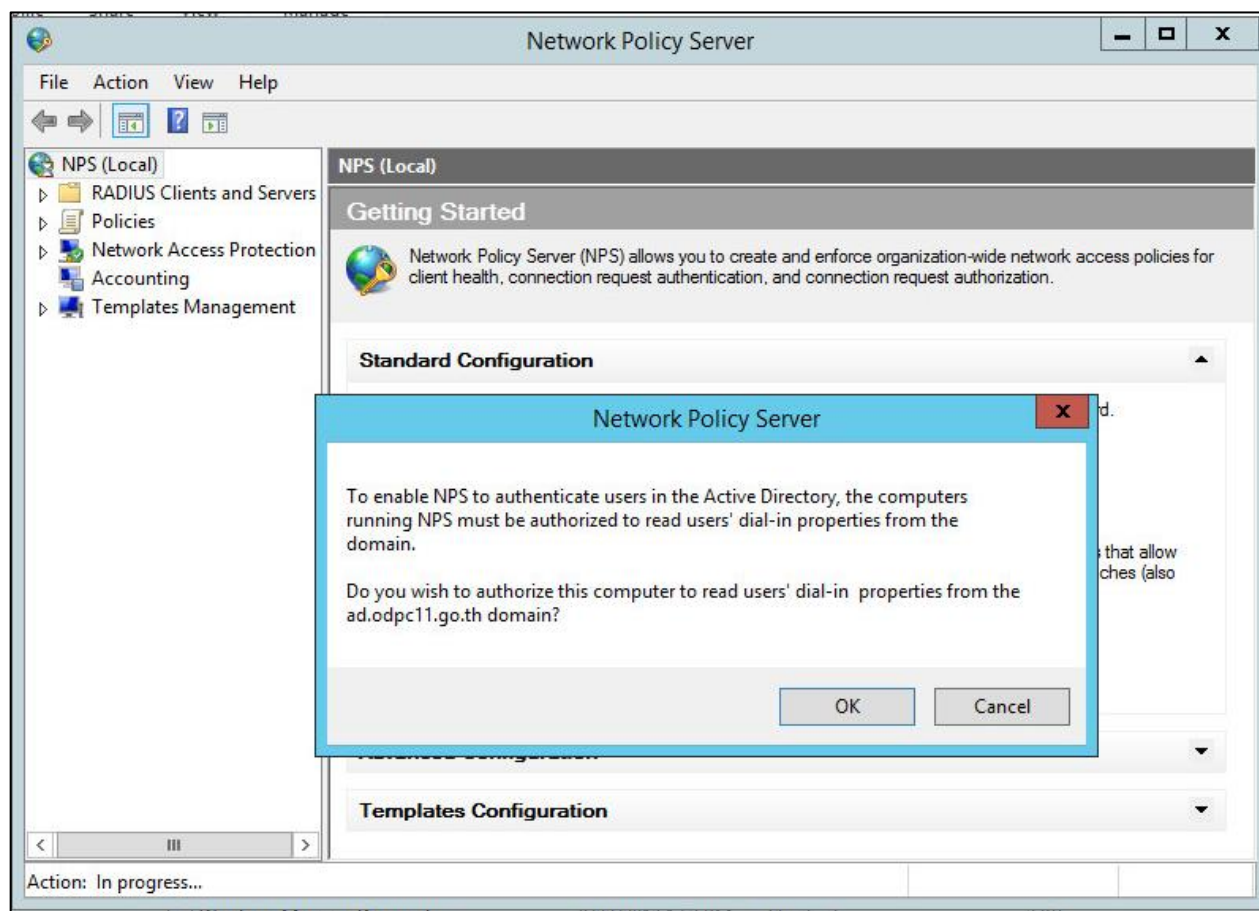
3.7 หลังจากติดตั้งการตั้งค่าเรียบร้อยแล้ว ในหน้า Server Manager จะแสดงผลสรุปการติดตั้ง Roles and Features ทั้งหมด



ภาพที่ 28 แสดงหน้าต่าง Server Manager ผลการติดตั้ง Roles ของ Server หลังจาก Install เสร็จแล้ว

จากภาพแสดงหน้าต่าง Server Manager Dashboard ที่แสดงให้เห็นถึง Roles and Features ที่ได้ทำการติดตั้ง สำหรับใช้งานบนเครื่องเซิร์ฟเวอร์ที่ได้ทำการติดตั้งเรียบร้อยแล้วพร้อมใช้งาน

3.8 ขั้นตอนถัดมาเป็นการเปิดใช้ Network Policy Server เพื่อเป็น Services ที่ใช้เชื่อมต่อกับไฟร์วอลล์ โดยพิมพ์ที่ช่องค้นหาว่า Network Policy Server แล้วกดเปิด



ภาพที่ 29 แสดงหน้าต่างการเปิดใช้งาน Network Policy Server

จากภาพแสดงหน้าต่างการเปิดใช้งาน Network Policy Server ที่ได้ทำการเปิดใช้งานใน Roles ก่อนหน้านี้ โดยทำการคลิกขวาที่ NPS(Local) เลือก Start NPS services ระบบจะแจ้งเตือนการเปิด NPS ขึ้นมา กด OK เป็นอันเสร็จสิ้น



#### 4. ผลของการกำหนด Password Policy [14] สำหรับผู้ใช้งาน

Password policy [14] หรือนโยบายรหัสผ่าน คือ กฎและข้อกำหนดที่กำหนดวิธีการในการกำหนดรหัสผ่านที่ปลอดภัยและการจัดการรหัสผ่านในระบบคอมพิวเตอร์ โดยสำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช ได้ทำตามมาตรฐานของ Windows Server คือ มีความจำเป็นจะต้องมีความ Complexity โดยความ Complexity นั้น มีรายละเอียดดังนี้

##### 4.1 จำนวนความยาวต้องมีอย่างน้อย 8 ตัวอักษร และประกอบด้วย 3 ใน 4 ข้อนี้

ภาษาอังกฤษ A ถึง Z ในแบบตัวพิมพ์ใหญ่, ภาษาอังกฤษ a ถึง z ในแบบตัวพิมพ์เล็ก

ตัวเลข 0 ถึง 9 และ ตัวอักษรสัญลักษณ์ เช่น (for example, !, \$, #, %)

##### 4.2 การกำหนด Password policy ให้กับ Active Directory User สามารถทำได้โดย

เปิด server manager > tools > group policy management editor > windows settings > account policy > password policy โดย Policy ที่กำหนด คือ

Password ต้องมีสูงสุด 360 วัน คือต้องเปลี่ยน password หลังจาก 360 วัน

Password มีอายุน้อยที่สุดคือ 0 วัน คือสามารถเปลี่ยน password ได้ตลอดเวลาไม่มีขั้นต่ำ

Password ต้องมีความยาว 8 ตัวอักษรขึ้นไป

Password จำเป็นต้องมีความ complexity

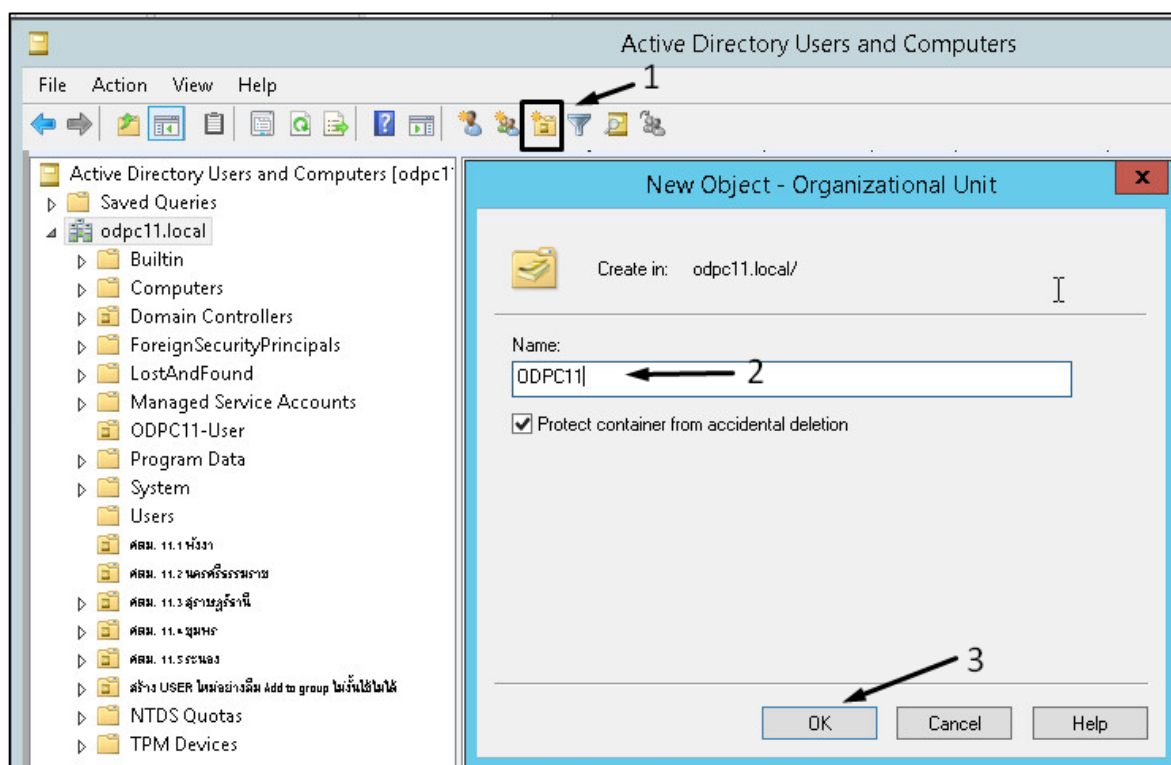
Policy	Policy Setting
Enforce password history	24 passwords remembered
Maximum password age	360 days
Minimum password age	0 days
Minimum password length	8 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

ภาพที่ 30 แสดงผลของการกำหนด Password Policy

## 5. การบันทึกข้อมูลบุคลากรเข้าสู่ Active Directory

การเพิ่มข้อมูลที่ได้จัดเตรียมไว้เข้าสู่ Active directory ดำเนินการดังนี้

5.1 เปิด Active directory บนเครื่อง Server ที่จัดเตรียมไว้ ดำเนินการสร้าง organization unit (OU) ตามข้อมูลที่ได้จัดเตรียมไว้ เพื่อความสะดวกในการบริหารจัดการ

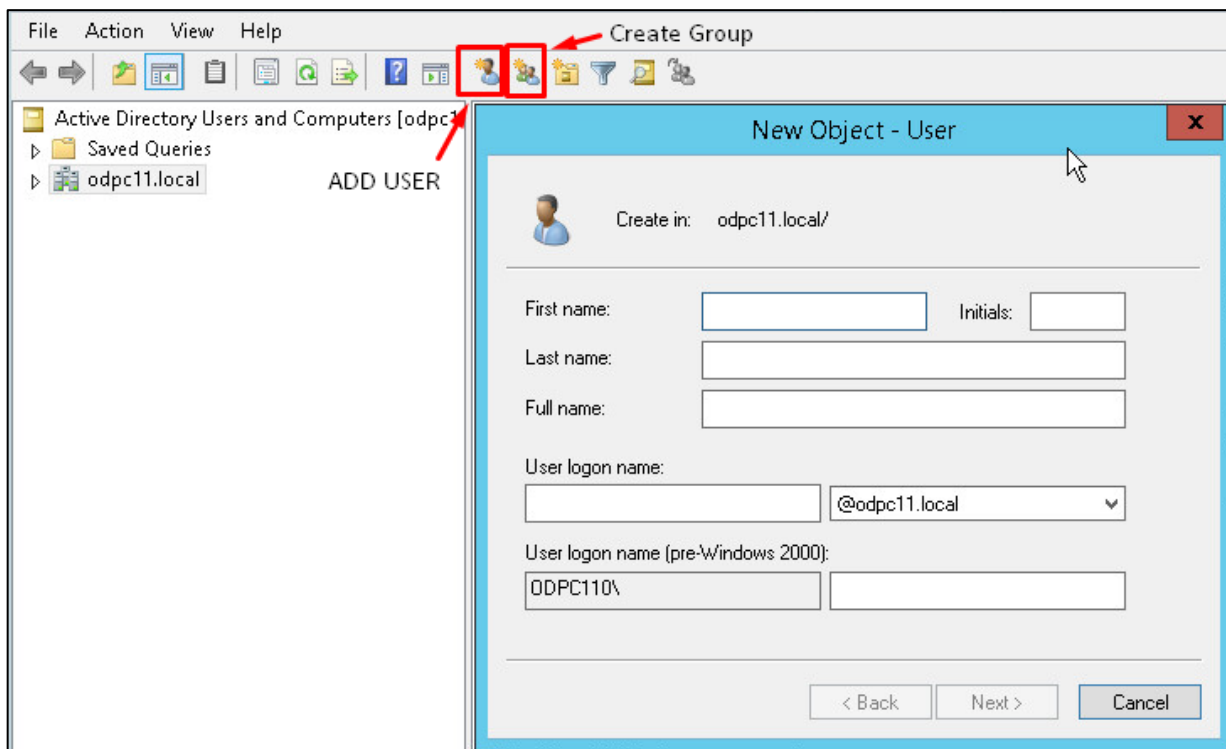


ภาพที่ 31 การสร้าง organization unit (OU) เพื่อกำหนดชื่อตามกลุ่มงาน

จากภาพแสดงขั้นตอนการสร้าง Organizational Unit เพื่อใช้ในการบริหารจัดการ Unit ซึ่งก็คือผู้ใช้งานทั้งหมดในหน่วยงานที่จะทำการสร้างต่อไป จากนั้นกดที่ Icon คนสองคน เพื่อทำการสร้าง Group สำหรับไว้เพิ่มข้อมูลของผู้ใช้งานเข้าไปในการบริหารจัดการผู้ใช้งานแบบกลุ่ม



5.2 เลือก organization unit (OU) ที่ต้องการเพิ่มข้อมูลบุคลากร แล้วกดปุ่ม Create a new user เพิ่มข้อมูล first name, last name, full name และ User log on



ภาพที่ 32 แสดงหน้าต่างรายละเอียดข้อมูล New User

จากภาพแสดงขั้นตอนการสร้างผู้ใช้งาน โดยเลือกที่ Icon รูปคน หรือคลิกขวา New User เพื่อทำการสร้างผู้ใช้งานใหม่แล้ว กรอกข้อมูลผู้ใช้งานที่ได้รับการลงทะเบียนที่ได้จัดเตรียมไว้

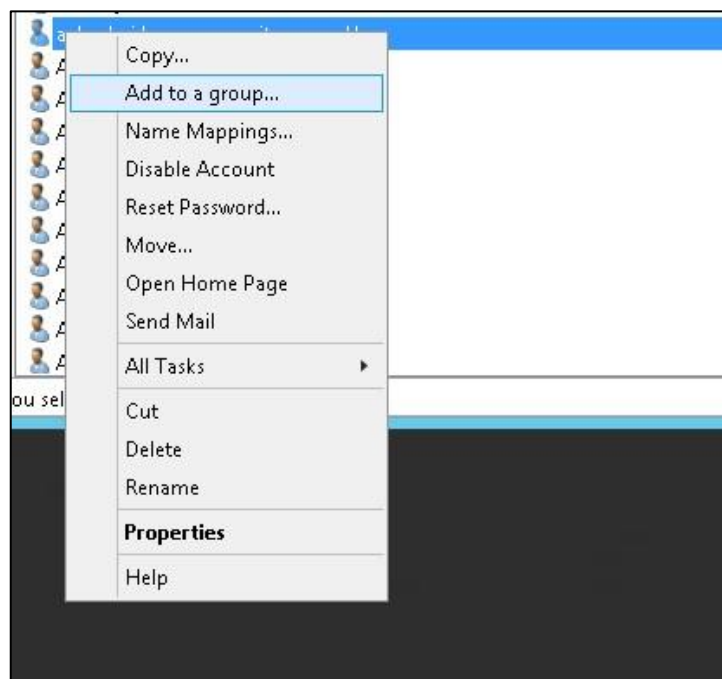
5.3 กด Next นำไปสู่หน้ากำหนด Password เช็ค ที่ User must change password at next logon แล้วกำหนด password เริ่มต้นที่จัดเตรียมไว้

ภาพที่ 33 แสดงหน้าต่างการกำหนด Password New User

5.4 กด Next จะแสดงหน้าต่างสรุปผลการตั้งค่าที่ได้กำหนดไว้ จากนั้นกด Finish

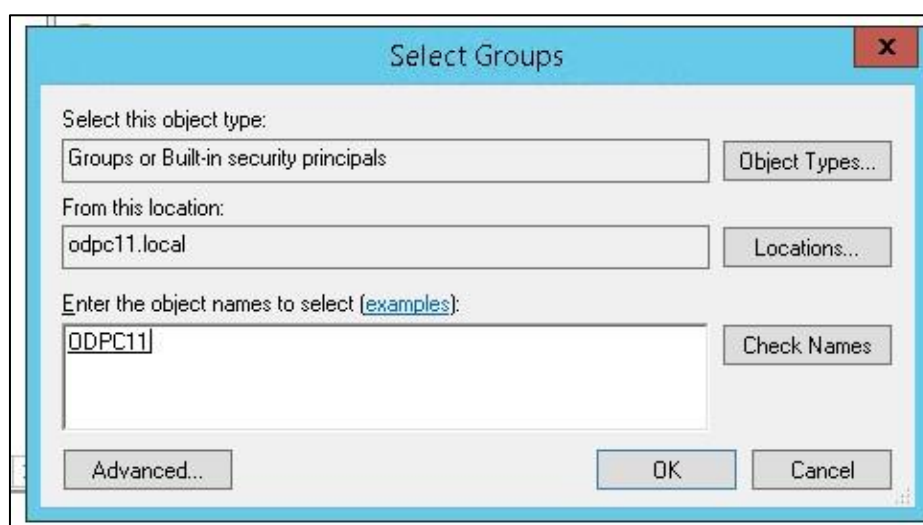
ภาพที่ 34 แสดงหน้าต่างสรุปผลการสร้าง User

5.5 หลังจากทำการสร้าง User เรียบร้อยแล้ว ให้ทำการคลิกขวาที่ Icon User ที่เพิ่งได้รับการสร้าง แล้วเลือกหัวข้อ Add to a Group เพื่อเป็นการกำหนดให้ User ใน Active Directory จัดเก็บไว้ใน Group ที่ได้สร้างไว้



ภาพที่ 35 แสดงตัวอย่างการคลิกขวาที่ New User แล้วเลือกเมนู Add to a group

5.6 หลังจากนั้นจะเจอหน้าต่าง Select Groups ให้ พิมพ์ชื่อ group ลงในช่อง แล้วกด Check Names ถ้าชื่อที่พิมพ์ถูกต้องจะมีเส้นขีดใต้ชื่อที่ได้พิมพ์ไว้แสดงให้เห็นว่าค้นหา groups เจอแล้ว จากนั้นกด OK จะเป็นการเสร็จสิ้นการเพิ่ม User จากนั้นทำการทำซ้ำจนครบจำนวน User ทั้งหมด



ภาพที่ 36 แสดงหน้าต่างการ Select Groups หลังจากที่ได้ทำการ Check Names

## 6. การเชื่อมต่อ Active Directory กับ Firewall

การเชื่อมต่อ Firewall กับ Active Directory ดำเนินการตามขั้นตอนดังนี้

6.1 เข้าสู่ Watch guard management > Authentication > Server กดเลือกที่ Active Directory เนื่องจากใช้ Server แบบ Active Directory

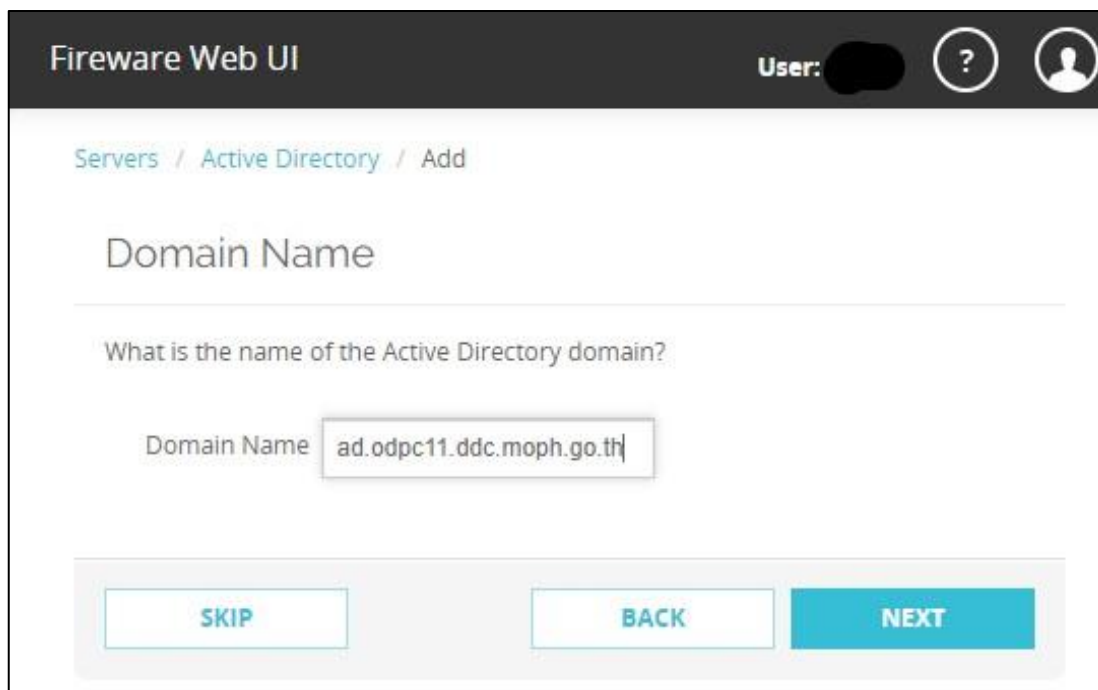
SERVER	STATUS
Firebox-DB	6 Users
RADIUS	Primary
	Backup
SecurID	Primary
	Backup
LDAP	Primary
	Backup
Active Directory	1 domains

**TEST CONNECTION FOR LDAP AND ACTIVE DIRECTORY**

ภาพที่ 37 แสดงจำนวนรูปแบบการเชื่อมต่อที่สามารถเชื่อมต่อได้บน Firewall

จากภาพแสดงขั้นตอนการเชื่อมต่อเครื่องเซิร์ฟเวอร์กับไฟร์วอลล์เพื่อให้ไฟร์วอลล์สามารถเข้าถึงและเรียกข้อมูลผู้ใช้งานที่จัดเก็บอยู่ในเซิร์ฟเวอร์มาตรวจสอบสิทธิ์การใช้งานได้ โดยทำการเพิ่มเซิร์ฟเวอร์ประเภท Active Directory

6.2 จากนั้น กด Add เพื่อทำงานเพิ่ม Domain name ที่จัดเตรียมไว้มาเชื่อมต่อกับไฟร์วอลล์โดยการนำ Domain Name ของ Server ที่สร้างไว้มากรอกในช่อง Domain Name ใน Firewall settings > Server > Active Directory > Add > Domain Name



The screenshot shows the 'Fireware Web UI' interface. At the top, there is a navigation breadcrumb: 'Servers / Active Directory / Add'. The main heading is 'Domain Name'. Below it, a question asks 'What is the name of the Active Directory domain?'. A text input field contains the domain name 'ad.odpc11.ddc.moph.go.th'. At the bottom, there are three buttons: 'SKIP', 'BACK', and 'NEXT'.

ภาพที่ 38 แสดงวิธีการกำหนด Domain Name

จากภาพแสดงขั้นตอนการกำหนด Domain Name ของเครื่อง Active Directory ที่ได้ทำการสร้างไว้ในขั้นตอนของการกำหนด Server Domain Name ไปกำหนดไว้ที่ไฟร์วอลล์โดยไปที่ใน Firewall settings > Server > Active Directory > Add > ระบุ Domain Name ในช่องที่กำหนด จากนั้นกด Next

## 7. กำหนด Session Authentication บน Firewall

การกำหนดระยะเวลาการเข้าใช้งานหลังจาก Authentication เข้าสู่เครือข่าย โดยเข้าไปตั้งค่า Policy ส่วนนี้ใน Watchguard firewall management > Authentication > Settings จากนั้นกำหนดค่าในหัวข้อ Firewall Authentication ดังนี้

Session timeout คือ ระยะเวลาในการ Login เข้าใช้งาน แต่ครั้งคือ 8 ชั่วโมง

Idle timeout คือ ระยะเวลาการไม่ใช้งาน 2 ชั่วโมง

limit concurrent user คือ จำนวนที่ 1 user จำนวนอุปกรณ์สูงสุดคือ 3 อุปกรณ์

Fireware Web UI

Settings

### Firewall Authentication

These timeout settings apply to users who authenticate to external third-party authentication servers that do not already have a timeout configured.  
**Note:** A value of 0 means "never time out".

Session Timeout: 8 Hours

Idle Timeout: 2 Hours

Allow unlimited concurrent firewall authentication logins from the same account

Limit concurrent user sessions to 3

When the limit is reached: Allow subsequent login attempts and log off the first session

Default authentication server on the authentication page: odpc11.local

Automatically redirect users to the authentication page

Redirect traffic sent to the IP address of the Firebox device to this host name: ddc11.watchguard.in.th

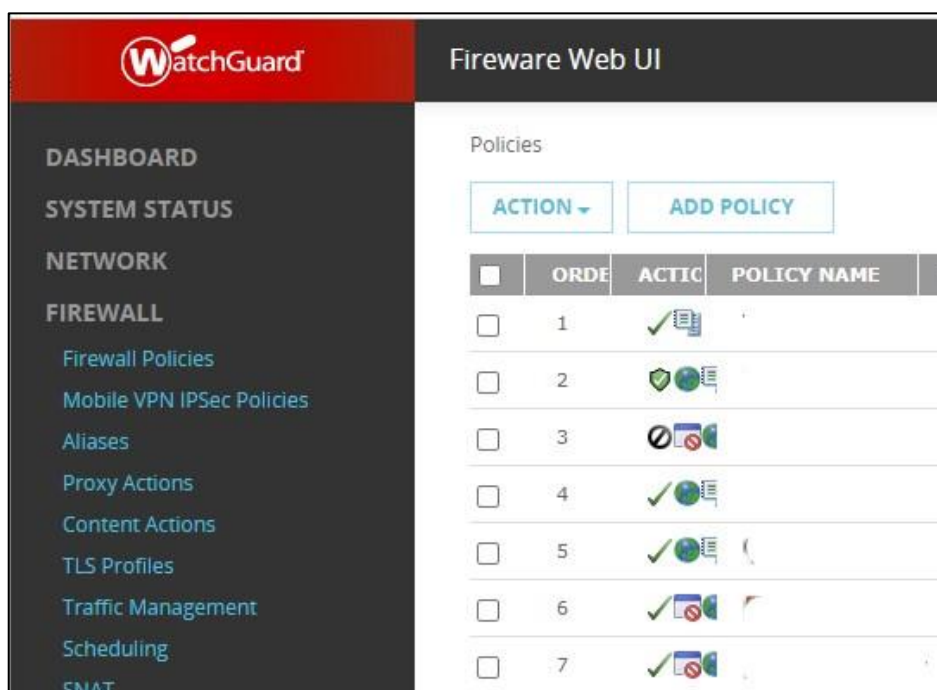
The host name must match the Common Name (CN) from the web server certificate. Make sure that this host name is specified in the DNS settings for your organization, and that the value of the host name is the IP address of the Firebox device.

