

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 จึงต้องมีการควบคุมการเข้าถึงการบริการทางเครือข่าย ผู้รับการประเมินในนำหลักงาน PDCA (Plan – Do – Check - Act) มาเป็นแนวทางในการพัฒนาระบบ และได้นำเครื่องมือ VMware ESXi ซึ่งเป็นเครื่องมือในการบริหารจัดการเครื่องคอมพิวเตอร์เสมือนจริงมาใช้ รวมทั้งการใช้ Windows Server 2012 พร้อมทั้งการจัดทำ Active Directory Domain Services และ Watchguard Firebox M4600 ที่ใช้ในการกำหนด Policy เพื่อเป็นการควบคุมการเข้าถึงเครือข่าย หลังจากที่ได้พัฒนาแล้วจึงได้มีการทดสอบจากผู้พัฒนาระบบเพื่อตรวจสอบความถูกต้องของการทำงาน และมีการวางแผนปรับปรุงข้อผิดพลาดที่จะนำไปสู่การพัฒนาระบบให้ดียิ่งขึ้นต่อไป

ดังนั้น จากการพัฒนาระบบงานดังกล่าว สำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช จึงมีระบบการยืนยันตัวตนบุคคลในการเข้าใช้งานอินเทอร์เน็ตเพื่อใช้ในการตรวจสอบ กำกับดูแล ผู้ใช้งานให้ใช้ระบบเทคโนโลยีสารสนเทศ และการสื่อสารให้เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง

## กิตติกรรมประกาศ

การจัดทำเอกสารผลงาน เรื่อง “การยืนยันตัวบุคคลเพื่อเข้าใช้งานระบบเครือข่ายอินเทอร์เน็ตของสำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช” ฉบับนี้ สำเร็จลุล่วงได้ด้วยดี ขอขอบพระคุณผู้บริหารทุกท่านที่เล็งเห็นความสำคัญความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศซึ่งควรนำมาใช้ในการดำเนินงานภายในหน่วยงาน และนางสาวกรรณิกา สุวรรณหา หัวหน้ากลุ่มงานยุทธศาสตร์ แผนงาน 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	ซ
<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	13
2.7 ทฤษฎีการคำนวณหากลุ่มตัวอย่าง	14
<b>บทที่ 3 วิธีการดำเนินการ</b>	<b>15</b>
3.1 เครื่องมือที่ใช้วิจัย	15
3.2 การเก็บรวบรวมข้อมูล	15
3.3 วิเคราะห์ข้อมูล	16
3.4 การดำเนินการวิจัย	17
3.5 การพัฒนากระบวนการงานตามหลัก PDCA	21

## สารบัญ (ต่อ)

	หน้า
<b>บทที่ 4 ผลการดำเนินการ</b>	<b>28</b>
4.1 ดำเนินการตามแผนการพัฒนา	28
4.2. ผลการตรวจสอบการทำงาน	45
<b>บทที่ 5 บทสรุป และข้อเสนอแนะ</b>	<b>75</b>
5.1 สรุปผล	75
5.2 การนำไปใช้ประโยชน์/ผลกระทบ	77
5.3 ความยุ่งยากและซับซ้อนในการดำเนินงาน	77
5.4 ปัญหาและอุปสรรคในการดำเนินงาน	78
5.5 ข้อเสนอแนะ	78
<b>บรรณานุกรม</b>	<b>79</b>
<b>ภาคผนวก</b>	<b>81</b>
ภาคผนวก ก ประกาศใช้แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	81
ภาคผนวก ข ประกาศการใช้งานระบบพิสูจน์ยืนยันตัวตน	83
ภาคผนวก ค คู่มือการใช้งานบนคอมพิวเตอร์	85
ภาคผนวก ง คู่มือการใช้งานบนมือถือ	89
ภาคผนวก จ คู่มือการเปลี่ยนรหัสผ่าน	95
ภาคผนวก ฉ แบบสอบถาม	101

## สารบัญภาพ

	หน้า
ภาพที่ 2.1 หลักการพัฒนา PDCA (Plan – Do – Check - Act)	4
ภาพที่ 2.2 ตัวอย่างการแบ่ง Organizational Unit	10
ภาพที่ 2.3 จำลองการทำงานของ Lightweight Directory Access Protocol (LDAP)	11
ภาพที่ 3.1 แสดงผังงาน (Flowchart) เปรียบเทียบการเข้าถึงเครือข่ายด้วยรูปแบบเดิม เปรียบเทียบกับระบบใหม่	21
ภาพที่ 3.2 แสดงลำดับกระบวนการทำงานของระบบในภาพรวมโดยแสดงลำดับ การทำงานของระบบตามหมายเลขที่ได้กำกับไว้ตามลำดับ	22
ภาพที่ 3.3 แสดงลำดับการทำงานของระบบกรณีที่ User เป็นผู้ใช้งาน	22
ภาพที่ 3.4 แสดงลำดับกระบวนการทำงานของระบบในกรณีที่เป็นผู้ดูแลระบบ	23
ภาพที่ 3.5 แสดงขั้นตอนการเข้าสู่ระบบและการขอสิทธิ์การใช้งาน	23
ภาพที่ 3.6 แสดงขั้นตอนการเปลี่ยนรหัสผ่าน	24
ภาพที่ 3.7 แสดงขั้นตอนการรับข้อมูลจากงานการเจ้าหน้าที่	24
ภาพที่ 3.8 แสดงแผนผังการทำงานของระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์	25
ภาพที่ 3.9 แสดงตัวอย่างข้อมูลที่ได้ทำการวิเคราะห์แล้วก่อนบันทึกลงระบบ Active Directory	26
ภาพที่ 4.1 แสดงหน้าต่างการเข้าใช้งานโปรแกรม VMware vSphere Client	28
ภาพที่ 4.2 แสดงหน้าต่างการกำหนด CPUs cores ของเครื่อง Virtual	28
ภาพที่ 4.3 แสดงหน้าต่างการกำหนด Memory ของเครื่อง Virtual	29
ภาพที่ 4.4 แสดงหน้าต่างการกำหนด Disk size	29
ภาพที่ 4.5 แสดงหน้าต่างรายละเอียดการตั้งค่าทั้งหมดของเครื่อง virtual ตามที่ได้กำหนดไว้	30
ภาพที่ 4.6 แสดงการเลือก ISO Files ของ Windows ในช่อง CD/DVD Drive 1 โดย ISO ที่เลือกต้องจัดเก็บไว้ใน Virtual machine storage	30
ภาพที่ 4.7 แสดงการกำหนด IP address ของเครื่อง Server	31
ภาพที่ 4.8 แสดงหน้าต่างการเลือกรูปแบบการติดตั้ง โดยเลือกการตั้งค่าแบบ Roles-based or feature-based installation	31
ภาพที่ 4.9 ทำการเลือกเซิร์ฟเวอร์ที่จะทำการติดตั้ง Roles	32

## สารบัญภาพ (ต่อ)

	หน้า
ภาพที่ 4.10 แสดงหน้าต่างการเลือก Roles ที่ได้ทำการเลือก	32
ภาพที่ 4.11 แสดงหน้าต่างสรุปการตั้งค่า Roles ที่ได้ทำการเลือกติดตั้ง	33
ภาพที่ 4.12 แสดงหน้าต่างการกำหนด domain name โดยเลือก Add a new forest แล้ว กำหนดชื่อ domain name	33
ภาพที่ 4.13 แสดงหน้าต่างรายละเอียดการตั้งค่า domain controller และปุ่ม Install	34
ภาพที่ 4.14 แสดงหน้าต่าง Server Manager ผลการติดตั้ง Roles ของ Server	34
ภาพที่ 4.15 แสดงหน้าต่างการเปิดใช้งาน Network Policy Server	35
ภาพที่ 4.16 แสดงผลของการกำหนด Password Policy	36
ภาพที่ 4.17 การสร้าง organization unit (OU) เพื่อกำหนดชื่อตามกลุ่มงาน	36
ภาพที่ 4.18 แสดงหน้าต่างรายละเอียดข้อมูล New User	37
ภาพที่ 4.19 แสดงหน้าต่างการกำหนด Password New User	37
ภาพที่ 4.20 แสดงหน้าต่างสรุปผลการสร้าง User	38
ภาพที่ 4.21 แสดงตัวอย่างการคลิกขวาที่ New User แล้วเลือกเมนู Add to a group	38
ภาพที่ 4.22 แสดงหน้าต่างการ Select Groups หลังจากที่ได้ทำการ Check Names	39
ภาพที่ 4.23 แสดงจำนวนรูปแบบการเชื่อมต่อที่สามารถเชื่อมต่อได้บน Firewall โดยได้เลือกใช้แบบ Active Directory	39
ภาพที่ 4.24 แสดงวิธีการกำหนด Domain Name	40
ภาพที่ 4.25 แสดงการกำหนด session Authentication โดยกำหนดค่าการใช้งาน	40
ภาพที่ 4.26 แสดงหน้าต่าง Firewall Policies > ADD Policy	41
ภาพที่ 4.27 แสดงหน้าต่างการ ADD Member type เป็น group ที่ได้กำหนดไว้ใน ADDS	41
ภาพที่ 4.28 แสดงผลการ configure firewall policy ที่ได้กำหนดให้ User จาก group ODPC11 สามารถเข้าถึงเครือข่าย	42
ภาพที่ 4.29 แสดงหน้าต่างการเลือก Windows 10 ISO Files สำหรับติดตั้ง	42
ภาพที่ 4.30 แสดงหน้าต่างการกำหนด IP Address เป็น Static	43
ภาพที่ 4.31 แสดงหน้าต่างการติดตั้ง Watchguard System manager	43
ภาพที่ 4.32 แสดงหน้าต่างการกำหนดการเชื่อมต่อ WatchGuard System Manager	44

## สารบัญภาพ (ต่อ)

	หน้า
ภาพที่ 4.33 แสดงรายการ Device ของ Firebox ที่ได้ทำการเชื่อมต่อไว้	44
ภาพที่ 4.34 แสดงหน้าตาการกำหนดการตั้งค่าการ์ดเก็บ Log Files	45
ภาพที่ 4.35 แสดงหน้าตา Firewall Management เมนู TEST CONNECTION FOR LDAP AND ACTIVE DIRECTORY	45
ภาพที่ 4.36 แสดงหน้าตาการทดสอบด้วย Username และ Password ที่ถูกต้อง	46
ภาพที่ 4.37 แสดงหน้าตาการทดสอบด้วย Username และ Password ที่ถูกต้อง	46
ภาพที่ 4.38 หน้าตาแสดงการเข้าสู่ระบบสำเร็จ	48
ภาพที่ 4.39 แสดงหน้าตาการเข้าใช้งานไม่สำเร็จ	48
ภาพที่ 4.40 แสดงหน้าตาการเข้าสู่โปรแกรมจัดเก็บ Log Files	49
ภาพที่ 4.41 แสดงหน้าตาการเข้าสู่โปรแกรมจัดเก็บ Log Files	49
ภาพที่ 4.42 แสดงหน้าตา Dashboard ของการจัดเก็บ Log Files	50
ภาพที่ 4.43 แสดงหน้าตาโปรแกรม PuTTY สำหรับเชื่อมต่อไปยัง Firewall	50
ภาพที่ 4.44 แสดงหน้าตาโปรแกรม PuTTY สำหรับ login เข้าใช้งาน	51
ภาพที่ 4.45 แสดงการใช้คำสั่ง show log-setting watchdog-log-server เพื่อดูปลายทางในการจัดเก็บ Log ของ Firewall	51
ภาพที่ 4.46 แสดงระยะเวลาในการค้นหาข้อมูล Log ย้อนหลัง	52
ภาพที่ 4.47 แสดงตัวอย่างข้อมูลการค้นหา Log Files ย้อนหลัง	53
ภาพที่ 4.48 แสดงผลการทดสอบหลังใช้งานระบบ Authentication	55
ภาพที่ 4.49 แสดงผลการตรวจสอบผู้ใช้งานระบบเครือข่ายก่อนการใช้งานระบบ Authentication	56
ภาพที่ 4.50 แสดงผลการตรวจสอบผู้ใช้งานระบบเครือข่ายหลังการใช้งาน ระบบ Authentication	56
ภาพที่ 4.51 แสดงผลปรับปรุงขนาดของพื้นที่ในการจัดเก็บเพิ่มจากเดิม 100 GB เป็น 300 GB	57
ภาพที่ 4.52 แสดงการจัดลำดับ Policy บน Firewall	59
ภาพที่ 4.53 แสดงภาพแสดงข้อมูลจราจรคอมพิวเตอร์ในรูปแบบ Dashboard	63
ภาพที่ 4.54 การค้นหาประวัติข้อมูลจราจรคอมพิวเตอร์	63
ภาพที่ 4.55 แสดงรายละเอียดพื้นที่การจัดเก็บข้อมูลจราจรคอมพิวเตอร์	64



## สารบัญตาราง

	หน้า
ตารางที่ 3.1 แสดงผลการจัดเก็บข้อมูล	15
ตารางที่ 3.2 ประเด็นและรายละเอียดเกณฑ์การให้คะแนน	20
ตารางที่ 3.3 แสดงผลการเปรียบเทียบทรัพยากรของหน่วยงาน	21
ตารางที่ 3.4 แสดงตารางโครงสร้างการจัดเก็บข้อมูล	26
ตารางที่ 4.1 แสดงผลการทดสอบระบบ	47
ตารางที่ 4.2 แสดงผลการตรวจสอบการทำงาน	48
ตารางที่ 4.3 แสดงความหมายของข้อมูลที่จัดเก็บเป็น Log Files	53
ตารางที่ 4.4 การตรวจสอบคุณลักษณะเครื่องเซิร์ฟเวอร์	54
ตารางที่ 4.5 การตรวจสอบคุณลักษณะเฉพาะเครื่องคอมพิวเตอร์ log files	54
ตารางที่ 4.6 แสดงผลการเปรียบเทียบการทดสอบการใช้งานก่อนและหลังติดตั้งระบบ	55
ตารางที่ 4.7 เปรียบเทียบการทำงานก่อนและหลังการใช้งานระบบ	57
ตารางที่ 4.8 แสดงตารางการบำรุงรักษาเครื่อง Server	60
ตารางที่ 4.9 แสดงสถิติการใช้งานระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log Files) ของ สำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช จำนวน 47 วัน ระหว่างวันที่ 24 กันยายน พ.ศ. 2566 ถึงวันที่ 9 พฤศจิกายน พ.ศ. 2566	60
ตารางที่ 4.10 แสดงรายงานสรุปประวัติการเข้าใช้งานและการป้องกันการเข้าใช้งาน โดยไม่ได้รับอนุญาต	62
ตารางที่ 4.11 ผลการประเมิน	65
ตารางที่ 4.12 ผลการศึกษาปัจจัยส่วนบุคคล แยกตามช่วงอายุ	66
ตารางที่ 4.13 ผลการศึกษาปัจจัยส่วนบุคคล ด้านกลุ่มที่ปฏิบัติงาน	66
ตารางที่ 4.14 ผลการศึกษาปัจจัยด้านระดับการปฏิบัติงาน	67
ตารางที่ 4.15 แสดงผลการประเมินประสิทธิผลและความสำเร็จด้านประสิทธิภาพของระบบ ของผู้บริหารและหัวหน้ากลุ่ม	69
ตารางที่ 4.16 แสดงผลการประเมินประสิทธิผลและความสำเร็จด้านประสิทธิภาพของระบบ ของผู้ปฏิบัติงาน	69
ตารางที่ 4.17 แสดงผลการประเมินประสิทธิผลและความสำเร็จด้านประสิทธิภาพของระบบ	69

## สารบัญตาราง (ต่อ)

	หน้า
ตารางที่ 4.18 แสดงผลการประเมินประสิทธิผลและความสำเร็จด้านความสำคัญของ การป้องกันระบบ ของผู้บริหารและหัวหน้ากลุ่ม	70
ตารางที่ 4.19 แสดงผลการประเมินประสิทธิผลและความสำเร็จด้านความสำคัญของ การป้องกันระบบ ของผู้ปฏิบัติงาน	71
ตารางที่ 4.20 แสดงผลการประเมินประสิทธิผลและความสำเร็จด้านความสำคัญของ การป้องกันระบบ	71
ตารางที่ 4.21 แสดงผลการประเมินประสิทธิผลและความสำเร็จด้านความน่าเชื่อถือของระบบ ของผู้บริหารและหัวหน้ากลุ่ม	72
ตารางที่ 4.22 แสดงผลการประเมินประสิทธิผลและความสำเร็จด้านความน่าเชื่อถือของระบบ ของผู้ปฏิบัติ	72
ตารางที่ 4.23 แสดงผลการประเมินประสิทธิผลและความสำเร็จด้านความน่าเชื่อถือของระบบ	72
ตารางที่ 4.24 แสดงผลการประเมินประสิทธิผลและความสำเร็จด้านคุณภาพการให้บริการ ของผู้บริหารและหัวหน้ากลุ่ม	73
ตารางที่ 4.25 แสดงผลการประเมินประสิทธิผลและความสำเร็จด้านคุณภาพการให้บริการ ของผู้ปฏิบัติ	74
ตารางที่ 4.26 แสดงผลการประเมินประสิทธิผลและความสำเร็จด้านคุณภาพการให้บริการ	74
ตารางที่ 5.1 แสดงผลการประเมินประสิทธิผลและความสำเร็จของการใช้งานระบบ	75

## บทที่ 1

### บทนำ

#### 1.1 ความเป็นมาและความสำคัญของการดำเนินงาน

สำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช สังกัดกรมควบคุมโรค เป็นหน่วยงานวิชาการด้านป้องกันควบคุมโรค มีบทบาทหน้าที่ในการเฝ้าระวัง ติดตาม นิเทศ ถ่ายทอด องค์ความรู้ด้านการป้องกันควบคุมโรคแก่หน่วยงานเครือข่าย ซึ่งโดยทั่วไปการปฏิบัติงานของบุคลากรมีความจำเป็นต้องใช้เทคโนโลยีสารสนเทศในการวิเคราะห์ ประมวลผลข้อมูลด้านโรคและสุขภาพ และได้จัดเก็บไว้ในเครื่องคอมพิวเตอร์ที่อยู่ในเครือข่ายของหน่วยงาน ส่งผลให้มีความเสี่ยงในงานเทคโนโลยีสารสนเทศ

สำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช ได้ดำเนินการตามนโยบายระบบราชการ 4.0 ของรัฐบาล เพื่อให้มีการนำระบบเทคโนโลยีสารสนเทศและการสื่อสาร มาใช้ในการสนับสนุนการปฏิบัติงานให้เป็นไปอย่างเหมาะสม มีประสิทธิภาพ แม้การนำเทคโนโลยีสารสนเทศและการสื่อสารมาใช้ในหน่วยงานจะช่วยให้การดำเนินงานมีประสิทธิภาพมากยิ่งขึ้น แต่ส่งผลให้มีความเสี่ยงต่อความมั่นคงปลอดภัยของข้อมูล การใช้งานระบบอินเทอร์เน็ต และการป้องกันโปรแกรมไม่ประสงค์ดี เพื่อให้การเข้าถึงสารสนเทศและการสื่อสารต่าง ๆ รวมทั้งระบบอินเทอร์เน็ตมีความมั่นคงปลอดภัย ป้องกันการรั่วไหลของข้อมูล รวมทั้งเป็นการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงสาธารณสุข พ.ศ. 2565 [1]

หน่วยงานจึงได้ตระหนักถึงความสำคัญของการควบคุมการเข้าถึงระบบเครือข่ายเพื่อเป็นการป้องกันปัญหาที่อาจเกิดขึ้นจากการให้บริการเครือข่ายทั้งทางตรงและทางอ้อม จึงต้องมีการควบคุมการเข้าถึงการบริการทางเครือข่าย โดยต้องกำหนดสิทธิ์ในการเข้าถึงเครือข่าย ผู้ที่จะเข้าใช้งานต้องลงบันทึกเข้าใช้งาน (Login) ซึ่งจะแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใส่รหัสผ่านก่อนเข้าใช้งาน และกำหนดระยะเวลาเชื่อมต่อระบบสารสนเทศเพื่อให้การใช้งานระบบเครือข่ายและอินเทอร์เน็ตของหน่วยงานมีความมั่นคงปลอดภัยสามารถควบคุมการเข้าถึงโดยไม่ได้รับอนุญาตจากบุคคลภายนอกได้

ดังนั้น การยืนยันตัวบุคคลเพื่อการเข้าใช้งานระบบเครือข่ายอินเทอร์เน็ต ของสำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช จึงเป็นไปตามนโยบายและแนวปฏิบัติ ทำให้มีการพัฒนาระบบการยืนยันตัวบุคคลที่เข้าใช้งานระบบเครือข่ายอินเทอร์เน็ตเพื่อทำการจัดเก็บข้อมูลบุคลากรของหน่วยงานที่มีสิทธิ์การเข้าใช้งาน และเป็นการจัดเก็บข้อมูลการจราจรทางคอมพิวเตอร์ซึ่งเป็นไปตามพระราชบัญญัติว่าด้วยการ

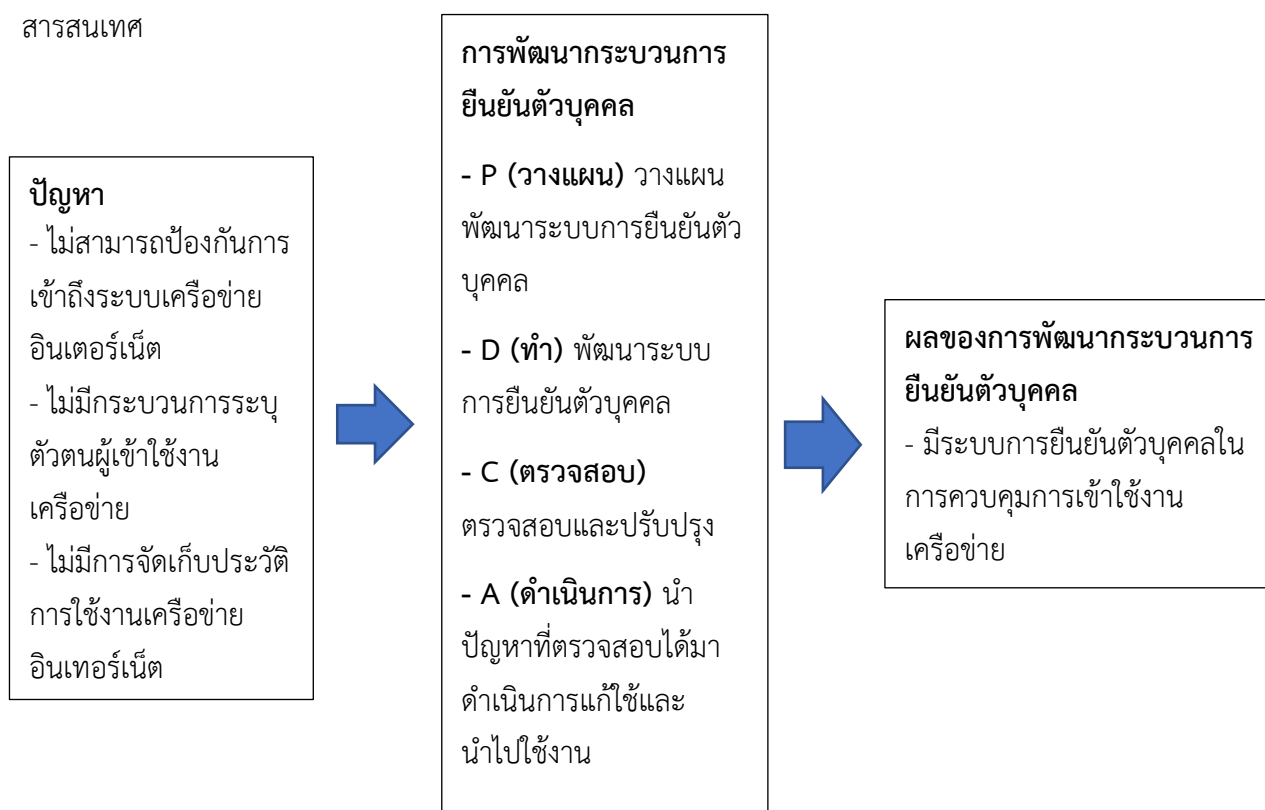
กระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 ฉบับที่ 2 [2] รวมทั้งเป็นการสร้างความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน

## 1.2 วัตถุประสงค์ของการดำเนินการ

1. เพื่อให้สามารถควบคุมการเข้าถึงการใช้งานระบบเครือข่ายอินเทอร์เน็ตของสำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช
2. เพื่อให้สามารถยืนยันตัวตนบุคคลที่ใช้งานระบบเครือข่ายอินเทอร์เน็ตของสำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช
3. เพื่อให้สามารถสืบค้นข้อมูลการจราจรทางคอมพิวเตอร์ (Log File) ย้อนหลังได้