ภาพที่ 39 แสดงการกำหนด session Authentication โดยกำหนดค่าการใช้งาน

จากภาพแสดงขั้นตอนการกำหนดรายละเอียด การใช้งานของผู้ใช้งานที่เข้าใช้งานในเครือข่าย รวมถึงการกำหนดให้ระบบ redirect ผู้ใช้งานที่ยังไม่ยืนยันตัวตนไปสู่หน้าต่างการยืนยันตัวตน

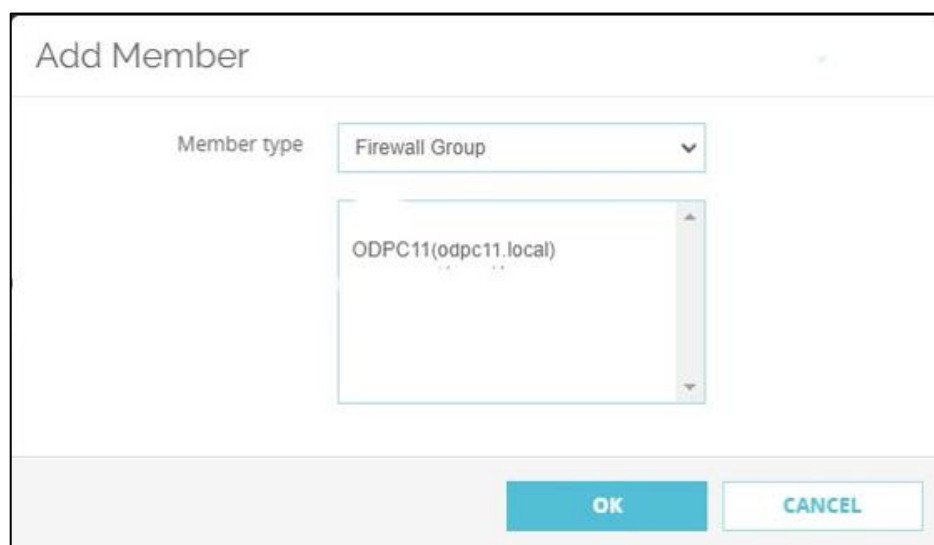
## 8. กำหนด Firewall Policy สำหรับการเปิดการใช้งาน Authentication

8.1 เข้าสู่ Watchguard firewall management > Firewall Policies > ADD Policy



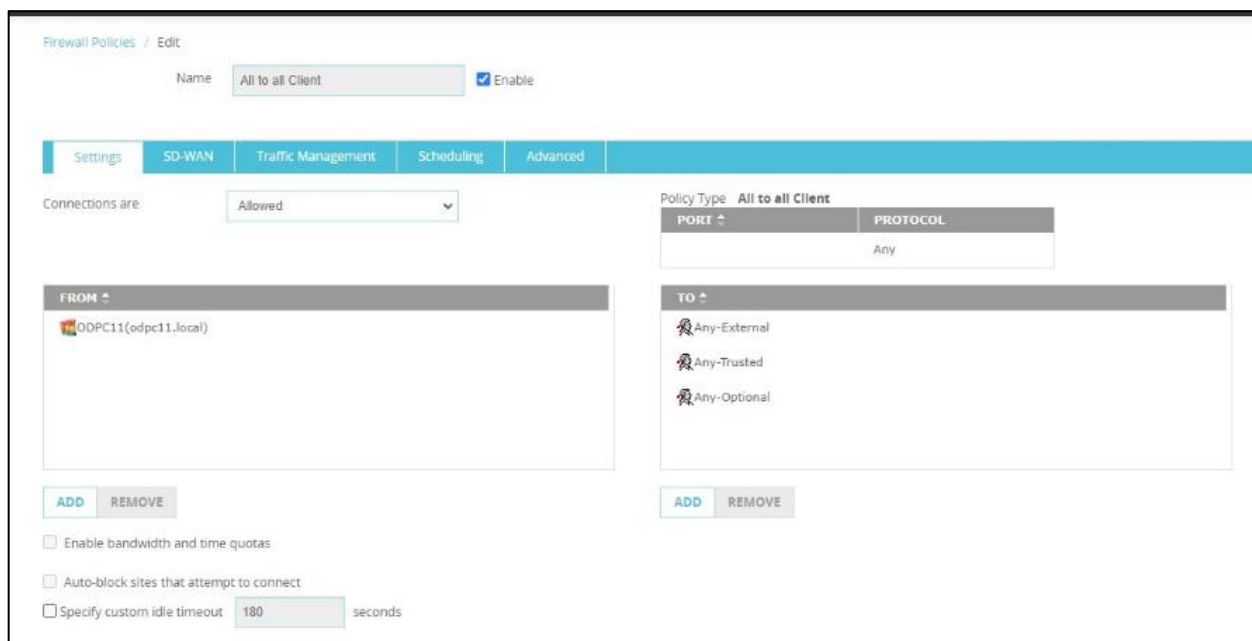
ภาพที่ 40 แสดงหน้าต่าง Firewall Policies > ADD Policy

8.2 หลังจากเปิดหน้าต่าง ADD Policy ฝั่งของ From ให้เลือก ADD จากนั้น เลือก Member Type เป็น Firewall Group แล้วเลือก ODPC11 Group ซึ่งเป็น group ที่ได้รับการทำการ Add User ไว้ใน Active Directory Domain Services



ภาพที่ 41 แสดงหน้าต่างการ ADD Member type เป็น group ที่ได้กำหนดไว้ใน ADDS

8.3 ในฝั่งของ To เป็นการกำหนดเครือข่ายใด ๆ ที่ต้องการให้ User มีสิทธิ์ในการเข้าถึง จากนั้นกด Save Policy



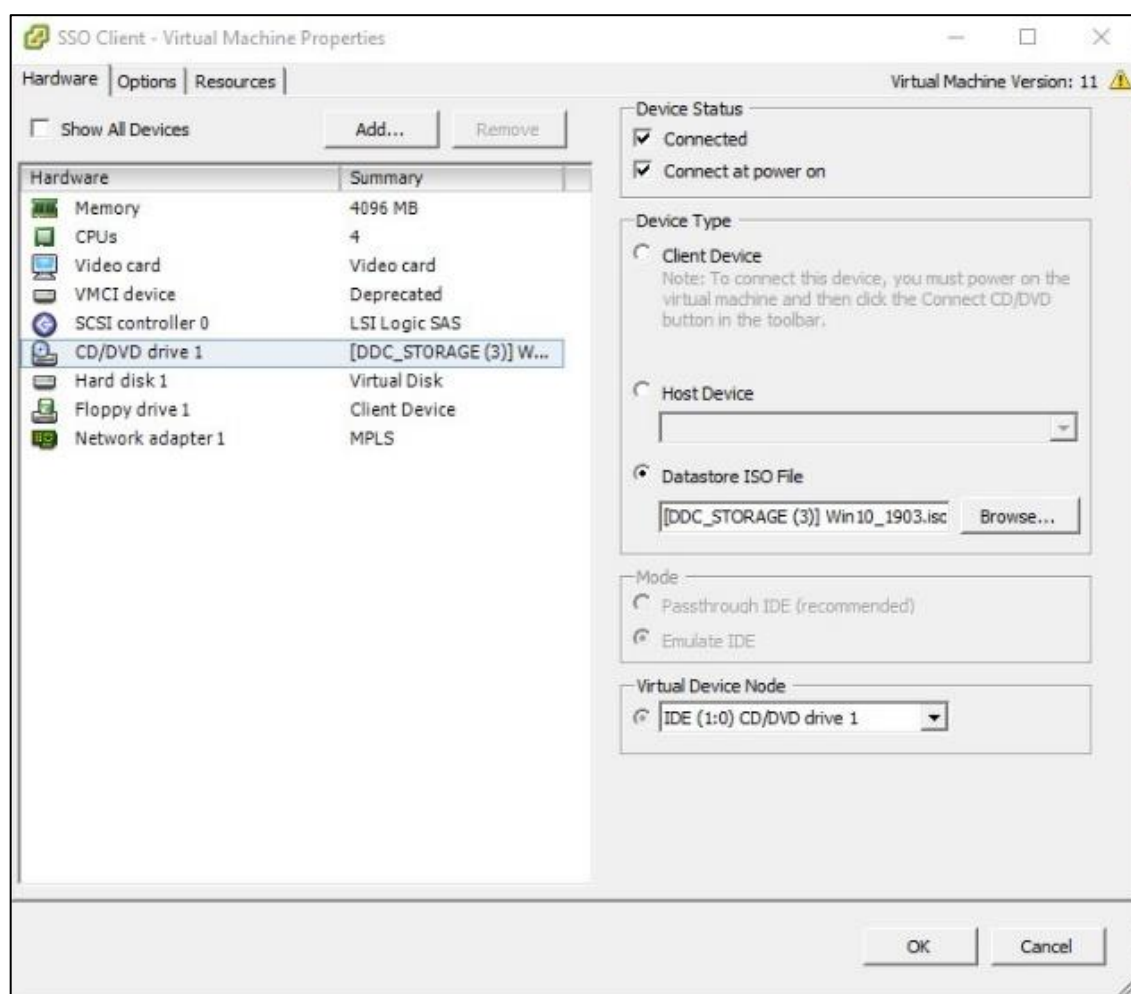
ภาพที่ 42 แสดงผลการ configure firewall policy ที่ได้กำหนดให้ User จาก group ODPC11 สามารถเข้าถึงเครือข่าย

จากภาพแสดงขั้นตอนการกำหนด Policy ในฝั่งของ FROM เพื่อให้ผู้ที่ใช้งานเครือข่ายของหน่วยงาน จำเป็นต้องเป็นผู้ใช้งานที่ได้รับการยืนยันตัวตนจาก ADDS ใน Group ODPC11 เท่านั้น ถึงจะสามารถเข้าถึงเครือข่ายที่กำหนดไว้ในฝั่งของ TO ได้ คือ Any-External, Any-Trusted และ Any-Optional



## 9. ติดตั้ง Windows 10 บน Log Client และดำเนินการกำหนดการตั้งค่า

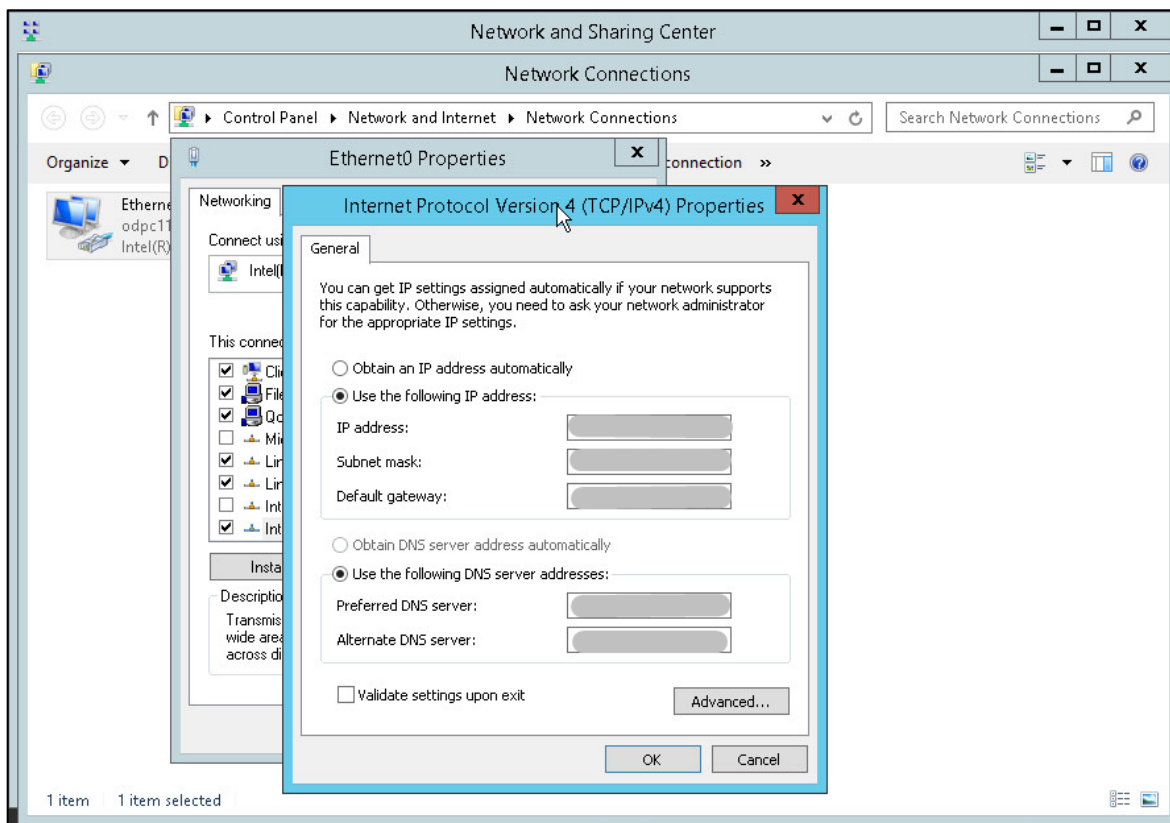
9.1 หลังจากที่ได้มีการสร้างเซิร์ฟเวอร์และคอมพิวเตอร์เสมือนไว้ในขั้นตอนก่อนหน้า จากนั้นทำการเข้าสู่โปรแกรมบริหารจัดการคอมพิวเตอร์เสมือนจริง VMware vSphere Client เลือกเครื่องคอมพิวเตอร์ Log Files ที่สร้างไว้ คลิกขวา Edit Settings จากนั้นเลือก CD/DVD Drive 1 เพื่อทำการเลือก Windows 10 Pro iso จากนั้นทำการติดตั้ง



ภาพที่ 43 แสดงหน้าต่างการเลือก Windows 10 ISO Files สำหรับติดตั้ง

จากภาพแสดงหน้าต่าง Virtual Hardware ที่ได้ทำการสร้างขึ้นมา เป็นเครื่องคอมพิวเตอร์เสมือน โดยหลังจากทำการสร้างเครื่องคอมพิวเตอร์เสร็จเรียบร้อยแล้ว จำเป็นต้องติดตั้งระบบปฏิบัติการโดยสามารถดำเนินการได้ โดยไปที่ CD/DVD Drive เสมือนที่ได้สร้างไว้ กดเลือก ISO Files ของระบบปฏิบัติการ และติ๊ก Connect at power on เพื่อให้ระบบจำลองการทำงานของ CD/DVD Drive จากนั้นดำเนินการเปิดเครื่องคอมพิวเตอร์เสมือน และติดตั้งระบบปฏิบัติการเหมือนคอมพิวเตอร์ทั่วไปได้เลย

9.2 หลังจากติดตั้ง Windows 10 แล้วทำการกำหนด IP Address เป็น Static เพื่อใช้ในการเชื่อมต่อ การเก็บ Log Files

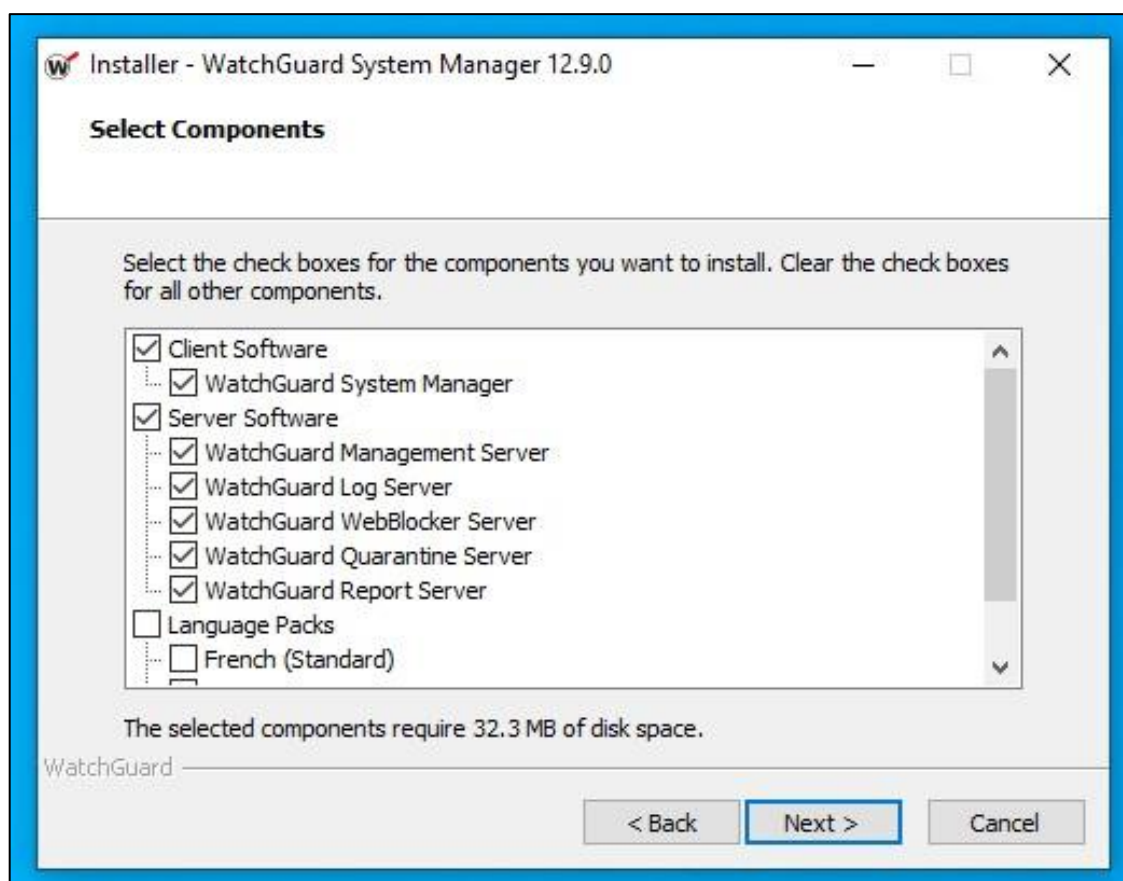


ภาพที่ 44 แสดงหน้าต่างการกำหนด IP Address

จากภาพแสดงหน้าต่างการกำหนด IP Address ของเครื่องคอมพิวเตอร์เสมือน หลังจากที่ได้มีการติดตั้งระบบปฏิบัติการเรียบร้อยแล้ว ขั้นตอนถัดไปคือการกำหนด IP Address คอมพิวเตอร์เสมือน เพื่อให้เครื่องคอมพิวเตอร์เสมือนที่ได้ทำการสร้างขึ้นมา อยู่ในเครือข่ายเดียวกันกับระบบเครือข่ายที่ต้องการใช้งาน

## 10. ติดตั้ง โปรแกรม Watchguard System manager

การติดตั้ง โปรแกรม Watchguard System manager โดยเลือก server software ทั้งหมด จากนั้น Next และติดตั้ง



ภาพที่ 45 แสดงหน้าต่างการติดตั้ง Watchguard System manager

จากภาพแสดงขั้นตอนการติดตั้งโปรแกรม Watchguard System manager บนเครื่องคอมพิวเตอร์เสมือน หลังจากที่ได้ติดตั้งระบบปฏิบัติการและกำหนด IP Address เพื่อเชื่อมต่อเข้าสู่เครือข่ายเรียบร้อยแล้ว หลังจากเปิดตัวติดตั้ง Watchguard System manager จะปรากฏหน้าต่างการเลือก Option สำหรับติดตั้ง Features การทำงานของ Watchguard System manager โดยทำการเลือก หัวข้อทั้งหมดในหมวดหมู่ของ Server Software

## 11. ทำการเชื่อมต่อ Watchguard System manager กับ Firewall

11.1 เปิดโปรแกรม WatchGuard System Manager 12.9.4 เพื่อทำการตั้งค่าการเชื่อมต่อโปรแกรม จากนั้นเลือกที่ Files > Connect to Device..

The screenshot shows a dialog box titled "Connect to Firebox" with the WatchGuard logo. The text inside says "Please enter the user login information of your Firebox." Below this are several input fields: "IP Address or Name" with the value "172.0.0.1", "User Name" with "loguser", "Passphrase" with a masked field of dots, "Authentication Server" with "Firebox-DB", "Domain" which is empty, and "Timeout" set to "25 seconds". At the bottom are three buttons: "Login", "Cancel", and "Help".

ภาพที่ 46 แสดงหน้าต่างการกำหนดการเชื่อมต่อ WatchGuard System Manager

จากภาพแสดงขั้นตอนการเชื่อมต่อโปรแกรม Watchguard system manager เข้ากับ Firewall Watchguard M4600 โดยการกรอกข้อมูลต่างๆ ดังนี้

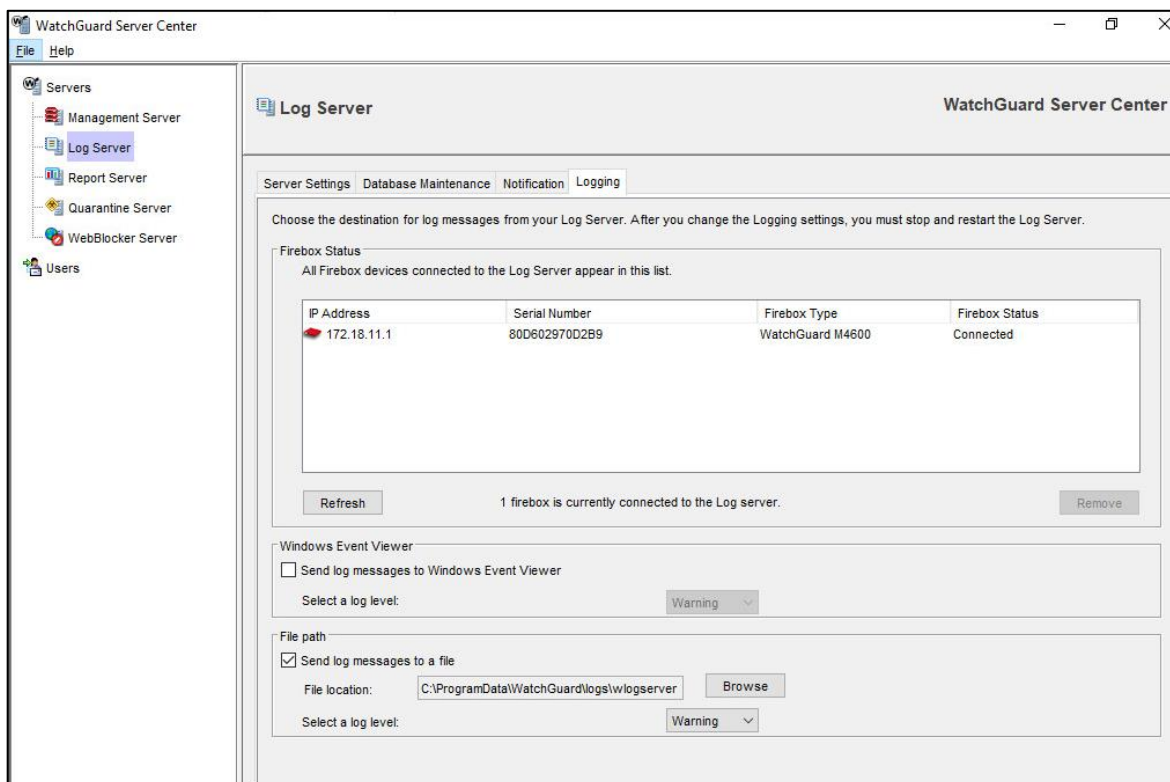
IP Address : หมายเลข IP Address ของ Watchguard Firebox

User Name : คือ Username ที่กำหนดสิทธิ์โดย Firebox ให้มีสิทธิ์อ่านข้อมูล

Passphrase : คือ Passphrase เฉพาะที่เป็นค่าที่ได้มาพร้อมกับตัว Firebox

จากนั้นทำการกด Login โปรแกรมจะทำการเชื่อมกับ Firewall Watchguard M4600 ในเครือข่าย

11.2 เข้าสู่ Watchguard System manager ไปยังหัวข้อ Log Server ที่เมนูบาร์ Logging จะพบตัว Watchguard ที่ใช้งานอยู่ หากไม่พบให้ทำการกดปุ่ม Refresh



ภาพที่ 47 แสดงรายการ Device ของ Firebox ที่ได้ทำการเชื่อมต่อไว้

จากภาพแสดงหน้าต่างการเชื่อมต่อระหว่าง WatchGuard System Manager และ Firewall Watchguard M4600 โดยจะมีรายละเอียด คือ

IP Address: หมายเลข IP Address ของ Watchguard Firebox

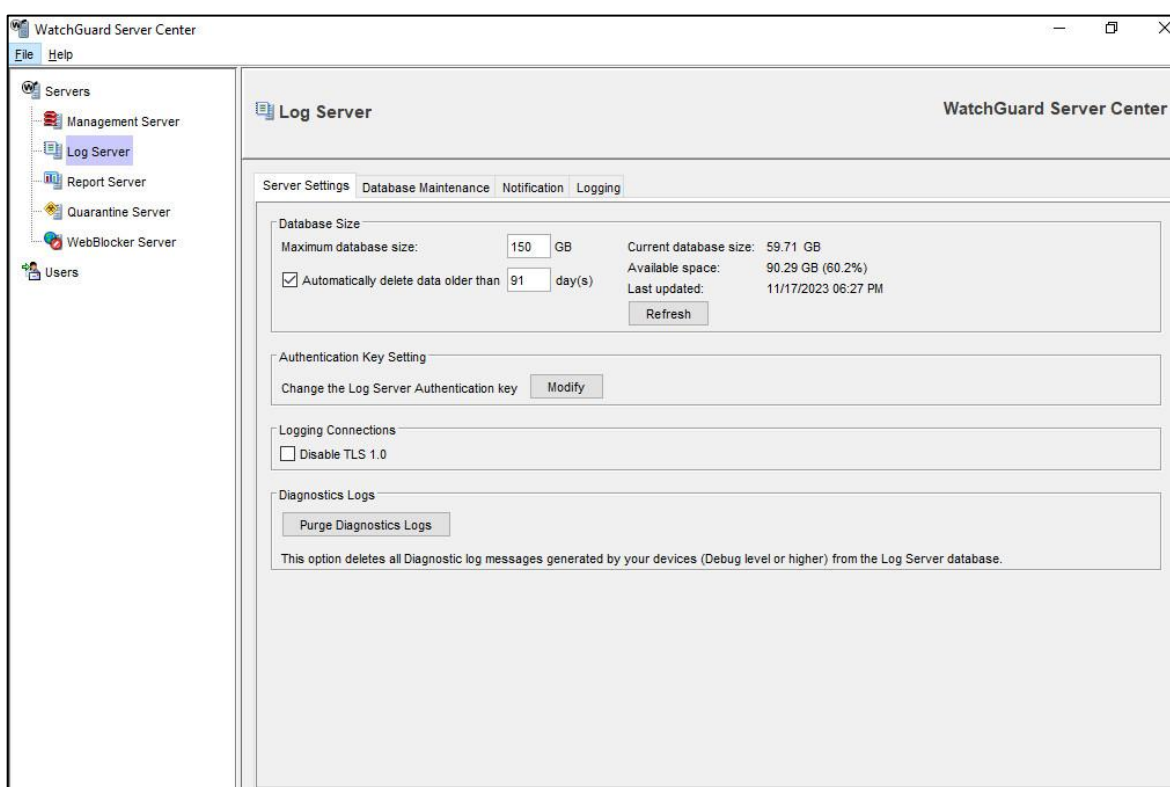
Serial Number: หมายเลข Serial Number ของ Watchguard Firebox

Firebox Type: รุ่นของ Watchguard ที่ใช้งานอยู่

Firebox Status: สถานการณ์เชื่อมต่อระหว่าง WatchGuard System Manager และ Firewall

## 12. ตั้งค่าขนาดพื้นที่จัดเก็บ Log Files เพื่อกำหนดระยะเวลาในการจัดเก็บ Log Files

12.1 ทำการกำหนดรายละเอียดในการจัดเก็บ Log ในเมนู log server > server settings โดยกำหนดขนาดของพื้นที่ที่ใช้ในการจัดเก็บ



ภาพที่ 48 แสดงหน้าต่างการกำหนดการตั้งค่าการจัดเก็บ Log Files

จากภาพแสดงหน้าต่างการตั้งค่ารายละเอียดของการจัดเก็บข้อมูลจราจรคอมพิวเตอร์โดยโปรแกรม WatchGuard System Manager โดยสามารถกำหนดรายละเอียดได้ดังนี้

ขนาดของพื้นที่ที่จะใช้ในการจัดเก็บ Log Files

ระยะเวลาในการจัดเก็บ Log Files

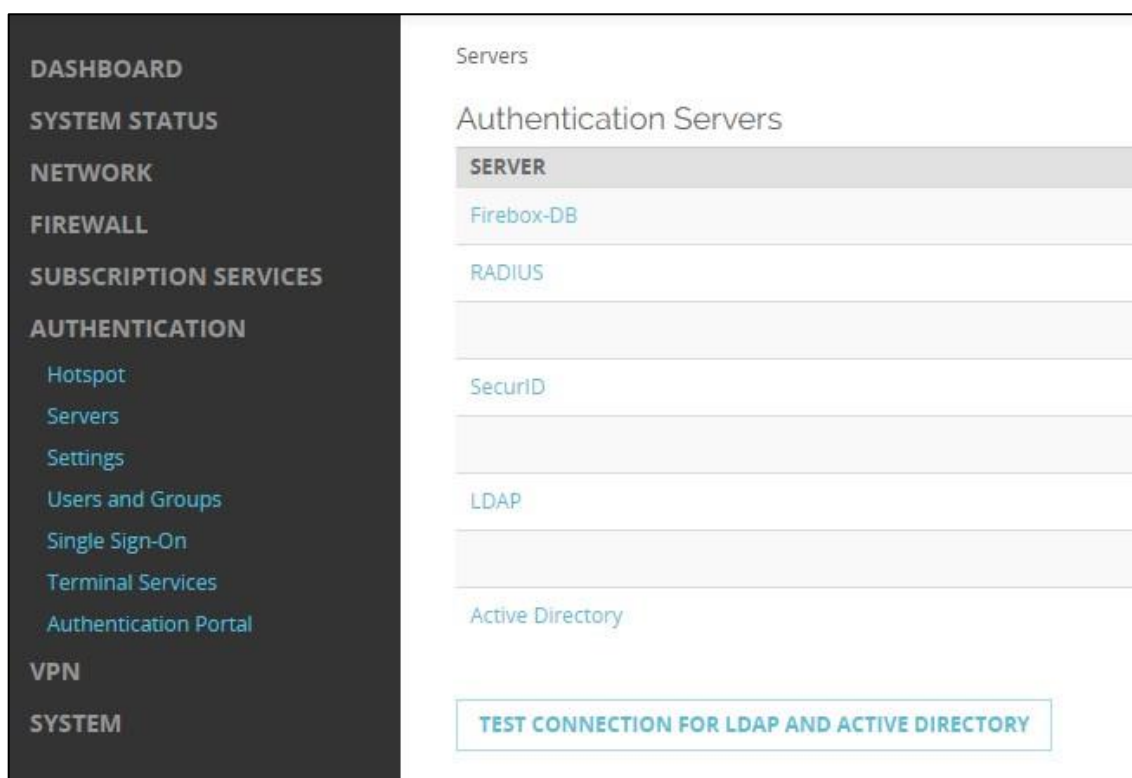
ระยะเวลาในการจัดเก็บ Report สำหรับเข้าดูข้อมูล Log Files ผ่านหน้าเว็บไซต์

### 4.3 ผลการตรวจสอบการทำงาน (Check)

4.2.1 ตรวจสอบความถูกต้องของการทำงานของระบบ โดยทำการเปรียบเทียบกับขั้นตอนการวางแผนที่กำหนดไว้ ว่าผลลัพธ์ขั้นตอนการดำเนินการเป็นไปตามแผนที่วางไว้หรือไม่

#### 1. ทดสอบการเชื่อมต่อระหว่าง Firewall และ Active Directory

1.1 การเชื่อมต่อ Firewall กับ Active Directory Domain Services เพื่อเป็นการทำให้ Firewall สามารถเข้าถึงฐานข้อมูล Active Directory ซึ่งใช้สำหรับการตรวจสอบสิทธิ์การใช้งานเครือข่าย โดยสามารถตรวจสอบผลการเชื่อมต่อได้โดยการ Test Connection บน Firewall Management >Authentication > Servers ในเมนู TEST CONNECTION FOR LDAP AND ACTIVE DIRECTORY



ภาพที่ 49 แสดงหน้าต่าง Firewall Management เมนู TEST CONNECTION FOR LDAP AND ACTIVE DIRECTORY

1.2 เมื่อกดที่เมนู เมนู TEST CONNECTION FOR LDAP AND ACTIVE DIRECTORY เลือก Server สำหรับการทดสอบเป็น Domain Names ของ Server ที่ได้ทำการสร้างไว้ จากนั้นใช้ Username และ Password ที่ได้ทำการ ADD ไว้ใน Active Directory แล้วกด TEST Connection จะได้ผลลัพธ์ดังต่อไปนี้

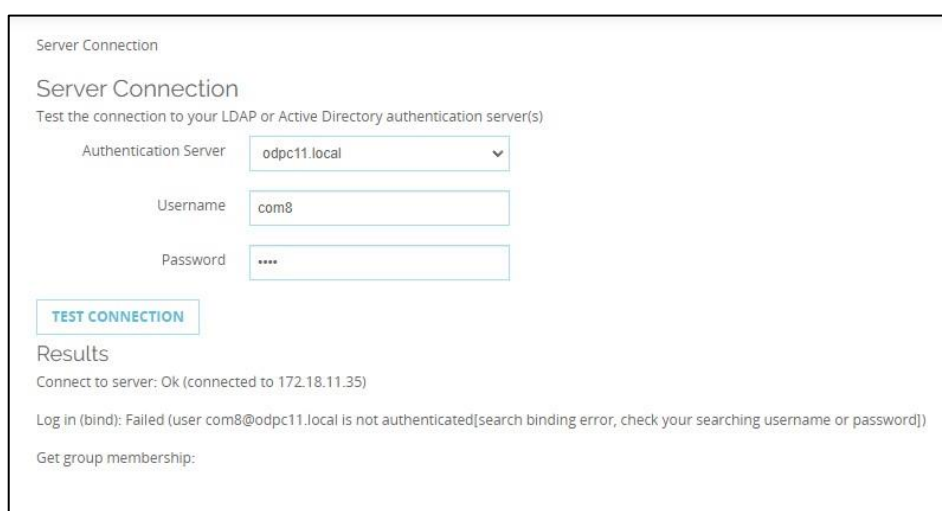
1.2.1 การทดสอบด้วย Username และ Password ที่ถูกต้องผลคือ connection server : Ok Log in : Ok



The screenshot shows a web interface titled "Server Connection". It prompts the user to "Test the connection to your LDAP or Active Directory authentication server(s)". The "Authentication Server" is set to "odpc11.local". The "Username" is "com1" and the "Password" is masked with "\*\*\*\*". A "TEST CONNECTION" button is visible. Below the button, the "Results" section shows: "Connect to server: Ok (connected to 172.18.11.35)", "Log in (bind): Ok (user com1@odpc11.local is authenticated)", and "Get group membership: Users, Domain Users, ODPC11".

ภาพที่ 50 แสดงหน้าต่างการทดสอบด้วย Username และ Password ที่ถูกต้อง

1.2.2 ทำการทดสอบด้วย Username และ Password ที่ไม่ได้ลงทะเบียนไว้ผลคือ connection server : Ok Log in : bind : Failed user is not authenticated



The screenshot shows the same "Server Connection" interface. The "Authentication Server" is "odpc11.local". The "Username" is "com8" and the "Password" is masked with "\*\*\*\*". The "TEST CONNECTION" button is present. The "Results" section shows: "Connect to server: Ok (connected to 172.18.11.35)", "Log in (bind): Failed (user com8@odpc11.local is not authenticated[search binding error, check your searching username or password])", and "Get group membership:".

ภาพที่ 51 แสดงหน้าต่างการทดสอบด้วย Username และ Password ที่ถูกต้อง



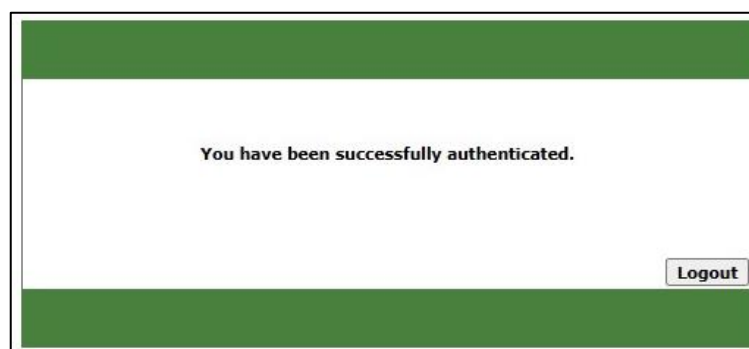
### 1.3 สรุปผลการตรวจสอบการเชื่อมต่อระหว่าง Firewall และ Active Directory

สรุปผลได้ว่าการดำเนินงานของการเชื่อมต่อระหว่าง Firewall และ Active Directory สามารถใช้งานได้ เป็นไปตามที่วางแผนไว้

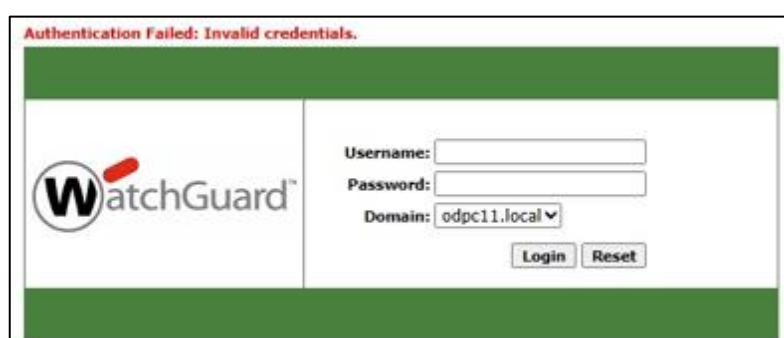
## 2. ทดสอบการใช้งานระบบยืนยันตัวตนบุคคล

2.1 การทดสอบการใช้งานระบบ ซึ่งจะใช้วิธีการทดสอบระบบแบบ Black Box Testing โดยการนำเอาเหตุการณ์ที่คาดว่าจะเกิดขึ้นมากำหนดให้อยู่ในรูปแบบเหตุการณ์เพื่อระบุผลของการทำงานได้ดังนี้ ตารางที่ 5 แสดงผลการทดสอบระบบ

เหตุการณ์ (Test Case)	ขั้นตอน (Test Step)	ผลลัพธ์ (Expect Result)
(ตัวอย่างที่ถูกต้อง) ผู้ใช้งานเข้าสู่ระบบด้วย Username และ Password ที่ ถูกต้อง	1.เชื่อมต่อเครือข่าย 2.เปิดหน้า Login 3.ใส่ Username (abc1) 4.ใส่ Password (1234) 5.กดปุ่ม Login	1.ผู้ใช้งานสามารถเข้าสู่ระบบได้ 3.ระบบแสดงหน้า you have been successfully authentication
(ตัวอย่างที่ไม่ถูกต้อง) ผู้ใช้งานไม่ สามารถเข้าสู่ระบบได้หากใส่ Username หรือ Password ผิด	1.เชื่อมต่อเครือข่าย 2.เปิดหน้า Login 3.ใส่ Username (abc1) 4.ใส่ Password (4568) 5.กดปุ่ม Login	1.ผู้ใช้งานไม่สามารถเข้าสู่ระบบ ได้ 2.ระบบแสดงแจ้งเตือน Authentication Failed: Invalid credentials.
(ตัวอย่างที่ไม่ถูกต้อง) ผู้ใช้งานไม่สามารถเข้าสู่ระบบได้ หากไม่ใส่ Username หรือ Password	1.เชื่อมต่อเครือข่าย 2.เปิดหน้า Login 3.กดปุ่ม Login	1.ระบบแสดง Pop up แจ้งเตือน Invalid credentials!



ภาพที่ 52 หน้าต่างแสดงผลการเข้าสู่ระบบสำเร็จ



ภาพที่ 53 แสดงหน้าต่าการแจ้งเตือนเข้าใช้งานไม่สำเร็จ

2.2 ผลของการตรวจสอบการใช้งานระบบ Authentication ระบบได้ทำงานได้ตามที่วางแผนไว้ ซึ่งได้ผลลัพธ์ ดังนี้

ตารางที่ 6 แสดงผลการตรวจสอบการทำงาน

แผนที่วางไว้	การปฏิบัติจริง	ตรงวัตถุประสงค์หรือไม่
1.เชื่อมต่อเข้าสู่ระบบเครือข่าย	1.เชื่อมต่อเข้าสู่ระบบเครือข่าย	ตรง
2.ระบบ Pop หน้าต่าการเข้าสู่ระบบ	2.ระบบ Pop หน้าต่าการเข้าสู่ระบบ	ตรง เกิดปัญหาการใช้งานบน IOS
3.เข้าสู่ระบบสำเร็จระบบจะแจ้งเตือน	3.เข้าสู่ระบบสำเร็จระบบจะแจ้งเตือน	ตรง
4.ใช้งานอินเทอร์เน็ตได้ โดยจะมีการเก็บประวัติการใช้งาน	4.ใช้งานอินเทอร์เน็ตได้ โดยจะมีการเก็บประวัติการใช้งาน	ตรง
5.Log in ไม่สำเร็จแจ้งเตือนรหัสผ่านผิดพลาด	5.Log in ไม่สำเร็จแจ้งเตือนรหัสผ่านผิดพลาด	ตรง
6.เมื่อไม่ใช้งานนาน 2 ชม ระบบจะตัดสิทธิ์การใช้งานอัตโนมัติ	6.เมื่อไม่ใช้งานนาน 2 ชม ระบบจะตัดสิทธิ์การใช้งานอัตโนมัติ	ตรง

### 2.3 สรุปผลการตรวจสอบการเข้าใช้งานระบบ Authentication

จากผลการทดสอบในตารางที่ 5 จะได้ว่าผลการทดสอบการเข้าใช้งานระบบยืนยันตัวตนบุคคลเป็นไปตามที่คาดไว้ คือสามารถเข้าใช้งานได้เมื่อ Username และ Password ตรงกับฐานข้อมูลของผู้มีสิทธิใช้งานที่ได้ลงทะเบียนไว้ และจากผลการตรวจสอบในตารางที่ 6 การเข้าใช้งานส่วนใหญ่เป็นไปตามแผนที่วางไว้ พบปัญหาการใช้งานบนอุปกรณ์ที่ใช้ระบบปฏิบัติการ iOS ที่บางครั้งหน้าต่างการเข้าสู่ระบบไม่ปรากฏ

### 3. ตรวจสอบการเข้าใช้งานระบบจัดเก็บ Log Files

ผลจากที่ได้ติดตั้งเครื่องคอมพิวเตอร์สำหรับจัดเก็บ Log Files ผู้ดูแลระบบจะสามารถเชื่อมต่อเข้าไปตรวจสอบข้อมูลของ Log ได้โดยสามารถทดสอบการเข้าใช้งานเพื่อตรวจสอบข้อมูลได้ ดังนี้

3.1 เชื่อมต่อเข้าระบบจัดเก็บ Log Files ผ่านทาง <https://172.18.11.37:4130> และทำงานระบุ Username และ Password ของผู้ดูแลระบบ



ภาพที่ 54 แสดงหน้าต่างการเข้าสู่โปรแกรมจัดเก็บ Log Files

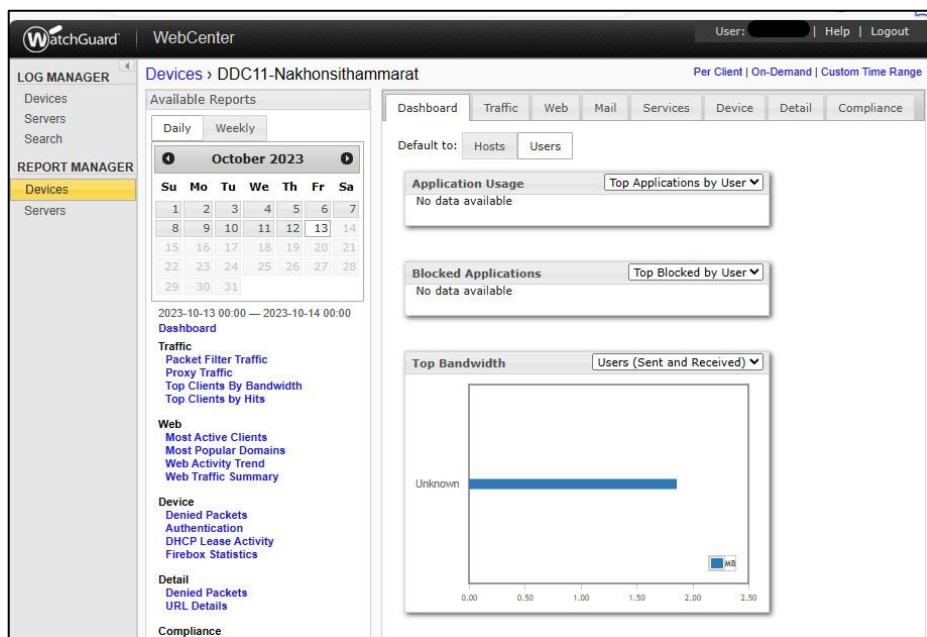
3.2 เมื่อเข้าสู่ระบบแล้วจะพบกับหน้าต่างแสดงอุปกรณ์เพื่อเลือกอุปกรณ์ที่ทำการจัดเก็บ Log Files



Name	Connected	IP Address	Serial Number	Version	Model
DDC11-Nakhonsithamarat	Yes	172.18.11.37	D602970D2	12.3.1	WatchGuard M4600

ภาพที่ 55 แสดงหน้าต่างการเข้าสู่โปรแกรมจัดเก็บ Log Files

### 3.3 เมื่อทำการเลือกอุปกรณ์จะแสดงหน้าต่างสำหรับดูรายละเอียดต่างๆ ของการจัดเก็บ Log Files

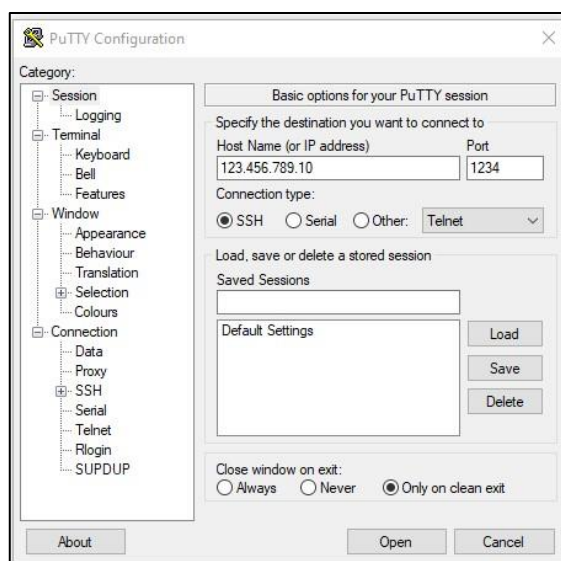


ภาพที่ 56 แสดงหน้าต่าง Dash board ของการจัดเก็บ Log Files

## 4. ตรวจสอบการทำงานของเครื่องเก็บ Log Files

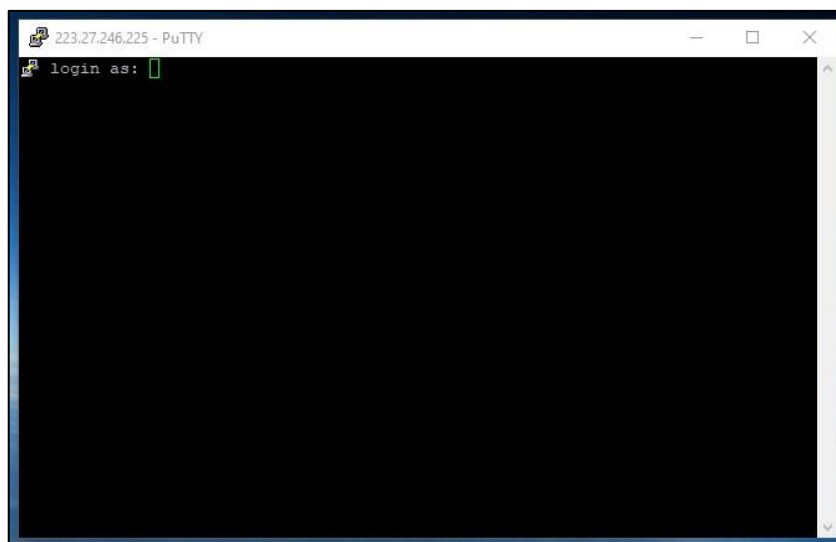
จากที่ได้มีการกำหนดค่าให้ Firewall ดำเนินการจัดเก็บ Log Files ส่งไปยังเครื่องคอมพิวเตอร์ Log Files IP Address 172.18.11.37 สามารถตรวจสอบการทำงานโดยใช้คำสั่ง Command line ได้ดังนี้

4.1 เข้าสู่การใช้งานคำสั่ง Command line โดยใช้งานโปรแกรม PuTTY เลือกการเชื่อมต่อผ่าน IP Address โดยใช้ชนิดการเชื่อมต่อแบบ SSH



ภาพที่ 57 แสดงหน้าต่างโปรแกรม PuTTY สำหรับเชื่อมต่อไปยัง Firewall

4.2 เมื่อทำการกด Open จะเป็นการเชื่อมต่อไปยัง Firewall ระบบจะให้กรอก Username และ Password สำหรับผู้ที่มีสิทธิ์เข้าถึง Command line ของ Firewall



ภาพที่ 58 แสดงหน้าต่างโปรแกรม PuTTY สำหรับ login เข้าใช้งาน

4.3 เมื่อทำการ login เรียบร้อยแล้วให้ใช้คำสั่ง show log-setting [component] เพื่อดูการทำงานของ log ที่ได้กำหนดค่าไว้กับ Firewall โดยให้เลือก component เป็น watchguard-log-server เพื่อที่จะดูข้อมูลของ Log Server ที่ Firewall ได้ส่งข้อมูล log ไปให้ จะได้คำสั่ง คือ show log-setting watchguard-log-server ซึ่งจะได้ผลตรงกับคอมพิวเตอร์ Log Server ที่กำหนดไว้ คือ 172.18.11.37

```
[FAULT]WG#[FAULT]WG#show log-setting watchguard-log-server
--
--WatchGuard Log Server
--
Send log messages to these Log Servers      :Enabled
First Log Server addresses
                                     172.18.11.37
                                     203.157.41.38
[FAULT]WG#
```

ภาพที่ 59 แสดงการใช้คำสั่ง show log-setting watchguard-log-server เพื่อดูปลายทางในการจัดเก็บ Log ของ Firewall

## 5. ตรวจสอบผลการกำหนดความต้องการของระบบ

แบ่งออกเป็นเซิร์ฟเวอร์และเครื่องคอมพิวเตอร์ Log Files ดังนี้

### 5.1 ตรวจสอบเซิร์ฟเวอร์

ตารางที่ 7 การตรวจสอบคุณลักษณะเครื่องเซิร์ฟเวอร์

แผนที่วางไว้	การปฏิบัติจริง	ตรงวัตถุประสงค์หรือไม่
1.ระบบปฏิบัติการ windows Server 2012	1.ระบบปฏิบัติการ windows Server 2012	ตรง
2. CPUs : 4 cores	2. CPUs : 4 cores	ตรง
3. Memory: 12 GB	3. Memory: 12 GB	ตรง
4. Hard Drive : 100 GB	4. Hard Drive : 100 GB	ตรง

### 5.2 ตรวจสอบคอมพิวเตอร์ Log Files

ตารางที่ 8 การตรวจสอบคุณลักษณะเฉพาะเครื่องคอมพิวเตอร์ log files

แผนที่วางไว้	การปฏิบัติจริง	ตรงวัตถุประสงค์หรือไม่
1. ระบบปฏิบัติการ: Windows 10	1. ระบบปฏิบัติการ: Windows 10	ตรง
2. CPUs : 4 cores	2. CPUs : 4 cores	ตรง
3. Memory: 8 GB	3. Memory: 8 GB	ตรง
4.Hard Drive : 100 GB	4.Hard Drive : 100 GB	ไม่เพียงพอต่อการใช้งาน

### 5.3 ผลการตรวจสอบคุณลักษณะเครื่องคอมพิวเตอร์เซิร์ฟเวอร์ และคอมพิวเตอร์ Log Files

จากตารางที่ 7 แสดงให้เห็นว่าการกำหนดคุณลักษณะเครื่องเซิร์ฟเวอร์เป็นไปตามแผนที่วางไว้และจากตารางที่ 8 แสดงให้เห็นว่าการตรวจสอบคุณลักษณะเฉพาะเครื่องคอมพิวเตอร์ log files ปริมาณพื้นที่จัดเก็บข้อมูลไม่เพียงพอ จึงมีการปรับปรุงเพิ่มความจุเป็น 300 GB

## 6. ตรวจสอบประสิทธิภาพการทำงานของเครือข่ายอินเทอร์เน็ต

ดำเนินการตรวจสอบประสิทธิภาพการทำงานของเครือข่ายอินเทอร์เน็ตโดยใช้เครื่องมือ Microsoft 365 network connectivity test tool ดำเนินการทดสอบเปรียบเทียบผลการใช้งานก่อนและหลังติดตั้งระบบ Authentication ได้ผลดังตารางที่ 9

ตารางที่ 9 แสดงผลการเปรียบเทียบการทดสอบการใช้งานก่อนและหลังติดตั้งระบบ

เหตุการณ์(Test Case)	ก่อนใช้งานระบบ AD	หลังใช้งานระบบ AD
Media Connectivity	No errors	No errors
Packet loss	0.00% (target < 1%)	0.00% (target < 1%)
Latency	86ms (target < 100ms)	100ms (target< 100ms)
Jitter	3ms (target <30ms)	2ms (target <30ms)

จากตารางที่ 9 แสดงให้เห็นว่าหลังติดตั้งการใช้งานระบบ Authentication ไม่ส่งผลกระทบต่อประสิทธิภาพการทำงานของระบบเครือข่ายอินเทอร์เน็ตของสำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช

Microsoft Teams	
Test	Result
✓ Media connectivity (audio, video, and application sharing)	No errors
✓ Packet loss	0.00% (target < 1% during 15 s)
▲ Latency	100 ms (target < 100 ms)
✓ Jitter	2 ms (target < 30 ms)
Connectivity	
All connectivity tests passed	

ภาพที่ 60 แสดงผลการทดสอบหลังใช้งานระบบ Authentication

6.1 ตรวจสอบความสามารถการทำงานของระบบ ทำการเปรียบเทียบการทำงานของระบบก่อนการใช้งานระบบ และหลังการใช้งานระบบ เพื่อเปรียบเทียบประสิทธิภาพการทำงานของระบบ ดังต่อไปนี้

1) ตรวจสอบผู้ใช้งานระบบเครือข่ายก่อนการใช้งานระบบ Authentication โดยการทำการเข้าไปตรวจสอบ IP Address ของผู้ใช้งานระบบด้วย Firewall โดยแสดงผลดังภาพที่ 4.49 คือไม่สามารถระบุถึงตัวตนผู้ใช้งานที่ไม่ได้มีการตั้งชื่อเครื่องคอมพิวเตอร์ให้สอดคล้องกับชื่อผู้ใช้งานจริงได้

INTERFACE	IP ADDRESS	HOST	MAC ADDRESS	START TIME	END TIME
V100-LAN	192.168.100.216	DESKTOP-KJC4M7F	a0:8c:fd:da:c9:ae	2023/11/16 08:55:49	2023/11/16 16:55:49
V100-LAN	192.168.100.50	Aekachai-k	74:56:3c:57:68:31	2023/11/16 08:31:18	2023/11/16 16:31:18
V100-LAN	192.168.100.235	LekAdmin	34:64:a9:34:62:98	2023/11/16 08:22:55	2023/11/16 16:22:55
V140-LAN	192.168.140.20	DESKTOP-F3J4QH9	1c:69:7a:97:f6:7e	2023/11/16 08:33:51	2023/11/16 16:33:51
V141-LAN	192.168.141.39	DESKTOP-HMGP343	50:eb:f6:26:19:f3	2023/11/16 09:03:37	2023/11/16 17:03:37
V141-LAN	192.168.141.45	DESKTOP-N7HLFH5	1c:69:7a:7c:bc:4a	2023/11/16 08:44:30	2023/11/16 16:44:30
V141-LAN	192.168.141.47	DESKTOP-VFECGMP	c0:18:03:b4:cc:8c	2023/11/16 08:43:15	2023/11/16 16:43:15
V141-LAN	192.168.141.44	DESKTOP-4NFFMTM	1c:66:6d:90:e5:9f	2023/11/16 08:42:32	2023/11/16 16:42:32
V141-LAN	192.168.141.43	TEMPIT	1c:66:6d:90:e6:68	2023/11/16 08:34:49	2023/11/16 16:34:49
V141-LAN	192.168.141.40	DESKTOP-K9LQH6L	1c:69:7a:98:32:81	2023/11/16 08:24:10	2023/11/16 16:24:10

ภาพที่ 61 แสดงผลการตรวจสอบผู้ใช้งานระบบเครือข่ายก่อนการใช้งาน ระบบ Authentication

2) ตรวจสอบผู้ใช้งานระบบเครือข่ายหลังการใช้งานระบบ Authentication โดยการเข้าไปตรวจสอบจำนวนผู้ใช้งาน Authentication List บน Firewall โดยแสดงดังภาพที่ 4.50 คือสามารถระบุตัวตนของผู้ใช้งานได้จาก User ที่ทำการใช้งาน

USER	TYPE	DOMAIN	CLIENT	ELAPSED TIME	IP ADDRESS
haris.h	Firewall User	odpc11.local	Authentication portal	0 days 00:48:29	192.168.40.179
kanaphot.t	Firewall User	odpc11.local	Authentication portal	0 days 00:40:56	192.168.143.25
nopparat.b	Firewall User	odpc11.local	Authentication portal	0 days 00:08:01	192.168.100.69

ภาพที่ 62 แสดงผลการตรวจสอบผู้ใช้งานระบบเครือข่ายหลังการใช้งาน ระบบ Authentication



3) ตรวจสอบประวัติการใช้งานระบบก่อนการใช้งานระบบ การใช้งานระบบเครือข่ายก่อนการใช้งานระบบ Authentication ไม่มีการจัดเก็บประวัติการใช้งานเครือข่าย

4) ตรวจสอบการใช้งานระบบหลังการใช้งานระบบ Authentication โดยสามารถเข้าตรวจสอบประวัติการใช้งานเครือข่ายได้ผ่าน Log Files Server

#### 4.2.2 ตรวจสอบผลลัพธ์การทำงานของระบบ เพื่อให้เป็นไปตามวัตถุประสงค์ของการดำเนินการวิจัย

โดยมีขั้นตอนดังนี้

##### 1. ตรวจสอบความสามารถการควบคุมการเข้าถึงเครือข่ายอินเทอร์เน็ต

ตารางที่ 10 เปรียบเทียบการทำงานก่อนและหลังการใช้งานระบบ

ก่อนใช้งานระบบ	หลังใช้งานระบบ
ไม่สามารถรู้ได้ว่ามีใครใช้งานระบบอยู่บ้าง	สามารถระบุตัวตนผู้ใช้งานระบบได้
ไม่สามารถตรวจสอบประวัติการใช้งานย้อนหลังได้	สามารถตรวจสอบประวัติการใช้งานย้อนหลังได้
ไม่สามารถปกป้องข้อมูลภายในจากการเข้าถึงที่ไม่ได้รับอนุญาต	สามารถควบคุมการเข้าเครือข่ายจากการเข้าถึงที่ไม่ได้รับอนุญาต
ไม่มีการป้องกันการเข้าถึงเครือข่าย	มีการป้องกันการเข้าถึงเครือข่ายด้วยระบบ

จากตารางที่ 10 แสดงให้เห็นว่าการใช้ Authentication ทำให้ความสามารถในการป้องกันเครือข่ายมีประสิทธิภาพมากขึ้น

ตารางที่ 11 สรุปผลการเข้าใช้งานระบบเครือข่ายอินเทอร์เน็ตของบุคลากรในระยะเวลา 90 วัน

จำนวนบุคลากรที่ลงทะเบียน	จำนวนบุคลากรที่เข้าใช้งานระบบ	จำนวนบุคลากรที่ไม่เข้าใช้งานระบบ
160	160	0

จากตารางที่ 11 ซึ่งแสดงข้อมูลการเข้าใช้งานเครือข่ายอินเทอร์เน็ตที่สำเร็จของบุคลากรทั้งหมดตลอดระยะเวลาที่ได้จัดเก็บข้อมูลเพื่อทำการวิจัยเป็นเวลาจำนวน 90 วัน ช่วงระหว่างวันที่ 24 กันยายน พ.ศ. 2566 ถึงวันที่ 22 ธันวาคม พ.ศ. 2566 สามารถสรุปได้ดังนี้ จำนวนผู้ลงทะเบียนเข้าใช้งานระบบเครือข่ายอินเทอร์เน็ตของสำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช มีผู้ใช้งานทั้งหมด 160 user

โดยมีบุคลากรที่เข้าใช้งานระบบการยืนยันตัวตนเพื่อใช้งานเครือข่ายอินเทอร์เน็ตอย่างน้อย 1 ครั้ง ในระยะเวลา 90 วัน จำนวน 160 user และไม่มีบุคลากรที่ลงทะเบียนเข้าใช้งานเครือข่ายอินเทอร์เน็ต แต่ไม่เคยเข้าใช้งานระบบเลยในระยะเวลา 90 วัน คิดเป็นร้อยละของการเข้าใช้งานอยู่ที่ร้อยละ 100.00 ของการใช้งานทั้งหมด ซึ่งแสดงให้เห็นว่าระบบการยืนยันตัวตนบุคคลเพื่อเข้าใช้งานเครือข่ายอินเทอร์เน็ตของ สำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช สามารถควบคุมการเข้าถึงเครือข่าย เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตได้ และสามารถทำให้บุคลากรที่มีความจำเป็นต้องใช้งานเครือข่าย อินเทอร์เน็ตต้องเข้าใช้งานผ่านระบบระบบการยืนยันตัวตนบุคคลเพื่อเข้าใช้งานเครือข่ายอินเทอร์เน็ตเท่านั้น สามารถเข้าดูผลการเข้าใช้งานระบบเครือข่ายอินเทอร์เน็ตของบุคลากรในระยะเวลา 90 วัน ในภาคผนวก ข

## 2. ทดสอบผลของการจัดเก็บ Log Files

เพื่อให้บรรลุวัตถุประสงค์ในการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log File) ตามพระราชบัญญัติ ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 ฉบับที่ 2 “มาตรา 26 ผู้ให้บริการต้องเก็บรักษา ข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์” และ เพื่อสามารถดูข้อมูลประวัติการใช้งานอินเทอร์เน็ตได้ จึงจำเป็นต้องสามารถค้นหาข้อมูล Log Files การใช้งานย้อนหลังได้ และทำการทดสอบการค้นหาข้อมูลการใช้งานย้อนหลัง มีขั้นตอนดังนี้

2.1 เชื่อมต่อเข้าระบบจัดเก็บ Log Files ผ่านทาง <https://172.18.11.37:4130> และทำงานระบุ Username และ Password ของผู้ดูแลระบบ จากนั้นเลือกหัวข้อ โดยสามารถระบุรายละเอียดการค้นหา ได้ดังนี้

Time Range คือ สามารถระบุช่วงเวลาในการค้นหาได้

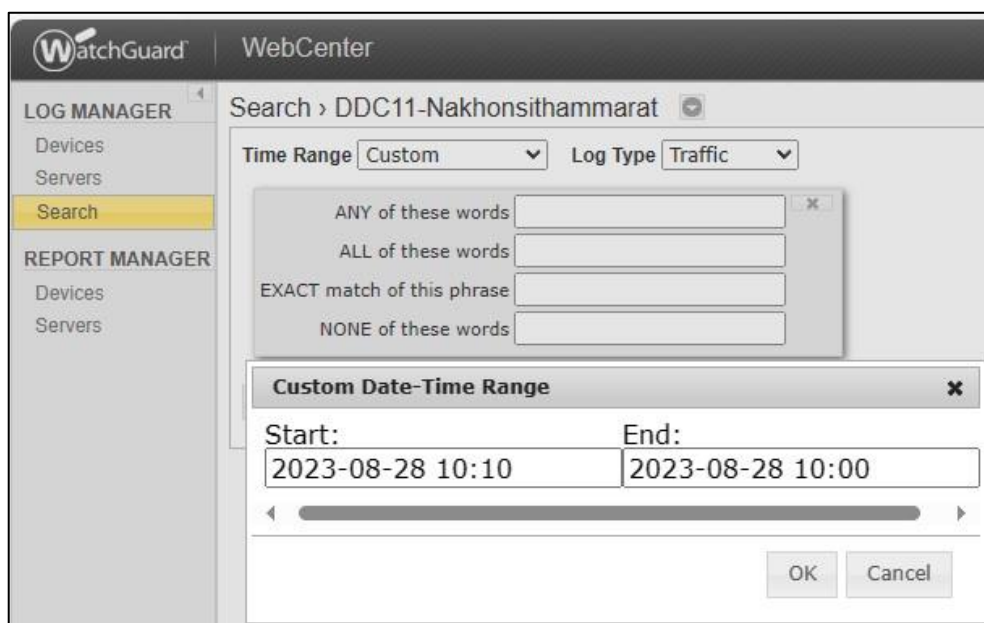
Log Type คือ ชนิดของ Log ที่ต้องการค้นหา

Any of these words คือ หาข้อมูลทีส่วนของคำที่ระบุ

ALL of these words คือ หาข้อมูลที่มีคำที่ระบุ

EXACT match of this phase คือ ข้อมูลที่ตรงกับที่ระบุทุกประการ

NONE of these words คือ ข้อมูลทั้งหมดยกเว้นที่มีส่วนของที่ระบุ



ภาพที่ 63 แสดงระยะเวลาในการค้นหาข้อมูล Log ย้อนหลัง

2.2 ผลการค้นหาระบบจะโชว์ข้อมูล Log Files ที่ตรงกับเงื่อนไขที่ทำการค้นหาโดยมีข้อมูลที่ตรงกับวัตถุประสงค์ในการจัดเก็บ ดังนี้