## 1.3 กรอบแนวคิด

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



## 1.4 ประโยชน์ที่คาดว่าจะได้รับ

1. สำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช ได้ปฏิบัติตามแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ทำให้หน่วยงานมีความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ป้องกันการเข้าถึงระบบเครือข่ายจากบุคคลภายนอกที่ไม่ได้รับอนุญาต

2. สำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช มีระบบที่สามารถยืนยันตัวตนบุคคลที่ใช้งานระบบเครือข่ายอินเทอร์เน็ตโดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใส่รหัสผ่านก่อนเข้าใช้งาน

3. สำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช มีระบบที่สามารถจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log File) 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 หรือ ระบบ Authentication หมายถึง ระบบยืนยันตัวตนบุคคลเพื่อเข้าใช้งานระบบเครือข่ายอินเทอร์เน็ตของสำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช

6. Log Files คือ ข้อมูลการจราจรทางคอมพิวเตอร์ที่เกิดขึ้นจากการใช้งานระบบเครือข่ายอินเทอร์เน็ต

## 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

#### 2.1 หลักการของวงจรคุณภาพ (PDCA)

PDCA หรือวงจรเดมมิง (Deming Cycle) หรือวงจรชูฮาร์ต (Shewhart Cycle) [3] คือ วงจรบริหารงานคุณภาพ ประกอบไปด้วย 4 ขั้นตอน Plan – Do – Check - Act เป็นกระบวนการที่ใช้ปรับปรุงการทำงานขององค์กรอย่างเป็นระบบ โดยมีเป้าหมายเพื่อแก้ปัญหาและเกิดการพัฒนาอย่างต่อเนื่อง (Continuous improvement)



ภาพที่ 2.1 หลักการพัฒนา PDCA (Plan – Do – Check - Act)

โครงสร้าง PDCA ประกอบ 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 โดยขั้นตอนนี้ต้องกำหนดให้ครอบคลุมทั้งกระบวนการตั้งแต่เริ่มไปจนถึงสุดสิ้นสุด

การค้นหาปัญหาขององค์กร (Problem Recognition) คือการกำหนดเป้าหมายที่ชัดเจนในการปรับปรุงโดยใช้ระบบเข้ามาช่วยนำข้อมูลปัญหาที่ได้มาจำแนกจัดกลุ่มและจัดลำดับความสำคัญ เพื่อใช้คัดเลือกโครงการที่เหมาะสมที่สุดมาพัฒนา โดยโครงการที่จะทำการพัฒนาต้องสามารถแก้ปัญหาที่มีในองค์กรและให้ประโยชน์กับองค์กรมากที่สุด

Action Plan [4] คือ แผนปฏิบัติการทำงาน ที่ผ่านการคิดและการวางแผนมาอย่างละเอียดแล้ว เพื่อเป็นตัวกำหนดแผนการดำเนินงานทั้งหมดให้บรรลุวัตถุประสงค์ หรือกล่าวง่าย ๆ คือ ถูกสร้างมาให้เป็นแบบแผนในการปฏิบัติงาน โดยจะระบุรายละเอียดในแต่ละช่วงของการปฏิบัติงานว่า มีกิจกรรมอะไรบ้าง หรือมีการปฏิบัติงานกันอย่างไร ซึ่ง Action Plan นี้จะช่วยตรวจสอบการทำงานในแต่ละขั้นตอนของแผนปฏิบัติการทำงาน ให้สำเร็จลุล่วงตามเป้าหมายนั่นเอง

นอกจากนี้การใช้ Action Plan ยังสามารถบ่งบอกได้ถึงความสำเร็จของแต่ละงานได้ด้วย ช่วยให้ทุกคนที่มีความเกี่ยวข้องกับงาน มีแนวโน้มเข้าใจและปฏิบัติไปในทิศทางเดียวกัน ซึ่งก็จะช่วยให้การทำงานสำเร็จได้อย่างราบรื่น เร็ว และง่ายขึ้น

องค์ประกอบของ Action Plan มีดังนี้

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

- ผู้รับผิดชอบ (Owner) ในแผนการทำงานทั้งหมด จะต้องเป็นผู้รับผิดชอบเพื่อคอยตรวจสอบและติดตามงานทั้งกระบวนการ เพื่อให้งานสำเร็จตามแผนที่วางไว้

- งบประมาณ (Budget) ขึ้นตอนใด ๆ ที่กำหนดไว้จะต้องคำนึงถึงงบประมาณที่ตั้งเอาไว้ด้วย เพื่อลดความเสียหายที่อาจเกิดขึ้นได้

### 2.1.2 D – DO พัฒนาทางออกและดำเนินการตามแผน

หลังจากกำหนดแผนแล้วก็ถึงเวลาที่จะลงมือทำ เพราะจะต้องนำแผนดังกล่าวมาใช้จริง ดำเนินการจริง เพื่อให้เห็นผลลัพธ์จริง

ในขั้นตอนนี้ต้องระลึกไว้เสมอว่า การดำเนินการจะเกิดปัญหาอื่นตามมาเสมอ นั่นจึงเป็นเหตุผลว่าควรใช้แผนดังกล่าวกับทีมงานหรือไม่ก็คนหรือเป็นโปรเจกต์เล็ก ๆ เสียก่อน เพราะสภาพแวดล้อมที่ควบคุมได้จะป้องกันความเสียหายที่เกิดขึ้นไม่ให้ส่งผลกระทบต่อทั้งบริษัท

### 2.1.3 C – Check ประเมินและสรุปผล

เมื่อดำเนินการมาถึงจุดหนึ่งแล้ว จะต้องตรวจสอบให้ได้ว่า แผนดังกล่าวมีผลลัพธ์เป็นไปตามตัวชี้วัดที่ต้องการหรือไม่

ถ้าประสบความสำเร็จตามตัวชี้วัด ก็สามารถดำเนินการไปสู่ขั้นตอนสุดท้ายได้เลย แต่ถ้าไม่ประสบความสำเร็จ ก็ควรนำข้อมูลที่ได้มาวิเคราะห์หาสาเหตุของปัญหา แล้วดำเนินการขั้นตอนที่ 1 – 3 ใหม่จนกว่าจะประสบความสำเร็จหรือผ่านตัวชี้วัดที่กำหนดไว้

### 2.1.4 A – Act ปรับปรุงแก้ไขและวางแผนใหม่ต่อไป

ถ้าการปฏิบัติแผนดังกล่าวประสบความสำเร็จเป็นอย่างดี ก็ถึงเวลานำแผนนั้นมาประยุกต์ใช้กับทุกคนองค์กร ผ่านการประกาศ ประชุม อีเมล หรือการจัดการอบรมภายในบริษัท เพื่อสร้างการเปลี่ยนแปลงจนเกิดตามมาตรฐานใหม่



## 2.2 การพิสูจน์ตัวตน (Authentication) [5]

การระบุตัวตนการพิสูจน์ตัวตน และการให้สิทธิ์ เป็นกระบวนการที่นำเทคโนโลยีมาใช้ควบคู่กับทรัพยากรคนและกระบวนการ เพื่อเป็นการเพิ่มประสิทธิภาพและศักยภาพในการรักษาความลับ (Confidentiality) ความถูกต้อง (Integrity) และความพร้อมใช้ของข้อมูล (Availability) รวมถึงเพื่อไม่ให้เกิดการถูกคุกคามโดยผู้ไม่ประสงค์ดีหรือจากโปรแกรมบางประเภทได้เพิ่มมากขึ้น หากเกิดการคุกคามหรือถูกบุกรุกขึ้นอาจนำมาซึ่งความเสียหายอย่างมากมายต่อองค์กร ในการดำเนินการนี้จะช่วยให้รูปแบบการรักษาความปลอดภัยของข้อมูลเป็นไปอย่างเหมาะสม และช่วยลดความเสี่ยงจากการปลอมแปลงตัวบุคคลที่เกิดมาจากการทำธุรกรรมต่าง ๆ โดยรูปแบบของกระบวนการเหล่านี้ถือว่าเป็นองค์ประกอบที่สำคัญเนื่องจากจำเป็นต้องอาศัยเทคโนโลยี และความรู้เฉพาะทางเพื่อที่จะใช้ในการควบคุมข้อมูลต่าง ๆ ซึ่งสามารถแบ่งออกเป็น 3 ขั้นตอน ดังนี้

### 2.2.1 การระบุตัวตน (Identification)

การระบุตัวตน เป็นการค้นหาและเปรียบเทียบตัวบุคคลโดยดึงข้อมูลจากระบบที่เป็นฐานข้อมูลของผู้ใช้งาน ซึ่งเป็นขั้นตอนที่ผู้ใช้งานจำเป็นต้องแสดงตัวตน เช่น การกรอกชื่อผู้ใช้งาน (Username) หรือรหัสผู้ใช้งาน (User ID) เพื่อเข้าใช้งานในระบบ หรือการใช้บัตรประจำตัวประชาชนในการระบุตัวตนของแต่ละบุคคล ทั้งนี้ ในปัจจุบันชื่อผู้ใช้งาน และรหัสผู้ใช้งาน อาจจะยังไม่เพียงพอที่จะใช้ในการระบุตัวตนของผู้ใช้งานจริง ดังนั้น จำเป็นที่จะต้องเก็บข้อมูลอย่างอื่น 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 เป็นวิธีการที่ที่พบเจอได้มากที่สุด อย่างไรก็ตามกลไกของการพิสูจน์ตัวตน (Authentication mechanisms) ที่นำมาช่วยในการสร้างความปลอดภัย สามารถแบ่งได้ 3 คุณลักษณะ ดังนี้

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 รูปแบบ ดังนี้

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 [6]

The CIA Triad เป็นแนวคิดที่สำคัญในด้านการรักษาความปลอดภัยของข้อมูล ช่วยให้เรามั่นใจได้ในเรื่องของการปกป้องข้อมูลที่ละเอียดอ่อนจากการเข้าถึง การดัดแปลง 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 สามารถ

ทำได้ด้วยวิธีต่างๆ 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) และ ผู้ใช้ (User)

### 2.4.2 Active Directory [7]

Active Directory เป็นเทคโนโลยี หรือการบริการที่เรียกได้ว่า 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

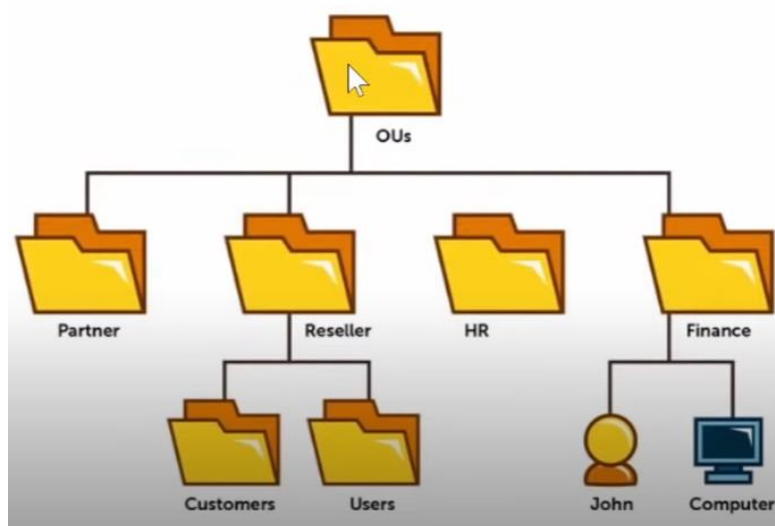
### 2.4.3 Group Policy [8]

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 จึงจะ

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



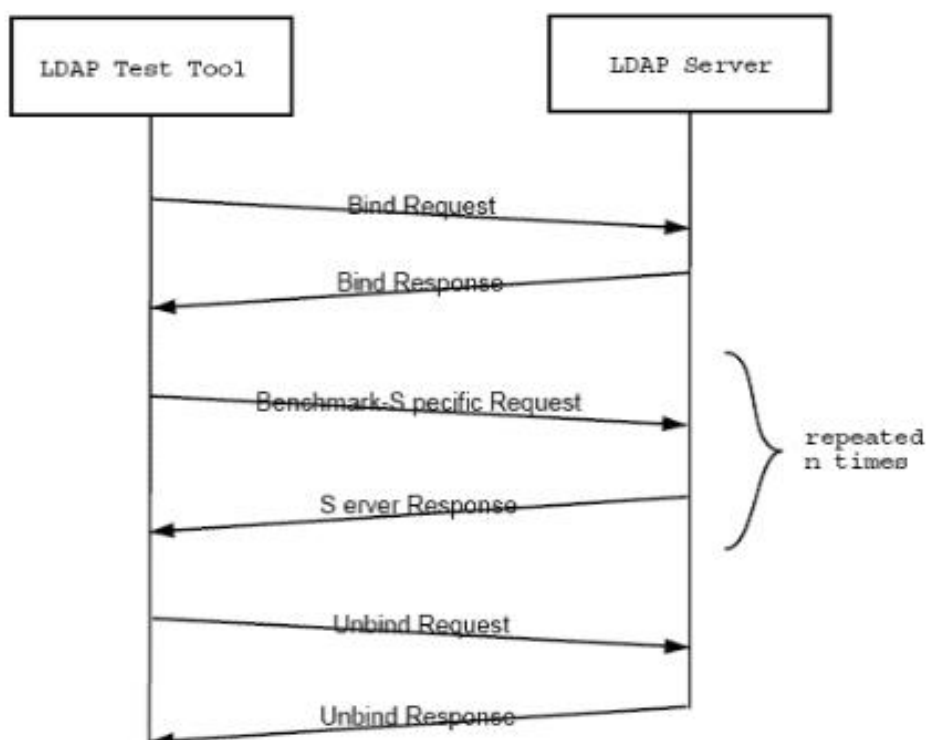
ภาพที่ 2.2 ตัวอย่างการแบ่ง Organizational Unit

#### 2.4.5 Lightweight Directory Access Protocol (LDAP) [9]

Lightweight Directory Access Protocol (LDAP) เป็น Protocol ที่ใช้สำหรับค้นหาข้อมูลในฐานข้อมูล ก่อนที่จะลงลึกกว่า LDAP คืออะไร มาดูที่มากันก่อน Directory Access Protocol (DAP) คือมาตรฐาน X.500 ของ Directory ในระบบ Network ซึ่ง LDAP เป็น “lightweight” นั้น หมายถึง มีขนาดเล็ก เพราะ Version เริ่มต้นไม่ได้มีระบบ Security มาด้วย ส่วนใหญ่จะนำเอามาใช้กับข้อมูลจำพวกรายละเอียดของพนักงาน 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 2.3 จำลองการทำงานของ Lightweight Directory Access Protocol (LDAP)

#### 2.4.6 WatchGuard Log Server [10]

WatchGuard Log Server เป็นส่วนหนึ่งของ WatchGuard Server Center มันเป็นฐานข้อมูลที่สามารถเก็บรวบรวมข้อมูลข้อความบันทึกจาก Watchguard Firebox ที่เชื่อมต่อกับระบบ คุณสามารถติดตั้ง WatchGuard Log Server ได้ทั้งบนคอมพิวเตอร์ที่ใช้สำหรับการจัดการหรือบนคอมพิวเตอร์อื่น ๆ คุณยังสามารถเพิ่มเซิร์ฟเวอร์บันทึกเพิ่มเติมเพื่อการสำรองข้อมูลและการขยายขนาดได้อีกด้วยในการทำเช่นนี้ คุณจะใช้โปรแกรมติดตั้ง WatchGuard System Manager (WSM) และเลือกติดตั้งเฉพาะส่วนประกอบของ Log Server เท่านั้น โดย Log Server บันทึกข้อมูลรับข้อมูลผ่านพอร์ต TCP 4107 และ 4115 Watchguard Firebox ทุกเครื่องที่เชื่อมต่อกับ Log Server จะบันทึกข้อมูลจะส่งชื่อเครื่องหมายเลขซีเรียล โซนเวลา ข้อมูลบันทึกเรื่องการจราจรของตัวเองมายัง Log Server

## 2.5 กฎหมาย นโยบาย มาตรฐาน ที่เกี่ยวข้องกับการปฏิบัติงาน

### 2.5.1 นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงสาธารณสุข พ.ศ. 2565

กระทรวงสาธารณสุขได้ประกาศใช้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ ของกระทรวงสาธารณสุข พ.ศ. 2565 [1] เมื่อวันที่ 23 มีนาคม 2565 ตามแนวทางพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 สำนักงานปลัดกระทรวงสาธารณสุข จึงขอให้หน่วยงานในสังกัดกระทรวงสาธารณสุขทุกแห่งถือปฏิบัติตามประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ พ.ศ. 2565 โดยเคร่งครัด

### 2.5.2 พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560

พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 [ได้ประกาศลงในราชกิจจานุเบกษาแล้ว เมื่อวันที่ 23 มกราคม พ.ศ.2560 และมีผลใช้บังคับตั้งแต่วันที่ 24 มกราคม พ.ศ. 2560 เป็นต้นไป พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 คือพระราชบัญญัติที่ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ซึ่งคอมพิวเตอร์ในปัจจุบันก็รวมถึงคอมพิวเตอร์ตั้งโต๊ะ คอมพิวเตอร์โน้ตบุ๊ก สมาร์ทโฟน รวมถึงระบบต่างๆ ที่ถูกควบคุมด้วยระบบคอมพิวเตอร์ด้วย ซึ่งเป็นพ.ร.บ.ที่ตั้งขึ้นมาเพื่อป้องกัน ควบคุมการกระทำผิดที่จะเกิดขึ้นได้จากการใช้คอมพิวเตอร์ หากใครกระทำความผิดตาม พ.ร.บ. คอมพิวเตอร์นี้ ก็จะต้องได้รับการลงโทษตามที่ พ.ร.บ. กำหนดไว้

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

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

- สิทธิได้รับการแจ้งให้ทราบ (Right to be informed)

ผู้มีส่วนเกี่ยวข้องทั้งหมด ไม่ว่าจะเป็น HR ฝ่าย IT ต้องแจ้งเจ้าของข้อมูลให้ทราบถึงวัตถุประสงค์ที่จะนำข้อมูลไปใช้ รวมถึงช่องทางในการติดต่อผู้ควบคุมข้อมูล นอกจากนี้ยังต้องบอกระยะเวลาใช้งานข้อมูลอย่างชัดเจน

- สิทธิขอเข้าถึงข้อมูลส่วนบุคคล (Right of access)

พนักงานมีสิทธิเข้าถึงข้อมูลที่เกี่ยวข้องกับตนเองและขอสำเนาข้อมูลจากผู้ควบคุมข้อมูล ทั้งยังขอทราบข้อมูลที่ได้มาโดยไม่ได้ขออนุญาตได้อีกด้วย (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 แนวคิดทฤษฎีเกี่ยวกับการประเมิน

การประเมินแบบ Goal Base Evaluation [12] เป็นรูปแบบการประเมินที่เสนอโดย เป็นการประเมินที่ยึดเป้าหมายหรือวัตถุประสงค์ของโครงการเป็นเกณฑ์ในการประเมินความสำเร็จของโครงการ โดยการนำผลที่ได้จากการวัดหรือเก็บรวบรวมข้อมูลมาเปรียบเทียบกับเป้าหมายทั้งในเชิงปริมาณและเชิงคุณภาพของโครงการ

การประเมินแบบ Goal Free Evaluation เป็นรูปแบบการประเมินที่เสนอโดย Scriven เป็นการประเมินที่ไม่ได้ยึดเฉพาะเป้าหมายของโครงการเป็นเกณฑ์เท่านั้น แต่จะพิจารณาผลที่เกิดขึ้นทั้งหมดอันเนื่องมาจากโครงการ ได้แก่ ผลโดยตรง ผลโดยอ้อม และผลกระทบทั้งทางบวกและทางลบ

เนื่องมาจากโครงการ ได้แก่ ผลโดยตรง ผลโดยอ้อม และผลกระทบทั้งทางบวกและทางลบ

## 2.7 ทฤษฎีการคำนวณหากลุ่มตัวอย่าง Taro Yamane

Taro Yamane[13] คือ หนึ่งในสูตรคำนวณขนาดกลุ่มตัวอย่างที่เหมาะสมสำหรับงานวิจัยเพื่อแจกแบบสอบถามโดยการใช้สูตร ทาโร่ ยามาเน (Taro Yamane) ในการ คำนวณขนาดกลุ่มตัวอย่าง จะทำให้รู้ว่าควรแจกแบบสอบถามให้กับกลุ่มตัวอย่างกี่คน แทนที่จะต้องแจกให้กับกลุ่มตัวอย่างทุกคน สูตร Taro Yamane (ทาโร่ ยามาเน) หรือสูตรอื่นในการ คำนวณหาขนาดกลุ่มตัวอย่าง ที่เหมาะสมเป็นสิ่งจะช่วยให้ผู้วิจัย (สำหรับงานวิจัยเชิงสำรวจ) ไม่ต้องแจกแบบสอบถามให้กับกลุ่มตัวอย่างของงานวิจัยทุกคนที่อาจมีจำนวนหลายพันคน โดยการใช้สูตร Taro Yamane คำนวณหาขนาดกลุ่มตัวอย่างที่เหมาะสมในงานวิจัยเชิงสำรวจ (Survey Research) ซึ่งจะช่วยลดจำนวนกลุ่มตัวอย่างที่ต้องแจกแบบสอบถามจากพันหรือหมื่นคน เหลือเพียงหลักร้อยคน



## บทที่ 3

### วิธีการดำเนินการ

การพัฒนาระบบยืนยันตัวตนบุคคลที่ใช้งานระบบเครือข่ายอินเทอร์เน็ตของสำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช มีจุดมุ่งหมายเพื่อควบคุมและยืนยันการเข้าถึงเครือข่ายอินเทอร์เน็ต เพื่อให้การใช้ระบบเทคโนโลยีสารสนเทศให้เป็นไปอย่างเหมาะสม มีความมั่นคงปลอดภัย

#### 3.1 เครื่องมือที่ใช้วิจัย

1. ระบบยืนยันตัวตนบุคคลที่ใช้งานระบบเครือข่ายอินเทอร์เน็ตที่ผู้วิจัยได้พัฒนาขึ้นใช้สำหรับจัดเก็บข้อมูลสิทธิ์การใช้งานและตรวจสอบสิทธิ์ผู้ใช้งานโดย Firewall
2. ระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์โดยใช้โปรแกรม WatchGuard Server Center ซึ่งเป็นโปรแกรมที่ใช้งานร่วมกับ Firewall WatchGuard M4600 ทำหน้าที่จัดเก็บและแสดงข้อมูลจราจรคอมพิวเตอร์โดยแสดงผลเป็นเว็บอินเทอร์เน็ตเพลสซึ่งสามารถใช้งานได้ง่าย
3. อุปกรณ์ป้องกันเครือข่าย (Firewall) เพื่อใช้เป็นระบบรักษาความปลอดภัยเครือข่าย ทำหน้าที่คอยตรวจจับ ตรวจสอบสิทธิ์ และให้สิทธิ์ในการเข้าถึงเครือข่าย คัดกรองผู้ใช้งานตามนโยบายที่ผู้วิจัยได้กำหนด
4. เครื่องคอมพิวเตอร์สำนักงานใช้สำหรับทดสอบการใช้งาน
5. ใช้แบบสอบถามที่ผู้วิจัยสร้างขึ้นเอง โดยกลุ่มตัวอย่างตอบด้วยตนเอง

#### 3.2 การเก็บรวบรวมข้อมูล

1. กำหนดการเก็บข้อมูลในส่วนของประวัติการเข้าใช้งานโดยกำหนดระยะเวลาเก็บข้อมูลจำนวน 47 วัน โดยคิดจากจำนวนวันที่จัดเก็บข้อมูลทั้งหมด 90 วันโดยวิธีคำนวณของ ทาโร่ ยามาเนะ ตั้งแต่วันที่ 24 กันยายน พ.ศ. 2566 ถึงวันที่ 9 พฤศจิกายน พ.ศ. 2566 เพื่อเป็นการตรวจสอบความสามารถในการป้องกันการเข้าถึงเครือข่ายและการระบุตัวตนผู้ใช้งานเครือข่าย โดยการ export ออกมาในรูปแบบไฟล์ CSV ข้อมูลที่จัดเก็บโดย WatchGuard Server Center ซึ่งข้อมูลที่ได้จะจัดเก็บอยู่ในรูปแบบตาราง เพื่อนำไปวิเคราะห์ต่อไป โดยแสดงตัวอย่างโครงสร้างตารางข้อมูลดังตารางที่ 3.1