ตารางที่ 12 แสดงความหมายของข้อมูลที่จัดเก็บเป็น Log Files

ชนิดข้อมูล	ความหมาย
Date-Time	วันที่และเวลาที่ใช้งาน
src_	IP Address เครื่องต้นทาง
dst_ip	IP Address เครื่องปลายทาง
src_user	ชื่อ User ผู้ใช้งาน

## 2.3 ตรวจสอบผลการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log Files)

การตรวจสอบผลการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์(Log Files) ว่าสามารถจัดเก็บข้อมูลได้ครบ 90 วัน ตามที่กำหนดไว้หรือไม่

The screenshot displays the 'Log Server' configuration page within the 'WatchGuard Server Center'. The page is divided into several sections:

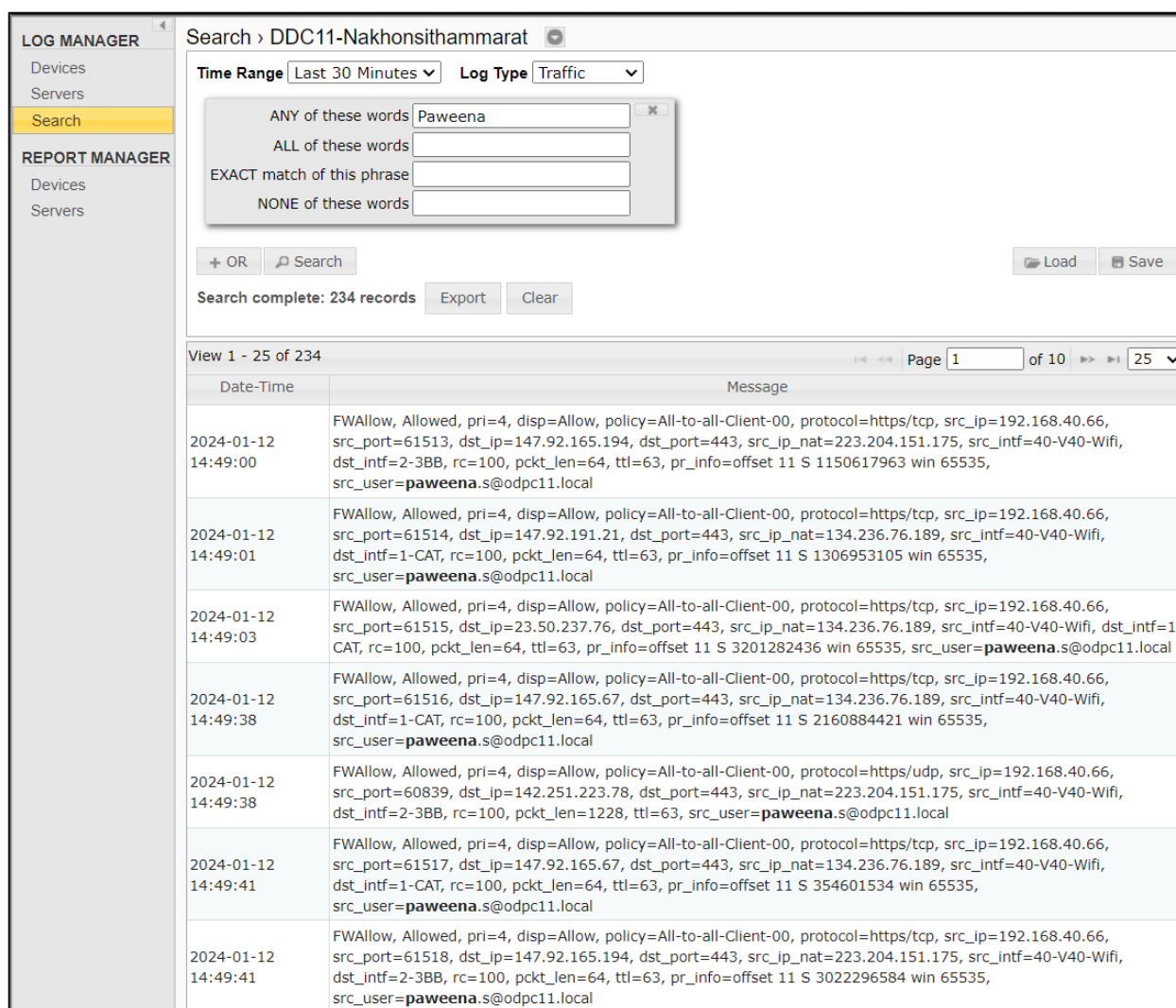
- Database Size:** Shows a maximum database size of 150 GB. The current database size is 143.31 GB, leaving 6.69 GB (4.5%) of available space. A checkbox for 'Automatically delete data older than 91 day(s)' is checked. The last update was on 02/20/2024 at 05:31 PM. A 'Refresh' button is present.
- Authentication Key Setting:** Includes a 'Modify' button to change the Log Server Authentication key.
- Logging Connections:** Features a checkbox for 'Disable TLS 1.0' which is currently unchecked.
- Diagnostics Logs:** Includes a 'Purge Diagnostics Logs' button and a note: 'This option deletes all Diagnostic log messages generated by your devices (Debug level or higher) from the Log Server database.'

ภาพที่ 64 แสดงผลการตรวจสอบการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log Files)

จากภาพแสดงให้เห็นถึงผลการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ ที่ได้ทำการจัดเก็บทั้งหมด 91 วัน โดยใช้พื้นที่ในการจัดเก็บจำนวน 143.31 GB จากพื้นที่ที่กำหนดไว้คือ 150 GB แสดงให้เห็นถึงความสามารถในการจัดเก็บข้อมูลได้ตามวัตถุประสงค์ที่กำหนดไว้

### 3. ผลการตรวจสอบความสามารถในการระบุตัวตนของผู้ใช้งานเครือข่ายอินเทอร์เน็ต

การตรวจสอบการระบุตัวตนผู้ใช้งานเครือข่ายอินเทอร์เน็ตสามารถระบุได้ด้วยตรวจสอบจากชื่อผู้ใช้งานที่พบจากข้อมูลจราจรคอมพิวเตอร์นำไปเปรียบเทียบกับข้อมูลที่ได้องค์ทะเบียนขอสิทธิใช้งานเครือข่ายอินเทอร์เน็ต



The screenshot shows a web-based log manager interface. The search criteria are set to 'Last 30 Minutes' and 'Traffic'. A search box contains the keyword 'Paweena'. The search results show 234 records. The first few records are as follows:

Date-Time	Message
2024-01-12 14:49:00	FWAllow, Allowed, pri=4, disp=Allow, policy=All-to-all-Client-00, protocol=https/tcp, src_ip=192.168.40.66, src_port=61513, dst_ip=147.92.165.194, dst_port=443, src_ip_nat=223.204.151.175, src_intf=40-V40-Wifi, dst_intf=2-3BB, rc=100, pkt_len=64, ttl=63, pr_info=offset 11 S 1150617963 win 65535, src_user= <b>paweena.s@odpc11.local</b>
2024-01-12 14:49:01	FWAllow, Allowed, pri=4, disp=Allow, policy=All-to-all-Client-00, protocol=https/tcp, src_ip=192.168.40.66, src_port=61514, dst_ip=147.92.191.21, dst_port=443, src_ip_nat=134.236.76.189, src_intf=40-V40-Wifi, dst_intf=1-CAT, rc=100, pkt_len=64, ttl=63, pr_info=offset 11 S 1306953105 win 65535, src_user= <b>paweena.s@odpc11.local</b>
2024-01-12 14:49:03	FWAllow, Allowed, pri=4, disp=Allow, policy=All-to-all-Client-00, protocol=https/tcp, src_ip=192.168.40.66, src_port=61515, dst_ip=23.50.237.76, dst_port=443, src_ip_nat=134.236.76.189, src_intf=40-V40-Wifi, dst_intf=1-CAT, rc=100, pkt_len=64, ttl=63, pr_info=offset 11 S 3201282436 win 65535, src_user= <b>paweena.s@odpc11.local</b>
2024-01-12 14:49:38	FWAllow, Allowed, pri=4, disp=Allow, policy=All-to-all-Client-00, protocol=https/tcp, src_ip=192.168.40.66, src_port=61516, dst_ip=147.92.165.67, dst_port=443, src_ip_nat=134.236.76.189, src_intf=40-V40-Wifi, dst_intf=1-CAT, rc=100, pkt_len=64, ttl=63, pr_info=offset 11 S 2160884421 win 65535, src_user= <b>paweena.s@odpc11.local</b>
2024-01-12 14:49:38	FWAllow, Allowed, pri=4, disp=Allow, policy=All-to-all-Client-00, protocol=https/udp, src_ip=192.168.40.66, src_port=60839, dst_ip=142.251.223.78, dst_port=443, src_ip_nat=223.204.151.175, src_intf=40-V40-Wifi, dst_intf=2-3BB, rc=100, pkt_len=1228, ttl=63, src_user= <b>paweena.s@odpc11.local</b>
2024-01-12 14:49:41	FWAllow, Allowed, pri=4, disp=Allow, policy=All-to-all-Client-00, protocol=https/tcp, src_ip=192.168.40.66, src_port=61517, dst_ip=147.92.165.67, dst_port=443, src_ip_nat=134.236.76.189, src_intf=40-V40-Wifi, dst_intf=1-CAT, rc=100, pkt_len=64, ttl=63, pr_info=offset 11 S 354601534 win 65535, src_user= <b>paweena.s@odpc11.local</b>
2024-01-12 14:49:41	FWAllow, Allowed, pri=4, disp=Allow, policy=All-to-all-Client-00, protocol=https/tcp, src_ip=192.168.40.66, src_port=61518, dst_ip=147.92.165.194, dst_port=443, src_ip_nat=223.204.151.175, src_intf=40-V40-Wifi, dst_intf=2-3BB, rc=100, pkt_len=64, ttl=63, pr_info=offset 11 S 3022296584 win 65535, src_user= <b>paweena.s@odpc11.local</b>

ภาพที่ 65 แสดงตัวอย่างข้อมูลการค้นหา Log Files

จากภาพแสดงให้เห็นถึงข้อมูลจราจรทางคอมพิวเตอร์ (Log Files) โดยสามารถระบุตัวตนของผู้ใช้งานเครือข่ายอินเทอร์เน็ตได้จากข้อมูล src\_user= ที่ได้จัดเก็บไว้ใน Log server โดยสามารถนำข้อมูล User ที่พบไปตรวจสอบกับข้อมูลที่ได้ทำการลงทะเบียนขอสิทธิใช้งานไว้และระบุตัวตนของผู้ใช้งานได้

## 4.4 ขั้นตอนการดำเนินงานให้เหมาะสม (Act)

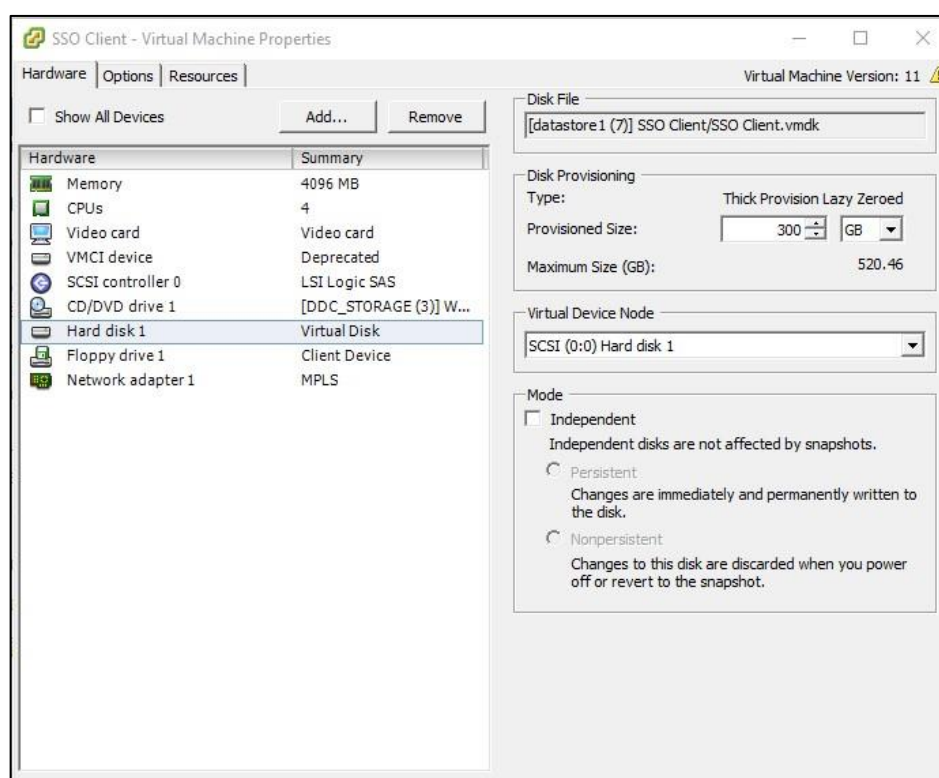
### 4.3.1 การปรับปรุงด้านเทคนิค

คือ วางแผน ปรับปรุง พัฒนา ตรวจสอบความถูกต้องของการทำงานของระบบ นำไปสู่การประกาศใช้งานระบบ และการบำรุงรักษาระบบ

#### 1. ผลการปรับปรุงด้านเทคนิค

จากการทบทวน วิเคราะห์ผลการดำเนินงาน ผลลัพธ์จากที่ได้ตรงกับที่ได้วางแผนไว้ โดยมีกรณีผลลัพธ์ที่ได้ไม่เป็นไปตามขั้นการวางแผน คือขนาดพื้นที่จัดเก็บข้อมูล Log Files จึงได้ดำเนินการค้นหาสาเหตุที่มาของผลดำเนินการแก้ไข โดยมีผลลัพธ์ที่ไม่เป็นไปตามที่วางแผนไว้ ดังนี้

1) เครื่องคอมพิวเตอร์จัดเก็บ Log Files มีพื้นที่ Hard Drive น้อยกว่าที่วางแผนไว้ โดยหลังจากที่ได้ทำการตรวจเช็ค จึงได้วางแผนปรับปรุงขนาดของพื้นที่ในการจัดเก็บเพิ่มจากเดิม 100 GB เป็น 300 GB



ภาพที่ 66 แสดงผลปรับปรุงขนาดของพื้นที่ในการจัดเก็บเพิ่มจากเดิม 100 GB เป็น 300 GB

2) การใช้งานระบบ Authentication ผ่านอุปกรณ์โทรศัพท์มือถือ และแท็บเล็ตที่ใช้ระบบปฏิบัติการ iOS พบปัญหาการระบบ Authentication ไม่ขึ้นให้ใช้งานแก้ปัญหาเบื้องต้น โดยให้ผู้ใช้งาน

บู๊คมาร์กหน้าต่างที่เข้าใช้งานไว้ กรณีระบบไม่ขึ้นสามารถกดเข้าไปใช้งานเองได้ พร้อมทั้งจะหาสาเหตุและวิธีการแก้ไขต่อไป

## 2. ผลการบำรุงรักษาระบบ

สำหรับการดูแลรักษาระบบใช้วิธีการ Preventive Maintenance (PM) คือ การบำรุงรักษาเชิงป้องกัน เป็นหนึ่งในรูปแบบการดูแลสภาพเครื่องจักรและอุปกรณ์ที่ใช้การตรวจสอบ ซ่อมแซม หรือเปลี่ยนแปลง อุปกรณ์ต่างๆ ตามเวลาที่มีการกำหนดเอาไว้ โดยมีแผนการบำรุงรักษาตั้งแต่เริ่มใช้งานระบบดังนี้

ตารางที่ 13 แสดงตารางการบำรุงรักษาเครื่อง Server

วันที่ (Date)	รายละเอียด
มีนาคม 2566	ตรวจสอบความพร้อมใช้ของเซิร์ฟเวอร์และการทำงานของระบบ
กรกฎาคม 2566	ตรวจสอบความพร้อมใช้ของเซิร์ฟเวอร์และการทำงานของระบบ

## 3. ประกาศการใช้งานระบบ

หลังจากได้มีการทดสอบระบบจนแน่ใจแล้ว จึงได้ดำเนินการประกาศใช้งานระบบการยืนยันตัวตน เพื่อเข้าใช้งานระบบเครือข่ายอินเทอร์เน็ต เมื่อวันที่ 27 กุมภาพันธ์ พ.ศ. 2566 ทำให้ทุกครั้งที่มีการเข้าถึงเครือข่ายไม่ว่าจะเป็นเครือข่ายภายใน Intranet หรือ เครือข่ายภายนอก Internet จำเป็นต้องมีการ Authentication ก่อนทุกครั้ง ช่วยให้หน่วยงานมีความความมั่นคงปลอดภัยในการใช้งานระบบเครือข่ายที่เพิ่มมากขึ้น โดยสามารถป้องกันบุคคลภายนอก หรือประชาชนที่อาศัยอยู่รอบข้างสำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช ไม่สามารถเข้าถึงระบบเครือข่ายของหน่วยงานโดยที่ไม่ได้รับอนุญาต รวมถึงเป็นการดำเนินการตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ กระทรวงสาธารณสุข พ.ศ. 2565 และตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 ฉบับที่ 2 อีกด้วย โดยมีขั้นตอนดังนี้

- 1) จัดทำหนังสือราชการแจ้งเวียนก่อนการเปิดใช้งานล่วงหน้า 2 สัปดาห์ (ภาคผนวก ก)
- 2) จัดทำคู่มือการใช้งานบนเครื่องคอมพิวเตอร์, คู่มือการใช้งานบนเครื่องคอมพิวเตอร์แท็บเล็ตและโทรศัพท์มือถือ, คู่มือการเปลี่ยนรหัสผ่าน และประชาสัมพันธ์ในกลุ่ม Line ล่วงหน้า 1 สัปดาห์ (ภาคผนวก ค-จ)
- 3) ดำเนินการส่งมอบ Username และ Password และคู่มือการใช้งาน ดำเนินการส่งมอบรหัสให้แก่บุคลากรรายบุคคลพร้อมกำหนดแนวทางการบริหารจัดการผู้ใช้งาน ดังนี้

4) ดำเนินการ Deploy Policy หลังจากการประกาศการใช้งานเพื่อให้ระบบสามารถทำงานได้ จำเป็นต้องกำหนด Policy เพื่อให้ Firewall ตรวจสอบเช็คการ Authentication ก่อนให้เข้าถึงเครือข่าย

ORDER	ACTION	POLICY NAME	TYPE	FROM	TO	PORT	SD-WAN	APP CONTROL	GEOLOCATION	TAGS
1	✓									
2	✓								Global	
3	✓							Global	Global	
4	✓								Global	
5	✓								Global	
6	✓								Global	
7	✓								Global	
8	✓								Global	
9	✓	All to all Client	All to all Client	OD#C11 f	Any-External, Any-Int	Any			Global	

ภาพที่ 67 แสดงการจัดลำดับ Policy บน Firewall

#### 4. กำหนดแนวทางในการเพิ่ม ลบ สิทธิการใช้งาน แก่งานการเจ้าหน้าที่

โดยมีขั้นตอนดังนี้

##### 4.1 ขั้นตอนการขอรับชื่อผู้เข้าใช้งานและรหัสผ่าน

1) งานการเจ้าหน้าที่ส่งข้อมูลบุคลากร หรือ บุคลากรใหม่ มาให้งานเทคโนโลยีสารสนเทศ ประกอบด้วย ชื่อ-สกุล ภาษาไทย และ ภาษาอังกฤษ ตำแหน่ง และ กลุ่มงาน

2) งานเทคโนโลยีสารสนเทศ นำข้อมูลไปบันทึกในฐานข้อมูล Active Directory และกำหนด ชื่อผู้เข้าใช้งานและรหัสผ่าน

3) งานเทคโนโลยีสารสนเทศส่งชื่อผู้เข้าใช้งาน รหัสผ่านและคู่มือการเข้าใช้งาน คู่มือการเปลี่ยนรหัสผ่าน ให้กับเจ้าหน้าที่

##### 4.2 ขั้นตอนแรกแจ้งบุคลากรลาออก ย้ายงาน หรือเกษียณอายุราชการ

1) งานการเจ้าหน้าที่แจ้งชื่อ-สกุล กลุ่มงาน ของบุคลากรที่ลาออก ย้ายงาน หรือเกษียณอายุราชการ

2) งานเทคโนโลยีสารสนเทศ ยกเลิกสิทธิการเข้าใช้งาน

#### 5. ขั้นตอนดำเนินงาน ในกรณีของการขอตรวจสอบประวัติการใช้งาน

การดำเนินการหากได้รับมอบหมายจากผู้อำนวยการในกรณีที่มีผู้ทำหนังสือขอความอนุเคราะห์ในการขอข้อมูลการจราจรทางคอมพิวเตอร์เพื่อใช้ประกอบหลักฐานการกระทำผิดทางคอมพิวเตอร์



ตัวอย่างเช่น มีผู้ร้องขอว่ามีบุคลากรภายในหน่วยงานใดที่ใช้อินเทอร์เน็ตภายในหน่วยงานไปใช้งาน Facebook ทำให้เกิดเป็นคดีความและนำหลักฐานมาขอข้อมูลเพื่อตรวจสอบว่าในวันเวลาดังกล่าว บุคคลดังกล่าวได้ใช้งาน Facebook โดยใช้อินเทอร์เน็ตของหน่วยงานจริงหรือไม่ โดยมีขั้นตอนดังนี้

1. เข้าสู่ระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ของหน่วยงาน

2. ดำเนินการตรวจสอบค้นหาข้อมูลตามที่ได้รับแจ้งดังนี้

เวลาที่ต้องการค้นหา เช่น 10.30 น ของวันที่ 23 ธันวาคม

IP ปลายทางของ Facebook ที่ได้รับมาคือ 157.240.236.35

ชื่อ-สกุลของผู้ถูกกล่าวหา

ได้ผลลัพธ์การค้นหาดังนี้

Time Range 2023-12-23 10.00 ถึง 2023-12-23 11.00

IP Dest คือ 157.240.236.35

Search > DDC11-Nakhonsithammarat

Time Range Custom 2023-12-23 10:00 to 2023-12-23 11:00 UTC07:00 Change Log Type Traffic

ANY of these words 157.240.236.35

ALL of these words

EXACT match of this phrase

NONE of these words

+ OR Search Load Save

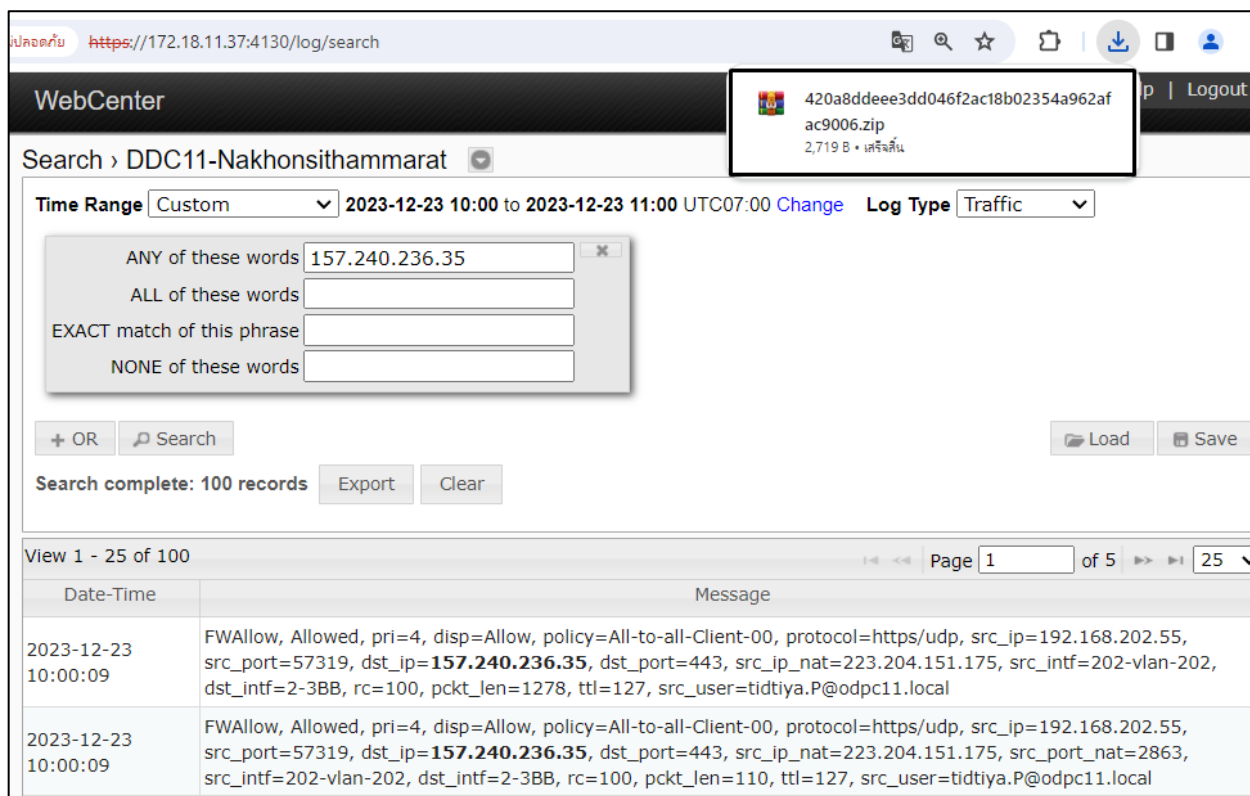
Search complete: 100 records Export Clear

View 1 - 25 of 100 Page 1 of 5 25

Date-Time	Message
2023-12-23 10:00:09	FWAllow, Allowed, pri=4, disp=Allow, policy=All-to-all-Client-00, protocol=https/udp, src_ip=192.168.202.55, src_port=57319, dst_ip=157.240.236.35, dst_port=443, src_ip_nat=223.204.151.175, src_intf=202-vlan-202, dst_intf=2-3BB, rc=100, pkt_len=1278, ttl=127, src_user=tidtiya.P@odpc11.local
2023-12-23 10:00:09	FWAllow, Allowed, pri=4, disp=Allow, policy=All-to-all-Client-00, protocol=https/udp, src_ip=192.168.202.55, src_port=57319, dst_ip=157.240.236.35, dst_port=443, src_ip_nat=223.204.151.175, src_port_nat=2863, src_intf=202-vlan-202, dst_intf=2-3BB, rc=100, pkt_len=110, ttl=127, src_user=tidtiya.P@odpc11.local
2023-12-23 10:01:55	FWAllow, Allowed, pri=4, disp=Allow, policy=All-to-all-Client-00, protocol=https/udp, src_ip=192.168.200.50, src_port=50706, dst_ip=157.240.236.35, dst_port=443, src_ip_nat=134.236.155.90, src_intf=200-V200-LAN, dst_intf=1-CAT, rc=100, pkt_len=1278, ttl=127, src_user=pathom.k@odpc11.local
2023-12-23 10:01:55	FWAllow, Allowed, pri=4, disp=Allow, policy=All-to-all-Client-00, protocol=https/udp, src_ip=192.168.200.50, src_port=50706, dst_ip=157.240.236.35, dst_port=443, src_ip_nat=134.236.155.90, src_intf=200-V200-LAN, dst_intf=1-CAT, rc=100, pkt_len=106, ttl=127, src_user=pathom.k@odpc11.local
2023-12-23 10:02:42	FWAllow, Allowed, pri=4, disp=Allow, policy=All-to-all-Client-00, protocol=https/udp, src_ip=192.168.202.55, src_port=54368, dst_ip=157.240.236.35, dst_port=443, src_ip_nat=223.204.151.175, src_intf=202-vlan-202, dst_intf=2-3BB, rc=100, pkt_len=1278, ttl=127, src_user=tidtiya.P@odpc11.local
2023-12-23 10:02:42	FWAllow, Allowed, pri=4, disp=Allow, policy=All-to-all-Client-00, protocol=https/udp, src_ip=192.168.202.55, src_port=54368, dst_ip=157.240.236.35, dst_port=443, src_ip_nat=223.204.151.175, src_port_nat=2863, src_intf=202-vlan-202, dst_intf=2-3BB, rc=100, pkt_len=107, ttl=127, src_user=tidtiya.P@odpc11.local
2023-12-23 10:03:19	FWAllow, Allowed, pri=4, disp=Allow, policy=All-to-all-Client-00, protocol=https/tcp, src_ip=192.168.200.86, src_port=43896, dst_ip=157.240.236.35, dst_port=443, src_ip_nat=223.204.151.175, src_intf=200-V200-LAN, dst_intf=2-3BB, rc=100, pkt_len=60, ttl=63, pr_info=offset 10 S 3544954902 win 65535, src_user=pathom.k@odpc11.local
2023-12-23 10:04:33	FWAllow, Allowed, pri=4, disp=Allow, policy=All-to-all-Client-00, protocol=https/udp, src_ip=192.168.200.50, src_port=63579, dst_ip=157.240.236.35, dst_port=443, src_ip_nat=134.236.155.90, src_intf=200-V200-LAN, dst_intf=1-CAT, rc=100, pkt_len=1278, ttl=127, src_user=pathom.k@odpc11.local

ภาพที่ 68 แสดงผลการค้นหาประวัติการใช้งานอินเทอร์เน็ตตามข้อมูลที่ได้รับการร้องขอ

3. ดำเนินการ Export ไฟล์ข้อมูลจราจรทางคอมพิวเตอร์ออกมาในรูปแบบ CSV เพื่อส่งมอบให้ผู้ทำการร้องขอนำไปตรวจสอบตามกระบวนการทางกฎหมาย



WebCenter

Search > DDC11-Nakhonsithammarat

Time Range Custom 2023-12-23 10:00 to 2023-12-23 11:00 UTC07:00 Change Log Type Traffic

ANY of these words 157.240.236.35

ALL of these words

EXACT match of this phrase

NONE of these words

+ OR Search Load Save

Search complete: 100 records Export Clear

View 1 - 25 of 100 Page 1 of 5 25

Date-Time	Message
2023-12-23 10:00:09	FWAllow, Allowed, pri=4, disp=Allow, policy=All-to-all-Client-00, protocol=https/udp, src_ip=192.168.202.55, src_port=57319, dst_ip= <b>157.240.236.35</b> , dst_port=443, src_ip_nat=223.204.151.175, src_intf=202-vlan-202, dst_intf=2-3BB, rc=100, pckt_len=1278, ttl=127, src_user=tidtiya.P@odpc11.local
2023-12-23 10:00:09	FWAllow, Allowed, pri=4, disp=Allow, policy=All-to-all-Client-00, protocol=https/udp, src_ip=192.168.202.55, src_port=57319, dst_ip= <b>157.240.236.35</b> , dst_port=443, src_ip_nat=223.204.151.175, src_port_nat=2863, src_intf=202-vlan-202, dst_intf=2-3BB, rc=100, pckt_len=110, ttl=127, src_user=tidtiya.P@odpc11.local

ภาพที่ 69 แสดงการ Export ข้อมูลให้อยู่ในรูปแบบ CSV เพื่อส่งมอบให้แก่ผู้ร้องขอ

## 4.5 การวัดผลการพัฒนาระบบและแบบประเมินประสิทธิภาพ

### 1. การนำผลสรุปของการทำงานของระบบ

การตรวจสอบผลการใช้งานของระบบ เพื่อปรับปรุงแนวทางการใช้งานเพื่อให้ระบบที่พัฒนาขึ้นมาสามารถตอบสนองต่อการใช้งานของผู้ใช้งานและเป็นไปตามวัตถุประสงค์ของการพัฒนาระบบ

ตารางที่ 14 แสดงสถิติการใช้งานระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log Files) ของสำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช จำนวน 90 วัน ระหว่างวันที่ 24 กันยายน พ.ศ. 2566 ถึงวันที่ 22 ธันวาคม พ.ศ. 2566

ลำดับ	วันที่	จำนวนผู้ใช้งาน (คน)	จำนวนอุปกรณ์ที่ เข้าใช้งาน (เครื่อง)	รหัสผ่านผิดพลาด (ครั้ง)	การเข้าใช้งานที่ไม่ได้ ลงทะเบียน (ครั้ง)
1	24/09/2023	12	19	12	0
2	25/09/2023	106	188	196	6
3	26/09/2023	102	169	175	1
4	27/09/2023	92	161	172	4
5	28/09/2023	93	156	204	41
6	29/09/2023	76	121	135	7
7	30/09/2023	14	23	29	3
8	1/10/2023	9	12	39	27
9	2/10/2023	100	166	180	12
10	3/10/2023	106	186	195	2
11	4/10/2023	113	193	195	0
12	5/10/2023	108	188	201	9
13	6/10/2023	110	188	199	6
14	7/10/2023	19	25	22	0
15	8/10/2023	10	15	13	0
16	9/10/2023	101	172	177	4
17	10/10/2023	100	169	177	4
18	11/10/2023	107	188	199	2
19	12/10/2023	102	182	186	0
20	13/10/2023	11	16	9	0

ลำดับ	วันที่	จำนวนผู้เข้าใช้งาน (คน)	จำนวนอุปกรณ์ที่ เข้าใช้งาน (เครื่อง)	รหัสผ่านผิดพลาด (ครั้ง)	การเข้าใช้งานที่ไม่ได้ ลงทะเบียน (ครั้ง)
21	14/10/2023	5	6	2	0
22	15/10/2023	5	5	5	0
23	16/10/2023	105	173	184	10
24	17/10/2023	109	191	212	12
25	18/10/2023	104	179	203	14
26	19/10/2023	97	163	167	0
27	20/10/2023	98	174	176	0
28	21/10/2023	17	25	13	0
29	22/10/2023	10	16	12	0
30	23/10/2023	12	20	18	0
31	24/10/2023	110	189	205	13
32	25/10/2023	113	184	184	0
33	26/10/2023	111	183	193	1
34	27/10/2023	107	172	174	0
35	28/10/2023	17	27	22	0
36	29/10/2023	12	21	17	0
37	30/10/2023	93	154	165	9
38	31/10/2023	111	190	196	0
39	1/11/2023	109	186	190	0
40	2/11/2023	110	193	209	10
41	3/11/2023	105	168	171	0
42	4/11/2023	12	19	14	0
43	5/11/2023	8	11	7	0
44	6/11/2023	115	198	224	26
45	7/11/2023	117	203	218	5
46	8/11/2023	115	190	192	0
47	9/11/2023	118	198	215	8
48	10/11/2023	117	197	208	0

ลำดับ	วันที่	จำนวนผู้เข้าใช้งาน (คน)	จำนวนอุปกรณ์ที่ เข้าใช้งาน (เครื่อง)	รหัสผ่านผิดพลาด (ครั้ง)	การเข้าใช้งานที่ไม่ได้ ลงทะเบียน (ครั้ง)
49	11/11/2023	16	24	26	0
50	12/11/2023	9	14	100	83
51	13/11/2023	108	188	274	83
52	14/11/2023	113	203	208	8
53	15/11/2023	98	138	144	7
54	16/11/2023	8	8	12	4
55	17/11/2023	111	187	201	14
56	18/11/2023	19	26	21	0
57	19/11/2023	7	8	6	0
58	20/11/2023	117	198	210	8
59	21/11/2023	109	181	195	0
60	22/11/2023	111	198	192	0
61	23/11/2023	109	188	196	0
62	24/11/2023	115	189	197	0
63	25/11/2023	15	22	17	0
64	26/11/2023	11	15	51	30
65	27/11/2023	108	172	272	95
66	28/11/2023	109	170	256	83
67	29/11/2023	83	122	216	84
68	30/11/2023	86	133	227	91
69	1/12/2023	83	139	234	84
70	2/12/2023	16	21	104	78
71	3/12/2023	10	13	92	79
72	4/12/2023	96	158	163	4
73	5/12/2023	10	14	11	0
74	6/12/2023	118	192	205	9
75	7/12/2023	112	180	184	0
76	8/12/2023	96	174	177	0

ลำดับ	วันที่	จำนวนผู้เข้าใช้งาน (คน)	จำนวนอุปกรณ์ที่ เข้าใช้งาน (เครื่อง)	รหัสผ่านผิดพลาด (ครั้ง)	การเข้าใช้งานที่ไม่ได้ ลงทะเบียน (ครั้ง)
77	9/12/2023	15	21	16	0
78	10/12/2023	9	11	10	0
79	11/12/2023	13	18	21	2
80	12/12/2023	96	177	210	33
81	13/12/2023	90	151	159	0
82	14/12/2023	91	152	162	0
83	15/12/2023	96	170	302	112
84	16/12/2023	21	30	133	95
85	17/12/2023	10	16	30	12
86	18/12/2023	98	169	175	6
87	19/12/2023	97	165	175	4
88	20/12/2023	99	172	179	0
89	21/12/2023	95	172	184	2
90	22/12/2023	101	171	183	0
รวม		6,587	11,042	12,641	1,346

จากตารางที่ 14 สถิติการใช้งานระบบการยืนยันตัวบุคคลเพื่อเข้าใช้งานระบบเครือข่ายอินเทอร์เน็ตของสำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช เป็นเวลาจำนวน 90 วัน ช่วงระหว่างวันที่ 24 กันยายน พ.ศ. 2566 ถึงวันที่ 22 ธันวาคม พ.ศ. 2566

ผลการวิเคราะห์ข้อมูลจากตารางที่ 14 ได้ผลดังนี้

1. จำนวนผู้เข้าใช้งานสูงสุดต่อวัน 118 คน มีจำนวนอุปกรณ์เข้าใช้งานสูงสุดต่อวัน 203 แสดงให้เห็นถึงจำนวนอุปกรณ์ที่มีการใช้งานมากกว่า 1 คนต่อ 1 เครื่อง สามารถนำผลที่ได้มาปรับปรุงออกแบบนโยบายการจำกัดอุปกรณ์เข้าใช้งาน 1 คนใช้งานได้ 3 อุปกรณ์

2. จำนวนผู้เข้าใช้งานที่ลงชื่อเข้าใช้ผิดพลาดสูงสุดต่อวันจำนวน 302 ครั้ง สามารถนำผลที่ได้มาวิเคราะห์หาสาเหตุ คือ ปัญหาความเข้าใจในการใช้งานระบบของผู้ใช้งานยังมีค่อนข้างน้อย หรือเป็นการพยายามโจมตีการเข้าใช้งานระบบเครือข่ายอินเทอร์เน็ตแบบโจมตีการเข้าใช้งานแบบสุ่มรหัสผ่าน (brute force attack) นำไปสู่การวางแผนออกแบบการป้องกันปัญหาที่เกิดขึ้นต่อไป

3. จำนวนผู้ใช้งานที่พยายามเข้าสู่ระบบผ่านชื่อผู้ใช้ที่ไม่ได้ลงทะเบียนสูงสุดต่อวันจำนวน 112 ครั้ง แสดงให้เห็นถึงการพยายามใช้งานระบบจากผู้ที่ไม่ได้รับอนุญาต สามารถนำผลที่ได้ไปออกแบบ Policy ป้องกันการโจมตีบน Firewall เพื่อให้ทำการปิดกั้น IP Address ที่มีการพยายามเข้าใช้แบบปกติได้

## 2. การวัดผลการพัฒนาระบบ

จากข้อมูลการประเมินการพัฒนาระบบสามารถประเมินคะแนนความสามารถการทำงานของระบบที่อ้างอิงจากวัตถุประสงค์ของการพัฒนาระบบ เพื่อให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงสาธารณสุข พ.ศ. 2565 และพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 ฉบับที่ 2 โดยในแต่ละประเด็นจะมีคะแนนเต็มอยู่ที่ 1 คะแนน ซึ่งได้ผลคะแนนจากการประเมินดังนี้

ตารางที่ 15 ผลการประเมิน

รายละเอียดการวัดผล	คะแนน	คะแนนเต็ม
<b>1. การควบคุมการเข้าถึงและการทำงานของระบบสารสนเทศ</b>		<b>1</b>
1.1 มีการควบคุมการเข้าถึงเครือข่าย	0.25	0.25
1.2 มีการควบคุมการเข้าถึงอุปกรณ์	0	0.25
1.3 มีการกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตการเข้าถึง	0	0.25
1.4 มีการกำหนดนโยบายเพื่อให้บุคลากรสามารถปฏิบัติตามแนวทางได้	0.25	0.25
<b>2. มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน</b>		<b>1</b>
2.1 มีการกำหนดให้มีการลงทะเบียนผู้ใช้งาน	0.5	0.5
2.2 มีการบริหารจัดการสิทธิ์การเข้าถึงข้อมูล	0.5	0.5
<b>3. สามารถควบคุมการเข้าถึงเครือข่าย</b>		<b>1</b>
3.1 มีการกำหนดให้ใช้การลงชื่อเข้าใช้ (Login) เพื่อแสดงตัวตนผู้ใช้งาน	0.33	0.33
3.2 มีการกำหนดให้ต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยรหัสผ่าน	0.33	0.33
3.3 มีการออกแบบเครือข่ายโดยแบ่งเขตการใช้งาน	0.33	0.33
<b>4. มีการควบคุมการเข้าถึงระบบปฏิบัติการและโปรแกรมประยุกต์</b>		<b>1</b>
4.1 มีการป้องกันการเข้าถึงระบบปฏิบัติการด้วยการลงชื่อเข้าใช้งานด้วยรหัสผ่าน	0.5	0.5
4.2 มีการควบคุมการเข้าถึงโปรแกรมประยุกต์และแอปพลิเคชัน	0	0.5
<b>5.สามารถเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์</b>	<b>1</b>	<b>1</b>
<b>รวม</b>	<b>4</b>	<b>5</b>

จากตารางที่ 15 แสดงให้เห็นผลการประเมินคะแนนจากเกณฑ์คะแนนที่ได้กำหนดไว้ โดยแบ่งการประเมินออกเป็น 5 ประเด็นคือ

การควบคุมการเข้าถึงและการทำงานของระบบสารสนเทศ มีคะแนนเต็ม 1 คะแนน แบ่งเกณฑ์การให้คะแนนออกเป็น 4 หัวข้อย่อย ได้แก่ มีการควบคุมการเข้าถึงเครือข่าย คะแนนเต็ม 0.25 คะแนน โดยได้คะแนนอยู่ที่ 0.25 คะแนน เพราะมีการควบคุมการเข้าถึงเครือข่ายอินเทอร์เน็ต มีการควบคุมการเข้าถึงอุปกรณ์คะแนนเต็ม 0.25 โดยได้คะแนนอยู่ที่ 0 คะแนน เนื่องจากระบบการยืนยันตัวตนบุคคลเพื่อเข้าใช้งานอินเทอร์เน็ตไม่ได้ครอบคลุมถึงการควบคุมสิทธิ์การเข้าใช้งานอุปกรณ์ แต่อุปกรณ์จะไม่สามารถเข้าถึงเครือข่ายอินเทอร์เน็ตได้หากไม่ได้รับการยืนยันสิทธิ์ มีการกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตการเข้าถึง คะแนนเต็ม 0.25 โดยได้คะแนนอยู่ที่ 0 คะแนน เนื่องจากระบบไม่ได้กำหนดลำดับขั้นในการเข้าถึงสิทธิ์การใช้งานเนื่องจากปัจจุบันยังไม่มีกำหนดลำดับขั้นการเข้าถึงสิทธิ์การใช้งานของบุคลากรภายในหน่วยงาน จึงมีสิทธิ์การเข้าใช้งานแค่ได้รับสิทธิ์หรือไม่ได้รับสิทธิ์เท่านั้น มีการกำหนดนโยบายเพื่อให้บุคลากรสามารถปฏิบัติตามแนวทางได้ คะแนนเต็ม 0.25 โดยได้คะแนนอยู่ที่ 0.25 คะแนน เพราะมีการประกาศนโยบายแนวปฏิบัติให้บุคลากรในหน่วยงานรับทราบ

มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน แบ่งออกเป็น 2 ประเด็นคือ มีการกำหนดให้มีการลงทะเบียนผู้ใช้งาน คะแนนเต็ม 0.5 ได้คะแนน 0.5 เพราะมีการลงทะเบียนผู้เข้าใช้งาน มีการบริหารจัดการสิทธิ์การเข้าถึงข้อมูล คะแนนเต็ม 0.5 ได้คะแนน 0.5 เพราะมีการจำกัดสิทธิ์ผู้มีสิทธิ์ใช้งานและไม่มีสิทธิ์การใช้งาน

สามารถควบคุมการเข้าถึงเครือข่าย แบ่งออกเป็น 3 ประเด็นคือ มีการกำหนดให้ใช้การลงชื่อเข้าใช้ (Login) เพื่อแสดงตัวตนผู้ใช้งาน คะแนน 0.33 ได้คะแนน 0.33 เพราะมีการ Login เข้าใช้งาน มีการกำหนดให้ต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยรหัสผ่าน คะแนน 0.33 ได้คะแนน 0.33 เพราะมีการงานพิสูจน์ยืนยันตัวตนด้วยรหัสผ่าน มีการออกแบบเครือข่ายโดยแบ่งเขตการใช้งาน คะแนนเต็ม 0.33 ได้คะแนน 0.33 เพราะมีการแบ่งเขตการใช้งานของเครือข่าย

มีการควบคุมการเข้าถึงระบบปฏิบัติการและโปรแกรมประยุกต์แบ่งออกเป็น 2 ประเด็นคือ มีการป้องกันการเข้าถึงระบบปฏิบัติการด้วยการลงชื่อเข้าใช้งานด้วยรหัสผ่าน คะแนนเต็ม 0.5 ได้คะแนน 0.5 เพราะมีนโยบายให้มีการป้องกันเข้าใช้งานระบบปฏิบัติการด้วยรหัสผ่าน มีการควบคุมการเข้าถึงโปรแกรมประยุกต์และแอปพลิเคชัน คะแนนเต็ม 0.5 ได้คะแนน 0 เพราะระบบไม่ได้ครอบคลุมถึงการจำกัดสิทธิ์การเข้าใช้งานโปรแกรมประยุกต์

สามารถเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ มีประเด็นการให้คะแนน 1 ประเด็นคะแนนเต็ม 1 คะแนน ได้คะแนน 1 คะแนน เพราะระบบมีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ไม่น้อยกว่าเก้าสิบวัน



### 3. แบบสอบถามประเมินประสิทธิภาพ

ผลการศึกษาจากการรวบรวมข้อมูล ผู้วิจัยได้รวบรวมข้อมูลจากแบบสอบถามนำมาวิเคราะห์ข้อมูลทางสถิติ จากกลุ่มตัวอย่างจำนวนทั้งสิ้น 114 ชุด ได้ผลดังนี้

ส่วนที่ 1 แสดงข้อมูลลักษณะทั่วไปของบุคลากรในสำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช และ ศตม.11.2 นครศรีธรรมราช จากข้อมูลผลการศึกษสามารถแบ่งได้ดังนี้

ตารางที่ 16 ผลการศึกษาปัจจัยส่วนบุคคล แยกตามช่วงอายุ

ช่วงอายุ	กลุ่มตัวอย่าง(คน) N = 114	ร้อยละ
21-30 ปี	22	19.30
31-40 ปี	38	33.33
41-50 ปี	29	25.44
51-60 ปี	25	21.93

จากตารางที่ 16 แสดงผลให้เห็นถึงผลการศึกษาข้อมูลปัจจัยส่วนบุคคล ด้านอายุของกลุ่มตัวอย่าง ผู้ตอบแบบสอบถาม จำนวนทั้งสิ้น 114 คน อายุ 21 ถึง 30 ปี จำนวน 22 คน คิดเป็นร้อยละ 19.30 อายุตั้งแต่ 31 ถึง 40 ปี จำนวน 38 คน คิดเป็นร้อยละ 33.33 อายุตั้งแต่ 41 ถึง 50 ปี จำนวน 29 คน คิดเป็นร้อยละ 25.44 อายุตั้งแต่ 51 ถึง 60 ปี จำนวน 25 คนคิดเป็นร้อยละ 21.93 สรุปได้ว่ากลุ่มตัวอย่างที่ตอบแบบสอบถามส่วนใหญ่จะมีอายุ 31 ถึง 40 ปี มากที่สุด และอายุ 21 ถึง 30 ปี น้อยที่สุด

ตารางที่ 17 ผลการศึกษาปัจจัยส่วนบุคคล ด้านกลุ่มที่ปฏิบัติงาน

กลุ่มงาน	กลุ่มตัวอย่าง(คน) N = 114	ร้อยละ
กลุ่มบริหารทั่วไป	19	16.67
กลุ่มพัฒนาองค์กร	5	4.39
กลุ่มยุทธศาสตร์ แผนงานและเครือข่าย	9	7.89
กลุ่มระบาดวิทยาและตอบโต้ฉุกเฉินฯ	10	8.77
กลุ่มโรคไม่ติดต่อ	6	5.26
กลุ่มโรคจากการประกอบอาชีพและสิ่งแวดล้อม	4	3.51
กลุ่มสื่อสารความเสี่ยงโรคและภัยสุขภาพ	6	5.26
กลุ่มพัฒนานวัตกรรมและวิจัย	2	1.75

กลุ่มงาน	กลุ่มตัวอย่าง(คน) N = 114	ร้อยละ
กลุ่มห้องปฏิบัติการควบคุมโรคและภัยสุขภาพ	12	10.53
กลุ่มโรคติดต่อ	8	7.02
กลุ่มด้านควบคุมโรคติดต่อระหว่างประเทศ	2	1.75
กลุ่มโรคเอดส์ วัณโรค โรคติดต่อทางเพศสัมพันธ์และโรคเรื้อน	9	7.89
งานกฎหมาย	3	2.63
งานเภสัชกร	3	2.63
ศตม.11.2 นครศรีธรรมราช	16	14.04

จากตารางที่ 17 แสดงผลให้เห็นถึงผลการศึกษาปัจจัยส่วนบุคคล ด้านกลุ่มที่ปฏิบัติงานของกลุ่มตัวอย่าง ผู้ตอบแบบสอบถาม จำนวนทั้งสิ้น 114 คน กลุ่มบริหารทั่วไป จำนวน 19 คน คิดเป็นร้อยละ 16.67 กลุ่มพัฒนาองค์กร จำนวน 5 คน คิดเป็นร้อยละ 4.39 กลุ่มยุทธศาสตร์ แผนงานและเครือข่าย 9 คน คิดเป็นร้อยละ 7.89 กลุ่มระบาดวิทยาและตอบโต้ฉุกเฉินฯ จำนวน 10 คน คิดเป็นร้อยละ 8.77 กลุ่มโรคไม่ติดต่อ จำนวน 6 คน คิดเป็นร้อยละ 5.26 กลุ่มโรคจากการประกอบอาชีพและสิ่งแวดล้อม จำนวน 4 คน คิดเป็นร้อยละ 3.51 กลุ่มสื่อสารความเสี่ยงโรคและภัยสุขภาพ จำนวน 6 คน คิดเป็นร้อยละ 5.26 กลุ่มพัฒนานวัตกรรมและวิจัย จำนวน 2 คน คิดเป็นร้อยละ 1.75 กลุ่มห้องปฏิบัติการควบคุมโรคและภัยสุขภาพ จำนวน 12 คน คิดเป็นร้อยละ 10.53 กลุ่มโรคติดต่อ จำนวน 8 คน คิดเป็นร้อยละ 7.02 กลุ่มด้านควบคุมโรคติดต่อระหว่างประเทศ จำนวน 2 คน คิดเป็นร้อยละ 1.75 กลุ่มโรคเอดส์ วัณโรค โรคติดต่อทางเพศสัมพันธ์และโรคเรื้อน จำนวน 9 คน คิดเป็นร้อยละ 7.89 งานกฎหมาย จำนวน 3 คน คิดเป็นร้อยละ 2.63 งานเภสัชกร จำนวน 3 คน คิดเป็นร้อยละ 2.63 ศตม.11.2 นครศรีธรรมราช จำนวน 16 คน คิดเป็นร้อยละ 14.04 สรุปได้ว่ากลุ่มตัวอย่างที่ตอบแบบสอบถามส่วนใหญ่ เป็นกลุ่มบริหารทั่วไป มากที่สุด โดยกลุ่มพัฒนานวัตกรรมและวิจัย และกลุ่มด้านควบคุมโรคติดต่อระหว่างประเทศ มีจำนวนผู้ตอบแบบสอบถาม น้อยที่สุด

ตารางที่ 18 ผลการศึกษาปัจจัยด้านระดับการปฏิบัติงาน

ประเภทผู้ใช้งาน	กลุ่มตัวอย่าง(คน) N = 114	ร้อยละ
ผู้บริหารและหัวหน้ากลุ่ม	9	7.90
ผู้ปฏิบัติงาน	105	92.10
รวม	114	100

จากตารางที่ 18 แสดงผลให้เห็นถึงผลการศึกษาปัจจัยด้านระดับการปฏิบัติงานของกลุ่มตัวอย่าง ผู้ตอบแบบสอบถาม จำนวนทั้งสิ้น 114 คน ผู้บริหารและหัวหน้ากลุ่มจำนวน 9 คน คิดเป็นร้อยละ 7.90 ผู้ปฏิบัติงาน 105 คน คิดเป็นร้อยละ 92.10

ส่วนที่ 2 แสดงผลการประเมินความสำเร็จของระบบในการใช้งานระบบการยืนยันตัวบุคคล เพื่อเข้าใช้งานระบบเครือข่ายอินเทอร์เน็ตของสำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช จากบุคลากรภายในหน่วยงานซึ่งได้มีการให้คะแนนความสำเร็จของระบบเกี่ยวกับการใช้งานระบบโดยแบ่งเป็น 4 ปัจจัย ดังนี้

- 1) ด้านประสิทธิภาพของระบบ
- 2) ด้านความสำคัญของการป้องกันระบบ
- 3) ด้านความน่าเชื่อถือ
- 4) ด้านคุณภาพการบริการ

โดยได้กำหนดคะแนนของคำถามไว้ดังนี้

น้อยที่สุด	ค่าคะแนนเท่ากับ 1
น้อย	ค่าคะแนนเท่ากับ 2
ปานกลาง	ค่าคะแนนเท่ากับ 3
มาก	ค่าคะแนนเท่ากับ 4
มากที่สุด	ค่าคะแนนเท่ากับ 5

แปลความหมายจากระดับค่าคะแนนเฉลี่ย ดังนี้

คะแนนเฉลี่ย 4.21–5.00 หมายถึง มากที่สุด

คะแนนเฉลี่ย 3.41–4.20 หมายถึง มาก

คะแนนเฉลี่ย 2.61–3.40 หมายถึง ปานกลาง

คะแนนเฉลี่ย 1.81–2.60 หมายถึง น้อย

คะแนนเฉลี่ย 1.00–1.80 หมายถึง น้อยที่สุด

### ด้านประสิทธิภาพของระบบ

การประเมินความสำเร็จของระบบด้านประสิทธิภาพของระบบโดยแบ่งการวิเคราะห์ออกเป็น 3 ส่วน คือ ผู้บริหารและหัวหน้ากลุ่ม ผู้ปฏิบัติงาน และบุคลากรกลุ่มเป้าหมายทั้งหมด

ตารางที่ 19 แสดงผลการประเมินความสำเร็จของระบบด้านประสิทธิภาพของระบบ ของผู้บริหารและหัวหน้ากลุ่ม

ประเด็นความคิดเห็น	$\bar{x}$	S.D.	การแปลผล
ความเข้าใจเกี่ยวกับวิธีการใช้งานการยืนยันตัวตนบุคคล	4.11	0.93	มาก
ความสามารถในการใช้การยืนยันตัวตนบุคคลด้วยตนเอง	4.67	0.50	มากที่สุด
ความรวดเร็วของกระบวนการยืนยันตัวตนบุคคลเมื่อต้องการเข้าใช้งาน	4.44	0.73	มากที่สุด
ความสะดวกและง่ายต่อการเข้าใช้ระบบ	4.40	0.62	มากที่สุด
ค่าเฉลี่ยคะแนนด้านประสิทธิภาพของระบบ	4.42	0.72	มากที่สุด

ตารางที่ 20 แสดงผลการประเมินความสำเร็จของระบบด้านประสิทธิภาพของระบบ ของผู้ปฏิบัติงาน

ประเด็นความคิดเห็น	$\bar{x}$	S.D.	การแปลผล
ความเข้าใจเกี่ยวกับวิธีการใช้งานการยืนยันตัวตนบุคคล	4.20	0.66	มาก
ความสามารถในการใช้การยืนยันตัวตนบุคคลด้วยตนเอง	4.72	0.49	มากที่สุด
ความรวดเร็วของกระบวนการยืนยันตัวตนบุคคลเมื่อต้องการเข้าใช้งาน	4.33	0.70	มากที่สุด
ความสะดวกและง่ายต่อการเข้าใช้ระบบ	4.39	0.63	มากที่สุด
ค่าเฉลี่ยคะแนนด้านประสิทธิภาพของระบบ	4.41	0.62	มากที่สุด

ตารางที่ 21 แสดงผลการประเมินความสำเร็จของระบบด้านประสิทธิภาพของระบบ

ประเด็นความคิดเห็น	$\bar{x}$	S.D.	การแปลผล
ความเข้าใจเกี่ยวกับวิธีการใช้งานการยืนยันตัวตนบุคคล	4.17	0.67	มาก
ความสามารถในการใช้การยืนยันตัวตนบุคคลด้วยตนเอง	4.73	0.48	มากที่สุด
ความรวดเร็วของกระบวนการยืนยันตัวตนบุคคลเมื่อต้องการเข้าใช้งาน	4.34	0.71	มากที่สุด
ความสะดวกและง่ายต่อการเข้าใช้ระบบ	4.40	0.62	มากที่สุด
ค่าเฉลี่ยคะแนนด้านประสิทธิภาพของระบบ	4.41	0.62	มากที่สุด

จากตารางที่ 19 - 21 แสดงผลให้เห็นผลการวิเคราะห์การประเมินความสำเร็จของระบบด้านประสิทธิภาพของระบบ สามารถสรุปได้ดังนี้

ผู้ปฏิบัติงาน มีความเข้าใจเกี่ยวกับวิธีการใช้งานการยืนยันตัวบุคคลอยู่ที่ 4.20 ซึ่งมากกว่าผู้บริหาร และหัวหน้ากลุ่มที่มีผลคะแนนอยู่ที่ 4.11 โดยมีผลคะแนนภาพรวมอยู่ที่ 4.17 สามารถแปรผลได้ว่ากลุ่มตัวอย่างทั้งหมดมีความเข้าใจเกี่ยวกับวิธีการใช้งานการยืนยันตัวบุคคลอยู่ในระดับมาก

ผู้ปฏิบัติงาน มีความสามารถในการใช้การยืนยันตัวบุคคลด้วยตนเองอยู่ที่ 4.72 ซึ่งมากกว่าผู้บริหาร และหัวหน้ากลุ่มที่มีผลคะแนนอยู่ที่ 4.67 โดยมีผลคะแนนภาพรวมอยู่ที่ 4.73 สามารถแปรผลได้ว่ากลุ่มตัวอย่างทั้งหมดมีความสามารถในการใช้การยืนยันตัวบุคคลด้วยตนเองอยู่ในระดับมากที่สุด

ผู้บริหารและหัวหน้ากลุ่ม มีการให้คะแนนต่อความรวดเร็วของกระบวนการยืนยันตัวบุคคลเมื่อต้องการเข้าใช้งานอยู่ที่ 4.44 ซึ่งมากกว่าผู้ปฏิบัติงานที่มีผลคะแนนอยู่ที่ 4.33 โดยมีผลคะแนนภาพรวมอยู่ที่ 4.34 สามารถแปรผลได้ว่ากลุ่มตัวอย่างทั้งหมดมีความเห็นต่อความรวดเร็วของกระบวนการยืนยันตัวบุคคลเมื่อต้องการเข้าใช้งานอยู่ในระดับมากที่สุด

ผู้บริหารและหัวหน้ากลุ่ม มีการให้คะแนนต่อความสะดวกและง่ายต่อการเข้าใช้ระบบอยู่ที่ 4.40 ซึ่งมากกว่าผู้ปฏิบัติงานที่มีผลคะแนนอยู่ที่ 4.39 โดยมีผลคะแนนภาพรวมอยู่ที่ 4.40 สามารถแปรผลได้ว่ากลุ่มตัวอย่างทั้งหมดมีความเห็นต่อความสะดวกและง่ายต่อการเข้าใช้ระบบอยู่ในระดับมากที่สุด

กลุ่มตัวอย่างภาพรวม มีความสามารถในการใช้การยืนยันตัวบุคคลด้วยตนเองอยู่ในระดับสูงสุดอยู่ที่ 4.73 และมีความเข้าใจเกี่ยวกับวิธีการใช้งานการยืนยันตัวบุคคลอยู่ในระดับที่น้อยที่สุดอยู่ที่ 4.17

### ด้านความสำคัญของการป้องกันระบบ

การประเมินความสำเร็จของระบบด้านความสำคัญของการป้องกันระบบโดยแบ่งการวิเคราะห์ออกเป็น 3 ส่วน คือ ผู้บริหารและหัวหน้ากลุ่ม ผู้ปฏิบัติงาน และ บุคลากรกลุ่มเป้าหมายทั้งหมด

ตารางที่ 22 แสดงผลการประเมินความสำเร็จของระบบด้านความสำคัญของการป้องกันระบบ ของผู้บริหารและหัวหน้ากลุ่ม

ประเด็นความคิดเห็น	$\bar{x}$	S.D.	การแปรผล
ความเข้าใจเกี่ยวกับข้อกำหนดและเงื่อนไขของการยืนยันตัวบุคคล	4.56	0.73	มากที่สุด
ความสำคัญของการรักษาความปลอดภัยของข้อมูลขณะใช้งานอินเทอร์เน็ต	5.00	0.0	มากที่สุด
ความสำคัญของการป้องกันการเข้าถึงที่ไม่ได้รับอนุญาตในการใช้งานอินเทอร์เน็ต	4.78	0.44	มากที่สุด
ค่าเฉลี่ยคะแนนด้านความสำคัญของการป้องกันระบบ	4.78	0.39	มากที่สุด

ตารางที่ 23 การประเมินความสำเร็จของระบบด้านความสำคัญของการป้องกันระบบ ของผู้ปฏิบัติงาน