ตารางที่ 3.1 แสดงผลการจัดเก็บข้อมูล

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

โดยข้อมูลสามารถแสดงให้เห็นว่าใคร (User) ใช้งานจากที่ใด (IP Address) เริ่มต้นการใช้งานเมื่อไหร่ (Login Time) สิ้นสุดการใช้งานเมื่อไหร่ (Logout Time) ระยะเวลาการใช้งานรวมเท่าไหร่ (Duration) สิทธิการใช้งานอนุญาตผ่านช่องทางใด (Method) และสถานการณ์ใช้งานเป็นอย่างไร (Status) ซึ่งสถานะการใช้งานจะแสดงถึงว่าผู้ใช้งานผู้นั้นสามารถเข้าถึงระบบได้หรือไม่ เพื่อนำข้อมูลดังกล่าวไปวิเคราะห์ศักยภาพในการให้บริการระบบเครือข่ายและระดับความสามารถในการป้องกัน ควบคุม ระบุตัวตนผู้ใช้งานเครือข่าย

2. ผู้วิจัยได้เก็บรวบรวมข้อมูลโดยออกแบบสอบถามสร้างเป็นแบบสอบถามออนไลน์ให้บุคลากรในสำนักงานป้องกันควบคุมโรคที่ 11 และ ศตม.11.2 นครศรีธรรมราช ตอบแบบสอบถามเอง (Self-Administration) โดยได้ประเมินประสิทธิผลและความสำเร็จของระบบใน 4 ปัจจัย ดังนี้

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

### 3.3 วิเคราะห์ข้อมูล

1. วิเคราะห์ความสามารถในการป้องกันการเข้าใช้งานเครือข่าย ผู้วิจัยได้นำข้อมูลที่ได้ มาทำการวิเคราะห์ข้อมูลพร้อมทั้งเขียนรายงานผลในรูปแบบตาราง เพื่อสรุปผลให้เข้าใจง่าย การวิเคราะห์ข้อมูล โดยใช้สถิติพรรณนา ได้แก่ ค่าต่ำสุด ค่าสูงสุด ร้อยละ ส่วนเบี่ยงเบนมาตรฐานและค่าเฉลี่ย

2. วิเคราะห์ความสามารถในการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ โดยทำการค้นหาข้อมูลประวัติการใช้งานเครือข่ายเพื่อดูความครบถ้วน ถูกต้องของข้อมูล

3. วิเคราะห์ความสามารถในการจัดเก็บข้อมูลตามข้อกำหนด โดยการเปรียบเทียบระยะเวลาในการจัดเก็บที่ผ่านมา กับระยะเวลาในการจัดเก็บตามเป้าหมาย เพื่อดูขนาดพื้นที่ความจุว่าเพียงพอหรือไม่

4. วิเคราะห์ความสามารถในการปฏิบัติตามมาตรการที่ได้กำหนดไว้ โดยเปรียบเทียบความสามารถในการทำงานของระบบกับ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกระทรวงสาธารณสุข พ.ศ. 2565 และ พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560

5. จากการเก็บข้อมูลแบบสอบถาม ผู้วิจัยได้นำข้อมูลที่ได้ มาทำการวิเคราะห์และแปลผลข้อมูล พร้อมทั้งเขียนรายงานผลในรูปแบบตาราง เพื่อสรุปข้อมูลให้เข้าใจได้ง่าย ซึ่งสถิติที่ใช้ ได้แก่ เฉลี่ยและส่วนเบี่ยงเบนมาตรฐาน (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 ส่วนดังนี้

1. บุคลากรที่ใช้ในการวิจัยครั้งนี้ ได้แก่ บุคลากรในสำนักงานป้องกันควบคุมโรคที่ 11 และ ศตม.11.2 นครศรีธรรมราชที่มีสิทธิ์เข้าใช้งานเครือข่ายอินเทอร์เน็ตของหน่วยงานจำนวน 160 คน ผู้วิจัยได้ทำการสุ่มตัวอย่างของบุคลากรจำนวน 114 คน โดยได้จากการคำนวณของสูตรของ ทาโร่ ยามาเน ในการกำหนดตัวอย่าง โดยเลือกระดับความเชื่อมั่น 95% ค่าระดับความคลาดเคลื่อนยอมรับได้ไม่เกิน 5% หรือ 0.05 ของระดับนัยสำคัญ

การสุ่มตัวอย่างดังกล่าวของบุคลากรในสำนักงานป้องกันควบคุมโรคที่ 11 และ ศตม.11.2 นครศรีธรรมราช ที่มีสิทธิ์เข้าใช้งานเครือข่ายอินเทอร์เน็ตได้ดังนี้

ตามวิธีของ ยามาเน (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. การจัดเก็บข้อมูลจรรยาบรรณคอมพิวเตอร์ภายในสำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช ผู้วิจัยได้ทำการสุ่มตัวอย่างข้อมูลจำนวน 47 วัน โดยได้จากการคำนวณสูตรของ ทาโร่ ยามาเน ในการกำหนดตัวอย่าง โดยเลือกระดับความเชื่อมั่น 90% ค่าระดับความคลาดเคลื่อนยอมรับได้ไม่เกิน 10% หรือ 0.10 ของระดับนัยสำคัญ

ตามวิธีของ ยามาเน (Taro Yamane)

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

เมื่อ n คือ ขนาดกลุ่มตัวอย่าง

N คือ ขนาดประชากร

e คือ ความคลาดเคลื่อนของกลุ่มตัวอย่าง

$$\begin{aligned} \text{แทนค่าได้เท่ากับ} &= \frac{90}{1+(90(0.01))} \\ &= \frac{90}{1.9} \\ &= 47.3 \text{ จำนวนสุ่มตัวอย่าง} \end{aligned}$$

### 3.4.2 การชี้วัดความสำเร็จ

ความสำเร็จของการพัฒนาระบบในครั้งนี้ สามารถแบ่งการชี้วัดความสำเร็จได้เป็น 2 ส่วน ดังนี้

1. ส่วนของการให้บริการระบบ สามารถวัดผลได้โดยใช้แบบสอบถามเกี่ยวกับประสิทธิภาพการใช้งานของระบบ ด้านความสำคัญของการป้องกันระบบของระบบ ความน่าเชื่อถือของระบบ และคุณภาพการให้บริการ ซึ่งเป็นแบบสอบถามมาตราส่วนประมาณค่า มี 5 ระดับความพึงพอใจ 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)
-------------------------	------------------	----------------------	-------------------	-------------------------

เกณฑ์การประเมินในภาพรวม กำหนด 5 ระดับโดยใช้สูตรการคำนวณความกว้างของแต่ละอันตรภาคชั้น ดังนี้

โดยใช้ค่าคะแนนนำมาคำนวณความกว้างแต่ละอันตรภาคชั้นใช้สูตร

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

$$5$$

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

$$5$$

หลังจากได้ค่าที่ได้มาจากการคำนวณช่วงระดับคะแนนดังกล่าวแล้วนำค่าที่ได้นั้นมาแบ่งเป็นระดับความพึงพอใจ ได้ 5 ระดับดังนี้

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 เพื่อให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกระทรวงสาธารณสุข พ.ศ. 2565 และพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 ฉบับที่ 2 โดยมีประเด็นที่จะนำมาชี้วัดดังต่อไปนี้

2.1 นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกระทรวงสาธารณสุข พ.ศ. 2565

1) ข้อ 5.1.1 การเข้าถึงระบบสารสนเทศ ต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง กำหนดสิทธิ์ เพื่อให้ผู้ใช้งานในทุกระดับได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

2) ข้อ 5.1.2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงระบบสารสนเทศและป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ต้องกำหนดให้มีการลงทะเบียนผู้ใช้งาน ตรวจสอบบัญชีผู้ใช้งาน อนุมัติและกำหนดรหัสผ่านการลงทะเบียนผู้ใช้งาน เพื่อให้ผู้ใช้งานที่มีสิทธิ์เท่านั้นที่สามารถเข้าใช้ระบบสารสนเทศได้ และต้องเก็บบันทึกข้อมูลการเข้าถึงและข้อมูลจราจรทางคอมพิวเตอร์ตลอดจนบริหารจัดการสิทธิ์การเข้าถึงข้อมูลให้เหมาะสมตามระดับชั้นความลับของผู้ใช้งาน ต้องมีการทบทวนสิทธิ์การใช้งานและตรวจสอบการละเมิดความปลอดภัยเสมอ

3) ข้อ 5.1.3 การควบคุมการเข้าถึงเครือข่าย เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ต้องกำหนดสิทธิ์ในการเข้าถึงเครือข่าย ให้ผู้ที่เข้าใช้งานต้องลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใส่ รหัสผ่านก่อนการเข้าใช้งาน ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์สำหรับใช้งานอินเทอร์เน็ตโดยผ่านระบบ

รักษาความปลอดภัยตามที่กระทรวงสาธารณสุขจัดสรรไว้ และมีการออกแบบระบบเครือข่ายโดยแบ่งเขต (Zone) การใช้งาน เพื่อให้การควบคุมและป้องกันภัยคุกคามได้อย่างเป็นระบบและมีประสิทธิภาพ

4) ข้อ 5.1.4 การควบคุมการเข้าถึงโปรแกรมประยุกต์และแอปพลิเคชัน ต้องกำหนดสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศที่สำคัญ โปรแกรมประยุกต์หรือแอปพลิเคชันต่าง ๆ รวมถึง จดหมายอิเล็กทรอนิกส์(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”

จากนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกระทรวงสาธารณสุข พ.ศ. 2565 และพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2560 ดังข้างต้น ทำให้สามารถนำประเด็นดังกล่าวมาใช้เป็นเกณฑ์ชี้วัดได้ดังนี้

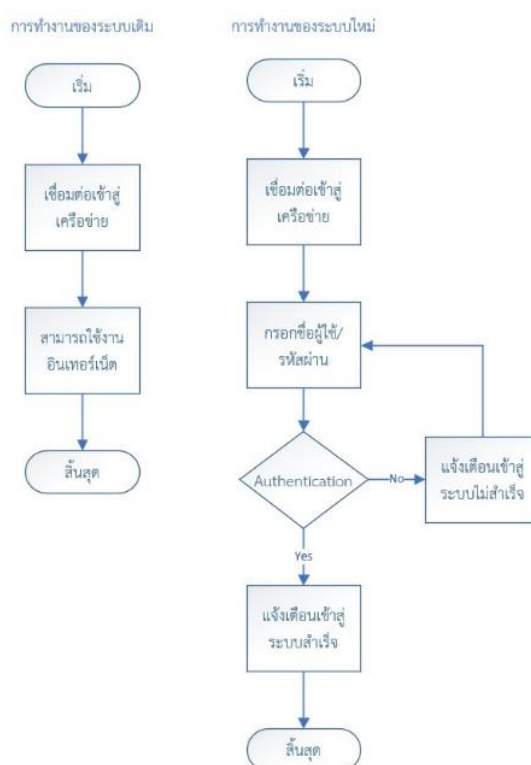
### ตารางที่ 3.2 ประเด็นและรายละเอียดเกณฑ์การให้คะแนน

รายละเอียดการวัดผล	คะแนน	คะแนนรวม
1. สามารถควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลได้	1	1
2. สามารถบริหารจัดการการเข้าถึงของผู้ใช้งานเพื่อควบคุมการเข้าถึงระบบสารสนเทศได้	1	2
3. สามารถควบคุมการเข้าถึงเครือข่าย เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาตได้	1	3
4. สามารถควบคุมการเข้าถึงโปรแกรมประยุกต์และแอปพลิเคชันได้	1	4
5.สามารถเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์	1	5

### 3.5 การพัฒนาระบบงานตามหลัก PDCA

#### ขั้นตอนการวางแผน (Plan)

1. ดำเนินการสำรวจปัญหาและข้อบกพร่องของกระบวนการเข้าถึงระบบเครือข่ายของสำนักงานป้องกันควบคุมโรคที่ 11 นครศรีธรรมราช กำหนดวัตถุประสงค์ พร้อมทั้งทำความเข้าใจในสิ่งที่ต้องการจะแก้ไขซึ่งสามารถนำผลการสำรวจมาเขียนเป็นแผนงานเปรียบเทียบกับขั้นตอนการทำงานได้ดังนี้



ภาพที่ 3.1 แสดงผังงาน (Flowchart) เปรียบเทียบการเข้าถึงเครือข่ายด้วยรูปแบบเดิมเปรียบเทียบกับระบบใหม่

2. เก็บรวบรวมข้อมูลและศึกษาความเป็นไปได้ในวิธีการที่ใช้ในการแก้ไขปัญหา จากทรัพยากรที่มีอยู่ โดยได้ทำการวิเคราะห์ความต้องการของระบบและเปรียบเทียบกับทรัพยากรที่มีอยู่ได้ดังนี้

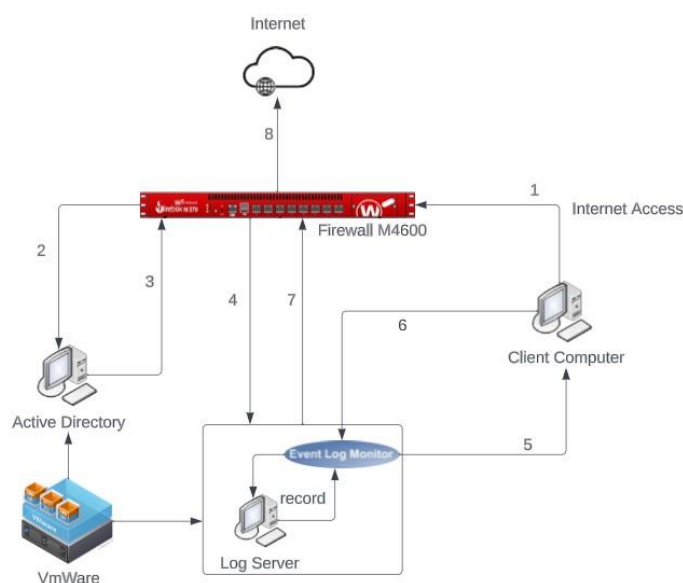
ตารางที่ 3.3 แสดงผลการเปรียบเทียบทรัพยากรของหน่วยงาน

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

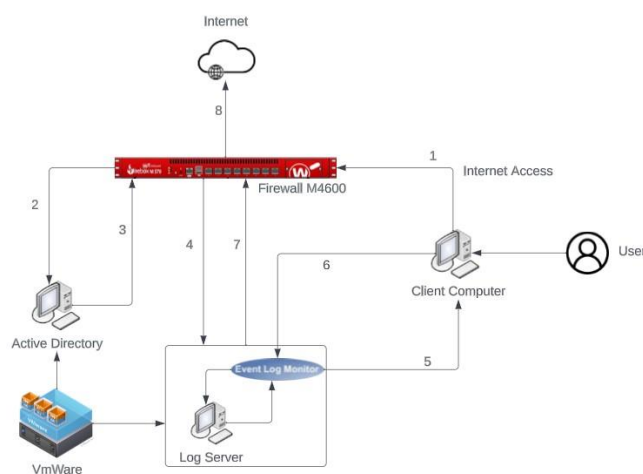
จากตารางที่ 3.3 แสดงผลการเปรียบเทียบทรัพยากรที่หน่วยงานจำเป็นต้องจัดหากับทรัพยากรที่หน่วยงานมีอยู่จึงสรุปได้ว่า สามารถดำเนินการได้ให้ระบบสามารถทำงานได้โดยไม่ต้องใช้งบประมาณในการดำเนินการเพิ่ม และสามารถปรับปรุงเครื่องมือให้ทันสมัยเพิ่มขึ้นได้ในอนาคต

### 3. วางแผนกำหนดวิธีดำเนินการแก้ปัญหา เพื่อให้บรรลุเป้าหมาย

3.1 กำหนดรูปแบบการทำงานของระบบที่กำลังจะพัฒนาเพื่อให้เห็นการทำงานของระบบภาพรวมซึ่งสามารถนำมาจำลองเป็นรูปภาพกระบวนการทำงานและลำดับของการทำงานได้ดังนี้

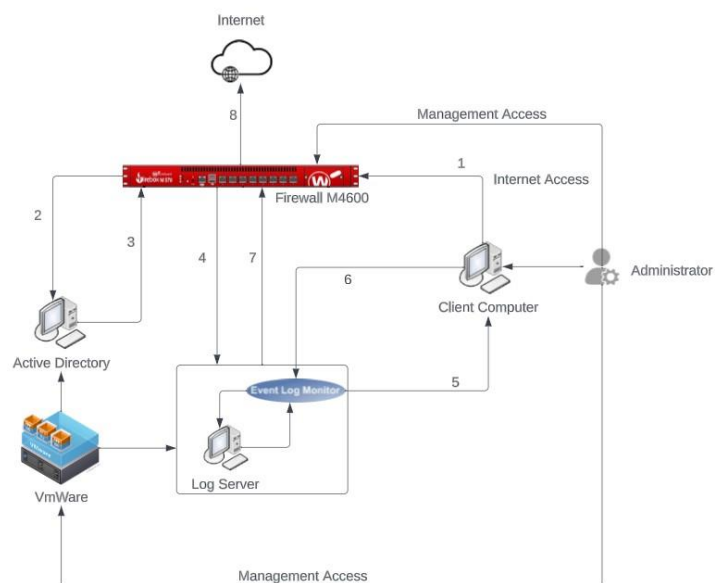


ภาพที่ 3.2 แสดงลำดับกระบวนการทำงานของระบบในภาพรวมโดยแสดงลำดับการทำงานของระบบตามหมายเลขที่ได้กำกับไว้ตามลำดับ



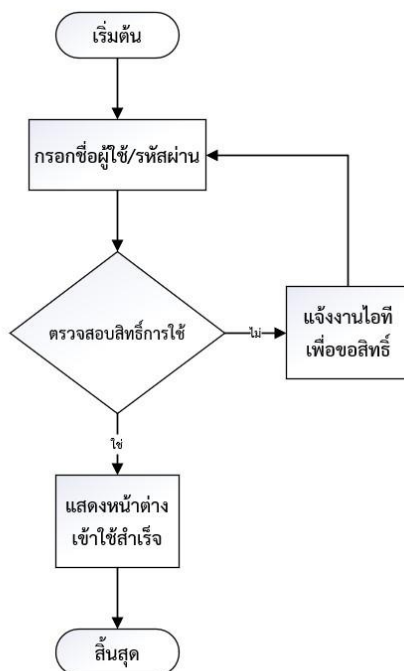
ภาพที่ 3.3 แสดงลำดับการทำงานของระบบกรณีที่ User เป็นผู้ใช้งาน



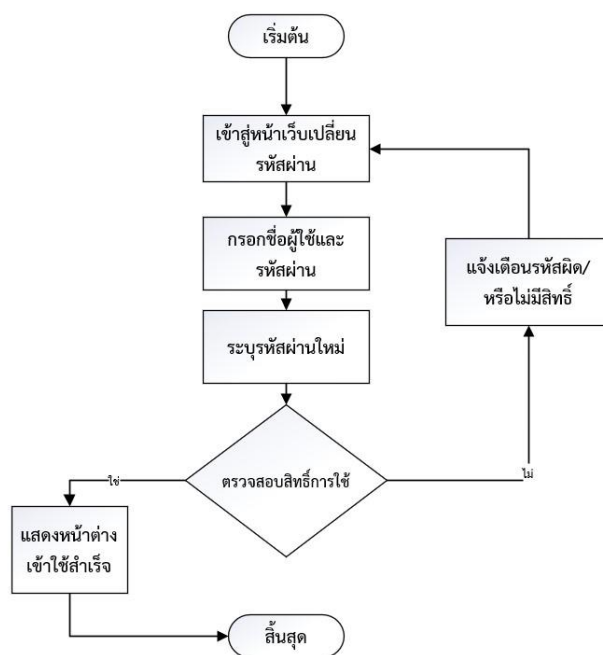


ภาพที่ 3.4 แสดงลำดับกระบวนการทำงานของระบบในกรณีที่เป็นผู้ดูแลระบบ ซึ่งผู้ดูแลระบบสามารถเข้าถึง Database และ Policy

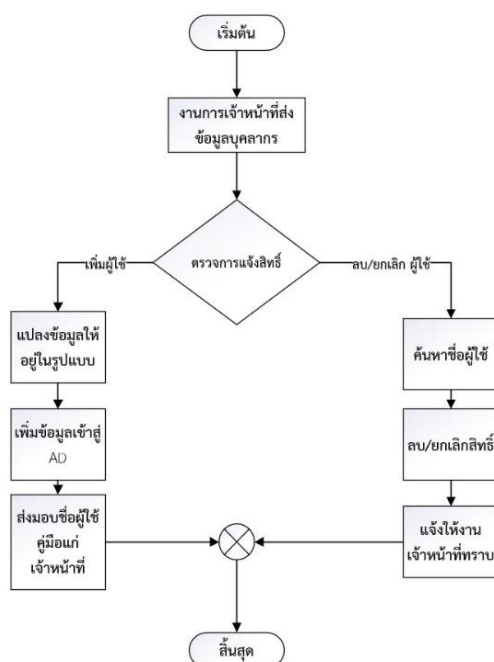
3.2 ออกแบบการใช้งานระบบในแต่ละงานและนำมาเขียนให้อยู่ในรูปแบบของผังงาน (Flowchart) ได้ดังนี้



ภาพที่ 3.5 แสดงขั้นตอนการเข้าสู่ระบบและการขอสิทธิ์การใช้งาน

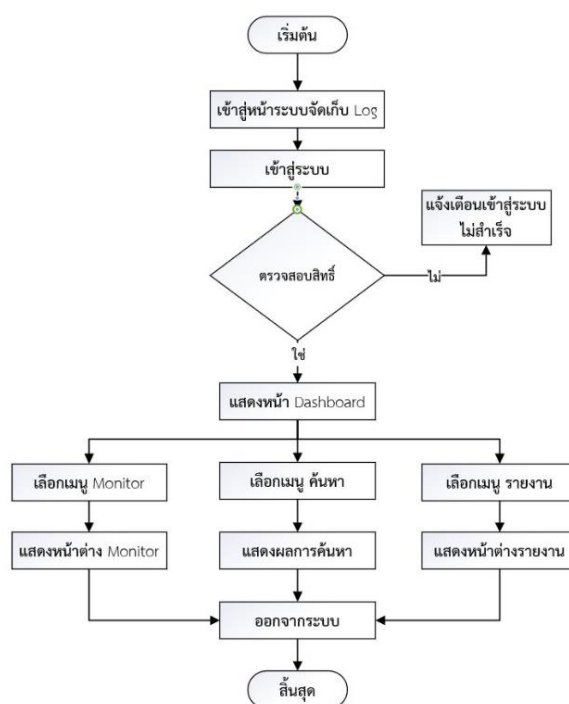


ภาพที่ 3.6 แสดงขั้นตอนการเปลี่ยนรหัสผ่าน



ภาพที่ 3.7 แสดงขั้นตอนการรับข้อมูลจากงานกรเจ้าหน้าที่ เพื่อทำการลงทะเบียนเพิ่ม/ลบ สิทธิการใช้งาน

3.3 นำการทำงานของโปรแกรมจัดเก็บและรายงานข้อมูลจราจรคอมพิวเตอร์มาเขียนให้อยู่ในรูปของผังงานเพื่อให้เห็นภาพการทำงานของระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์



ภาพที่ 3.8 แสดงผังการทำงานของระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์

#### 4. นำข้อมูลจากงานการเจ้าหน้าที่มาวิเคราะห์

เนื่องจากข้อมูลที่งานการเจ้าหน้าที่เก็บ เป็นส่วนหนึ่งของข้อมูลส่วนบุคคลของบุคลากร ซึ่งการนำข้อมูลมากำหนดให้อยู่ในรูปแบบของ Username และ Password จึงจำเป็นต้องตัดข้อมูลที่ไมจำเป็นต้องเก็บออก และดำเนินการแจ้งให้บุคลากรมีสิทธิ์ตามพ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ทราบสิทธิ์ดังนี้

- 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)

โดยข้อมูลที่รับมาประกอบด้วย ลำดับ ประเภทการจ้าง เลขที่ตำแหน่ง ชื่อ-สกุล ภาษาไทยและภาษาอังกฤษ ตำแหน่ง ระดับ ซึ่งทั้งหมดเป็นข้อมูลพื้นฐานและข้อมูลส่วนบุคคลประเภททั่วไปไม่มีข้อมูลส่วนบุคคลที่มีความอ่อนไหว

ภายใต้วัตถุประสงค์ของการใช้ระบบการยืนยันตัวตนบุคคลเพื่อให้สามารถระบุตัวตนของผู้ใช้งานได้จึงได้กำหนดรูปแบบของการตั้ง Username ไว้ดังนี้

1.1 ใช้ชื่อภาษาอังกฤษตามด้วย. และตัวอักษรภาษาอังกฤษตัวแรกของนามสกุล

1.2 หากมีชื่อผู้ให้เข้าให้ใช้เป็นภาษาอังกฤษตามด้วย ‘.’ ตัวอักษรภาษาอังกฤษสองตัวแรกของนามสกุลและได้ดำเนินการกำหนด Password โดยใช้วิธีการ random password โดยกำหนดความยาวไว้ที่ 8 ตัวอักษร โดยมีโครงสร้างของข้อมูลดังนี้

ตารางที่ 3.4 แสดงตารางโครงสร้างการจัดเก็บข้อมูล

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

A	B	G	H	I	K
Organization Unit	Description	first name	last name	User logon	Password
กลุ่มห้องปฏิบัติการควบคุมโรคและภัยสุขภาพ	นายอภิชาติ คงทรัพย์	APICHAT	KONGSAP	apichat.k	****
กลุ่มห้องปฏิบัติการควบคุมโรคและภัยสุขภาพ	นางอรุณา ปิณโรว์ระโชติ	ARANYA	PINYORATANACHOT	aranya.p	****
กลุ่มห้องปฏิบัติการควบคุมโรคและภัยสุขภาพ	นางสาวอริสา พรหมณาเวช	ARISA	BROMNAVEJ	arisa.b	****
กลุ่มห้องปฏิบัติการควบคุมโรคและภัยสุขภาพ	นางสาวเบญจภรณ์ จงโรจักร	BENJAPORN	JONGKRIJUG	benjaporn.j	****
กลุ่มห้องปฏิบัติการควบคุมโรคและภัยสุขภาพ	นายบุญฤทธิ์ บุญสนอง	BUNRIT	BUNSANONG	bunrit.b	****
กลุ่มห้องปฏิบัติการควบคุมโรคและภัยสุขภาพ	นายชญาณิน จันทร์ระ	CHAYANIN	CHANTHARA	chayanin.c	****
กลุ่มห้องปฏิบัติการควบคุมโรคและภัยสุขภาพ	นางสาวกนกวรรณ ธิสมิณ	KANOKWAN	NGASAMAN	kanokwan.n	****
กลุ่มห้องปฏิบัติการควบคุมโรคและภัยสุขภาพ	นางสาวมนต์ชนก เต็มเกษม	MONCHANOK	THEMPACHANA	monchanok.t	****
กลุ่มห้องปฏิบัติการควบคุมโรคและภัยสุขภาพ	นายณัฐปัทม์ ศรีวิจิตร	NATTHAPAKHAM	SREEVIJIT	natthepakham.s	****
กลุ่มห้องปฏิบัติการควบคุมโรคและภัยสุขภาพ	นางสาวณิฏฐา เสนาพงศ์	NIDTHA	SENAPONG	nidtha.s	****
กลุ่มห้องปฏิบัติการควบคุมโรคและภัยสุขภาพ	นายปฐม ภาริยภูมิ	PATHOM	KARAIPOOM	pathom.k	****
กลุ่มห้องปฏิบัติการควบคุมโรคและภัยสุขภาพ	นางสาวปิ่นกมล วสิวิวัฒน์	PINKAMON	WESEEWIWAT	pinkamon.w	****
กลุ่มห้องปฏิบัติการควบคุมโรคและภัยสุขภาพ	นางสาวศิริมล ภูมิเนียม	SIWIMOL	THOOMNIYOM	siwimol.t	****

ภาพที่ 3.9 แสดงตัวอย่างข้อมูลที่ได้ทำการวิเคราะห์แล้วก่อนบันทึกลงระบบ Active Directory

## 5. ดำเนินการพัฒนาระบบโดยมีรายละเอียดขั้นตอนดังต่อไปนี้

- 5.1 ดำเนินการสร้างเครื่องเซิร์ฟเวอร์ และคอมพิวเตอร์เสมือนจริง
- 5.2 ติดตั้ง Windows Server 2012 บน Server และดำเนินการกำหนดการตั้งค่า
- 5.3 ติดตั้ง Role And Feature ที่จำเป็นบน Windows Server
- 5.4 กำหนด Password Policy สำหรับผู้ใช้งาน
- 5.5 การบันทึกข้อมูลบุคลากรเข้าสู่ Active Directory
- 5.6 เชื่อมต่อ Active Directory กับ Firewall
- 5.7 กำหนด Session Authentication บน Firewall
- 5.8 กำหนด Firewall Policy สำหรับการเปิดการใช้งาน Authentication
- 5.9 ติดตั้ง Windows 10 บน Log Client และดำเนินการกำหนดการตั้งค่า
- 5.10 ติดตั้งโปรแกรม Watchguard System manager
- 5.11 ทำการเชื่อมต่อ Watchguard System manager กับ Firewall
- 5.12 กำหนดระยะเวลาในการจัดเก็บ Log Files

### ขั้นตอนการปฏิบัติ (DO)

1. ดำเนินการตามขั้นตอนการปฏิบัติ ตามแผนที่วางไว้
2. เก็บรวบรวม บันทึกข้อมูลในขั้นตอนการปฏิบัติ เช่น วิธีดำเนินการ ผลของการปฏิบัติงาน

### ขั้นตอนการตรวจสอบ (Check)

1. ตรวจสอบความถูกต้องของการทำงานของระบบ เพื่อเปรียบเทียบกับขั้นตอนการวางแผนที่กำหนดไว้

### ขั้นตอนการดำเนินงานให้เหมาะสม (Act)

1. ทบทวน วิเคราะห์ ผลการดำเนินการ เพื่อปรับปรุงขั้นตอน หรือกระบวนการ
2. กรณีผลลัพธ์ที่ได้ไม่เป็นไปตามขั้นการวางแผน ดำเนินการค้นหาสาเหตุที่มาของผล ปรึกษาผู้เชี่ยวชาญ และปรับเปลี่ยนวิธีการ และนำไปใช้ และดำเนินการวัดผลการปฏิบัติ ว่าเป็นไปตามวัตถุประสงค์ที่วางไว้หรือไม่
3. หลังจากปรับปรุงผลลัพธ์เป็นไปตามวัตถุประสงค์แล้วดำเนินการประกาศใช้งานและเปิดใช้งานระบบ
4. บำรุงรักษาระบบ

## บทที่ 4

### ผลการดำเนินงาน

ผลการศึกษาการพัฒนากระบวนการยืนยันตัวบุคคลเพื่อเข้าใช้งานระบบเครือข่ายอินเทอร์เน็ตของสำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช โดยแบ่งผลการศึกษาออกเป็น 2 ส่วนคือ 1) การพัฒนากระบวนการตามหลัก PDCA 2) ผลการประเมินการพัฒนากระบวนการ โดยได้ดำเนินการดังนี้

#### 4.1 ดำเนินการตามแผนการพัฒนา

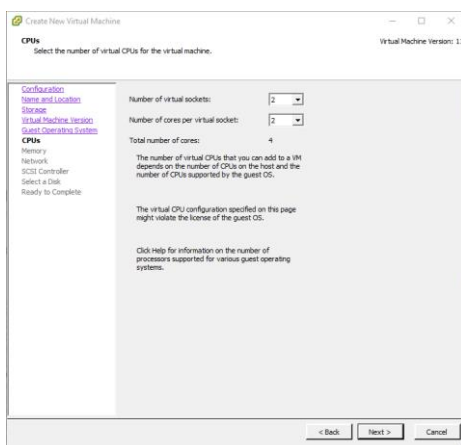
##### 1. ผลการดำเนินการสร้างเซิร์ฟเวอร์และคอมพิวเตอร์เสมือนจริง

1.1 ดำเนินการสร้างเซิร์ฟเวอร์และคอมพิวเตอร์ virtualization โดยใช้โปรแกรม VMware vSphere Client



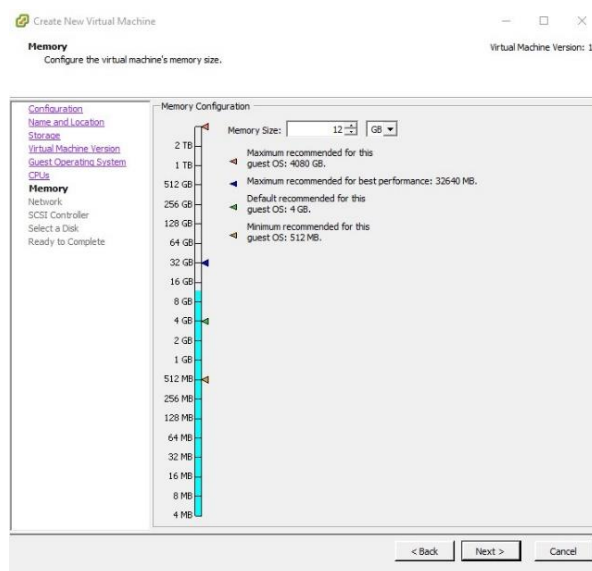
ภาพที่ 4.1 แสดงหน้าต่างการเข้าใช้งานโปรแกรม VMware vSphere Client

1.2 กดปุ่ม create a new virtual machine แล้ว next ไปยังหน้า กำหนด CPUs ของเครื่อง โดยได้กำหนดรายละเอียดไว้ดังนี้ socket core และ 2 virtual socket core รวมเป็น 4 cores



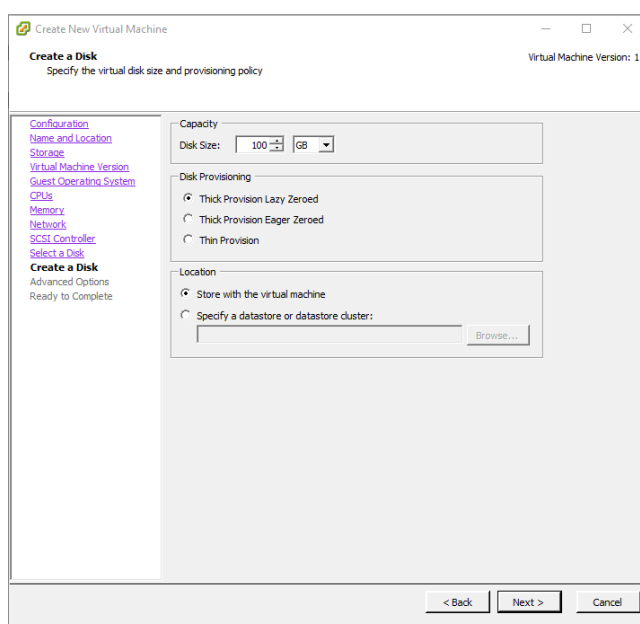
ภาพที่ 4.2 แสดงหน้าต่างการกำหนด CPUs cores ของเครื่อง Virtual

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



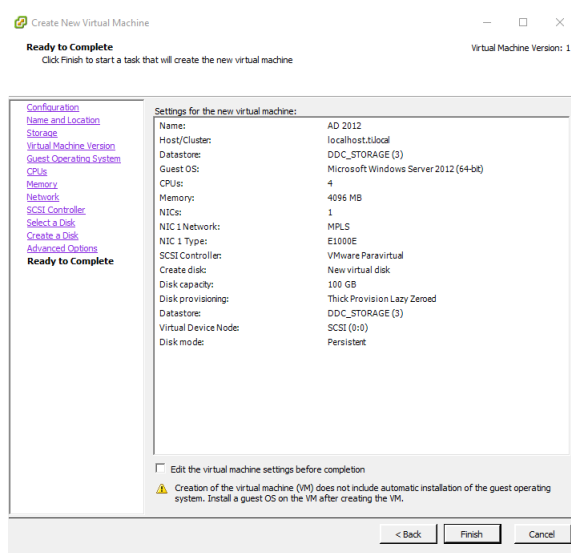
ภาพที่ 4.3 แสดงหน้าต่างการกำหนด Memory ของเครื่อง Virtual

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



ภาพที่ 4.4 แสดงหน้าต่างการกำหนด Disk size

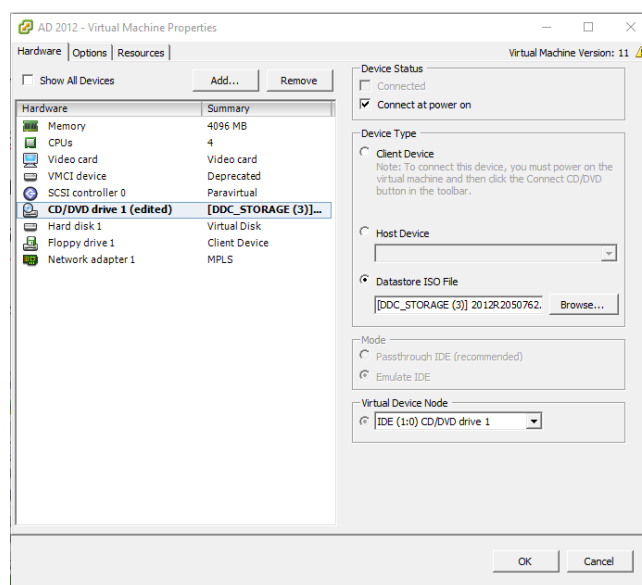
1.5 เมื่อกำหนดรายละเอียดต่างๆ เรียบร้อยโปรแกรมจะแสดงหน้าต่าง สรุปผลการตั้งค่าให้ตรวจเช็คอีกครั้ง โดยสามารถกด back เพื่อไปทำการแก้ไขรายละเอียดได้ เมื่อตรวจสอบเรียบร้อยแล้วกดปุ่ม Finish



ภาพที่ 4.5 แสดงหน้าต่างรายละเอียดการตั้งค่าทั้งหมดของเครื่อง virtual ตามที่ได้กำหนดไว้

2. ติดตั้ง Windows Server 2012 บน Server และดำเนินการกำหนดการตั้งค่าเครือข่าย

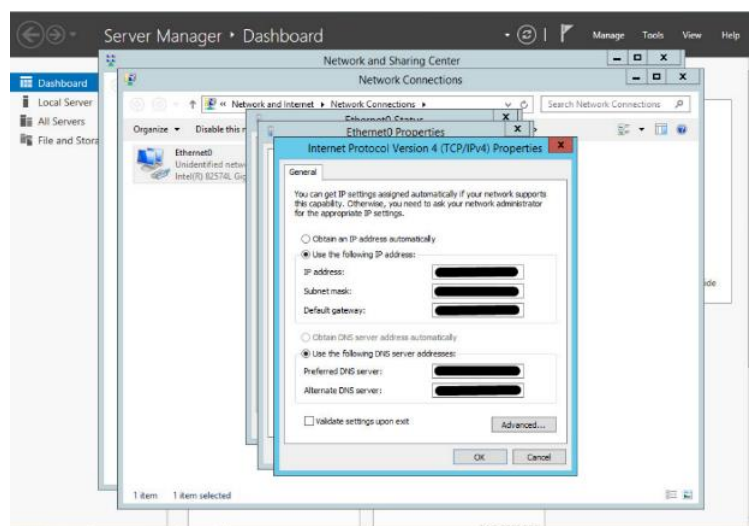
2.1 เมื่อสร้างเครื่อง Virtual เรียบร้อยแล้ว ดำเนินการเลือกไฟล์ ISO windows server 2012 นำมาวางไว้ใน virtual cd/dvd drive เพื่อทำการติดตั้ง windows



ภาพที่ 4.6 แสดงการเลือก ISO Files ของ Windows ในช่อง CD/DVD Drive 1 โดย ISO ที่เลือกต้องจัดเก็บไว้ใน Virtual machine storage



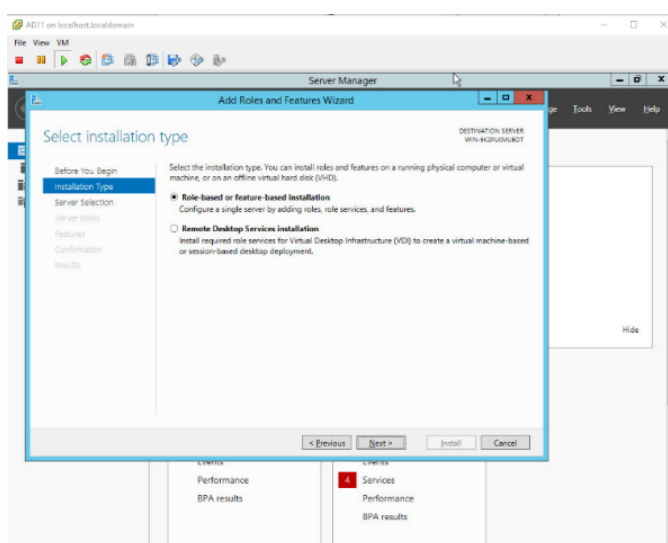
2.2 เมื่อติดตั้ง Windows server 2012 เรียบร้อยแล้วเข้าสู่การกำหนด IP ให้เครื่อง Server โดยกำหนดให้เป็นแบบ Static เพื่อง่ายต่อการเชื่อมต่อ



ภาพที่ 4.7 แสดงการกำหนด IP address ของเครื่อง Server

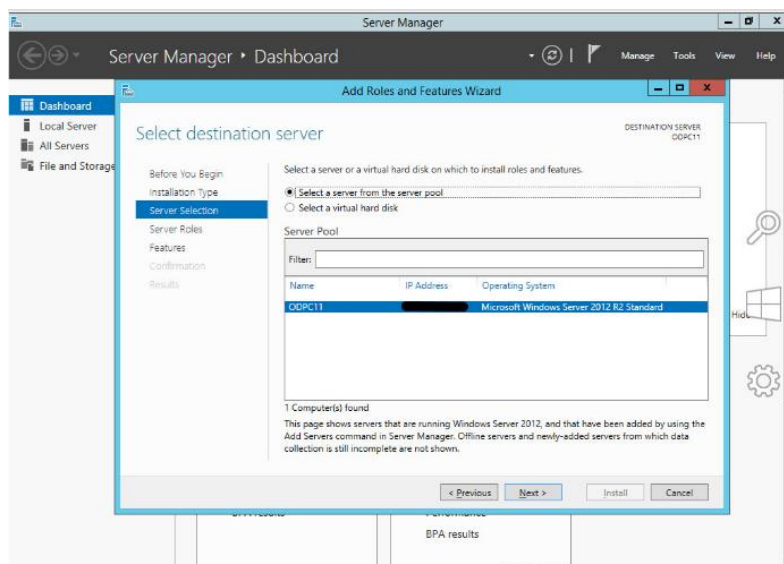
3. ติดตั้ง Role and Feature ที่จำเป็นบน Windows Server เพื่อเป็นการกำหนดรูปแบบของ server ให้กลายเป็น Active Directory Domain Services จึงต้องมีการติดตั้ง Roles and Features โดยมีขั้นตอนการติดตั้ง ดังนี้

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



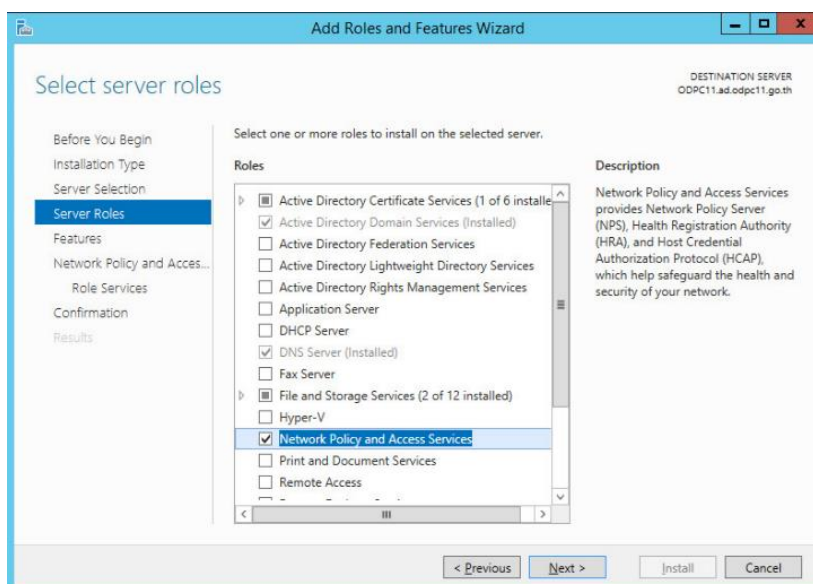
ภาพที่ 4.8 แสดงหน้าต่างการเลือกรูปแบบการติดตั้ง โดยเลือกการตั้งค่าแบบ Roles-based or feature-based installation

3.2 กด Next นำไปสู่ขั้นตอนการเลือกเซิร์ฟเวอร์ปลายทางในการติดตั้งซึ่งจะเป็นเซิร์ฟเวอร์ปัจจุบัน  
ที่ดำเนินการติดตั้ง Roles อยู่



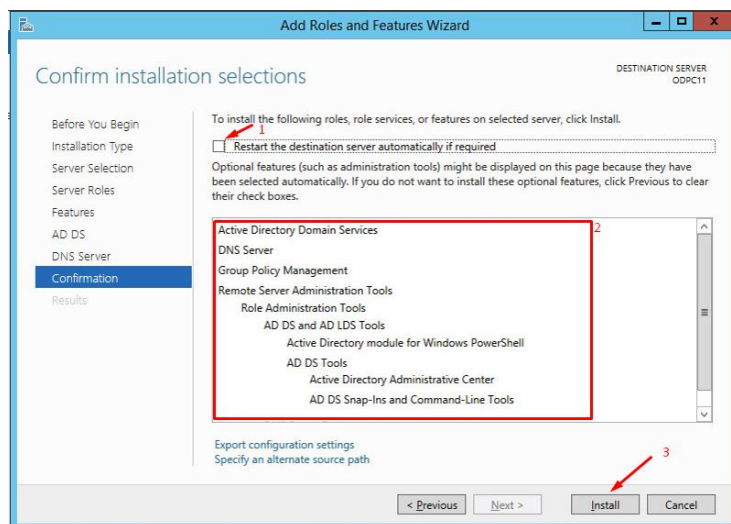
ภาพที่ 4.9 ทำการเลือกเซิร์ฟเวอร์ที่จะทำการติดตั้ง Roles

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



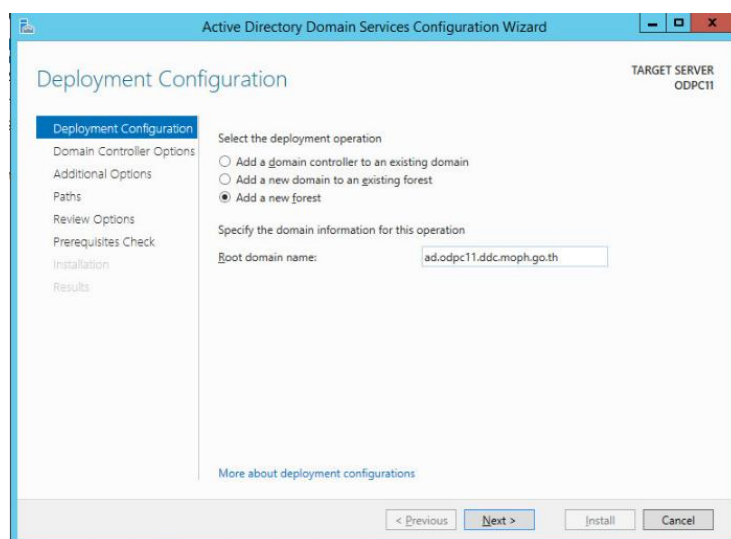
ภาพที่ 4.10 แสดงหน้าต่างการเลือก Roles โดยทำการเลือก Roles ดังนี้ Active directory domain  
services (AD DS), DNS Server และ Network policy and Access Services

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



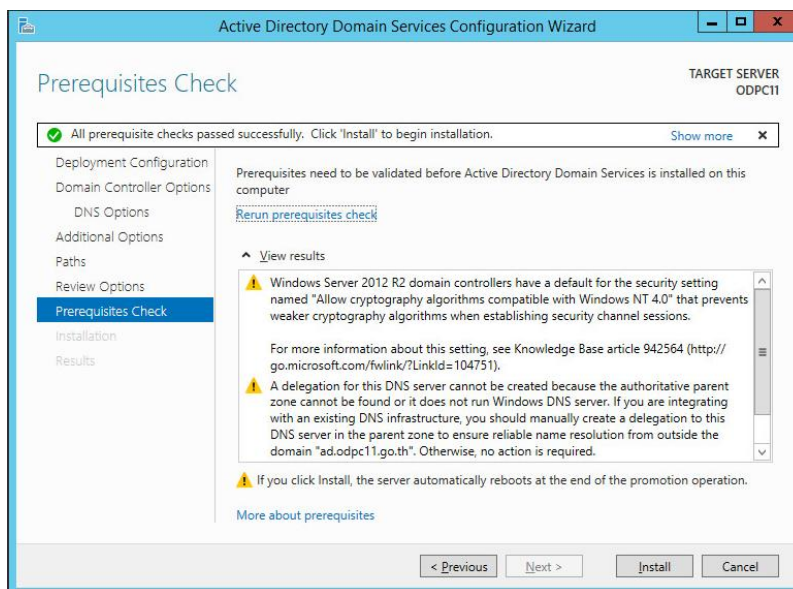
ภาพที่ 4.11 แสดงหน้าต่างสรุปการตั้งค่า Roles ที่ได้ทำการเลือกติดตั้ง

3.5 เมื่อติดตั้งเรียบร้อยแล้วเซิร์ฟเวอร์จะทำการรีสตาร์ทอัตโนมัติเพื่อเป็นการกำหนดค่าเริ่มต้นใหม่ จากนั้นไปที่ server manager อีกครั้งกด Promote this server to a domain controller เพื่อเป็นการกำหนด domain name ของเครื่องเซิร์ฟเวอร์