ประเด็นความคิดเห็น	$\bar{x}$	S.D.	การแปลผล
ความเข้าใจเกี่ยวกับข้อกำหนดและเงื่อนไขของการยืนยันตัวบุคคล	4.20	0.69	มาก
ความสำคัญของการรักษาความปลอดภัยของข้อมูลขณะใช้งานอินเทอร์เน็ต	4.52	0.54	มากที่สุด
ความสำคัญของการป้องกันการเข้าถึงที่ไม่ได้รับอนุญาตในการใช้งานอินเทอร์เน็ต	4.41	0.58	มากที่สุด
ค่าเฉลี่ยคะแนนด้านความสำคัญของการป้องกันระบบ	4.38	0.60	มากที่สุด

ตารางที่ 24 แสดงผลการประเมินความสำเร็จของระบบด้านความสำคัญของการป้องกันระบบ

ประเด็นความคิดเห็น	$\bar{x}$	S.D.	การแปลผล
ความเข้าใจเกี่ยวกับข้อกำหนดและเงื่อนไขของการยืนยันตัวบุคคล	4.19	0.69	มาก
ความสำคัญของการรักษาความปลอดภัยของข้อมูลขณะใช้งานอินเทอร์เน็ต	4.56	0.53	มากที่สุด
ความสำคัญของการป้องกันการเข้าถึงที่ไม่ได้รับอนุญาตในการใช้งานอินเทอร์เน็ต	4.43	0.59	มากที่สุด
ค่าเฉลี่ยคะแนนด้านความสำคัญของการป้องกันระบบ	4.40	0.60	มากที่สุด

จากตารางที่ 22 - 24 แสดงผลให้เห็นผลการประเมินความสำเร็จของระบบด้านความสำคัญของการป้องกันระบบ สามารถสรุปได้ดังนี้

ผู้บริหารและหัวหน้ากลุ่ม มีความเข้าใจเกี่ยวกับข้อกำหนด และเงื่อนไขของการยืนยันตัวบุคคลอยู่ที่ 4.56 ซึ่งมากกว่าผู้ปฏิบัติงานที่มีผลคะแนนอยู่ที่ 4.20 โดยมีผลคะแนนภาพรวมอยู่ที่ 4.19 สามารถแปลผลได้ว่าผู้บริหารและหัวหน้ากลุ่มมีความเข้าใจเกี่ยวกับข้อกำหนด และเงื่อนไขของการยืนยันตัวบุคคลอยู่ในระดับมากที่สุด ผู้ปฏิบัติงานมีความเข้าใจเกี่ยวกับข้อกำหนด และเงื่อนไขของการยืนยันตัวบุคคลอยู่ในระดับมาก

ผู้บริหารและหัวหน้ากลุ่ม เห็นความสำคัญของการรักษาความปลอดภัยของข้อมูลขณะใช้งานอินเทอร์เน็ตอยู่ที่ 5.00 ซึ่งมากกว่าผู้ปฏิบัติงานที่มีผลคะแนนอยู่ที่ 4.52 โดยมีผลคะแนนภาพรวมอยู่ที่ 4.56 สามารถแปลผลได้ว่ากลุ่มตัวอย่างทั้งหมดเห็นความสำคัญของการรักษาความปลอดภัยของข้อมูลขณะใช้งานอินเทอร์เน็ตอยู่ในระดับมากที่สุด

ผู้บริหารและหัวหน้ากลุ่ม เห็นความสำคัญของการป้องกันการเข้าถึงที่ไม่ได้รับอนุญาตในการใช้งานอินเทอร์เน็ตอยู่ที่ 4.78 ซึ่งมากกว่าผู้ปฏิบัติงานที่มีผลคะแนนอยู่ที่ 4.41 โดยมีผลคะแนนภาพรวมอยู่ที่ 4.43 สามารถแปลผลได้ว่ากลุ่มตัวอย่างทั้งหมดเห็นความสำคัญของการป้องกันการเข้าถึงที่ไม่ได้รับอนุญาตในการใช้งานอินเทอร์เน็ตอยู่ในระดับมากที่สุด

กลุ่มตัวอย่างภาพรวม มีความเข้าใจเกี่ยวกับข้อกำหนด และเงื่อนไขของการยืนยันตัวบุคคลน้อยที่สุด ซึ่งมีค่าคะแนนอยู่ที่ 4.19 และเห็นความสำคัญของการรักษาความปลอดภัยของข้อมูลขณะใช้งาน อินเทอร์เน็ตอยู่ในระดับสูงที่สุด โดยมีค่าคะแนนอยู่ที่ 4.56

### ด้านความน่าเชื่อถือ

ตารางที่ 25 แสดงผลการประเมินความสำเร็จของระบบด้านความน่าเชื่อถือของระบบของผู้บริหารและหัวหน้ากลุ่ม

ประเด็นความคิดเห็น	$\bar{x}$	S.D.	การแปลผล
ระดับความปลอดภัยของระบบยืนยันตัวบุคคล	4.33	0.71	มากที่สุด
ความพร้อมของระบบยืนยันตัวบุคคลต่อการป้องกันการแฮกเกอร์หรือการละเมิดความปลอดภัย	4.22	0.44	มากที่สุด
ระดับความน่าเชื่อถือของระบบยืนยันตัวบุคคล	4.33	0.71	มากที่สุด
ค่าเฉลี่ยคะแนนด้านความน่าเชื่อถือ	4.30	0.62	มากที่สุด

ตารางที่ 26 แสดงผลการประเมินความสำเร็จของระบบด้านความน่าเชื่อถือของระบบของผู้ปฏิบัติงาน

ประเด็นความคิดเห็น	$\bar{x}$	S.D.	การแปลผล
ระดับความปลอดภัยของระบบยืนยันตัวบุคคล	4.16	0.71	มาก
ความพร้อมของระบบยืนยันตัวบุคคลต่อการป้องกันการแฮกเกอร์หรือการละเมิดความปลอดภัย	4.17	0.63	มาก
ระดับความน่าเชื่อถือของระบบยืนยันตัวบุคคล	4.27	0.72	มากที่สุด
ค่าเฉลี่ยคะแนนด้านความน่าเชื่อถือ	4.20	0.69	มาก

ตารางที่ 27 แสดงผลการประเมินความสำเร็จของระบบด้านความน่าเชื่อถือของระบบ

ประเด็นความคิดเห็น	$\bar{x}$	S.D.	การแปลผล
ระดับความปลอดภัยของระบบยืนยันตัวบุคคล	4.15	0.71	มาก
ความพร้อมของระบบยืนยันตัวบุคคลต่อการป้องกันการแฮกเกอร์หรือการละเมิดความปลอดภัย	4.17	0.61	มาก
ระดับความน่าเชื่อถือของระบบยืนยันตัวบุคคล	4.25	0.72	มากที่สุด
ค่าเฉลี่ยคะแนนด้านความน่าเชื่อถือ	4.19	0.68	มาก

จากตารางที่ 25 - 27 แสดงผลให้เห็นผลการประเมินความสำเร็จของระบบด้านความน่าเชื่อถือสามารถสรุปได้ดังนี้

ผู้บริหารและหัวหน้ากลุ่ม มีความเชื่อมั่นต่อระดับความปลอดภัยของระบบยืนยันตัวบุคคลอยู่ที่ 4.33 ซึ่งมากกว่าผู้ปฏิบัติงานที่มีผลคะแนนอยู่ที่ 4.16 สามารถแปลผลได้ว่าผู้บริหารและหัวหน้ากลุ่มมีความเชื่อมั่นต่อระดับความปลอดภัยของระบบยืนยันตัวบุคคลอยู่ในระดับมากที่สุด ผู้ปฏิบัติงานมีความเชื่อมั่นต่อระดับความปลอดภัยของระบบยืนยันตัวบุคคลอยู่ในระดับมาก

ผู้บริหารและหัวหน้ากลุ่ม มีความเชื่อมั่นต่อความพร้อมของระบบยืนยันตัวบุคคลต่อการป้องกันการแฮกเกอร์หรือการละเมิดความปลอดภัยอยู่ที่ 4.22 ซึ่งมากกว่าผู้ปฏิบัติงานที่มีผลคะแนนอยู่ที่ 4.17 สามารถแปลผลได้ว่าผู้บริหารและหัวหน้ากลุ่มมีความเชื่อมั่นความพร้อมของระบบยืนยันตัวบุคคลต่อการป้องกันการแฮกเกอร์หรือการละเมิดความปลอดภัยอยู่ในระดับมากที่สุด ผู้ปฏิบัติงานมีความเชื่อมั่นต่อความพร้อมของระบบยืนยันตัวบุคคลต่อการป้องกันการแฮกเกอร์หรือการละเมิดความปลอดภัยอยู่ในระดับมาก

ผู้บริหารและหัวหน้ากลุ่ม มีความเชื่อมั่นต่อความน่าเชื่อถือของระบบยืนยันตัวบุคคลอยู่ที่ 4.33 ซึ่งมากกว่าผู้ปฏิบัติงานที่มีผลคะแนนอยู่ที่ 4.27 สามารถแปลผลได้ว่ากลุ่มตัวอย่างทั้งหมด มีความเชื่อมั่นต่อความน่าเชื่อถือของระบบยืนยันตัวบุคคลอยู่ในระดับมากที่สุด

กลุ่มตัวอย่างภาพรวม มีความเชื่อมั่นต่อระดับความปลอดภัยของระบบยืนยันตัวบุคคลอยู่ในระดับน้อยที่สุดซึ่งมีผลคะแนนอยู่ที่ 4.15 และมีความเชื่อมั่นต่อความน่าเชื่อถือของระบบยืนยันตัวบุคคลอยู่ในระดับสูงที่สุด โดยมีค่าคะแนนอยู่ที่ 4.25

### ด้านคุณภาพการบริการ

ตารางที่ 28 แสดงผลการประเมินความสำเร็จของระบบด้านคุณภาพการให้บริการของผู้บริหารและหัวหน้ากลุ่ม

ประเด็นความคิดเห็น	$\bar{x}$	S.D.	การแปลผล
การได้รับความรู้และการสนับสนุนในการใช้งานการยืนยันตัวตน	4.56	0.73	มากที่สุด
ระบบมีการแจ้งเตือนในกรณีเกิดข้อผิดพลาด	4.22	0.44	มากที่สุด
การได้รับการแก้ปัญหาในกรณีเกิดข้อผิดพลาด	4.78	0.44	มากที่สุด
ค่าเฉลี่ยคะแนนด้านคุณภาพการบริการ	4.52	0.54	มากที่สุด



ตารางที่ 29 แสดงผลการประเมินความสำเร็จของระบบด้านคุณภาพการให้บริการของผู้ปฏิบัติงาน

ประเด็นความคิดเห็น	$\bar{x}$	S.D.	การแปรผล
การได้รับความรู้และการสนับสนุนในการใช้งานการยืนยันตัวตน	4.44	0.59	มากที่สุด
ระบบมีการแจ้งเตือนในกรณีเกิดข้อผิดพลาด	4.10	0.65	มาก
การได้รับการแก้ไขปัญหาในกรณีเกิดข้อผิดพลาด	4.58	0.60	มากที่สุด
ค่าเฉลี่ยคะแนนด้านคุณภาพการบริการ	4.37	0.61	มากที่สุด

ตารางที่ 30 แสดงผลการประเมินความสำเร็จของระบบด้านคุณภาพการให้บริการ

ประเด็นความคิดเห็น	$\bar{x}$	S.D.	การแปรผล
การได้รับความรู้และการสนับสนุนในการใช้งานการยืนยันตัวตน	4.45	0.59	มากที่สุด
ระบบมีการแจ้งเตือนในกรณีเกิดข้อผิดพลาด	4.08	0.65	มาก
การได้รับการแก้ไขปัญหาในกรณีเกิดข้อผิดพลาด	4.60	0.58	มากที่สุด
ค่าเฉลี่ยคะแนนด้านคุณภาพการบริการ	4.38	0.61	มากที่สุด

จากตารางที่ 28 – 30 แสดงผลให้เห็นผลการประเมินความสำเร็จของระบบด้านคุณภาพการบริการสามารถสรุปได้ดังนี้

ผู้บริหารและหัวหน้ากลุ่ม ได้รับความรู้และการสนับสนุนในการใช้งานการยืนยันตัวตนอยู่ที่ 4.56 ซึ่งมากกว่าผู้ปฏิบัติงานที่มีผลคะแนนอยู่ที่ 4.44 สามารถแปรผลได้ว่ากลุ่มตัวอย่างทั้งหมด ได้รับความรู้และการสนับสนุนในการใช้งานการยืนยันตัวตนอยู่ในระดับมากที่สุด

ผู้บริหารและหัวหน้ากลุ่ม มีความเห็นว่าระบบมีการแจ้งเตือนในกรณีเกิดข้อผิดพลาดถูกต้องอยู่ที่ 4.22 ซึ่งมากกว่าผู้ปฏิบัติงานที่มีผลคะแนนอยู่ที่ 4.10 สามารถแปรผลได้ว่าผู้บริหารและหัวหน้ากลุ่มมีความเห็นว่าระบบมีการแจ้งเตือนในกรณีเกิดข้อผิดพลาดถูกต้องอยู่ในระดับมากที่สุด ผู้ปฏิบัติงานมีความเห็นว่าระบบมีการแจ้งเตือนในกรณีเกิดข้อผิดพลาดถูกต้องอยู่ในระดับมาก

ผู้บริหารและหัวหน้ากลุ่ม ได้รับการแก้ไขปัญหาในกรณีเกิดข้อผิดพลาดอยู่ที่ 4.78 ซึ่งมากกว่าผู้ปฏิบัติงานที่มีผลคะแนนอยู่ที่ 4.58 สามารถแปรผลได้ว่ากลุ่มตัวอย่างทั้งหมด ได้รับการแก้ไขปัญหาในกรณีเกิดข้อผิดพลาดอยู่ในระดับมากที่สุด

กลุ่มตัวอย่างภาพรวม มีความเห็นว่าระบบมีการแจ้งเตือนในกรณีเกิดข้อผิดพลาดถูกต้องอยู่ในระดับน้อยที่สุด ซึ่งมีผลคะแนนอยู่ที่ 4.08 และได้รับการแก้ไขปัญหาในกรณีเกิดข้อผิดพลาดอยู่ในระดับสูงสุด โดยมีผลคะแนนอยู่ที่ 4.60

## บทที่ 5

### บทสรุป และข้อเสนอแนะ

#### 5.1 สรุปผล

การพัฒนากระบวนการยืนยันตัวบุคคลเพื่อเข้าใช้งานระบบเครือข่ายอินเทอร์เน็ตของสำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช เป็นการพัฒนาระบบให้สามารถควบคุมการเข้าใช้งานเครือข่ายอินเทอร์เน็ตของสำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช โดยมีการใช้อุปกรณ์ที่ทำหน้าที่ตรวจสอบข้อมูลที่ผ่านเข้า-ออกระบบเครือข่าย (Firewall) ในการตรวจสอบการเข้าใช้งานแล้วตรวจสอบสิทธิ์การใช้งานบนฐานข้อมูลที่จัดเก็บอยู่ใน Active Directory บนระบบปฏิบัติการ Windows Server 2012 และบันทึกข้อมูลจราจรคอมพิวเตอร์ไว้บนเครื่องสำหรับการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log Server) โดยได้มีการดำเนินการปรับปรุงอย่างต่อเนื่องตามหลักการ PDCA (Plan-Do-Check-Act) จนระบบสามารถทำงานได้ตรงความต้องการและสามารถจัดเก็บข้อมูลจราจรคอมพิวเตอร์ได้ครบถ้วนตามที่กฎหมายกำหนดตั้งแต่วันที่ 24 กันยายน พ.ศ. 2566

ตารางที่ 31 ผลของการตรวจสอบการใช้งานระบบการยืนยันตัวบุคคลเพื่อเข้าใช้งานระบบเครือข่ายอินเทอร์เน็ต

จำนวนผู้ลงทะเบียนทั้งหมด (คน)	จำนวนผู้ใช้งาน	จำนวนผู้ใช้งานสูงสุด (คน)	จำนวนอุปกรณ์ที่เข้าใช้งานสูงสุด (เครื่อง)	จำนวนใช้รหัสผ่านผิดพลาดสูงสุด (ครั้ง)	การเข้าใช้งานที่ไม่ได้ลงทะเบียนสูงสุด (ครั้ง)
160	160	118	203	302	112

ผลของการตรวจสอบการใช้งานระบบการยืนยันตัวบุคคลเพื่อเข้าใช้งานระบบเครือข่ายอินเทอร์เน็ตของสำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช ตั้งแต่วันที่ 24 กันยายน พ.ศ. 2566 จนถึงวันที่ 22 ธันวาคม 2566 จำนวน 90 วัน พบว่าจากจำนวนผู้ลงทะเบียนเข้าใช้งานทั้งหมด 160 คน มีจำนวนผู้ใช้งานที่เข้าใช้งานระบบจำนวน 160 คน คิดเป็นร้อยละ 100 ของสถิติการใช้งานต่อวัน มีจำนวนผู้ใช้งานมากที่สุด จำนวน 118 ผู้ใช้งาน จำนวนอุปกรณ์ที่ใช้งานมากที่สุด จำนวน 203 อุปกรณ์ การใช้รหัสผ่านผิดพลาดมากที่สุดโดยบุคลากรภายในสำนักงาน 302 ครั้ง และการพยายามเข้าถึงเครือข่ายจากบุคคลที่ไม่ได้รับการกำหนดสิทธิ์ให้ใช้งานของสำนักงานป้องกันควบคุมโรคที่ 11 นครศรีธรรมราชมากที่สุด 112 ครั้ง

ผลแบบสอบถามประเมินประสิทธิผลและความสำเร็จของการใช้งานระบบ กลุ่มตัวอย่างที่ตอบแบบสอบถามจำนวน 114 คน ประกอบด้วยผู้บริหารและหัวหน้ากลุ่มจำนวน 9 คน และผู้ปฏิบัติงานจำนวน 105 คน แบบประเมินได้นำมาวิเคราะห์หาค่าทางสถิติ สถิติที่ใช้ประกอบด้วย ร้อยละ ค่าเฉลี่ย และส่วนเบี่ยงเบนมาตรฐาน ภาพรวมอยู่ในระดับมากที่สุดมีค่าเฉลี่ยอยู่ที่ 4.35 โดยประเด็นที่มีคะแนนมากที่สุดคือ

ประเด็นด้านประสิทธิภาพของระบบ มีค่าเฉลี่ย 4.41 รองลงมาคือประเด็นด้านความสำคัญของการป้องกันระบบ มีค่าเฉลี่ย 4.40 ประเด็นด้านคุณภาพการบริการ มีค่าเฉลี่ยคือ 4.38 และประเด็นด้านประเด็นด้านความน่าเชื่อถือมีค่าเฉลี่ยน้อยที่สุดคือ 4.19

ตารางที่ 32 แสดงผลการประเมินความสำเร็จของระบบในการใช้งานระบบใน 4 ปีวิจัย

ประเด็นความคิดเห็น	$\bar{x}$	S.D.	การแปรผล
ประเด็นด้านประสิทธิภาพของระบบ	4.41	0.62	มากที่สุด
ประเด็นด้านความสำคัญของการป้องกันระบบ	4.40	0.60	มากที่สุด
ประเด็นด้านความน่าเชื่อถือ	4.19	0.68	มากที่สุด
ประเด็นด้านคุณภาพการบริการ	4.38	0.61	มากที่สุด
ภาพรวมเฉลี่ย	4.35	0.63	มากที่สุด

## 5.2 การนำไปใช้ประโยชน์/ผลกระทบ

1. เพื่อให้สอดคล้องกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงสาธารณสุข พ.ศ. 2565 และสามารถจัดเก็บ สืบค้น ข้อมูลจราจรคอมพิวเตอร์ได้ไม่น้อยกว่าเก้าสิบวันตาม มาตรา 26 ของพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560

2. เพื่อยืนยันตัวบุคคลในการเข้าใช้งานระบบเครือข่ายอินเทอร์เน็ตของสำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช

3. เมื่อมีผู้กระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์สามารถตรวจสอบย้อนหลังจาก logfile ได้

4. การเข้าใช้งานระบบเครือข่ายอินเทอร์เน็ตของสำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช มีการเพิ่มกระบวนการโดยการต้องยืนยันตัวบุคคลด้วย ผู้ใช้งาน รหัสผ่าน เพื่อการยืนยันตัวบุคคล และการจำกัดจำนวนอุปกรณ์ที่ใช้งานเครือข่าย สำหรับบุคลากรในองค์กร

## 5.3 ความยุ่งยากและซับซ้อนในการดำเนินงาน

1. อุปกรณ์ไฟร์วอลล์ที่ใช้งานมีข้อจำกัดไม่สามารถเก็บฐานข้อมูลการยืนยันตัวบุคคลจึงจำเป็นต้องเชื่อมโยงการเก็บข้อมูลการยืนยันตัวบุคคลไว้บน Active Directory

2. การปรับเปลี่ยนวิธีการเข้าใช้งานระบบเครือข่ายอินเทอร์เน็ตของบุคลากรภายในหน่วยงาน

3. การเข้าใช้ระบบเครือข่ายจำเป็นต้องเปิดใช้งานตลอดเวลา ทำให้ต้องจัดเตรียมอุปกรณ์ที่เหมาะสมเพื่อให้ระบบสามารถทำงานได้อย่างต่อเนื่อง

## 5.4 ปัญหาและอุปสรรคในการดำเนินงาน

1. ข้อจำกัดทางด้านงบประมาณ ในการจัดซื้อเครื่องแม่ข่ายที่ใช้ในการเก็บข้อมูล log file และปรับปรุงระบบให้มีความทันสมัย
2. การลืมหุ้สผ่านในการเข้าใช้งานของบุคลากรในองค์กร เนื่องจากการเก็บข้อมูลใน Active Directory เป็นการเก็บข้อมูลในรูปแบบ ไบนารี จึงไม่สามารถดู รหัสผ่านได้ ต้องทำการ reset รหัสผ่านจากหน้าต่างการทำงานของ Active Directory
3. การสร้างความรู้ความเข้าใจเกี่ยวกับความจำเป็นในการยืนยันตัวบุคคลในการใช้งานอินเทอร์เน็ตให้แก่บุคลากรในองค์กร

## 5.5 ข้อเสนอแนะ

### ข้อเสนอแนะเชิงนโยบาย

1. ผู้บริหารควรสนับสนุนให้บุคลากรภายในหน่วยงานเห็นความสำคัญของการใช้งานระบบการยืนยันตัวบุคคล และการป้องกันเครือข่ายจากภัยคุกคามทางไซเบอร์ รวมถึงสนับสนุนด้านงบประมาณในการปรับปรุงอุปกรณ์ให้ทันสมัย
2. ควรวางแผนจัดหางบประมาณสำหรับปรับปรุงอุปกรณ์ป้องกันเครือข่ายเช่นอุปกรณ์วิเคราะห์ความเสี่ยงจากข้อมูลจราจรคอมพิวเตอร์ (Log Analyzer) หรือ อุปกรณ์ป้องกันการโจมตีทางเครือข่ายโดยเฉพาะ (Intrusion Prevention System) เข้ามาใช้งานเพื่อให้การป้องกันเครือข่ายมีประสิทธิภาพมากยิ่งขึ้น

### ข้อเสนอแนะเชิงปฏิบัติ

1. ควรมีการจัดอบรมการใช้งานระบบแก่บุคลากรภายในหน่วยงานเพื่อให้มีความเข้าใจในถึงกระบวนการทำงานการยืนยันตัวบุคคลเพื่อเข้าใช้งานระบบเครือข่ายอินเทอร์เน็ตของสำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช
2. ดำเนินการจัดหาอุปกรณ์ป้องกันเครือข่ายที่เป็น Next Generation Firewall ซึ่งสนับสนุนการทำงานแบบ IPS (Intrusion Protection System) เพื่อสนับสนุนการป้องกันภัยคุกคามทางไซเบอร์อย่างเหมาะสม
3. ปรับปรุงระบบปฏิบัติการเซิร์ฟเวอร์ที่ใช้ในการบริหารจัดการข้อมูลผู้ใช้งานให้เป็นเวอร์ชันล่าสุดเพื่อเป็นการป้องกันการโจมตีที่เกิดจากการใช้ระบบปฏิบัติการเวอร์ชันเก่า
4. ระบบมีการจัดเก็บข้อมูลส่วนบุคคล ควรมีการปรับปรุงให้เป็นตามแนวทางพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

## บรรณานุกรม

1. HREX.asia. (2563). PDCA : ความหมาย ประโยชน์ และตัวอย่างใช้ 4 ขั้นตอนเพื่อพัฒนาองค์กร.  
สืบค้นเมื่อ 24 สิงหาคม พ.ศ. 2566.  
จาก <https://th.hrnote.asia/orgdevelopment/what-is-pdca-210610/>
2. Professional One. (2557). Action Plan คืออะไร?. สืบค้นเมื่อ 24 สิงหาคม พ.ศ. 2566.  
จาก <https://www.professional-one.com/การเขียน-action-plan/>
3. ACIS Professional Center. (2564). แนวคิดการระบุตัวตน การพิสูจน์ตัวตน และการให้สิทธิ์.  
สืบค้นเมื่อ 25 พฤษภาคม พ.ศ. 2566. จาก <https://www.acisonline.net/?p=9723>
4. สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. (2563). ทำความรู้จักกับ The CIA Triad.  
สืบค้นเมื่อ 25 สิงหาคม พ.ศ. 2566. จาก <https://www.etda.or.th/th/Useful-Resource/terminology/%E0%B8%AB%E0%B8%A1%E0%B8%A7%E0%B8%94%E0%B8%AB%E0%B8%A1-T/470.aspx>
5. mvpskill. (2560). Active Directory คือ. สืบค้นเมื่อ 25 พฤษภาคม พ.ศ. 2566.  
จาก <https://www.mvpskill.com/kb/active-directory-คือ.html>
6. TECH ADOPT. (2567). เจาะลึกการใช้ Group Policy Object (GPO) แบบเข้าใจง่าย EP1 (ปี2022).  
สืบค้นเมื่อ 25 พฤษภาคม พ.ศ. 2566.  
จาก <https://www.youtube.com/watch?v=qOsKijZ2egA>
7. Suphakit Annoppornchai. (2560). Lightweight Directory Access Protocol.  
สืบค้นเมื่อ 18 พฤษภาคม พ.ศ. 2566. จาก <https://saixiii.com/what-is-ldap/>
8. watchguard. (2560). Set Up Your Log Server. สืบค้นเมื่อ 24 สิงหาคม พ.ศ. 2566.  
จาก [https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Fireware/logging/ls\\_setup\\_wsm.html](https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Fireware/logging/ls_setup_wsm.html)
9. กระทรวงสาธารณสุข. (2565). เรื่องนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย  
ด้านสารสนเทศของกระทรวงสาธารณสุข พ.ศ. 2565. สืบค้นเมื่อ 24 สิงหาคม พ.ศ. 2566.  
จาก <https://ict.moph.go.th/>
10. สำนักงานพัฒนารัฐบาลดิจิทัล. (2560). พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์  
ฉบับที่ 2 พ.ศ. 2560. สืบค้นเมื่อ 24 สิงหาคม พ.ศ. 2566  
จาก <https://www.dga.or.th/document-sharing/media-file/>

## บรรณานุกรม (ต่อ)

11. วันพิชิต ชินตระกูลชัย. (2563). 7 สิทธิ PDPA พนักงานควรรู้ ก่อนบริษัทเก็บข้อมูลส่วนตัว. สืบค้นเมื่อ 25 สิงหาคม พ.ศ. 2566. จาก <https://openpdpa.org/7-data-subject-rights-5-things-business-have-to-done-before-pdpa-use/>
12. Software Testing พื้นฐาน  
สืบค้นเมื่อ วันที่ 31 สิงหาคม พ.ศ. 2566. จาก <https://codinggun.com/testing/>
13. สถาบันนวัตกรรมและกรรมาภิบาลข้อมูล. (2567). คำนวนกลุ่มตัวอย่างสูตร "ทาโร่ ยามาเน่" Taro Yamane. สืบค้นเมื่อ 24 ตุลาคม 2566. จาก <https://digi.data.go.th/blog/method-of-controlling-the-sample/>
14. สำนักบริหารเทคโนโลยีสารสนเทศ จุฬาลงกรณ์มหาวิทยาลัย. (2564). รหัสผ่าน (Password) ตั้งค่าอย่างไรให้ปลอดภัย. สืบค้นเมื่อ 24 ตุลาคม 2566. จาก <https://www.it.chula.ac.th/%E0%B8%A3%E0%B8%AB%E0%B8%B1%E0%B8%AA%E0%B8%9C%E0%B9%88%E0%B8%B2%E0%B8%99-password-%E0%B8%95%E0%B8%B1%E0%B9%89%E0%B8%87%E0%B8%84%E0%B9%88%E0%B8%B2%E0%B8%AD%E0%B8%A2%E0%B9%88%E0%B8%B2%E0%B8%87/>

## ภาคผนวก ก

ประกาศใช้แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ



## บันทึกข้อความ

ส่วนราชการ สำนักงานป้องกันควบคุมโรคที่ ๑๑ จังหวัดนครศรีธรรมราช โทร. ๐ ๗๕๓๔ ๑๑๕๑ ต่อ ๑๔  
 ที่ สร ๐๔๒๘.๓/ว ๖๔๗ วันที่ ๑๔ กรกฎาคม ๒๕๖๖

เรื่อง ประกาศแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานป้องกันควบคุมโรค  
 ที่ ๑๑ จังหวัดนครศรีธรรมราช

เรียน รอง ผอ.สคร.๑๑/ หัวหน้ากลุ่มทุกกลุ่ม / หัวหน้างานทุกงาน/ หัวหน้าศตม.ทุกศตม.