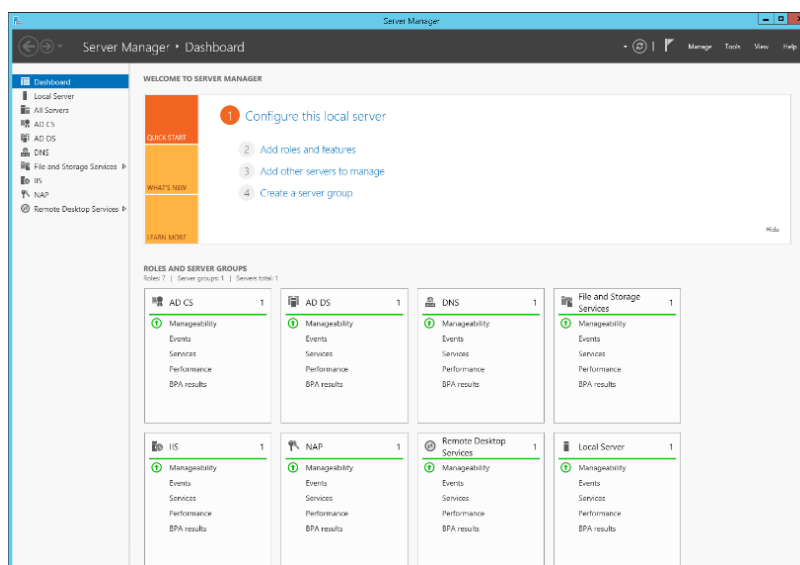


ภาพที่ 4.12 แสดงหน้าต่างการกำหนด domain name โดยเลือก Add a new forest แล้วกำหนดชื่อ domain name

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

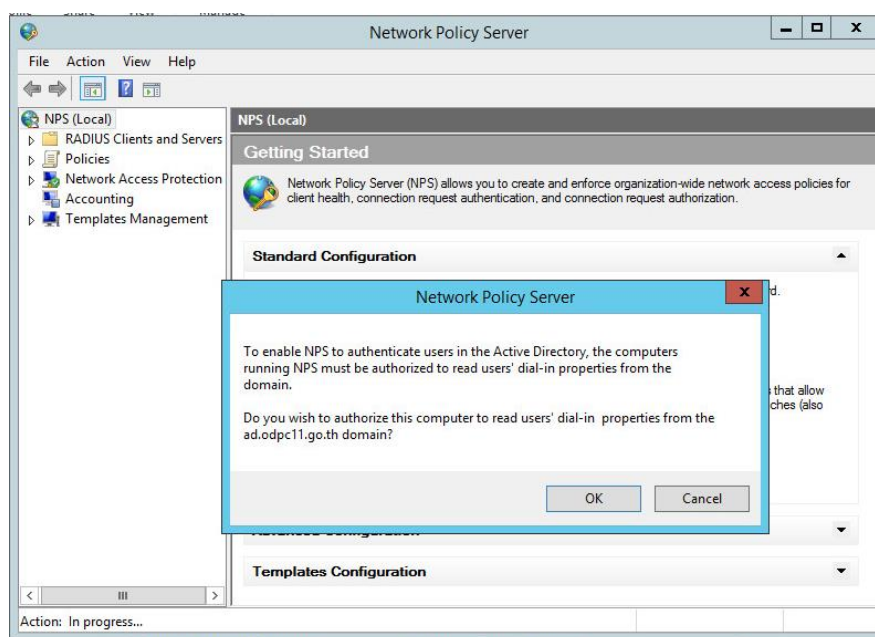


ภาพที่ 4.13 แสดงหน้าต่างรายละเอียดการตั้งค่า domain controller และปุ่ม Install



ภาพที่ 4.14 แสดงหน้าต่าง Server Manager ผลการติดตั้ง Roles ของ Server หลังจาก Install เสร็จแล้ว

3.7 ขั้นตอนถัดมาเป็นการเปิดใช้ Network Policy Server เพื่อเป็น Services ที่ใช้เชื่อมต่อกับ Firewall โดยพิมพ์ที่ช่องค้นหาว่า Network Policy Server แล้วกดเปิดจากนั้น โดยคลิกขวาที่ NPS(Local) เลือก Start NPS services ระบบจะแจ้งเตือนการเปิด NPS ขึ้นมา กด OK เป็นอันเสร็จสิ้น



ภาพที่ 4.15 แสดงหน้าต่างการเปิดใช้งาน Network Policy Server

#### 4. ผลของการกำหนด Password Policy สำหรับผู้ใช้งาน

Password policy หรือ นโยบายรหัสผ่านคือกฎและข้อกำหนดที่กำหนดวิธีการในการกำหนดรหัสผ่านที่ปลอดภัยและการจัดการรหัสผ่านในระบบคอมพิวเตอร์โดยสำนักงานป้องกันควบคุมโรคได้ใช้ตามมาตรฐานของ Windows Server คือต้องมีความ จำเป็นต้องมีความ Complexity โดย ความ Complexity มีรายละเอียด ดังนี้

##### 4.1 จำนวนความยาวต้องไม่น้อยกว่า 8 ตัวอักษรและประกอบด้วย 3 ใน 4 ข้อนี้

ภาษาอังกฤษ A ถึง Z ในแบบตัวพิมพ์ใหญ่, ภาษาอังกฤษ a ถึง z ในแบบตัวพิมพ์เล็ก  
ตัวเลข 0 ถึง 9 และ ตัวอักขระสัญลักษณ์ 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

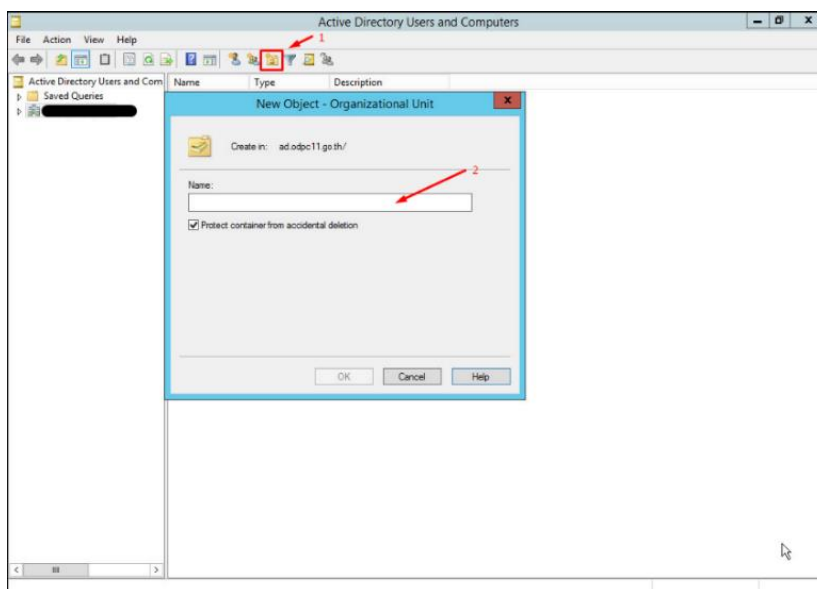
Policy	Policy Setting
Enforce password history	24 passwords remember
Maximum password age	360 days
Minimum password age	0 days
Minimum password length	8 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption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

ภาพที่ 4.16 แสดงผลของการกำหนด Password Policy

## 5. การบันทึกข้อมูลบุคลากรเข้าสู่ Active Directory

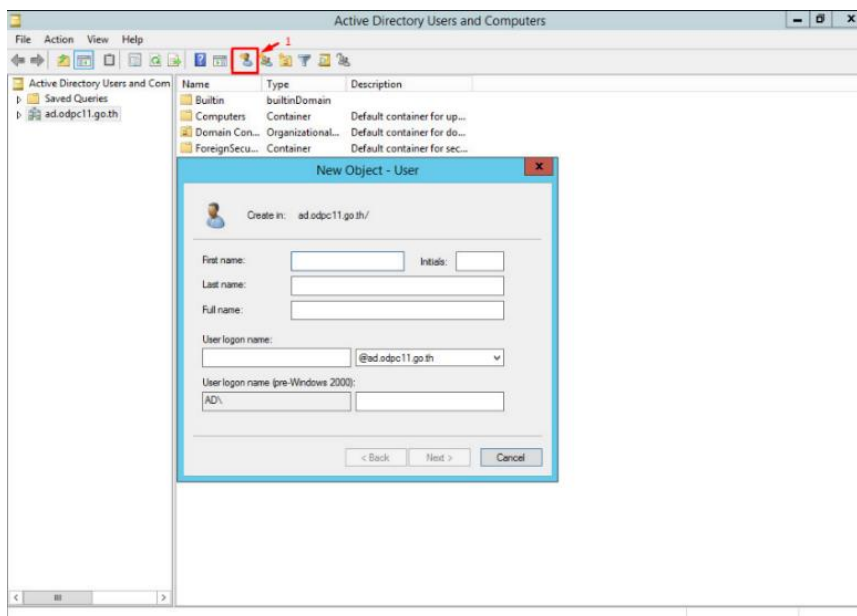
การเพิ่มข้อมูลที่ได้จัดเตรียมไว้เข้าสู่ Active directory ดำเนินการ ดังนี้

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



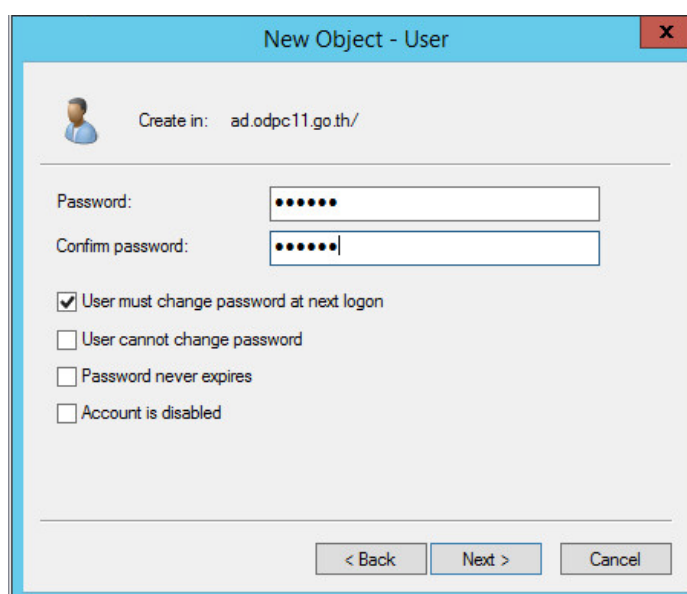
ภาพที่ 4.17 การสร้าง organization unit (OU) เพื่อกำหนดชื่อตามกลุ่มงาน

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



ภาพที่ 4.18 แสดงหน้าต่างรายละเอียดข้อมูล New User

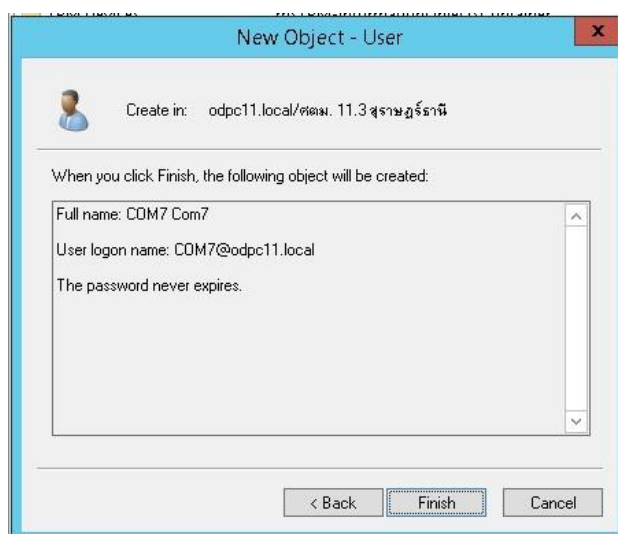
5.3 กด Next นำไปสู่หน้ากำหนด Password เช็ค ที่ User must change password at next logon แล้วกำหนด password เริ่มต้นที่จัดเตรียมไว้



ภาพที่ 4.19 แสดงหน้าต่างการกำหนด Password New User

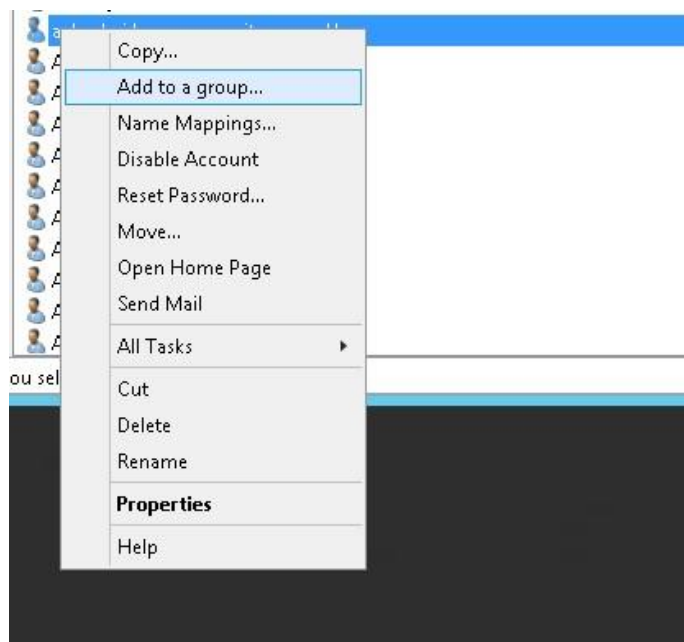


5.4 กด Next จะแสดงหน้าต่างสรุปผลการตั้งค่าที่ได้กำหนดไว้ จากนั้นกด Finish



ภาพที่ 4.20 แสดงหน้าต่างสรุปผลการสร้าง User

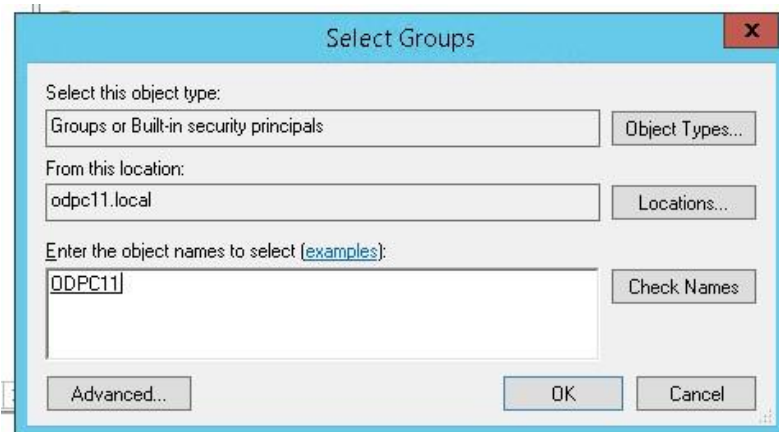
5.5 หลังจากทำการสร้าง User เรียบร้อยแล้วให้ทำการคลิกขวาที่ Icon User ที่เพิ่งได้รับการสร้างแล้วเลือกหัวข้อ Add to a Group เพื่อเป็นการกำหนดให้ User ใน Active Directory จัดเก็บไว้ใน Group ที่ได้สร้างไว้



ภาพที่ 4.21 แสดงตัวอย่างการคลิกขวาที่ New User แล้วเลือกเมนู Add to a group



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

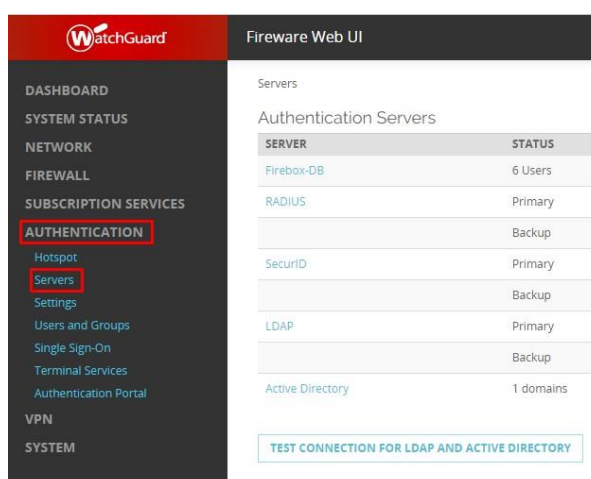


ภาพที่ 4.22 แสดงหน้าต่างการ Select Groups หลังจากที่ได้ทำการ Check Names

## 6. การเชื่อมต่อ Active Directory กับ Firewall

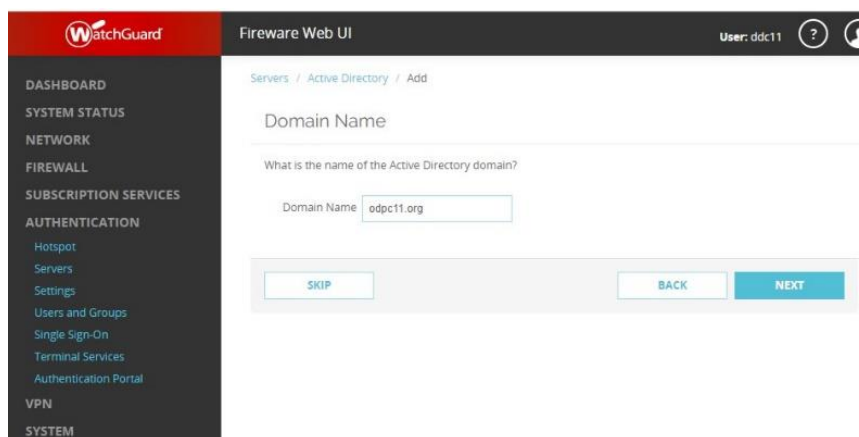
การเชื่อมต่อ Firewall กับ Active Directory ดำเนินการตามขั้นตอนดังนี้

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



ภาพที่ 4.23 แสดงจำนวนรูปแบบการเชื่อมต่อที่สามารถเชื่อมต่อได้บน Firewall โดยได้เลือกใช้แบบ Active Directory

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



ภาพที่ 4.24 แสดงวิธีการกำหนด Domain Name

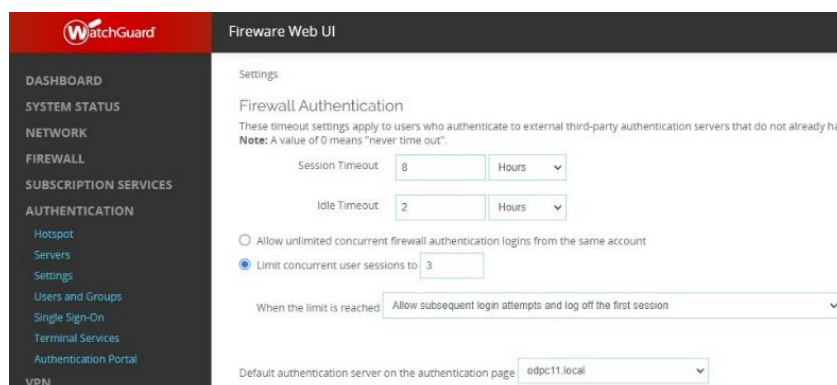
## 7. กำหนด Session Authentication บน Firewall

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

Session timeout คือ ระยะเวลาในการ Login เข้าใช้งานแต่ละครั้งคือ 8 ชม

Idle timeout คือ ระยะเวลาการไม่ใช้งาน 2 ชม

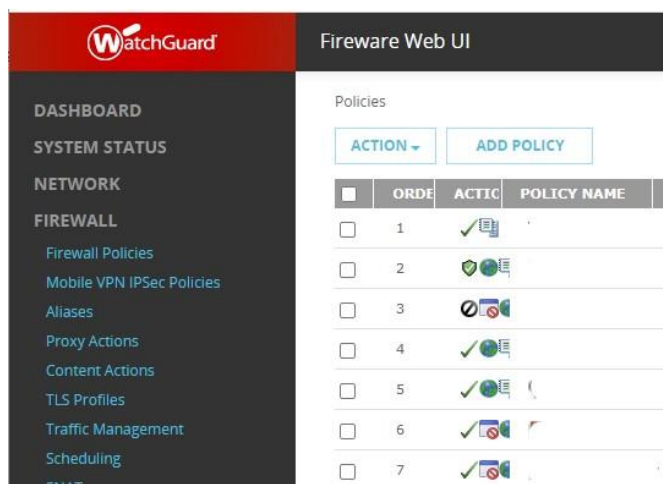
limit concurrent user คือ จำนวนที่ 1 user จำนวนอุปกรณ์สูงสุดคือ 3 อุปกรณ์



ภาพที่ 4.25 แสดงการกำหนด session Authentication โดยกำหนดค่าการใช้งาน

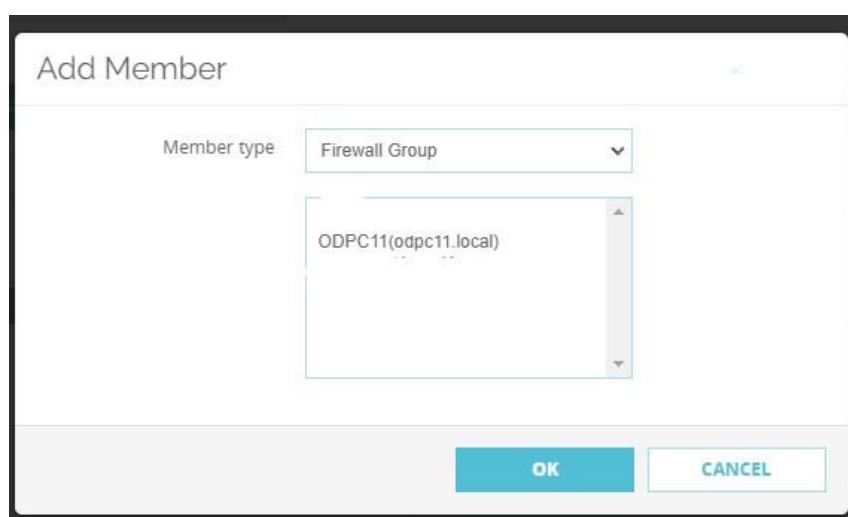
## 8. กำหนด Firewall Policy สำหรับการเปิดการใช้งาน Authentication โดยมีขั้นตอน ดังนี้

### 8.1 เข้าสู่ Watchguard firewall management > Firewall Policies > ADD Policy



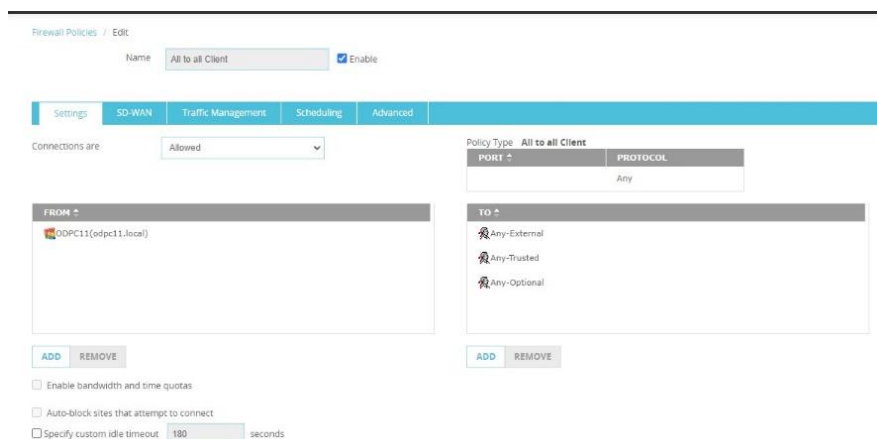
ภาพที่ 4.26 แสดงหน้าต่าง Firewall Policies > ADD Policy

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



ภาพที่ 4.27 แสดงหน้าต่างการ ADD Member type เป็น group ที่ได้กำหนดไว้ใน ADDS

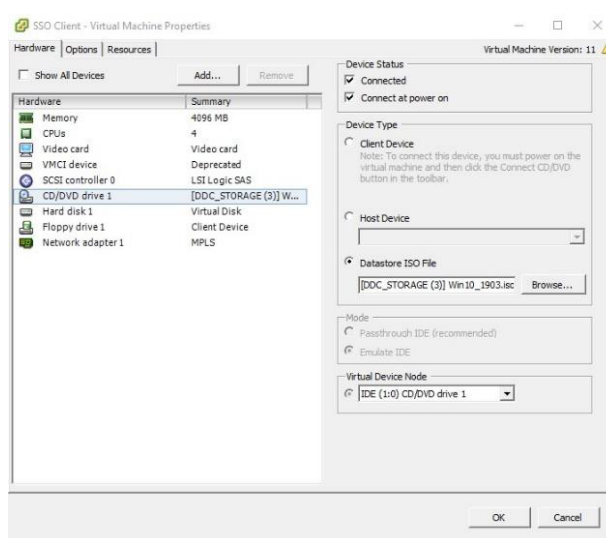
8.3 ในฝั่งของ To เป็นการกำหนดเครือข่ายใดๆ ที่ต้องการให้ User มีสิทธิ์ในการเข้าถึงจากนั้นกด Save Policy



ภาพที่ 4.28 แสดงผลการ configure firewall policy ที่ได้กำหนดให้ User จาก group ODPC11 สามารถเข้าถึงเครือข่าย

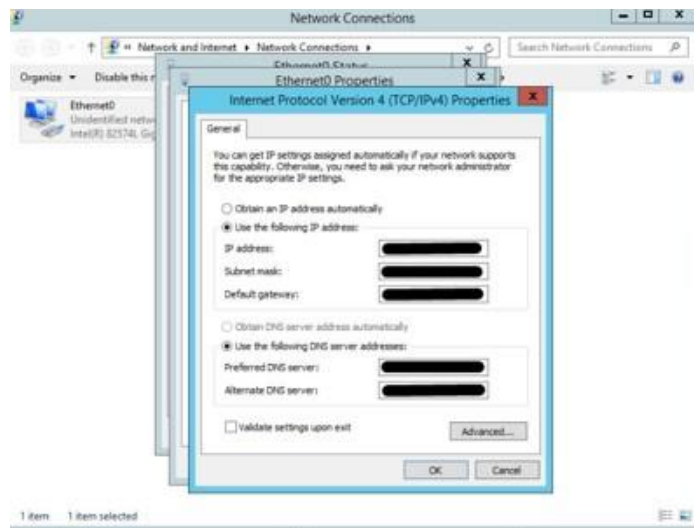
9. ติดตั้ง Windows 10 บน Log Client และดำเนินการกำหนดการตั้งค่าพื้นฐาน

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



ภาพที่ 4.29 แสดงหน้าต่างการเลือก Windows 10 ISO Files สำหรับติดตั้ง

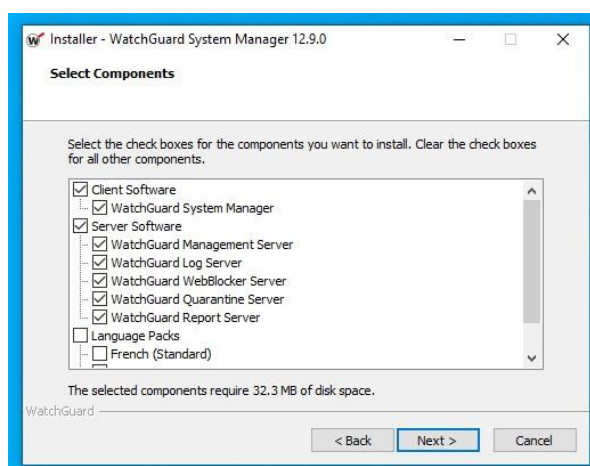
9.2 หลังจากติดตั้ง Windows 10 แล้วทำการกำหนด IP Address เป็น Static เพื่อใช้ในการเชื่อมต่อการเก็บ Log Files



ภาพที่ 4.30 แสดงหน้าต่างการกำหนด IP Address เป็น Static

## 10. ติดตั้ง โปรแกรม Watchguard System manager

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



ภาพที่ 4.31 แสดงหน้าต่างการติดตั้ง Watchguard System manager

## 11. ทำการเชื่อมต่อ Watchguard System manager กับ Firewall

11.1 เมื่อทำการติดตั้งโปรแกรมสำเร็จ ทำการเปิดโปรแกรม WatchGuard System Manager 12.9.4 เพื่อทำการตั้งค่าการเชื่อมต่อโปรแกรม จากนั้นเลือกที่ Files > Connect to Device.. เพื่อทำการกำหนดการเชื่อมต่อ โดยมีรายละเอียด ดังนี้

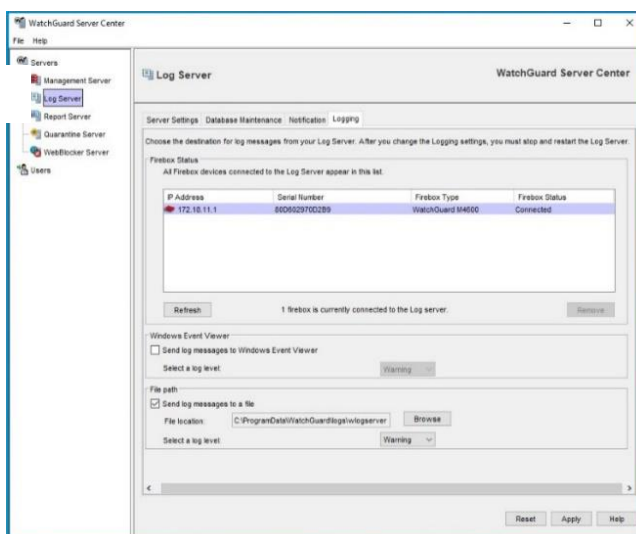
IP Address : หมายเลข IP Address ของ Watchguard Firebox

User Name : คือ Username ที่กำหนดสิทธิ์โดย Firebox ให้มีสิทธิ์อ่านข้อมูล

Passphrase : คือ Passphrase เฉพาะที่เป็นค่าที่ได้มาพร้อมกับตัว Firebox

ภาพที่ 4.32 แสดงหน้าต่างการกำหนดการเชื่อมต่อ WatchGuard System Manager

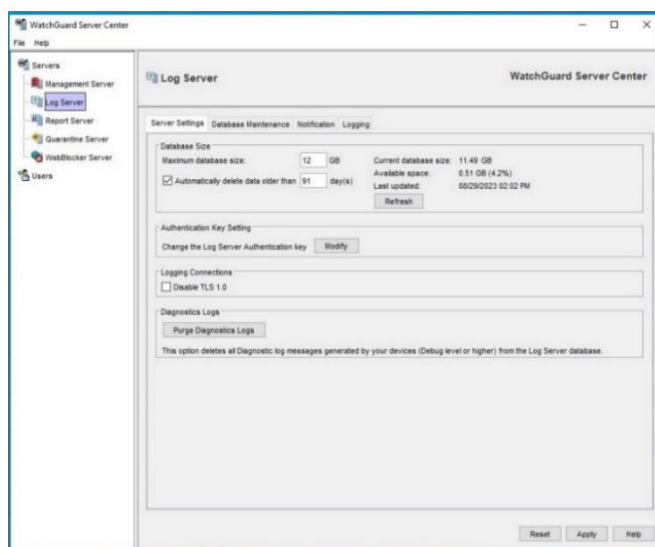
11.2 เข้าสู่ Watchguard System manager ไปยังหัวข้อ Log Server ที่เมนูบาร์ Logging จะพบตัว Watchguard ที่ใช้งานอยู่ หากไม่พบให้ทำการกดปุ่ม Refresh



ภาพที่ 4.33 แสดงรายการ Device ของ Firebox ที่ได้ทำการเชื่อมต่อไว้

## 12. ตั้งค่าขนาดพื้นที่จัดเก็บ Log Files

12.1 ทำการกำหนดรายละเอียดในการจัดเก็บ Log ในเมนู log server > server settings โดยกำหนดขนาดของพื้นที่ที่ใช้ในการจัดเก็บ



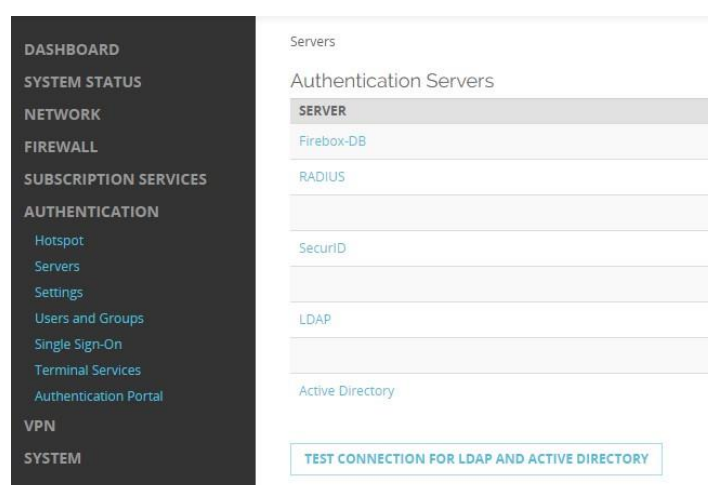
ภาพที่ 4.34 แสดงหน้าต่างการกำหนดการตั้งค่าการเก็บ Log Files

## 4.2. ผลการตรวจสอบการทำงาน

ตรวจสอบความถูกต้องของการทำงานของระบบ เพื่อเปรียบเทียบกับขั้นตอนการวางแผนที่กำหนดไว้

### 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 4.35 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 การทำสอบด้วย Username และ Password ที่ถูกต้องผลคือ connection server : Ok  
Log in : Ok

The screenshot shows a web interface for testing LDAP or Active Directory connections. It includes a 'Server Connection' section with a dropdown for 'Authentication Server' (set to 'odpc11.local'), a text input for 'Username' (set to 'com1'), and a password input field. A 'TEST CONNECTION' button is visible. Below the button, the 'Results' section displays the following text: '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 4.36 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 web interface as in the previous image, but with a different 'Username' value of 'com8'. The 'TEST CONNECTION' button has been clicked, and the 'Results' section now displays: '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 4.37 แสดงหน้าต่างการทดสอบด้วย Username และ Password ที่ถูกต้อง



### 1.3 สรุปผลการตรวจสอบการเชื่อมต่อระหว่าง Firewall และ Active Directory

สามารถสรุปผลได้ว่าการทำางานของการเชื่อมต่อระหว่าง Firewall และ Active Directory สามารถใช้งานได้ เป็นไปตามที่วางแผนไว้

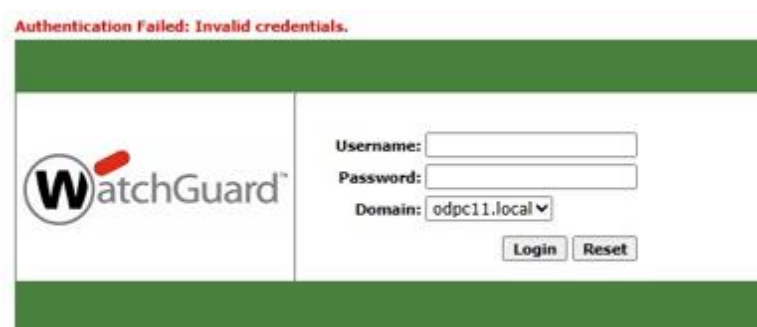
## 2. ทดสอบการเข้าใช้งานระบบยืนยันตัวตนบุคคล

2.1 การทดสอบการเข้าใช้งานระบบโดยใช้วิธีการทดสอบระบบแบบ Black Box Testing โดยการนำเอาเหตุการณ์ที่คาดว่าจะเกิดขึ้นมากำหนดให้อยู่ในรูปแบบเหตุการณ์เพื่อระบุผลของการทำงานได้ ดังนี้ ตารางที่ 4.1 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 แจ้ง เตือน Invalid credentials!



ภาพที่ 4.38 หน้าต่างแสดงผลการเข้าสู่ระบบสำเร็จ



ภาพที่ 4.39 แสดงหน้าต่าการแจ้งเตือนเข้าใช้งานไม่สำเร็จ

2.2 ผลของการตรวจสอบการใช้งานระบบ Authentication ระบบได้ทำงานได้ตามที่วางแผนไว้ ซึ่งได้ผลลัพธ์ ดังนี้

ตารางที่ 4.2 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 4.3 จะได้ว่าผลการทดสอบการเข้าใช้งานระบบยืนยันตัวตนเป็นไปตามที่คาดไว้คือสามารถเข้าใช้งานได้เมื่อ Username และ Password ตรงกับฐานข้อมูลของผู้มีสิทธิ์ใช้งานที่ได้ลงทะเบียนไว้ และจากผลการตรวจสอบในตารางที่ 4.4 การเข้าใช้งานส่วนใหญ่เป็นไปตามแผนที่วางไว้ พบปัญหาการใช้งานบนอุปกรณ์ที่ใช้ระบบปฏิบัติการ iOS ที่บางครั้งหน้าตาของการเข้าสู่ระบบไม่ปรากฏ

## 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 4.40 แสดงหน้าตาการเข้าสู่โปรแกรมจัดเก็บ Log Files

3.2 เมื่อเข้าสู่ระบบแล้วจะพบกับหน้าตาแสดงอุปกรณ์เพื่อเลือกอุปกรณ์ที่ทำการจัดเก็บ Log Files

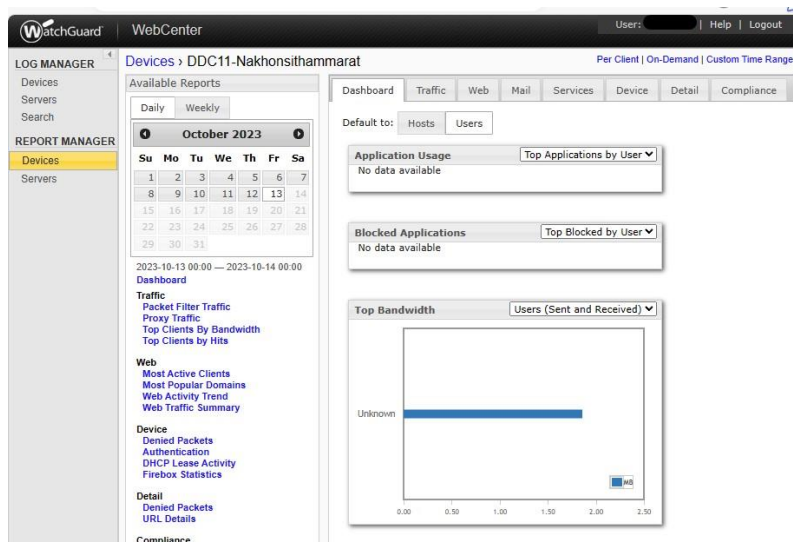


Name	Connected	IP Address	Serial Number	Version	Model
DDC11-Nakhonsithammarat	Yes	.18.1	D602970D2	12.3.1	WatchGuard M4600

ภาพที่ 4.41 แสดงหน้าตาการเข้าสู่โปรแกรมจัดเก็บ Log Files

### 3.3 เมื่อทำการเลือกอุปกรณ์จะแสดงหน้าต่างสำหรับดูรายละเอียดต่างๆ ของการจัดเก็บ Log

Files

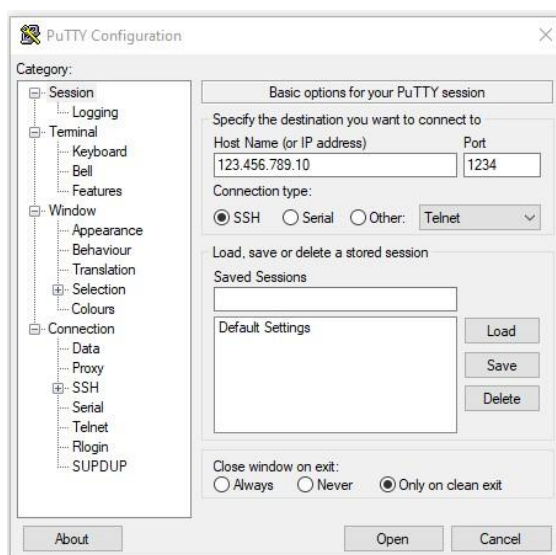


ภาพที่ 4.42 แสดงหน้าต่าง Dash board ของการจัดเก็บ Log Files

### 3.4 ตรวจสอบการทำงานของเครื่องเก็บ Log Files

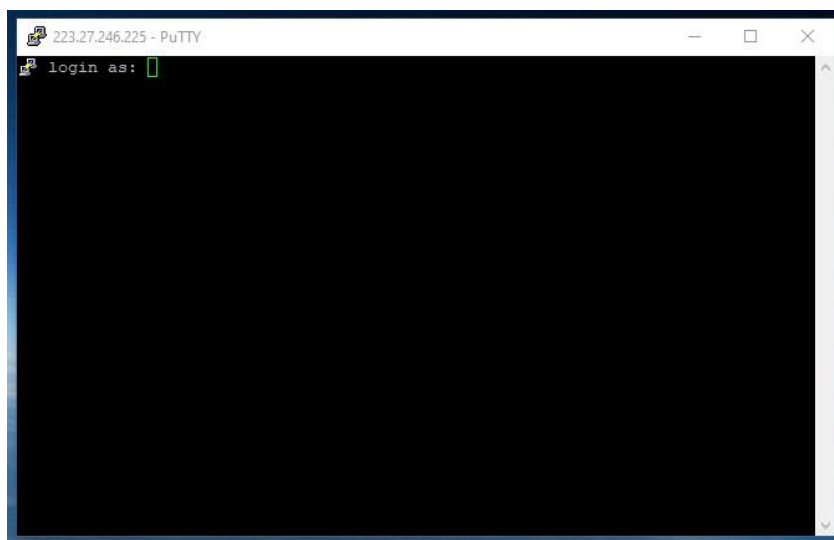
จากที่ได้มีการกำหนดค่าให้ Firewall ดำเนินการจัดเก็บ Log Files ส่งไปยังเครื่องคอมพิวเตอร์ Log Files IP Address 172.18.11.37 สามารถตรวจสอบการทำงานโดยใช้คำสั่ง Command line ได้ดังนี้

3.4.1 เข้าสู่การใช้งานคำสั่ง Command line โดยใช้งานโปรแกรม PuTTY เลือกการเชื่อมต่อผ่าน IP Address โดยใช้ชนิดการเชื่อมต่อแบบ SSH



ภาพที่ 4.43 แสดงหน้าต่างโปรแกรม PuTTY สำหรับเชื่อมต่อไปยัง Firewall

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



ภาพที่ 4.44 แสดงหน้าต่างโปรแกรม PuTTY สำหรับ login เข้าใช้งาน

3.4.3 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 จะได้คำสั่งคือ `show log-setting watchguard-log-server` ซึ่งจะได้ผลตรงกับคอมพิวเตอร์ Log Server ที่กำหนดไว้คือ `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 4.45 แสดงการใช้คำสั่ง `show log-setting watchguard-log-server` เพื่อดูปลายทางในการจัดเก็บ Log ของ Firewall

### 3.5 ทดสอบการใช้งานการค้นหา Log Files

เพื่อบรรลุวัตถุประสงค์ในการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log File) เพื่อสามารถดูข้อมูลประวัติการใช้งานอินเทอร์เน็ตได้จึงจำเป็นต้องสามารถค้นหาข้อมูล Log Files การใช้งานย้อนหลังได้จึงทำการทดสอบการค้นหาข้อมูลการใช้งานย้อนหลังมีขั้นตอน ดังนี้

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

Time Range คือ สามารถระบุช่วงเวลาในการค้นหาได้

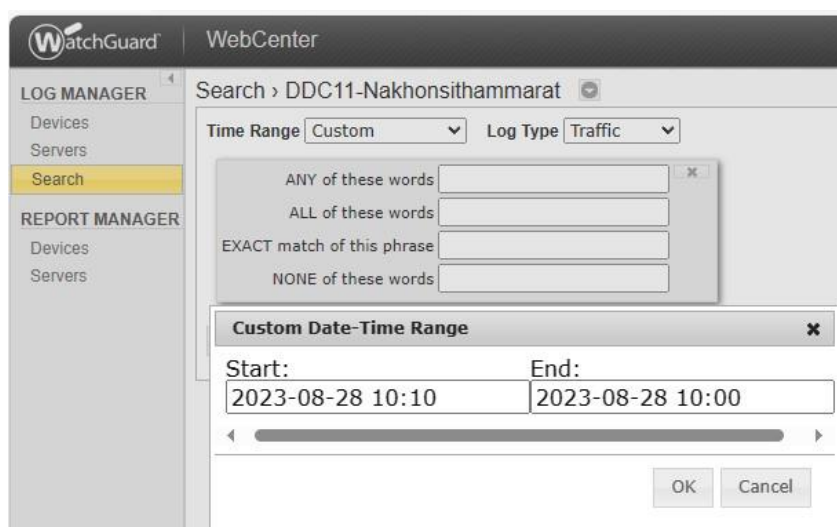
Log Type คือ ชนิดของ Log ที่ต้องการค้นหา

Any of these words คือ หาข้อมูลทีส่วนของคำที่ระบุ

ALL of these words คือ หาข้อมูลที่มีคำที่ระบุ

EXACT match of this phrase คือ ข้อมูลที่ตรงกับที่ระบุทุกประการ

NONE of these words คือ ข้อมูลทั้งหมดยกเว้นที่มีส่วนของที่ระบุ



ภาพที่ 4.46 แสดงระบุระยะเวลาในการค้นหาข้อมูล Log ย้อนหลัง

3.5.2 เมื่อทำการค้นหาระบบจะโชว์ข้อมูล Log Files ที่ตรงกับเงื่อนไขที่ทำการค้นหาโดยมีข้อมูลที่ตรงกับวัตถุประสงค์ในการจัดเก็บ ดังนี้

### ตารางที่ 4.3 แสดงความหมายของข้อมูลที่จัดเก็บเป็น Log Files

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

The screenshot displays the WatchGuard WebCenter interface. At the top, there's a search bar with the criteria 'ANY of these words: com1'. Below the search bar, a table of log entries is visible. The table has two main columns: 'Date-Time' and 'Message'. The 'Date-Time' column shows entries from 2023-08-28 09:11:49. The 'Message' column contains detailed log messages, such as 'FWAllow, Allowed, pri=4, disp=Allow, policy=All-to-all-Client-00, protocol=dns/udp, src\_ip=192.168.40.155, src\_port=60976, dst\_ip=8.8.8.8, dst\_port=53, src\_ip\_nat=223.204.146.59, src\_port\_nat=11780, src\_intf=40-V40-Wifi, dst\_intf=2-388, rc=100, pkt\_len=58, ttl=127, src\_user=com1@odpcc1.local'.