ด้วยกรมควบคุมโรค ประกาศใช้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้าน  
 สารสนเทศ ของกรมควบคุมโรค พ.ศ. ๒๕๖๖

สำนักงานป้องกันควบคุมโรคที่ ๑๑ จังหวัดนครศรีธรรมราช จึงขอประกาศแนวปฏิบัติในการ  
 รักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย  
 และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบเทคโนโลยี  
 สารสนเทศในลักษณะที่ไม่ถูกต้อง และจากการถูกคุกคามจากภัยต่างๆ ซึ่งอาจก่อให้เกิดความเสียหายต่อหน่วยงาน  
 รายละเอียดตามเอกสารที่แนบมาพร้อมนี้

จึงเรียนมาเพื่อทราบ และแจ้งผู้เกี่ยวข้องดำเนินการต่อไปด้วย

(นายไกรสร โตทับเที่ยง)

นายแพทย์เชี่ยวชาญ (ด้านเวชกรรมป้องกัน) รักษาการแทน

ผู้อำนวยการสำนักงานป้องกันควบคุมโรคที่ ๑๑

จังหวัดนครศรีธรรมราช



## ภาคผนวก ข

ประกาศการใช้งานระบบพิสูจน์ยืนยันตัวตน



## บันทึกข้อความ

ส่วนราชการ สำนักงานป้องกันควบคุมโรคที่ ๑๑ จังหวัดนครศรีธรรมราช โทร. ๐ ๗๕๓๔ ๑๑๕๑ ต่อ ๑๔  
ที่ สธ ๐๔๒๘.๓/๖๐๕๕ วันที่ ๒๐ กุมภาพันธ์ ๒๕๖๖

เรื่อง ประกาศการใช้งานระบบพิสูจน์ยืนยันตัวตนในการเข้าใช้อินเทอร์เน็ตของหน่วยงาน

เรียน ผอ.สคร.๑๑/ รอง ผอ.สคร.๑๑/ หัวหน้ากลุ่มทุกกลุ่ม/ หัวหน้างานทุกงาน/ หัวหน้า ศตม. ๑๑.๒

ด้วยสำนักงานป้องกันควบคุมโรคที่ ๑๑ จังหวัดนครศรีธรรมราช โดยกลุ่มยุทธศาสตร์ แผนงาน และเครือข่าย ได้ให้บริการระบบเครือข่ายอินเทอร์เน็ตแก่เจ้าหน้าที่ภายในสำนักงานป้องกันควบคุมโรคที่ ๑๑ นครศรีธรรมราช ซึ่งตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กระทรวงสาธารณสุข พ.ศ. ๒๕๕๖ และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ มาตรา ๒๖

ดังนั้น เพื่อให้เป็นไปตามนโยบายและกฎหมายดังกล่าว งานเทคโนโลยีสารสนเทศ กลุ่มยุทธศาสตร์ แผนงาน และเครือข่าย จะดำเนินการใช้งานระบบพิสูจน์ยืนยันตัวตนในการเข้าใช้อินเทอร์เน็ตของหน่วยงาน โดยเปิดใช้งานระบบดังกล่าวในวันที่ ๒๗ กุมภาพันธ์ ๒๕๖๖ และขอแจ้งรหัสผู้ใช้งาน (User) และรหัสผ่าน (Password) ให้กับเจ้าหน้าที่ทุกท่านสำหรับใช้งานอินเทอร์เน็ต โดยติดต่อขอรับรหัสผู้ใช้งาน (User) และรหัสผ่าน (Password) เป็นรายกลุ่มได้ที่งานเทคโนโลยีสารสนเทศ กลุ่มยุทธศาสตร์ แผนงาน และเครือข่าย

จึงเรียนมาเพื่อทราบ และแจ้งผู้เกี่ยวข้องดำเนินการต่อไปด้วย

(นายไกรสร โตทับเที่ยง)  
นายแพทย์เชี่ยวชาญ (ด้านเวชกรรมป้องกัน) ปฏิบัติหน้าที่  
ผู้อำนวยการสำนักงานป้องกันควบคุมโรคที่ ๑๑  
จังหวัดนครศรีธรรมราช

ภาคผนวก ค

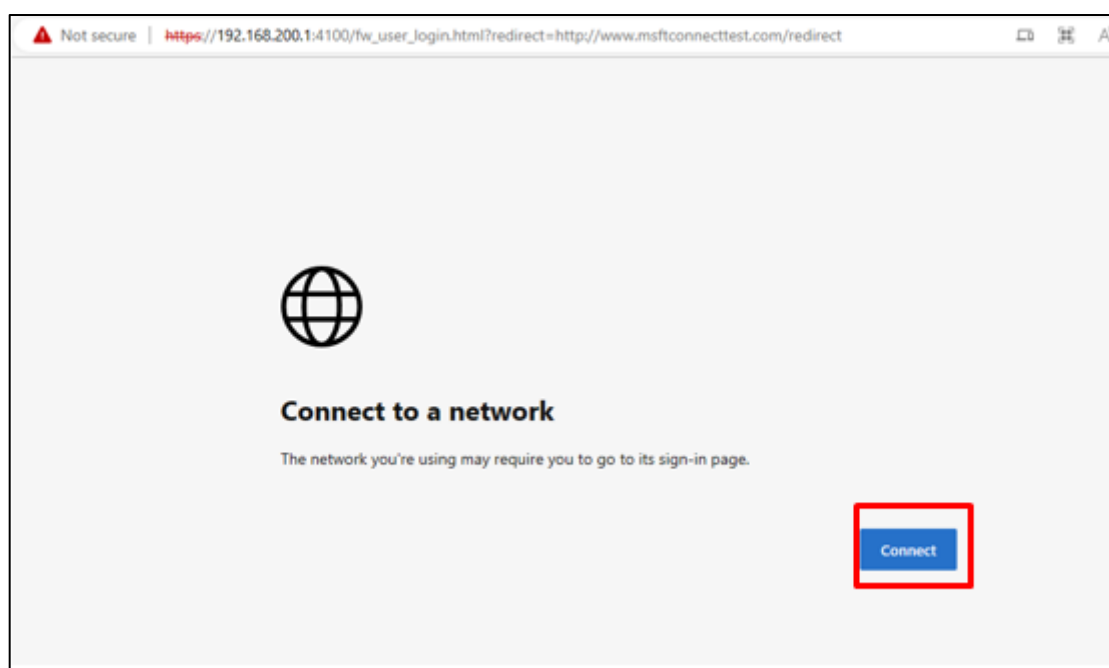
คู่มือการใช้งานบนคอมพิวเตอร์

## คู่มือการใช้งานบนคอมพิวเตอร์

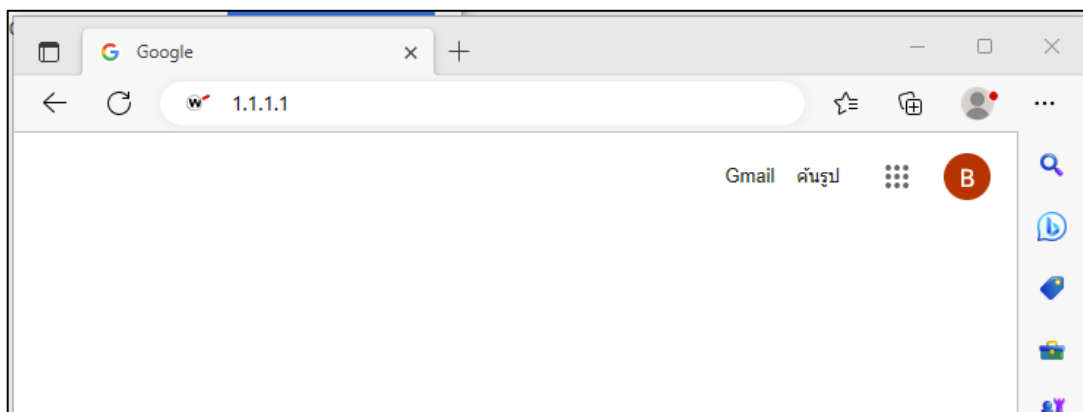
1. วิธีเข้าใช้งานอินเทอร์เน็ต เมื่อเข้าสู่อินเทอร์เน็ตระบบ จะนำไปสู่ (redirect) ไปยังหน้า Login <https://ddc11.watchguard.in.th:4100/> ตามรูปที่ 1 สามารถใส่ Username และ Password ที่ได้รับ และเข้าใช้งานได้เลย

ภาพที่ 72 หน้าต่างการเข้าสู่ระบบ

2. หากเป็นหน้าต่างดังรูปที่ 2 ให้กด Connect หากยังระบบไม่นำมาสู่หน้า Login ใช้งาน ให้เปิด Web browser ใดก็ได้ เช่น Chrome , Edge , Safari , หรืออื่นๆ แล้วพิมพ์ 1.1.1.1 ตามภาพที่ 3 แล้วกด Enter

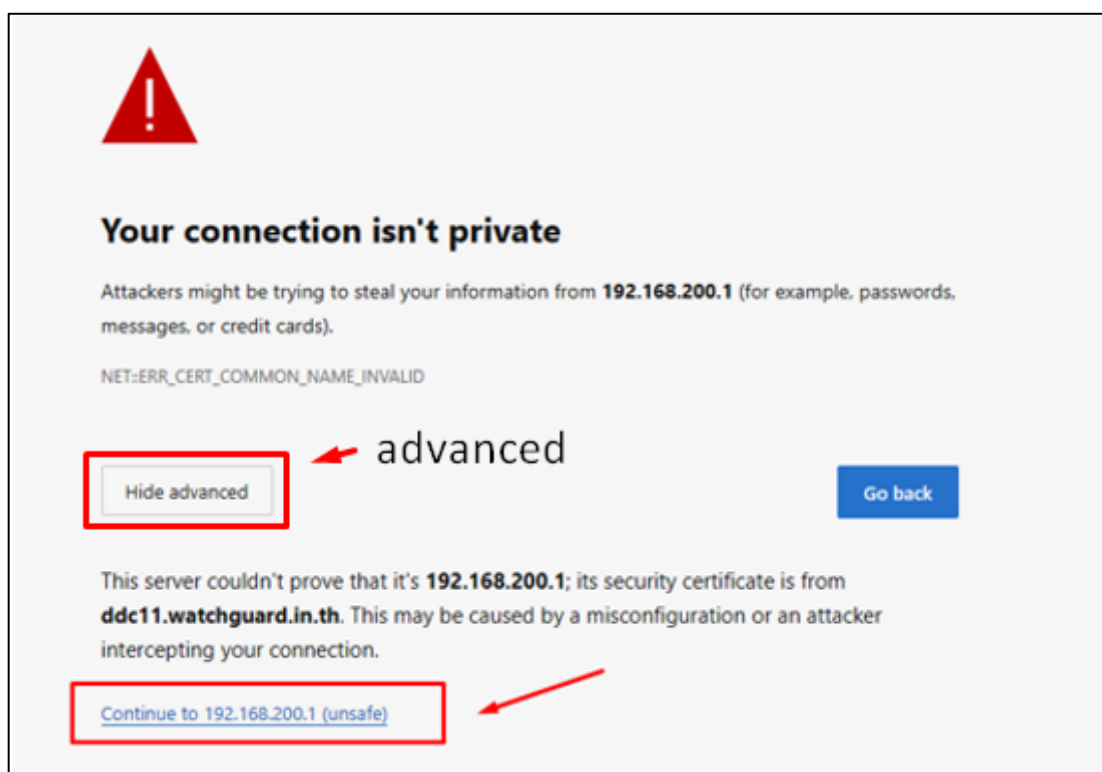


ภาพที่ 73 หน้าต่างแจ้งเตือนการเชื่อมต่อเครือข่าย



ภาพที่ 74 หน้าต่างการระบบ URL

3. หากเครื่องใด เกิดหน้าต่างดังภาพที่ 4 และยังไม่สามารถเข้าสู่หน้า Login เข้าใช้งานได้ ให้กดที่ คำว่า Advanced หรือ ขึ้นสูงในภาษาไทย เมื่อกด Advanced แล้วจะปรากฏหน้าต่างต่างตามภาพที่ 4 ให้กด Continue to 192.168.200.1 (Unsafe) \*\*\* ข้อความตรงนี้อาจจะไม่ใช้แบบนี้แต่กด Link นี้ได้เลย



ภาพที่ 75 หน้าต่างการอนุญาตการเข้าถึง

4. เมื่อกด Continue to 192.168.200.1 (Unsafe) จะเข้าสู่หน้าต่าง ตามภาพที่ 5

ให้กรอก Username : ที่ได้รับ Password :

เลือก Domain เป็น : odpc11.local (ปกติจะเป็นค่าเริ่มต้นอยู่แล้ว)

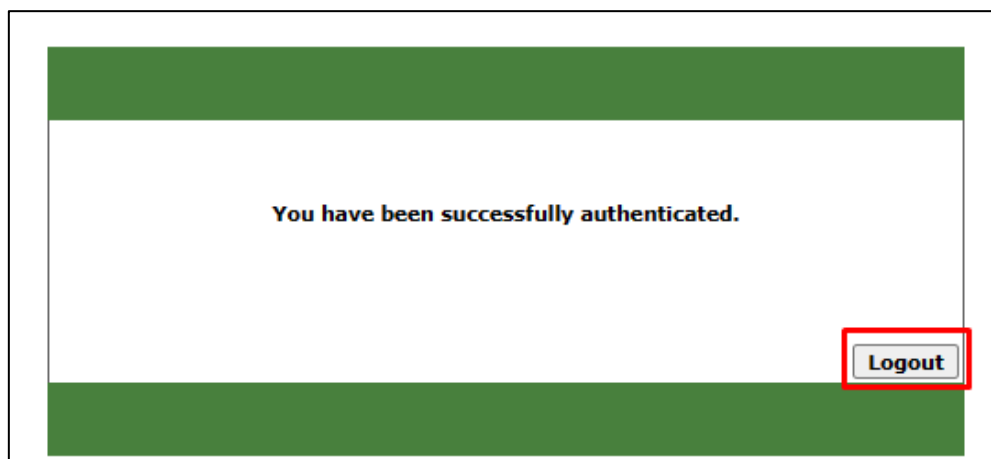
ภาพที่ 76 หน้าต่างการเข้าสู่ระบบ

5.เมื่อ Log in สำเร็จระบบนำไปสู่หน้าเว็บ google.in.th สามารถใช้งานได้เลย



ภาพที่ 77 หน้าเว็บไซต์ Google

6.หากต้องการ Log out ให้เข้าสู่ <https://ddc11.watchguard.in.th:4100> แล้วกด Logout



ภาพที่ 78 หน้าต่างการเข้าสู่ระบบสำเร็จ

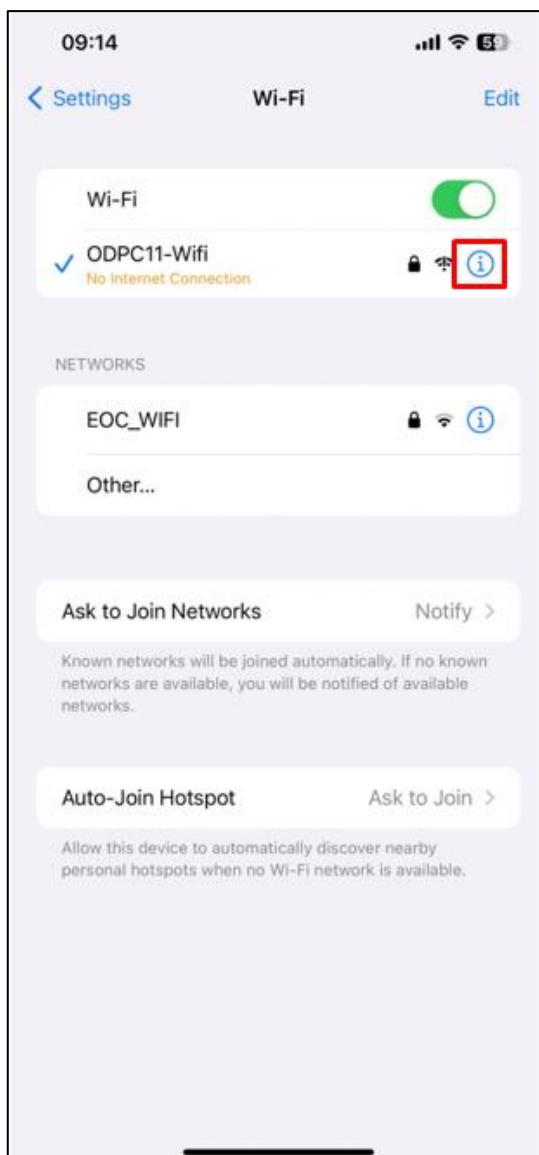
ภาคผนวก ง

คู่มือการใช้งานบนมือถือ

## คู่มือการใช้งานบนมือถือ

1. วิธีใช้งานระบบยืนยันตัวตนบน Tablet , Smartphone

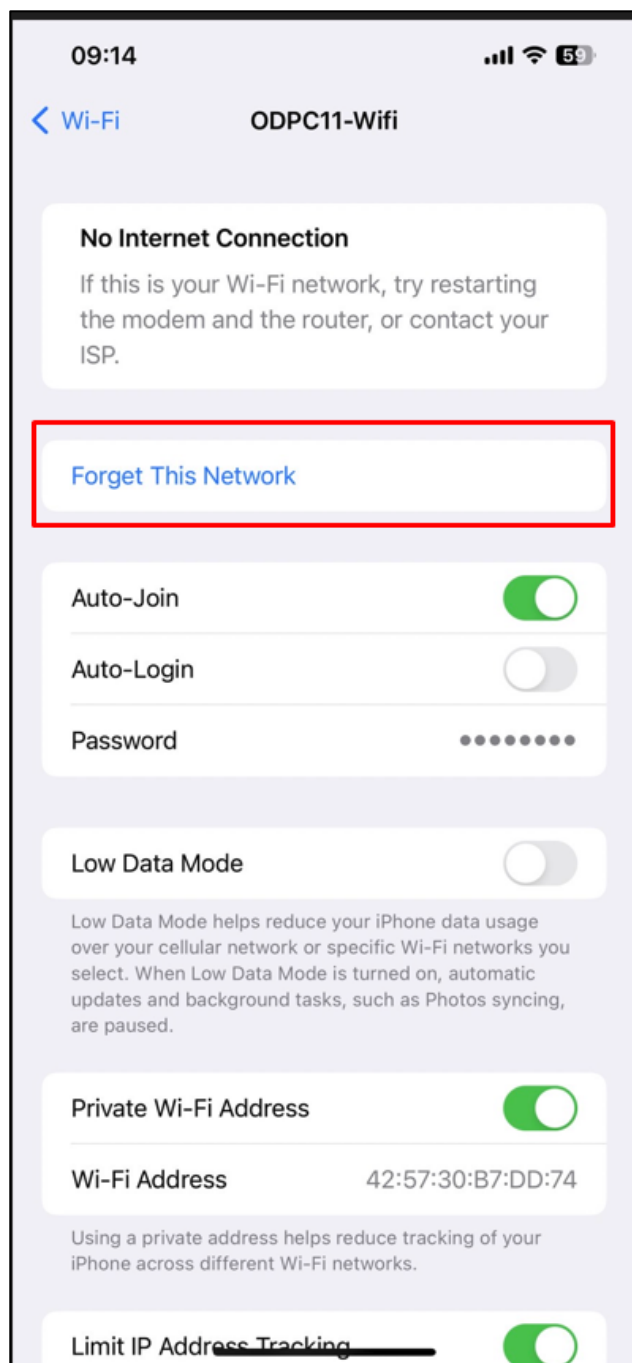
หากเคยเชื่อมต่ออินเทอร์เน็ตอยู่แล้วเข้าใช้งานไม่ได้ ให้กดสัญลักษณ์ ( i ) information icons



ภาพที่ 79 หน้าต่างการเชื่อมต่อ Wireless

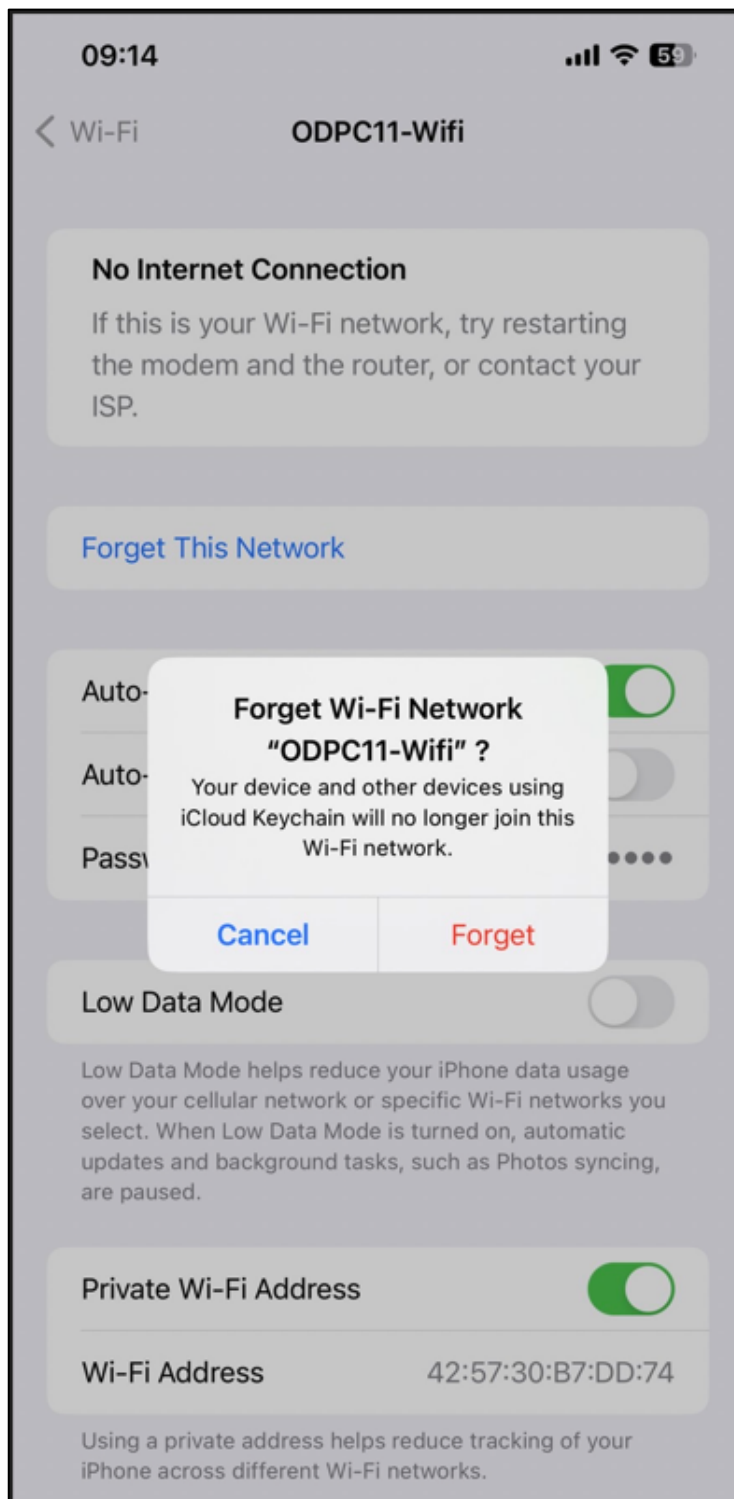


2. เมื่อเข้าสู่หน้า Information ให้กดที่ปุ่ม Forget This Network, หรือคำต่างกันต่างรุ่น ยี่ห้อของอุปกรณ์ เพื่อลืมเครือข่ายนี้



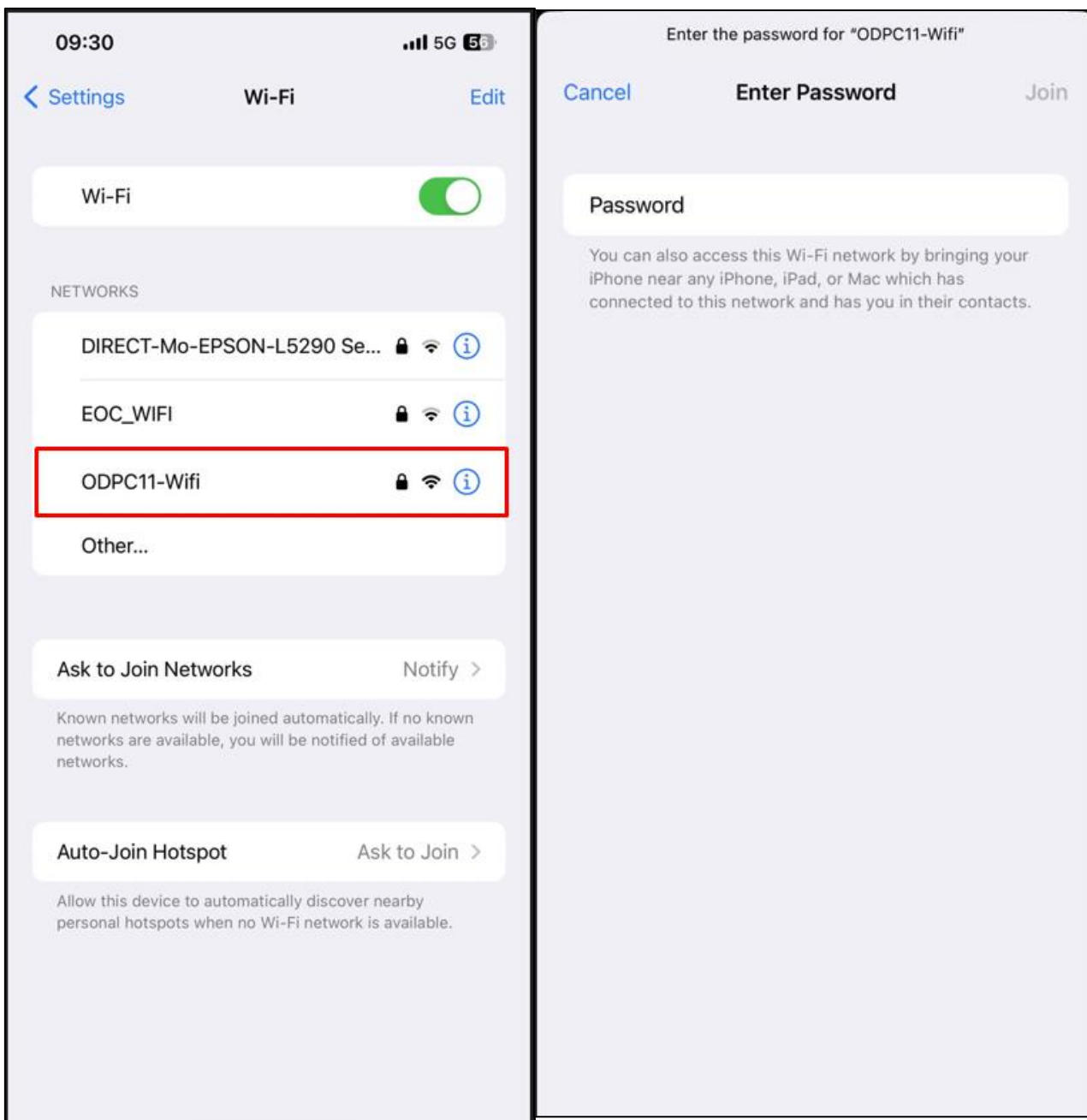
ภาพที่ 80 หน้าต่างการลืม Wireless

3. กดยืนยันการลืม เพื่อลืมการใช้งานเครือข่ายนี้



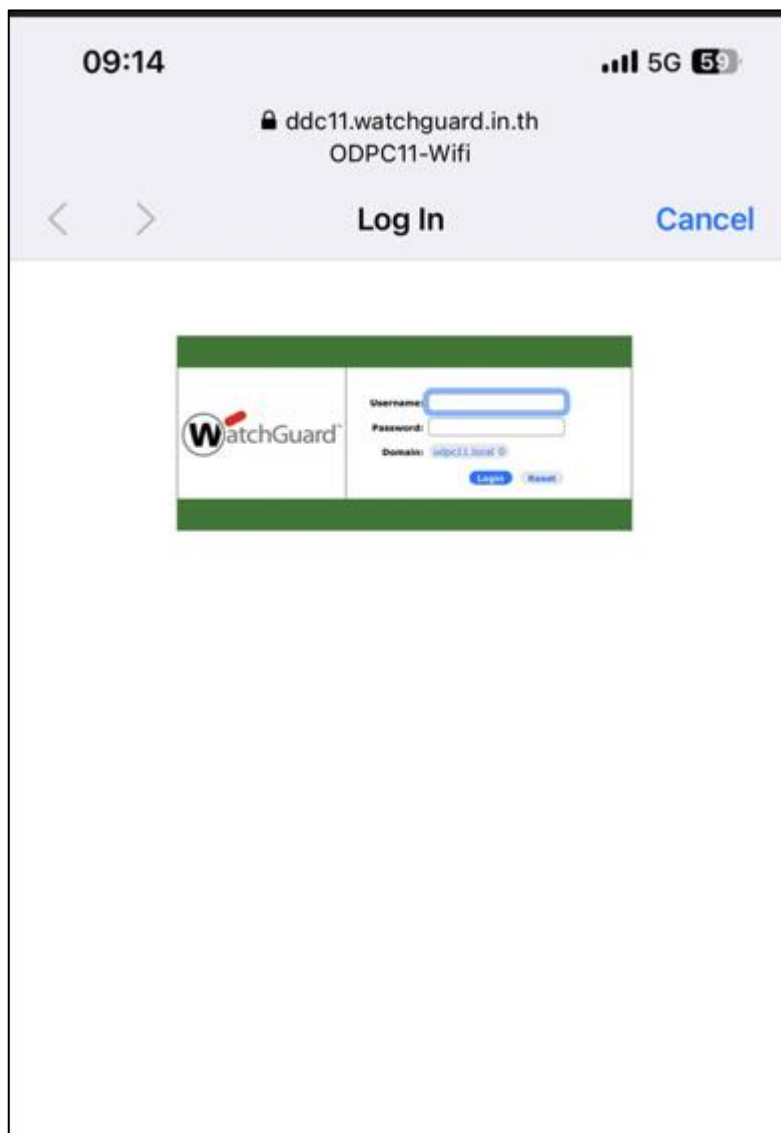
ภาพที่ 81 หน้าต่างการยืนยันการลืม Wireless

4. เมื่อสิ้นการใช้งานเรียบร้อยแล้ว กดเชื่อมต่อเข้าใช้งานเครือข่าย Wireless ที่ต้องการอีกครั้ง ใส่ password ของ Wifi หากมีการถาม



ภาพที่ 82 หน้าต่างการเชื่อมต่อ Wireless ใหม่อีกครั้ง

5. เมื่อเชื่อมต่อเรียบร้อยแล้วระบบจะปรากฏหน้าต่างสำหรับยืนยันตัวตนให้ กรอก Username password ที่ได้รับจากงานเทคโนโลยีสารสนเทศ



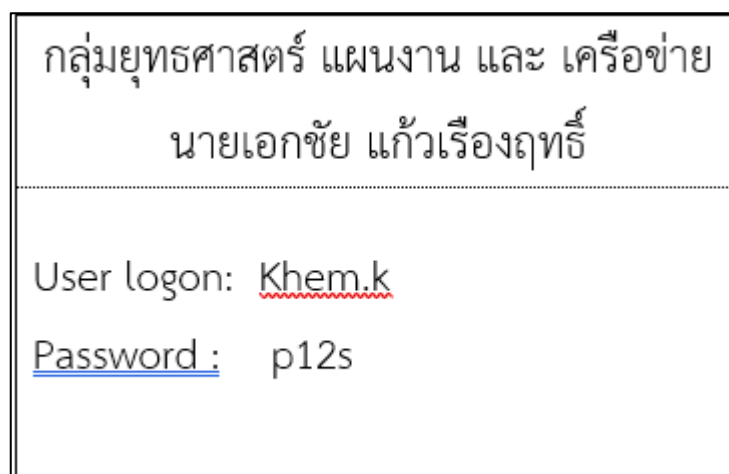
ภาพที่ 83 หน้าต่างการเข้าสู่ระบบ Authentication