ภาพที่ 4.47 แสดงตัวอย่างข้อมูลการค้นหา Log Files ย้อนหลัง

3.6 สรุปผลการตรวจสอบการใช้งานระบบจัดเก็บ Log Files จากที่ได้ทำงานทดสอบเข้าสู่ระบบตรวจสอบการเชื่อมต่อ และค้นหาข้อมูลย้อนหลัง สรุปได้กระบวนการจัดเก็บ Log Files ทำงานได้ตามแผนที่วางไว้

#### 4. ตรวจสอบผลการกำหนดความต้องการของระบบ

แบ่งออกเป็นเซิร์ฟเวอร์และเครื่องคอมพิวเตอร์ Log Files ดังนี้

##### 4.1 ตรวจสอบเซิร์ฟเวอร์

ตารางที่ 4.4 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

##### 4.2 ตรวจสอบคอมพิวเตอร์ Log Files

ตารางที่ 4.5 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

##### 4.3 ผลการตรวจสอบคุณลักษณะเครื่องคอมพิวเตอร์เซิร์ฟเวอร์และคอมพิวเตอร์ Log Files

จากตารางที่ 4.4 แสดงให้เห็นว่าการกำหนดคุณลักษณะเครื่องเซิร์ฟเวอร์เป็นไปตามแผนที่วางไว้ และจากตารางที่ 4.5 แสดงให้เห็นว่าการตรวจสอบคุณลักษณะเฉพาะเครื่องคอมพิวเตอร์ log files ปริมาณพื้นที่จัดเก็บข้อมูลไม่เพียงพอ



## 5. ตรวจสอบประสิทธิภาพการทำงานของเครือข่ายอินเทอร์เน็ต

5.1 ดำเนินการตรวจสอบประสิทธิภาพการทำงานของเครือข่ายอินเทอร์เน็ตโดยใช้เครื่องมือ Microsoft 365 network connectivity test tool ดำเนินการทดสอบเปรียบเทียบผลการใช้งานก่อนและหลังติดตั้งระบบ Authentication ได้ผลดังตารางที่ 4.8

ตารางที่ 4.6 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 4.6 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 4.48 แสดงผลการทดสอบหลังใช้งานระบบ Authentication

5.2 ตรวจสอบความสามารถการทำงานของระบบ ทำการเปรียบเทียบการทำงานของระบบ ก่อนการใช้งานระบบ และหลังการใช้งานระบบ เพื่อเปรียบเทียบประสิทธิภาพการทำงานของระบบ ดังต่อไปนี้

1. ตรวจสอบผู้ใช้งานระบบเครือข่ายก่อนการใช้งานระบบ Authentication โดยการทำการเข้าไปตรวจสอบ IP Address ของผู้ใช้งานระบบด้วย Firewall โดยแสดงผลดังภาพที่ 4.61 คือไม่สามารถระบุถึงตัวตนผู้ใช้งานที่ไม่ได้มีการตั้งชื่อเครื่องคอมพิวเตอร์ให้สอดคล้องกับชื่อผู้ใช้งานจริงได้

INTERFACE	IP ADDRESS	HOST	MAC ADDRESS	START TIME	END TIME
V100-LAN	192.168.100.216	DESKTOP-KJC4M7F	a0:8c:fd:dac:9: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-HMGPJ43	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-N7HLPH5	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 4.49 แสดงผลการตรวจสอบผู้ใช้งานระบบเครือข่ายก่อนการใช้งาน ระบบ Authentication

2. ตรวจสอบผู้ใช้งานระบบเครือข่ายหลังการใช้งานระบบ Authentication โดยการเข้าไปตรวจสอบจำนวนผู้ใช้งาน Authentication List บน Firewall โดยแสดงดังภาพที่ 4.62 คือสามารถระบุตัวตนของผู้ใช้งานได้จาก User ที่ทำการใช้งาน

USER	TYPE	DOMAIN	CLIENT	ELAPSED TIME	IP ADDRESS
hais.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 4.50 แสดงผลการตรวจสอบผู้ใช้งานระบบเครือข่ายหลังการใช้งาน ระบบ Authentication

3. ตรวจสอบประวัติการใช้งานระบบก่อนการใช้งานระบบ การใช้งานระบบเครือข่ายก่อนการใช้งานระบบ Authentication ไม่มีการจัดเก็บประวัติการใช้งานเครือข่าย

4. ตรวจสอบการใช้งานระบบหลังการใช้งานระบบ Authentication โดยสามารถเข้าตรวจสอบประวัติการใช้งานเครือข่ายได้ผ่าน Log Files Server

ตารางที่ 4.7 เปรียบเทียบการทำงานก่อนและหลังการใช้งานระบบ

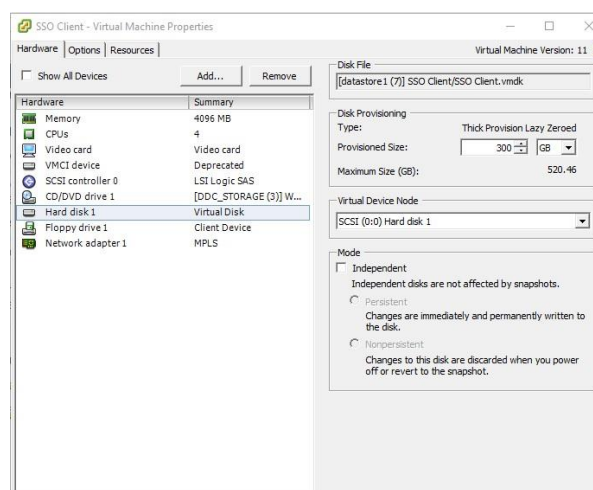
ก่อนใช้งานระบบ	หลังใช้งานระบบ
ไม่สามารถรู้ได้ว่ามีใครใช้งานระบบอยู่บ้าง	สามารถระบุตัวตนผู้ใช้งานระบบได้
ไม่สามารถตรวจสอบประวัติการใช้งานย้อนหลังได้	สามารถตรวจสอบประวัติการใช้งานย้อนหลังได้
ไม่สามารถปกป้องข้อมูลภายในจากการเข้าถึงที่ไม่ได้รับอนุญาต	สามารถควบคุมการเข้าเครือข่ายจากการเข้าถึงที่ไม่ได้รับอนุญาต
ไม่มีการป้องกันการเข้าถึงเครือข่าย	มีการป้องกันการเข้าถึงเครือข่ายด้วยระบบ

จากตารางที่ 4.7 แสดงให้เห็นว่าการใช้ Authentication ทำให้ความสามารถในการป้องกันเครือข่ายมีประสิทธิภาพมากขึ้น

#### 4.2.4 ขั้นตอนการดำเนินงานให้เหมาะสม (Act)

ตรวจสอบผลลัพธ์จากที่ได้วางแผนไว้โดยมีกรณีผลลัพธ์ที่ได้ไม่เป็นไปตามขั้นการวางแผน ดำเนินการค้นหาสาเหตุที่มาของผล ดำเนินการแก้ไขโดยมีผลลัพธ์ที่ไม่เป็นไปตามที่วางแผนไว้ ดังนี้

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



ภาพที่ 4.51 แสดงผลปรับปรุงขนาดของพื้นที่ในการจัดเก็บเพิ่มจากเดิม 100 GB เป็น 300 GB

2. การใช้งานระบบ Authentication ผ่านอุปกรณ์โทรศัพท์มือถือและแท็บเล็ตที่ใช้ระบบปฏิบัติการ iOS พบปัญหาระบบ Authentication ไม่ขึ้นให้เข้าใช้งานแก้ปัญหาเบื้องต้นโดยให้ผู้ใช้งาน

ผู้กมารถกหนดางเข้าใช้งานไว้กรณีระบบไม่ขึ้นสามารถกดเข้าไปใช้งานเองได้ และจะหาสาเหตุและวิธีการแก้ไขต่อไป

3. ประกาศการใช้งานระบบหลังจากได้มีการทดสอบระบบจนแน่ใจแล้วจึงได้ดำเนินการประกาศใช้งานระบบการยืนยันตัวบุคคลเพื่อเข้าใช้งานระบบเครือข่ายอินเทอร์เน็ตเมื่อวันที่ 27 กุมภาพันธ์ พ.ศ. 2566 ดังนั้นทำให้ทุกครั้งที่มีการเข้าถึงเครือข่ายไม่ว่าจะเป็นเครือข่ายภายใน Intranet หรือ เครือข่ายภายนอก Internet จำเป็นต้องมีการ Authentication ก่อนทุกครั้ง ทำให้หน่วยงานมีความความมั่นคงปลอดภัยในการใช้งานระบบเครือข่ายเพิ่มมากขึ้นโดยสามารถป้องกันบุคคลภายนอกหรือประชาชนที่อาศัยอยู่รอบข้างสำนักงานป้องกันควบคุมโรคที่ 11 ไม่สามารถเข้าถึงระบบเครือข่ายของหน่วยงานได้โดยไม่ได้รับอนุญาต อีกทั้งยังสามารถทำให้สำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราชได้ดำเนินการตามนโยบายนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกระทรวงสาธารณสุข พ.ศ. 2565 และ ตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 ฉบับที่ 2 ได้อีกด้วย โดยมีขั้นตอนดังนี้

3.1 จัดทำหนังสือราชการแจ้งเวียนก่อนการเปิดใช้งานล่วงหน้า 2 สัปดาห์ (ภาคผนวก ก)

3.2 จัดทำคู่มือการใช้งานบนเครื่องคอมพิวเตอร์, คอมพิวเตอร์แท็บเล็ตและโทรศัพท์มือถือ คู่มือการเปลี่ยนรหัสผ่าน ประชาสัมพันธ์ในกลุ่ม Line ล่วงหน้า 1 สัปดาห์ (ภาคผนวก ค-จ)

3.3 ดำเนินการส่งมอบ Username และ Password และคู่มือการใช้งาน ดำเนินการส่งมอบรหัสให้แก่บุคลากรรายบุคคลพร้อมกำหนดแนวทางการบริหารจัดการผู้ใช้งาน ดังนี้

3.3.1 เพื่อป้องกันการลวงรู้ชื่อผู้ใช้และรหัสผ่านเริ่มต้นของผู้อื่นพร้อมทั้งชี้แจงเกี่ยวกับมาตรฐานในการเปลี่ยนรหัสผ่านตามรายละเอียดต่อไปนี้ (ภาคผนวก ค-จ)

- 1) จำนวนความยาวต้องไม่น้อย 8 ตัวอักษรและประกอบด้วย 3 ใน 4 ข้อนี้
- 2) ภาษาอังกฤษ A ถึง Z ในแบบตัวพิมพ์ใหญ่
- 3) ภาษาอังกฤษ a ถึง z ในแบบตัวพิมพ์เล็ก
- 4) ตัวเลข 0 ถึง 9
- 5) ตัวอักษรสัญลักษณ์ เช่น (for example, !, \$, #, %)

3.4 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	00FC11 f					Global	

ภาพที่ 4.52 แสดงการจัดลำดับ Policy บน Firewall

4. กำหนดแนวทางในการเพิ่ม ลบ สิทธิการใช้งาน แก่งานการเจ้าหน้าที่โดยมีขั้นตอน ดังนี้
  - 4.1 ขั้นตอนการขอรับชื่อผู้ใช้งานและรหัสผ่าน
    1. งานการเจ้าหน้าที่ส่งข้อมูลบุคลากร หรือ บุคลากรใหม่ มาให้งานเทคโนโลยีสารสนเทศ ประกอบด้วย ชื่อ-สกุล ภาษาไทย และ ภาษาอังกฤษ ตำแหน่ง และ กลุ่มงาน
    2. งานเทคโนโลยีสารสนเทศ นำข้อมูลไปบันทึกในฐานข้อมูล Active Directory และกำหนด ชื่อผู้ใช้งานและรหัสผ่าน
    3. งานเทคโนโลยีสารสนเทศส่งชื่อผู้ใช้งาน รหัสผ่านและคู่มือการเข้าใช้งาน คู่มือการเปลี่ยนรหัสผ่าน ให้กับเจ้าหน้าที่
    - 4.2 ขั้นตอนแรกแจ้งบุคลากรลาออก ย้ายงาน หรือเกษียณอายุราชการ
      1. งานการเจ้าหน้าที่แจ้งชื่อ-สกุล กลุ่มงาน ของบุคลากรที่ลาออก ย้ายงาน หรือเกษียณอายุราชการ
      2. งานเทคโนโลยีสารสนเทศ ยกเลิกสิทธิการเข้าใช้งาน
5. ผลการบำรุงรักษาระบบ
 

ในการดูแลรักษาระบบใช้วิธีการ Preventive Maintenance (PM) คือ การบำรุงรักษาเชิงป้องกัน เป็นหนึ่งในรูปแบบการดูแลสภาพเครื่องจักรและอุปกรณ์ ที่ใช้การตรวจสอบ ซ่อมแซม หรือเปลี่ยนแปลง อุปกรณ์ต่างๆ ตามเวลาที่มีการกำหนดเอาไว้ โดยมีแผนการบำรุงรักษาตั้งแต่เริ่มใช้งานระบบดังนี้

ตารางที่ 4.8 แสดงตารางการบำรุงรักษาเครื่อง Server

วันที่ (Date)	รายละเอียด
มีนาคม 2566	ตรวจสอบความพร้อมใช้ของเซิร์ฟเวอร์และการทำงานของระบบ
กรกฎาคม 2566	ตรวจสอบความพร้อมใช้ของเซิร์ฟเวอร์และการทำงานของระบบ

### 4.3 ผลการประเมินการพัฒนาระบบ

4.3.1 แสดงสถิติการใช้งานระบบการยืนยันตัวตนบุคคลเพื่อเข้าใช้งานระบบเครือข่ายอินเทอร์เน็ตของสำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช

ตารางที่ 4.9 แสดงสถิติการใช้งานระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log Files) ของสำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช จำนวน 47 วัน ระหว่างวันที่ 24 กันยายน พ.ศ. 2566 ถึงวันที่ 9 พฤศจิกายน พ.ศ. 2566

ลำดับ	วันที่	จำนวนการเข้าใช้งาน สำเร็จ	จำนวนการเข้าใช้งานที่โดน ปฏิเสธ	จำนวนอุปกรณ์ที่เข้าใช้ งาน	จำนวนผู้เข้าใช้ งาน
1	24/09/2023	19	12	19	12
2	25/09/2023	190	196	188	106
3	26/09/2023	174	175	169	102
4	27/09/2023	168	172	161	92
5	28/09/2023	163	204	156	93
6	29/09/2023	128	135	121	76
7	30/09/2023	26	29	23	14
8	1/10/2023	12	39	12	9
9	2/10/2023	168	180	166	100
10	3/10/2023	193	195	186	106
11	4/10/2023	199	195	193	113
12	5/10/2023	192	201	188	108
13	6/10/2023	193	199	188	110
14	7/10/2023	35	22	25	19
15	8/10/2023	14	13	15	10
16	9/10/2023	173	177	172	101
17	10/10/2023	173	177	169	100

ลำดับ	วันที่	จำนวนการเข้าใช้งาน สำเร็จ	จำนวนการเข้าใช้งานที่โดน ปฏิเสธ	จำนวนอุปกรณ์ที่เข้าใช้ งาน	จำนวนผู้เข้าใช้ งาน
18	11/10/2023	197	199	188	107
19	12/10/2023	187	186	182	102
20	13/10/2023	20	9	16	11
21	14/10/2023	6	2	6	5
22	15/10/2023	5	5	5	5
23	16/10/2023	174	184	173	105
24	17/10/2023	200	212	191	109
25	18/10/2023	189	203	179	104
26	19/10/2023	169	167	163	97
27	20/10/2023	191	176	174	98
28	21/10/2023	27	13	25	17
29	22/10/2023	15	12	16	10
30	23/10/2023	21	18	20	12
31	24/10/2023	192	205	189	110
32	25/10/2023	189	184	184	113
33	26/10/2023	192	193	183	111
34	27/10/2023	185	174	172	107
35	28/10/2023	29	22	27	17
36	29/10/2023	22	17	21	12
37	30/10/2023	156	165	154	93
38	31/10/2023	203	196	190	111
39	1/11/2023	198	190	186	109
40	2/11/2023	199	209	193	110
41	3/11/2023	177	171	168	105
42	4/11/2023	22	14	19	12
43	5/11/2023	10	7	11	8
44	6/11/2023	198	224	198	115
45	7/11/2023	213	218	203	117
46	8/11/2023	194	192	190	115
47	9/11/2023	207	215	198	118
	<b>รวม</b>	<b>6,207</b>	<b>6,303</b>	<b>5,975</b>	<b>3,536</b>

จากตารางที่ 4.9 สถิติการใช้งานระบบการยืนยันตัวบุคคลเพื่อเข้าใช้งานระบบเครือข่ายอินเทอร์เน็ตของสำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช จำนวน 47 วัน ระหว่างวันที่ 24 กันยายน พ.ศ. 2566 ถึงวันที่ 9 พฤศจิกายน พ.ศ. 2566 สามารถแสดงให้เห็นถึงประสิทธิภาพของระบบในด้านต่างๆ ดังต่อไปนี้ ความสามารถในการให้บริการโดยได้มีการจัดเก็บประวัติการใช้งานระบบสำเร็จ จำนวน 6,207 ครั้ง คิดเป็นการใช้งานเฉลี่ย 132 ครั้งต่อวัน มีอุปกรณ์เข้าใช้งานเฉลี่ย 127 อุปกรณ์ต่อวัน ความสามารถในการควบคุมการเข้าถึงการใช้งานระบบเครือข่ายอินเทอร์เน็ตโดยได้มีการจัดเก็บประวัติการป้องกันการเข้าถึงเครือข่ายที่ไม่ได้รับอนุญาตสำเร็จ จำนวน 6,303 ครั้ง คิดเป็นการป้องกันเฉลี่ย 134 ครั้งต่อวัน

วัดผลจากการตั้งเป้าหมายด้านการใช้งานระบบโดยได้มีการตั้งเป้าหมายการเข้าใช้งานเฉลี่ยเฉพาะวันทำการไม่น้อยกว่าร้อยละ 50 ข้อมูลจากตารางที่ 4.12 แสดงให้เห็นว่ามีจำนวนผู้งานทั้งหมดจำนวน 3,536 คนคิดเป็นผู้ใช้งานเฉลี่ย 75 คนต่อวัน คิดเป็นผู้ใช้งานเฉลี่ยเฉพาะวันทำการเป็น 105 คนต่อวันคิดเป็นร้อยละ 65 จากจำนวนผู้ใช้งานทั้งหมด 160 คน

ตารางที่ 4.10 แสดงรายงานสรุปประวัติการใช้งานและการป้องกันการเข้าใช้งานโดยไม่ได้รับอนุญาต

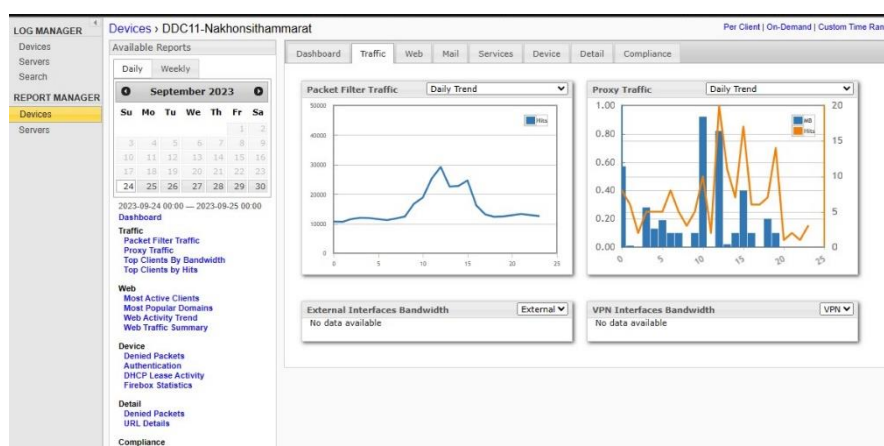
จำนวนการเข้าใช้งานทั้งหมด	จำนวนการเข้าใช้งานที่ปฏิเสธ	ผู้ใช้งานเข้าระบบไม่สำเร็จ	การเข้าใช้งานโดยไม่ได้ลงทะเบียน
12,510	6,303	5,880	423

จากตารางที่ 4.10 แสดงให้เห็นถึงความสามารถการป้องกันการเข้าใช้งานระบบเครือข่ายอินเทอร์เน็ตของสำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราชโดยไม่ได้รับอนุญาต จำนวน 47 วัน ระหว่างวันที่ 24 กันยายน พ.ศ. 2566 ถึงวันที่ 9 พฤศจิกายน พ.ศ. 2566 แสดงให้เห็นถึงจำนวนการเข้าใช้งานที่ระบบสามารถป้องกันไว้ได้ดังต่อไปนี้ จำนวนเข้าใช้งานระบบทั้งหมด 12,510 ครั้ง จำนวนการเข้าใช้งานที่โดนปฏิเสธทั้งหมด 6,303 ครั้งคิดเป็นร้อยละ 50.38 ของการเข้าใช้งานทั้งหมด สามารถแบ่งการเข้าใช้งานระบบไม่สำเร็จออกเป็น 2 ส่วนคือ 1) การเข้าใช้งานระบบไม่สำเร็จโดยผู้ใช้งานที่ได้ลงทะเบียนเข้าใช้งานไว้แล้ว จำนวน 5,880 ครั้งคิดเป็นร้อยละ 47.00ของการเข้าใช้งานทั้งหมด 2) การพยายามเข้าใช้งานโดยใช้ชื่อรหัสผู้ใช้งานที่ไม่เคยได้ลงทะเบียนไว้ก่อนจำนวน 423 ครั้ง คิดเป็นร้อยละ 3.38 ของการเข้าใช้งานทั้งหมด



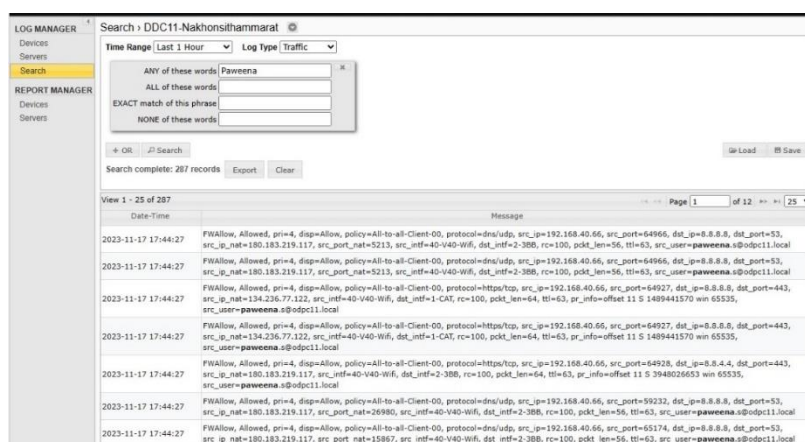
### 4.3.2 การจัดเก็บและรายงานข้อมูลจราจรคอมพิวเตอร์

ข้อมูลจราจรคอมพิวเตอร์ (Log Files) ทั้งหมดของระบบ ผู้ดูแลระบบสามารถดูรายละเอียดข้อมูลล่าสุดโดยแสดงข้อมูล สถานการณ์เข้าใช้งาน วันเดือนปี ชื่อผู้ใช้งาน ปลายทางที่ทำงานเชื่อมต่อ โปรโตคอลที่ใช้เชื่อมต่อและนโยบายการรักษาความมั่นคงปลอดภัยของไฟร์วอลล์ (Policy) ที่ปล่อยให้ผ่านการใช้งาน โดยสามารถเลือกแสดงผลในรูปแบบ Dashboard หรือ export ออกมาในรูปแบบไฟล์ CSV เพื่อง่ายต่อการประยุกต์ใช้ร่วมกับโปรแกรมอื่น



ภาพที่ 4.53 แสดงภาพแสดงข้อมูลจราจรคอมพิวเตอร์ในรูปแบบ Dashboard

ผู้ดูแลระบบสามารถเข้าถึงและตรวจสอบข้อมูลจราจรคอมพิวเตอร์ของผู้ใช้งานได้ตาม พ.ร.บ. คอมพิวเตอร์คือ วันเวลาที่ใช้งาน IP Address ต้นทาง IP Address ปลายทาง port และโปรโตคอลที่ใช้งาน รวมถึงสามารถระบุตัวตนผู้ใช้งานได้ตามวัตถุประสงค์ของงานวิจัย

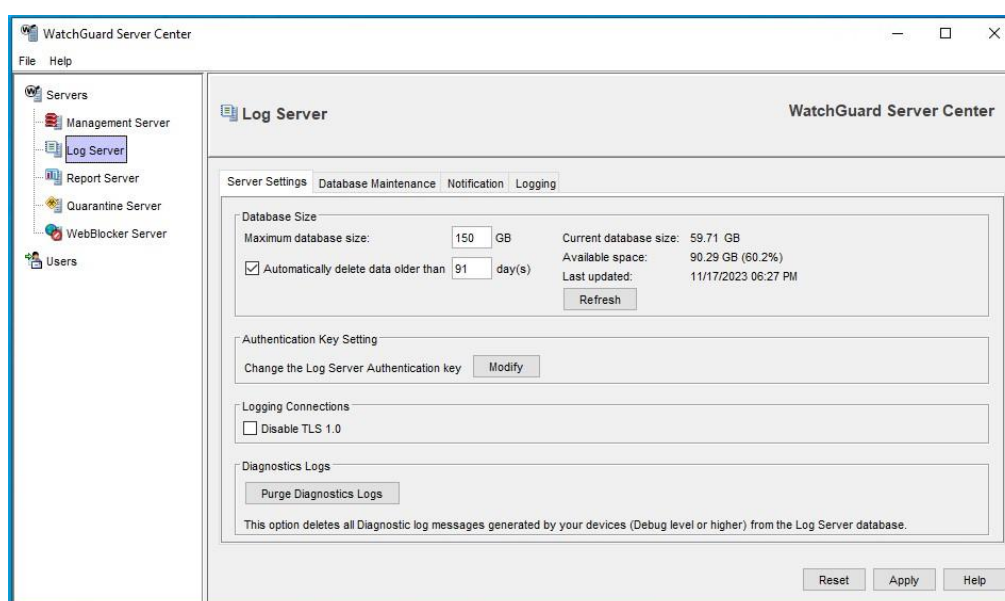


ภาพที่ 4.54 การค้นหาประวัติข้อมูลจราจรคอมพิวเตอร์ ผู้ดูแลสามารถกำหนดเงื่อนไขในการค้นหาได้ดังนี้

- 1) ช่วงเวลาในการค้นหา สามารถค้นหาได้ตามเวลาที่กำหนด
- 2) สามารถค้นหาประวัติทั้งหมดจาก Keyword
- 3) สามารถ export ข้อมูลที่ทำการค้นหาเป็นรูปแบบ CSV เพื่อนำไปใช้งานต่อ
- 4) สามารถเลือกดูรายละเอียดข้อมูลรายบรรทัด

ผู้ดูแลระบบสามารถกำหนดระยะเวลาและพื้นที่ในการจัดเก็บข้อมูลจราจรคอมพิวเตอร์และหน้ารายงานผลได้ดังต่อไปนี้

- 1) กำหนดขนาดสูงสุดของพื้นที่ที่ไว้จัดเก็บ
- 2) กำหนดระยะเวลาลบข้อมูลจราจรคอมพิวเตอร์
- 3) กำหนดระยะเวลาในการจัดเก็บหน้ารายงานของระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์
- 4) กำหนดเวลาในการลบหน้ารายงานที่มีอายุเกินกำหนด
- 5) กำหนดขนาดพื้นที่ในการจัดเก็บหน้ารายงาน



ภาพที่ 4.55 แสดงรายละเอียดพื้นที่การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ โดยผู้ดูแลระบบกำหนดพื้นที่ในการจัดเก็บสูงสุดอยู่ที่ 150 GB และแสดงจำนวนพื้นที่ที่ได้ทำการใช้งานไปแล้ว คือ 59.71 GB พื้นที่ว่างสำหรับการจัดเก็บข้อมูลในอนาคตคือ 90.29 GB คิดเป็นร้อยละ 60.2