ภาคผนวก จ

คู่มือการเปลี่ยนรหัสผ่าน

## คู่มือการเปลี่ยนรหัสผ่าน

1. หลังจากได้รับ User log on และ Password แล้ว



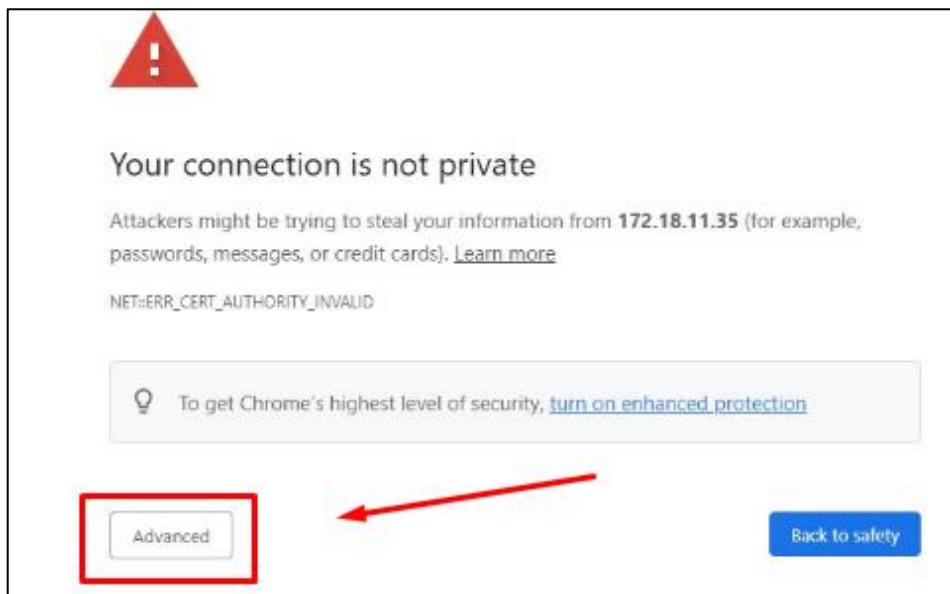
ภาพที่ 84 ตัวอย่าง User และ Password ที่ได้รับ

2. ให้ใช้เครื่องคอมพิวเตอร์หรือคอมพิวเตอร์โน้ตบุ๊กเท่านั้น ที่จะเข้าใช้งานอินเทอร์เน็ตของ สคร.11 โดยเข้าไปยังหน้าเว็บไซต์ : [172.18.11.35/RDWeb/Pages/en-US/password.aspx](https://172.18.11.35/RDWeb/Pages/en-US/password.aspx)  
หรือ <https://172.18.11.35/RDWeb/Pages/en-US/password.aspx>  
หรือ QR CODE



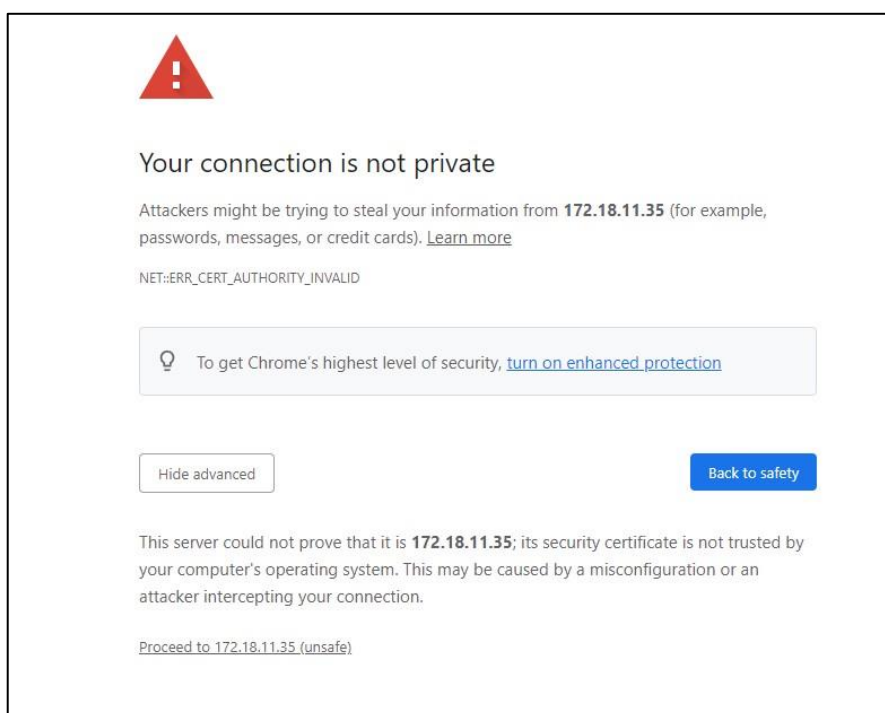
ภาพที่ 85 QR code เข้าสู่หน้าเว็บเปลี่ยนรหัสผ่าน

3. เมื่อเข้าไปยังลิงค์ในข้อที่ 2 แล้ว จะปรากฏหน้าเว็บไซต์ ให้กดปุ่ม Advanced หรือขั้นสูง ตามในรูปด้านล่างนี้



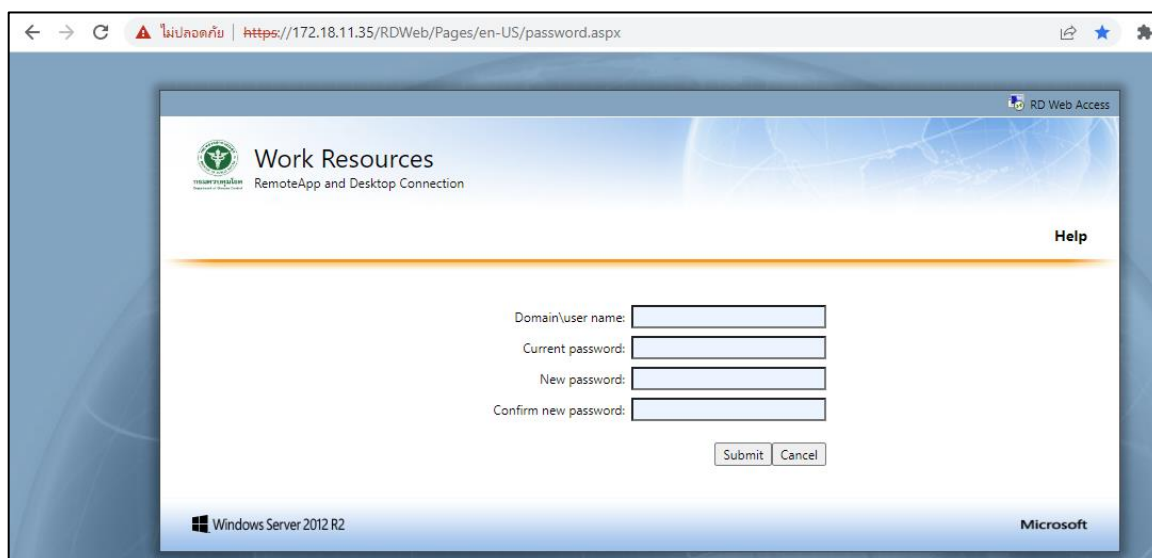
ภาพที่ 86 หน้าเว็บไซต์ ให้กดปุ่ม Advanced หรือขั้นสูง

4. หลังจากทีกดปุ่ม Advanced แล้ว จะปรากฏหน้าเว็บไซต์ ให้กดที่ลิงค์ข้อความ Proceed to 172.18.11.35 (unsafe) ตามในรูปด้านล่างนี้



ภาพที่ 87 หน้าต่างการ Proceed to unsafe

5. เมื่อเข้ากดลิงค์ [Proceed to 172.18.11.35 \(unsafe\)](https://172.18.11.35/RDWeb/Pages/en-US/password.aspx) จะปรากฏหน้าเว็บไซต์ ตามในรูปด้านล่างนี้



ภาพที่ 88 หน้าต่างการเปลี่ยนรหัสผ่าน

#### 6. วิธีการเปลี่ยน Password

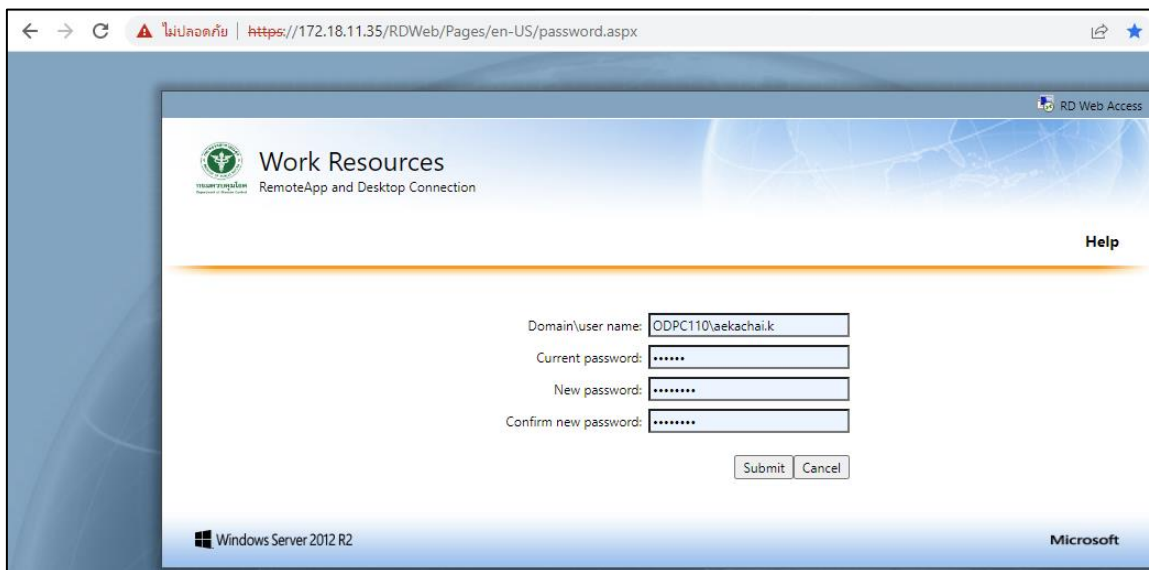
ช่องที่ 1 Domain\user name คือให้ใส่ข้อมูล Domain ตามด้วย “\” ตามด้วย Username ที่ได้รับ เช่น Domain คือ ODPC110 และตาม Username ที่ได้รับ “Khem.k” ดังนั้นให้กรอกในช่อง Domain\user name จะได้เป็น **ODPC110\khem.k**

ช่องที่ 2 Current password : ให้กรอกตาม password ที่ได้รับ คือ p12s

ช่องที่ 3 New Password : สำหรับการกำหนดรหัส Password ใหม่ ที่ต้องการจะต้องมีจำนวนอย่างน้อย 6 ตัวอักษร มีตัวภาษาอังกฤษและตัวเลขผสมกัน

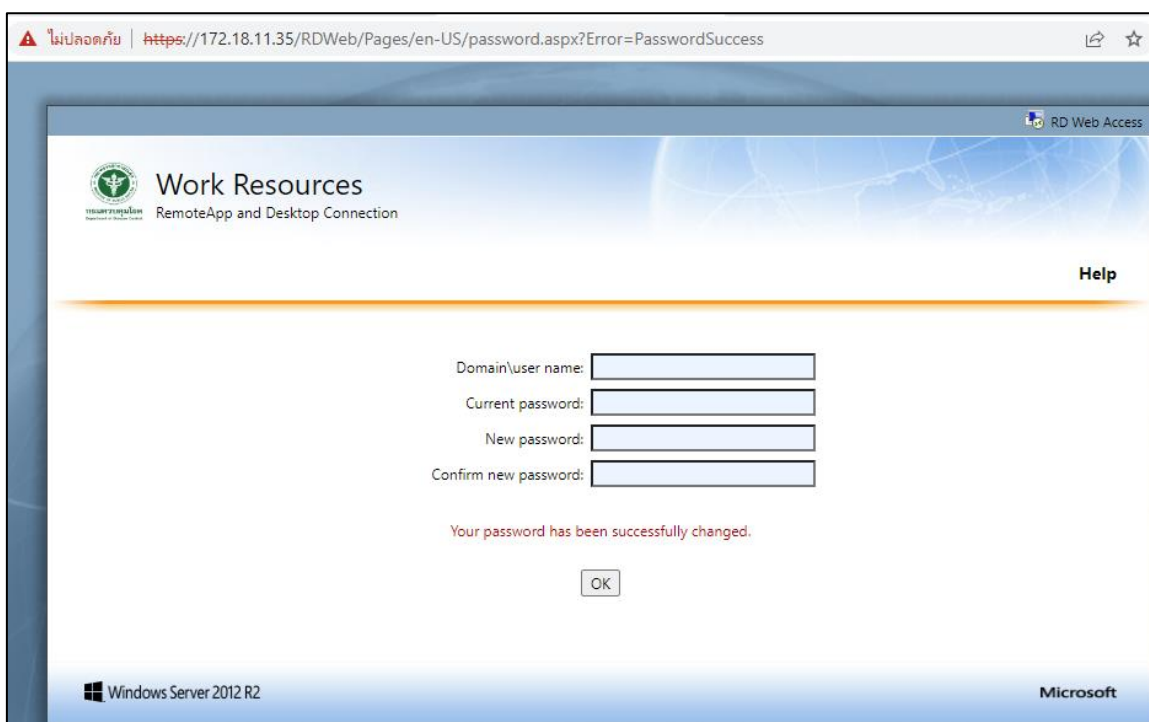
ช่องที่ 4 Confrim New Password : ให้กรอกตรงกับช่องที่ 3 ใส่ Password ใหม่ที่ต้องการอีกครั้งหลังจากกรอกข้อมูลครบทุกช่องแล้ว ให้กด Summit





ภาพที่ 89 หน้าต่างการเปลี่ยนรหัสผ่าน

7. เมื่อกดปุ่ม Summit จะได้นหน้าต่างตามภาพ



ภาพที่ 90 หน้าต่างการเปลี่ยนรหัสผ่าน

8. กรณีที่มีการลืม ชื่อ ผู้ใช้ หรือ รหัสการเข้าใช้งาน ต้องใช้แบบฟอร์ม ต่อไปนี้เพื่อติดต่อกอง  
เทคโนโลยีสารสนเทศ

แบบฟอร์มแจ้งลืมชื่อผู้ใช้หรือรหัสผ่าน

คำนำหน้า ..... ชื่อ ..... สกุล .....(ภาษาไทย)

ชื่อ.....สกุล.....(ภาษาอังกฤษ)

กลุ่มงาน.....

ในการให้งานเทคโนโลยีสารสนเทศ สำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช นำไปใช้  
เก็บ รวบรวม และเปิดเผยข้อมูลส่วนบุคคลของท่าน เพื่อวัตถุประสงค์ในการขอชื่อผู้ใช้หรือรหัสผ่านใหม่ โดย  
เอกสารแสดงความยินยอมฉบับนี้ถือเป็นส่วนหนึ่งของหนังสือแสดงความประสงค์ขอชื่อผู้ใช้หรือรหัสผ่านใหม่  
(reset password)

ทั้งนี้ ก่อนการแสดงเจตนา ข้าพเจ้าได้ทราบถึงวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วน  
บุคคลดังกล่าว และมีความเข้าใจดีแล้ว

ข้าพเจ้าให้ความยินยอมหรือปฏิเสธไม่ให้ความยินยอมในเอกสารนี้ด้วยความสมัครใจปราศจากการ บังคับ  
หรือชักจูง และข้าพเจ้าทราบว่าข้าพเจ้าสามารถถอนความยินยอมนี้เสียเมื่อใดก็ได้เว้นแต่ในกรณี มีข้อจำกัดสิทธิ  
ตามกฎหมาย

ให้ความยินยอม  ไม่ให้ความยินยอม

ลงชื่อ.....  
(.....)  
วันที่.....

---

ส่วนของผู้เจ้าหน้าที่

ดำเนินการเปลี่ยนรหัสผ่านเรียบร้อยแล้ว

Username : .....Password : .....

ลงชื่อ.....  
(.....)

ภาพที่ 91 แบบฟอร์มการแจ้งลืมชื่อผู้ใช้หรือรหัสผ่าน

ภาคผนวก ฉ

แบบสอบถาม

### แบบสอบถาม

ประเมินประสิทธิผลของการระบุตัวตนและยืนยันตัวบุคคลเข้าใช้งานอินเทอร์เน็ต

สำนักงานป้องกันควบคุมโรค ที่ 11 นครศรีธรรมราช

#### คำชี้แจง

แบบสอบถามนี้มีจุดประสงค์เพื่อประเมินประสิทธิผลของการระบุตัวตนและยืนยันตัวบุคคลเข้าใช้งานอินเทอร์เน็ต สำนักงานป้องกันควบคุมโรค ที่ 11 นครศรีธรรมราช เพื่อนำผลที่ได้ไปใช้ปรับปรุงคุณภาพการดำเนินงานระบบสารสนเทศต่อไป แบบสอบถามแบ่งออกเป็น 3 ส่วน ดังนี้

โปรดทำเครื่องหมาย  ลงในช่อง  หน้าข้อความที่ตรงกับความเป็นจริงของท่านมากที่สุด

**ส่วนที่ 1** ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม

1. กลุ่มงาน.....

2. อายุ

21 – 30 ปี

31 – 40 ปี

41 – 50 ปี

51 ปีขึ้นไป

โปรดทำเครื่องหมาย  ลงในช่องว่างในตารางที่ตรงกับความคิดเห็นของท่านมากที่สุด

**ส่วนที่ 2** ความคิดเห็นของบุคลากรสำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช ต่อการประเมิน

ประสิทธิผลและความสำเร็จของระบบสารสนเทศในด้าน ดังนี้

ประเด็นประสิทธิผล	มากที่สุด (5)	มาก (4)	ปานกลาง (3)	น้อย (2)	น้อยที่สุด (1)
<b>1.ด้านความสะดวกในการใช้งานระบบ</b>					
1.1 ท่านมีความเข้าใจเกี่ยวกับวิธีการใช้งานการยืนยันตัวบุคคล					
1.2 ท่านมีความสามารถในการใช้การยืนยันตัวบุคคลด้วยตนเอง					
1.3 ความรวดเร็วของกระบวนการยืนยันตัวบุคคลเมื่อต้องการเข้าใช้งาน					
1.4 ความสะดวกและง่ายต่อการเข้าใช้ระบบ					

ประเด็นประสิทธิผล	มากที่สุด (5)	มาก (4)	ปานกลาง (3)	น้อย (2)	น้อยที่สุด (1)
<b>2.ความเข้าใจเกี่ยวกับความปลอดภัย</b>					
2.1 ความเข้าใจเกี่ยวกับข้อกำหนดและเงื่อนไขของ การยืนยันตัวบุคคล					
2.2 ความสำคัญของการรักษาความปลอดภัยของ ข้อมูลและข้อมูลสำคัญขององค์กรขณะใช้งาน อินเทอร์เน็ต					
2.3 ความสำคัญของการป้องกันการเข้าถึงที่ไม่ได้รับ อนุญาตในการใช้งานอินเทอร์เน็ต.					
<b>3.ความปลอดภัยและความเชื่อถือ</b>					
3.1 ระดับความปลอดภัยของระบบยืนยันตัวบุคคล					
3.2 ความพร้อมที่ระบบยืนยันตัวบุคคลต่อการ ป้องกันการแฮกเกอร์หรือการละเมิดความปลอดภัย					
3.3 ความเชื่อถือในระบบยืนยันตัวบุคคลจากผู้ใช้					
<b>4. การสนับสนุนด้านการใช้งาน</b>					
4.1 การได้รับความรู้และการสนับสนุนในการใช้งาน การยืนยันตัวตน					
4.2 ระบบมีการแจ้งเตือนในกรณีเกิดข้อผิดพลาด					
4.3 การได้รับการแก้ปัญหาในกรณีเกิดข้อผิดพลาด					

**ส่วนที่ 3** ข้อเสนอแนะ/ ข้อคิดเห็นเพิ่มเติม

.....

.....

.....

.....

## ภาคผนวก ช

ผลการเข้าใช้งานระบบเครือข่ายอินเทอร์เน็ตของบุคลากรในระยะเวลา 90 วัน

ลำดับ	ชื่อ-สกุล	ชื่อผู้เข้าใช้	จำนวนการเข้าใช้ (ครั้ง)
1	นางกมล นามะ	namakorn.nam@11.co.th	55
2	นางกมล นามะ	namakorn.nam@11.co.th	66
3	นางกัญญา นามะ	namakorn.nam@11.co.th	63
4	นางกัญญา นามะ	namakorn.nam@11.co.th	3
5	นางจิตติมา นามะ	namakorn.nam@11.co.th	164
6	นางจุลภากร นามะ	namakorn.nam@11.co.th	115
7	นางชลา นามะ	namakorn.nam@11.co.th	69
8	นางชุตติมา นามะ	namakorn.nam@11.co.th	65
9	นางทิติมา นามะ	namakorn.nam@11.co.th	177
10	นางธนา นามะ	namakorn.nam@11.co.th	16
11	นางนงนุช นามะ	namakorn.nam@11.co.th	113
12	นางปฐมา นามะ	namakorn.nam@11.co.th	82
13	นางปรียา นามะ	namakorn.nam@11.co.th	69
14	นางผ่อง นามะ	namakorn.nam@11.co.th	65
15	นางพรนงนุช นามะ	namakorn.nam@11.co.th	9
16	นางพรนงนุช นามะ	namakorn.nam@11.co.th	140
17	นางเพ็ญ นามะ	namakorn.nam@11.co.th	2
18	นางพัชรา นามะ	namakorn.nam@11.co.th	1
19	นางวิไล นามะ	namakorn.nam@11.co.th	80
20	นางศิริ นามะ	namakorn.nam@11.co.th	73
21	นางสกุณา นามะ	namakorn.nam@11.co.th	7
22	นางสมน นามะ	namakorn.nam@11.co.th	126
23	นางสาธิตา นามะ	namakorn.nam@11.co.th	97
24	นางสาธิตา นามะ	namakorn.nam@11.co.th	77
25	นางสาธิตา นามะ	namakorn.nam@11.co.th	111
26	นางสาธิตา นามะ	namakorn.nam@11.co.th	112
27	นางสาธิตา นามะ	namakorn.nam@11.co.th	110
28	นางสาธิตา นามะ	namakorn.nam@11.co.th	147
29	นางสาธิตา นามะ	namakorn.nam@11.co.th	68
30	นางสาธิตา นามะ	namakorn.nam@11.co.th	36
31	นางสาธิตา นามะ	namakorn.nam@11.co.th	131
32	นางสาธิตา นามะ	namakorn.nam@11.co.th	64
33	นางสาธิตา นามะ	namakorn.nam@11.co.th	118
34	นางสาธิตา นามะ	namakorn.nam@11.co.th	12
35	นางสาธิตา นามะ	namakorn.nam@11.co.th	47
36	นางสาธิตา นามะ	namakorn.nam@11.co.th	172
37	นางสาธิตา นามะ	namakorn.nam@11.co.th	117
38	นางสาธิตา นามะ	namakorn.nam@11.co.th	80
39	นางสาธิตา นามะ	namakorn.nam@11.co.th	54
40	นางสาธิตา นามะ	namakorn.nam@11.co.th	91

ลำดับ	ชื่อ-สกุล	ชื่อผู้เข้าใช้	จำนวนการเข้าใช้ (ครั้ง)
41	นางสาว...	...	2
42	นางสาว...	...	43
43	นางสาว...	...	49
44	นางสาว...	...	96
45	นางสาว...	...	45
46	นางสาว...	...	117
47	นางสาว...	...	100
48	นางสาว...	...	48
49	นางสาว...	...	68
50	นางสาว...	...	30
51	นางสาว...	...	63
52	นางสาว...	...	112
53	นางสาว...	...	89
54	นางสาว...	...	77
55	นางสาว...	...	121
56	นางสาว...	...	1
57	นางสาว...	...	53
58	นางสาว...	...	62
59	นางสาว...	...	136
60	นางสาว...	...	108
61	นางสาว...	...	49
62	นางสาว...	...	62
63	นางสาว...	...	77
64	นางสาว...	...	55
65	นางสาว...	...	110
66	นางสาว...	...	171
67	นางสาว...	...	95
68	นางสาว...	...	109
69	นางสาว...	...	61
70	นางสาว...	...	82
71	นางสาว...	...	65
72	นางสาว...	...	22
73	นางสาว...	...	85
74	นางสาว...	...	122
75	นางสาว...	...	207
76	นางสาว...	...	70
77	นางสาว...	...	2
78	นางสาว...	...	52
79	นางสาว...	...	9
80	นางสาว...	...	98



ลำดับ	ชื่อ-สกุล	ชื่อผู้เข้าใช้	จำนวนการเข้าใช้ (ครั้ง)
81	นางสาว ธิติพร นนทวงษา	nnnnpn@suphonor.com	120
82	นางสาว อรุณ นนทวงษา	nnnnpn@suphonor.com	123
83	นางสาว อธิชา นนทวงษา	nnnnpn@suphonor.com	52
84	นางสาว อรุณ นนทวงษา	nnnnpn@suphonor.com	73
85	นางสาว อรุณ นนทวงษา	nnnnpn@suphonor.com	10
86	นางสาว ธิติพร นนทวงษา	nnnnpn@suphonor.com	82
87	นางสาว อรุณ นนทวงษา	nnnnpn@suphonor.com	40
88	นางสาว อรุณ นนทวงษา	nnnnpn@suphonor.com	39
89	นางสาว อธิชา นนทวงษา	nnnnpn@suphonor.com	74
90	นางสาว ธิติพร นนทวงษา	nnnnpn@suphonor.com	96
91	นางสาว อรุณ นนทวงษา	nnnnpn@suphonor.com	61
92	นางสาว อธิชา นนทวงษา	nnnnpn@suphonor.com	109
93	นางสาว อธิชา นนทวงษา	nnnnpn@suphonor.com	77
94	นางสาว อธิชา นนทวงษา	nnnnpn@suphonor.com	93
95	นางสาว อธิชา นนทวงษา	nnnnpn@suphonor.com	133
96	นางสาว อธิชา นนทวงษา	nnnnpn@suphonor.com	14
97	นางสาว อธิชา นนทวงษา	nnnnpn@suphonor.com	133
98	นางสาว อธิชา นนทวงษา	nnnnpn@suphonor.com	74
99	นางสาว อธิชา นนทวงษา	nnnnpn@suphonor.com	89
100	นางสาว อธิชา นนทวงษา	nnnnpn@suphonor.com	1
101	นางสาว อธิชา นนทวงษา	nnnnpn@suphonor.com	60
102	นางสาว อธิชา นนทวงษา	nnnnpn@suphonor.com	121
103	นางสาว อธิชา นนทวงษา	nnnnpn@suphonor.com	51
104	นางสาว อธิชา นนทวงษา	nnnnpn@suphonor.com	109
105	นางสาว อธิชา นนทวงษา	nnnnpn@suphonor.com	94
106	นางสาว อธิชา นนทวงษา	nnnnpn@suphonor.com	100
107	นางสาว อธิชา นนทวงษา	nnnnpn@suphonor.com	130
108	นางสาว อธิชา นนทวงษา	nnnnpn@suphonor.com	82
109	นางสาว อธิชา นนทวงษา	nnnnpn@suphonor.com	14
110	นางสาว อธิชา นนทวงษา	nnnnpn@suphonor.com	1
111	นางสุภา อธิชา นนทวงษา	nnnnpn@suphonor.com	50
112	นางสุพัตรา อธิชา นนทวงษา	nnnnpn@suphonor.com	110
113	นางสุพัตรา อธิชา นนทวงษา	nnnnpn@suphonor.com	111
114	นางสุภา อธิชา นนทวงษา	nnnnpn@suphonor.com	60
115	นางอรอุมา อธิชา นนทวงษา	nnnnpn@suphonor.com	53
116	นางอรอุมา อธิชา นนทวงษา	nnnnpn@suphonor.com	78
117	นางอำไพ อธิชา นนทวงษา	nnnnpn@suphonor.com	73
118	นายเกษม อธิชา นนทวงษา	nnnnpn@suphonor.com	8
119	นายเอก อธิชา นนทวงษา	nnnnpn@suphonor.com	68
120	นายโกวิท อธิชา นนทวงษา	nnnnpn@suphonor.com	91

ลำดับ	ชื่อ-สกุล	ชื่อผู้เข้าใช้	จำนวนการเข้าใช้ (ครั้ง)
121	นายโกศล ไชยสิทธิ์	ksorn.aj@pda.11.co.th	23
122	นายกีรติ นามะพันธ์	kitirong.aj@pda.11.co.th	1
123	นายกีรติ นามะพันธ์	kitirong.aj@pda.11.co.th	58
124	นายศุภ นามะพันธ์	suphat.aj@pda.11.co.th	62
125	นายชัชวาล นามะพันธ์	chawan.aj@pda.11.co.th	109
126	นายชัชวาล นามะพันธ์	chawan.aj@pda.11.co.th	42
127	นายชัชวาล นามะพันธ์	chawan.aj@pda.11.co.th	23
128	นายศุภ นามะพันธ์	suphat.aj@pda.11.co.th	12
129	นายทิว นามะพันธ์	tiwan.aj@pda.11.co.th	3
130	นายธนากร นามะพันธ์	thanasak.aj@pda.11.co.th	66
131	นายธนากร นามะพันธ์	thanasak.aj@pda.11.co.th	76
132	นายณัฐ นามะพันธ์	natth.aj@pda.11.co.th	63
133	นายณัฐ นามะพันธ์	natth.aj@pda.11.co.th	2
134	นายณัฐ นามะพันธ์	natth.aj@pda.11.co.th	71
135	นายบุญชู นามะพันธ์	boonsu.aj@pda.11.co.th	22
136	นายบุญชู นามะพันธ์	boonsu.aj@pda.11.co.th	180
137	นายบุญชู นามะพันธ์	boonsu.aj@pda.11.co.th	74
138	นายบุญชู นามะพันธ์	boonsu.aj@pda.11.co.th	231
139	นายบุญชู นามะพันธ์	boonsu.aj@pda.11.co.th	1
140	นายบุญชู นามะพันธ์	boonsu.aj@pda.11.co.th	2
141	นายพิเชษฐ นามะพันธ์	piseth.aj@pda.11.co.th	109
142	นายมงคล นามะพันธ์	mongkol.aj@pda.11.co.th	4
143	นายยุทธ นามะพันธ์	yuth.aj@pda.11.co.th	4
144	นายวิภากร นามะพันธ์	vipagr.aj@pda.11.co.th	59
145	นายวิภากร นามะพันธ์	vipagr.aj@pda.11.co.th	2
146	นายวิภากร นามะพันธ์	vipagr.aj@pda.11.co.th	2
147	นายสุภากร นามะพันธ์	supagr.aj@pda.11.co.th	47
148	นายสุภากร นามะพันธ์	supagr.aj@pda.11.co.th	4
149	นายสุภากร นามะพันธ์	supagr.aj@pda.11.co.th	34
150	นายสุภากร นามะพันธ์	supagr.aj@pda.11.co.th	81
151	นายสุภากร นามะพันธ์	supagr.aj@pda.11.co.th	107
152	นายสุภากร นามะพันธ์	supagr.aj@pda.11.co.th	84
153	นายทิว นามะพันธ์	tiwan.aj@pda.11.co.th	43
154	นายทิว นามะพันธ์	tiwan.aj@pda.11.co.th	113
155	นายอรรถ นามะพันธ์	athak.aj@pda.11.co.th	2
156	นายอรรถ นามะพันธ์	athak.aj@pda.11.co.th	66
157	นายอรรถ นามะพันธ์	athak.aj@pda.11.co.th	256
158	นายอรรถ นามะพันธ์	athak.aj@pda.11.co.th	73
159	นายอรรถ นามะพันธ์	athak.aj@pda.11.co.th	66
160	ว่าที่ร้อยตรี นามะพันธ์	wasat.aj@pda.11.co.th	29