4.3.3 จากข้อมูลการประเมินการพัฒนาระบบสามารถประเมินคะแนนความสามารถการทำงานของระบบโดยอ้างอิงจากวัตถุประสงค์ของการพัฒนาระบบเพื่อให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกระทรวงสาธารณสุข พ.ศ. 2565 และ พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 ฉบับที่ 2 โดยในแต่ละประเด็นจะมีคะแนนเต็มอยู่ที่ 1 คะแนน ซึ่งมีผลประเมินคะแนนได้ดังนี้

ตารางที่ 4.11 ผลการประเมิน

รายละเอียดการวัดผล	คะแนน ที่ได้	คะแนน รวม
1. สามารถควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลได้	0.5	0.5
2. สามารถบริหารจัดการการเข้าถึงของผู้ใช้งานเพื่อควบคุมการเข้าถึงระบบสารสนเทศได้	1	1.5
3. สามารถควบคุมการเข้าถึงเครือข่าย เพื่อป้องกันการเข้าถึงบริการทางเครือข่าย โดยไม่ได้รับอนุญาตได้	1	2.5
4. สามารถควบคุมการเข้าถึงโปรแกรมประยุกต์และแอปพลิเคชันได้	0.5	3
5.สามารถเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์	1	4

จากตารางที่ 4.11 แสดงให้เห็นว่าความสามารถควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลได้มีผลคะแนนอยู่ที่ 0.5 เนื่องจากระบบสามารถป้องกันการเข้าถึงข้อมูลได้แต่ไม่สามารถควบคุมการเข้าถึงอุปกรณ์ได้ ความสามารถบริหารจัดการการเข้าถึงของผู้ใช้งานเพื่อควบคุมการเข้าถึงระบบสารสนเทศได้มีผลคะแนนอยู่ที่ 1 ความสามารถควบคุมการเข้าถึงเครือข่าย เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาตได้มีผลคะแนนอยู่ที่ 1 ความสามารถควบคุมการเข้าถึงโปรแกรมประยุกต์และแอปพลิเคชันได้อยู่ที่ 0.5 เนื่องจากระบบสามารถป้องกันการเข้าถึงได้เฉพาะโปรแกรมประยุกต์และแอปพลิเคชันที่เป็นแบบออนไลน์ ความสามารถเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์อยู่ที่ 1 มีผลคะแนนการประเมินรวมอยู่ที่ 4 คะแนน

4.3.4 ผลการศึกษาจากการรวบรวมข้อมูล ผู้วิจัยได้รวบรวมข้อมูลจากแบบสอบถามนำมาวิเคราะห์ข้อมูลทางสถิติ จากกลุ่มตัวอย่างจำนวนทั้งสิ้น 114 ชุด ได้ผลดังนี้

ส่วนที่ 1 แสดงข้อมูลลักษณะทั่วไปของบุคลากรในสำนักงานป้องกันควบคุมโรคที่ 11 และ ศตม.  
11.2 นครศรีธรรมราช จากข้อมูลผลการศึกษสามารถแบ่งได้ดังนี้

ตารางที่ 4.12 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 4.12 แสดงผลให้เห็นถึง ผลการศึกษาข้อมูลปัจจัยส่วนบุคคล ด้านอายุของกลุ่มตัวอย่างผู้ตอบแบบสอบถาม 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 4.13 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
กลุ่มห้องปฏิบัติการควบคุมโรคและภัยสุขภาพ	12	10.53
กลุ่มโรคติดต่อ	8	7.02
กลุ่มด้านควบคุมโรคติดต่อระหว่างประเทศ	2	1.75

กลุ่มงาน	กลุ่มตัวอย่าง(คน) N = 114	ร้อยละ
กลุ่มโรคเอดส์ วัณโรค โรคติดต่อทางเพศสัมพันธ์และโรคเรื้อน	9	7.89
งานกฎหมาย	3	2.63
งานเภสัชกร	3	2.63
ศตม.11.2 นครศรีธรรมราช	16	14.04

จากตารางที่ 4.13 แสดงผลให้เห็นถึงผลการศึกษาปัจจัยส่วนบุคคล ด้านกลุ่มที่ปฏิบัติงานของกลุ่มตัวอย่างผู้ตอบแบบสอบถาม 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 โดยมี กลุ่มพัฒนานวัตกรรมและวิจัย และ กลุ่มด้านควบคุมโรคติดต่อระหว่างประเทศมีผู้ตอบแบบสอบถามน้อยที่สุด

ตารางที่ 4.14 ผลการศึกษาปัจจัยด้านระดับการปฏิบัติงาน

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

จากตารางที่ 4.14 แสดงผลให้เห็นถึงผลการศึกษาปัจจัยด้านระดับการปฏิบัติงาน ของกลุ่มตัวอย่างผู้ตอบแบบสอบถาม จำนวนทั้งสิ้น 114 คน ผู้บริหารและหัวหน้ากลุ่มจำนวน 9 คน คิดเป็นร้อยละ 7.90 ผู้ปฏิบัติงาน 105 คน คิดเป็นร้อยละ 92.10

ส่วนที่ 2 แสดงผลการประเมินประสิทธิผลและความสำเร็จของการใช้งานระบบการยืนยันตัวตนบุคคล เพื่อเข้าใช้งานระบบเครือข่ายอินเทอร์เน็ตของสำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช ว่าโดยภาพรวมโดยเฉลี่ย บุคลากรภายในหน่วยงานมีความคิดเห็นอย่างไรเกี่ยวกับการใช้งานระบบโดยแบ่งเป็น 4 ประเด็นดังนี้

- 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

การประเมินประสิทธิผลและความสำเร็จด้านประสิทธิภาพของระบบโดยแบ่งการวิเคราะห์ออกเป็น 3 ส่วนคือ ผู้บริหารและหัวหน้ากลุ่ม ผู้ปฏิบัติงาน และ บุคลากรกลุ่มเป้าหมายทั้งหมด

ตารางที่ 4.15 แสดงผลการประเมินประสิทธิผลและความสำเร็จด้านประสิทธิภาพของระบบ ของผู้บริหาร และหัวหน้ากลุ่ม

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

ตารางที่ 4.16 แสดงผลการประเมินประสิทธิผลและความสำเร็จด้านประสิทธิภาพของระบบ ของผู้ปฏิบัติงาน

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

ตารางที่ 4.17 แสดงผลการประเมินประสิทธิผลและความสำเร็จด้านประสิทธิภาพของระบบ

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

จากตารางที่ 4.15 - 4.17 แสดงผลให้เห็นผลการวิเคราะห์การประเมินประสิทธิผลและความสำเร็จด้านประสิทธิภาพของระบบ สามารถสรุปได้ดังนี้

ผู้ปฏิบัติงานมีความเข้าใจเกี่ยวกับวิธีการใช้งานการยืนยันตัวบุคคลอยู่ที่ 4.20 ซึ่งมากกว่าผู้บริหารและหัวหน้ากลุ่มที่มีผลคะแนนอยู่ที่ 4.11 โดยมีผลคะแนนภาพรวมอยู่ที่ 4.17 สามารถแปลผลได้ว่ากลุ่มตัวอย่างทั้งหมดมีความเข้าใจเกี่ยวกับวิธีการใช้งานการยืนยันตัวบุคคลอยู่ในระดับมาก

ผู้ปฏิบัติงานมีความสามารถในการใช้การยืนยันตัวบุคคลด้วยตนเองอยู่ที่ 4.72 ซึ่งมากกว่าผู้บริหารและหัวหน้ากลุ่มที่มีผลคะแนนอยู่ที่ 4.67 โดยมีผลคะแนนภาพรวมอยู่ที่ 4.73 สามารถแปลผลได้ว่ากลุ่มตัวอย่างทั้งหมดมีความสามารถในการใช้การยืนยันตัวบุคคลด้วยตนเองอยู่ในระดับมากที่สุด

ผู้บริหารและหัวหน้ากลุ่มมีความเห็นต่อความรวดเร็วของกระบวนการยืนยันตัวบุคคลเมื่อต้องการเข้าใช้งานอยู่ที่ 4.44 ซึ่งมากกว่าผู้ปฏิบัติงานที่มีผลคะแนนอยู่ที่ 4.33 โดยมีผลคะแนนภาพรวมอยู่ที่ 4.34 สามารถแปลผลได้ว่ากลุ่มตัวอย่างทั้งหมดมีความเห็นต่อความรวดเร็วของกระบวนการยืนยันตัวบุคคลเมื่อต้องการเข้าใช้งานอยู่ในระดับมากที่สุด

ผู้บริหารและหัวหน้ากลุ่มมีความเห็นต่อความสะดวกและง่ายต่อการเข้าใช้ระบบอยู่ที่ 4.40 ซึ่งมากกว่าผู้ปฏิบัติงานที่มีผลคะแนนอยู่ที่ 4.39 โดยมีผลคะแนนภาพรวมอยู่ที่ 4.40 สามารถแปลผลได้ว่ากลุ่มตัวอย่างทั้งหมดมีความเห็นต่อความสะดวกและง่ายต่อการเข้าใช้ระบบอยู่ในระดับมากที่สุด

กลุ่มตัวอย่างภาพรวมมีความสามารถในการใช้การยืนยันตัวบุคคลด้วยตนเองอยู่ในระดับสูงสุดคือ 4.73 และมีความเข้าใจเกี่ยวกับวิธีการใช้งานการยืนยันตัวบุคคลอยู่ในระดับที่น้อยที่สุดคือ 4.17

### ด้านความสำคัญของการป้องกันระบบ

การประเมินประสิทธิผลและความสำเร็จด้านความสำคัญของการป้องกันระบบโดยแบ่งการวิเคราะห์ออกเป็น 3 ส่วนคือ ผู้บริหารและหัวหน้ากลุ่ม ผู้ปฏิบัติงาน และ บุคลากรกลุ่มเป้าหมายทั้งหมด ตารางที่ 4.18 แสดงผลการประเมินประสิทธิผลและความสำเร็จด้านความสำคัญของการป้องกันระบบ ของผู้บริหารและหัวหน้ากลุ่ม

ประเด็นความคิดเห็น	$\bar{x}$	S.D.	การแปลผล
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 4.19 แสดงผลการประเมินประสิทธิผลและความสำเร็จด้านความสำคัญของการป้องกันระบบ 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 4.20 แสดงผลการประเมินประสิทธิผลและความสำเร็จด้านความสำคัญของการป้องกันระบบ

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 4.18 - 4.20 แสดงผลให้เห็นผลการประเมินประสิทธิผลและความสำเร็จด้านความสำคัญของการป้องกันระบบ สามารถสรุปได้ดังนี้

ผู้บริหารและหัวหน้ากลุ่มมีความเข้าใจเกี่ยวกับข้อกำหนดและเงื่อนไขของการยืนยันตัวบุคคลอยู่ที่ 4.56 ซึ่งมากกว่าผู้ปฏิบัติงานที่มีผลคะแนนอยู่ที่ 4.20 โดยมีผลคะแนนภาพรวมอยู่ที่ 4.19 สามารถแปลผลได้ว่าผู้บริหารและหัวหน้ากลุ่มมีความเข้าใจเกี่ยวกับข้อกำหนดและเงื่อนไขของการยืนยันตัวบุคคลอยู่ในระดับมากที่สุด ผู้ปฏิบัติงานมีความเข้าใจเกี่ยวกับข้อกำหนดและเงื่อนไขของการยืนยันตัวบุคคลอยู่ในระดับมาก

ผู้บริหารและหัวหน้ากลุ่มเห็นความสำคัญของการรักษาความปลอดภัยของข้อมูลขณะใช้งานอินเทอร์เน็ตอยู่ที่ 5.00 ซึ่งมากกว่าผู้ปฏิบัติงานที่มีผลคะแนนอยู่ที่ 4.52 โดยมีผลคะแนนภาพรวมอยู่ที่ 4.56 สามารถแปลผลได้ว่ากลุ่มตัวอย่างทั้งหมดเห็นความสำคัญของการรักษาความปลอดภัยของข้อมูลขณะใช้งานอินเทอร์เน็ตอยู่ในระดับมากที่สุด

ผู้บริหารและหัวหน้ากลุ่มเห็นความสำคัญของการป้องกันการเข้าถึงที่ไม่ได้รับอนุญาตในการใช้งานอินเทอร์เน็ตอยู่ที่ 4.78 ซึ่งมากกว่าผู้ปฏิบัติงานที่มีผลคะแนนอยู่ที่ 4.41 โดยมีผลคะแนนภาพรวมอยู่ที่ 4.43 สามารถแปลผลได้ว่ากลุ่มตัวอย่างทั้งหมดเห็นความสำคัญของการป้องกันการเข้าถึงที่ไม่ได้รับอนุญาตในการใช้งานอินเทอร์เน็ตอยู่ในระดับมากที่สุด

กลุ่มตัวอย่างภาพรวมมีความเข้าใจเกี่ยวกับข้อกำหนดและเงื่อนไขของการยืนยันตัวบุคคลน้อยที่สุด ซึ่งมีค่าคะแนนอยู่ที่ 4.19 และเห็นความสำคัญของการรักษาความปลอดภัยของข้อมูลขณะใช้งาน อินเทอร์เน็ตอยู่ในระดับสูงที่สุดโดยมีค่าคะแนนอยู่ที่ 4.56

### ด้านความน่าเชื่อถือ

ตารางที่ 4.21 แสดงผลการประเมินประสิทธิภาพและความสำเร็จด้านความน่าเชื่อถือของระบบ ของผู้บริหาร และหัวหน้ากลุ่ม

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 4.22 แสดงผลการประเมินประสิทธิภาพและความสำเร็จด้านความน่าเชื่อถือของระบบ ของผู้ปฏิบัติงาน

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 4.23 แสดงผลการประเมินประสิทธิภาพและความสำเร็จด้านความน่าเชื่อถือของระบบ

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 4.21 - 4.23 แสดงผลให้เห็นผลการประเมินประสิทธิผลและความสำเร็จด้านความน่าเชื่อถือสามารถสรุปได้ดังนี้

ผู้บริหารและหัวหน้ากลุ่มมีความเชื่อมั่นต่อระดับความปลอดภัยของระบบยืนยันตัวบุคคลอยู่ที่ 4.33 ซึ่งมากกว่าผู้ปฏิบัติงานที่มีผลคะแนนอยู่ที่ 4.16 สามารถแปลผลได้ว่าผู้บริหารและหัวหน้ากลุ่มมีความเชื่อมั่นต่อระดับความปลอดภัยของระบบยืนยันตัวบุคคลอยู่ในระดับมากที่สุด ผู้ปฏิบัติงานมีความเชื่อมั่นต่อระดับความปลอดภัยของระบบยืนยันตัวบุคคลอยู่ในระดับมาก

ผู้บริหารและหัวหน้ากลุ่มมีความเชื่อมั่นต่อความพร้อมของระบบยืนยันตัวบุคคลต่อการป้องกันการแฮกเกอร์หรือการละเมิดความปลอดภัยอยู่ที่ 4.22 ซึ่งมากกว่าผู้ปฏิบัติงานที่มีผลคะแนนอยู่ที่ 4.17 สามารถแปลผลได้ว่าผู้บริหารและหัวหน้ากลุ่มมีความเชื่อมั่นความพร้อมของระบบยืนยันตัวบุคคลต่อการป้องกันการแฮกเกอร์หรือการละเมิดความปลอดภัยอยู่ในระดับมากที่สุด ผู้ปฏิบัติงานมีความเชื่อมั่นต่อความพร้อมของระบบยืนยันตัวบุคคลต่อการป้องกันการแฮกเกอร์หรือการละเมิดความปลอดภัยอยู่ในระดับมาก

ผู้บริหารและหัวหน้ากลุ่มมีความเชื่อมั่นต่อความน่าเชื่อถือของระบบยืนยันตัวบุคคลอยู่ที่ 4.33 ซึ่งมากกว่าผู้ปฏิบัติงานที่มีผลคะแนนอยู่ที่ 4.27 สามารถแปลผลได้ว่ากลุ่มตัวอย่างทั้งหมดมีความเชื่อมั่นต่อความน่าเชื่อถือของระบบยืนยันตัวบุคคลอยู่ในระดับมากที่สุด

กลุ่มตัวอย่างภาพรวมมีความเชื่อมั่นต่อระดับความปลอดภัยของระบบยืนยันตัวบุคคลอยู่ในระดับน้อยที่สุดซึ่งมีผลคะแนนอยู่ที่ 4.15 และมีความเชื่อมั่นต่อความน่าเชื่อถือของระบบยืนยันตัวบุคคลอยู่ในระดับสูงที่สุดโดยมีค่าคะแนนอยู่ที่ 4.25

### ด้านคุณภาพการบริการ

ตารางที่ 4.24 แสดงผลการประเมินประสิทธิผลและความสำเร็จด้านคุณภาพการให้บริการ ของผู้บริหารและหัวหน้ากลุ่ม

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 4.25 แสดงผลการประเมินประสิทธิผลและความสำเร็จด้านคุณภาพการให้บริการ ของผู้ปฏิบัติงาน

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

ตารางที่ 4.26 แสดงผลการประเมินประสิทธิผลและความสำเร็จด้านคุณภาพการให้บริการ

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

จากตารางที่ 4.24 – 4.26 แสดงผลให้เห็นผลการประเมินประสิทธิผลและความสำเร็จด้านคุณภาพการบริการ สามารถสรุปได้ดังนี้

ผู้บริหารและหัวหน้ากลุ่มได้รับความรู้และการสนับสนุนในการใช้งานการยืนยันตัวตนอยู่ที่ 4.56 ซึ่งมากกว่าผู้ปฏิบัติงานที่มีผลคะแนนอยู่ที่ 4.44 สามารถแปรผลได้ว่ากลุ่มตัวอย่างทั้งหมดได้รับความรู้และการสนับสนุนในการใช้งานการยืนยันตัวตนอยู่ในระดับมากที่สุด

ผู้บริหารและหัวหน้ากลุ่มมีความเห็นว่าระบบมีการแจ้งเตือนในกรณีเกิดข้อผิดพลาดถูกต้องอยู่ที่ 4.22 ซึ่งมากกว่าผู้ปฏิบัติงานที่มีผลคะแนนอยู่ที่ 4.10 สามารถแปรผลได้ว่าผู้บริหารและหัวหน้ากลุ่มมีความเห็นว่าระบบมีการแจ้งเตือนในกรณีเกิดข้อผิดพลาดถูกต้องอยู่ในระดับมากที่สุด ผู้ปฏิบัติงานมีความเห็นว่าระบบมีการแจ้งเตือนในกรณีเกิดข้อผิดพลาดถูกต้องอยู่ในระดับมาก

ผู้บริหารและหัวหน้ากลุ่มได้รับการแก้ปัญหาในกรณีเกิดข้อผิดพลาดอยู่ที่ 4.78 ซึ่งมากกว่าผู้ปฏิบัติงานที่มีผลคะแนนอยู่ที่ 4.58 สามารถแปรผลได้ว่ากลุ่มตัวอย่างทั้งหมดได้รับการแก้ปัญหาในกรณีเกิดข้อผิดพลาดอยู่ในระดับมากที่สุด

กลุ่มตัวอย่างภาพรวมมีความเห็นว่าระบบมีการแจ้งเตือนในกรณีเกิดข้อผิดพลาดถูกต้องอยู่ในระดับน้อยที่สุดซึ่งมีผลคะแนนอยู่ที่ 4.08 และได้รับการแก้ปัญหาในกรณีเกิดข้อผิดพลาดอยู่ในระดับสูงสุดโดยมีผลคะแนนอยู่ที่ 4.60

## บทที่ 5

### บทสรุป และข้อเสนอแนะ

การพัฒนากระบวนการยืนยันตัวบุคคลเพื่อเข้าใช้งานระบบเครือข่ายอินเทอร์เน็ตของสำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช ได้ดำเนินการโดยใช้ทรัพยากรของหน่วยงานที่มีอยู่เพื่อพัฒนาระบบแก้ปัญหาการควบคุมการเข้าถึงการใช้งานอินเทอร์เน็ตของหน่วยงานโดยได้ใช้งาน ระบบเซิร์ฟเวอร์เสมือนจริง VMware vSphere Client เพื่อสร้างเครื่องเซิร์ฟเวอร์ และเครื่องคอมพิวเตอร์จัดเก็บ Log Files ได้ใช้งาน Active Directory บนระบบปฏิบัติการ Windows Server 2012 ในการบริหารจัดการผู้ใช้งาน และได้ใช้งาน Watchguard Firebox M4600 ซึ่งเป็นไฟร์วอลล์ทำหน้าที่ตรวจจับการใช้งานเครือข่าย โดยมีวัตถุประสงค์เพื่อตรวจสอบและยืนยันสิทธิ์เข้าถึงการใช้งานระบบเครือข่ายอินเทอร์เน็ตของสำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช ใช้แบบสอบถามประเมินประสิทธิผลและความสำเร็จของการใช้งานระบบ กลุ่มตัวอย่างที่ตอบแบบสอบถามจำนวน 114 คน ประกอบด้วยผู้บริหารและหัวหน้ากลุ่มจำนวน 9 คนและผู้ปฏิบัติงานจำนวน 105 คน แบบประเมินได้นำมาวิเคราะห์หาค่าทางสถิติ สถิติที่ใช้ประกอบด้วย ร้อยละ ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐาน

ตารางที่ 5.1 แสดงผลการประเมินประสิทธิผลและความสำเร็จของการใช้งานระบบในภาพรวม

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

### 5.1 สรุปผล

จากการศึกษาปัญหาและวางแผนการพัฒนาโดยใช้วงจรวงจร PDCA ผู้วิจัยได้พัฒนาระบบการยืนยันตัวบุคคลเพื่อเข้าใช้งานระบบเครือข่ายอินเทอร์เน็ตของสำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช จำนวน 1 ระบบ โดยมีผลการวิจัยดังต่อไปนี้

### 5.1.1 ผลการดำเนินงาน

1) ระบบที่ผู้วิจัยพัฒนาขึ้นคือระบบการยืนยันตัวตนบุคคลเพื่อเข้าใช้งานระบบเครือข่ายอินเทอร์เน็ตของสำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช สามารถตรวจสอบและยืนยันสิทธิ์การเข้าถึงเครือข่ายอินเทอร์เน็ตได้ตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของกระทรวงสาธารณสุข พ.ศ. 2565 โดยได้ใช้ Active Directory ช่วยจัดการทรัพยากรซึ่งติดตั้งอยู่บน Windows Server 2012 ที่ได้ใช้โปรแกรม VmWare จำลองเซิร์ฟเวอร์เสมือนขึ้นมาเพื่อติดตั้ง

2) ระบบสามารถจัดเก็บข้อมูลจราจรคอมพิวเตอร์ได้ตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 โดยได้ใช้โปรแกรม Watchguard Log Manager ในการบริหารจัดการข้อมูลจราจรคอมพิวเตอร์โดยได้ติดตั้งบนเครื่องคอมพิวเตอร์เสมือนที่ได้สร้างโดยใช้โปรแกรม VmWare

3) ระบบสามารถจัดเก็บข้อมูลจราจรคอมพิวเตอร์โดยสามารถค้นได้จาก วันที่ ชื่อผู้ใช้งาน IP Addressต้นทาง IP Addressปลายทาง และนำมาแสดงย้อนหลังได้ไม่น้อยกว่า 90 วันตรงตามที่พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 กำหนด

4) แสดงสถิติการใช้งานระบบโดยทำการเรียกใช้ข้อมูลจราจรทางคอมพิวเตอร์ที่ได้จัดเก็บไว้ในช่วงวันที่ 24 กันยายน พ.ศ. 2566 ถึงวันที่ 9 พฤศจิกายน พ.ศ. 2566 มาแสดงเป็นตัวอย่างข้อมูลตามทฤษฎีการสุ่มตัวอย่างของทาร์โรว์ ยามาเนะ มีจำนวนผู้ใช้งานจำนวน 6,207 ครั้งและสามารถป้องกันการเข้าใช้งานที่ไม่ได้รับอนุญาตจำนวน 6,303 ครั้ง

5) ระบบสามารถควบคุมการเข้าถึงเครือข่าย เพื่อป้องกันการเข้าถึงบริการทางเครือข่าย โดยไม่ได้รับอนุญาตได้ ตรงตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงสาธารณสุข พ.ศ. 2565

6) ผลแบบสอบถามประเมินประสิทธิผลและความสำเร็จของการใช้งานระบบจำนวน 4 ด้านโดยแบ่งกลุ่มตัวอย่างที่ตอบแบบสอบถามเป็น 2 กลุ่มคือ ผู้บริหารและหัวหน้ากลุ่ม และผู้ปฏิบัติงาน เพื่อให้ทราบถึงประเด็นที่มีความเห็นแตกต่างกัน โดยในด้านประสิทธิภาพของระบบผู้บริหารและหัวหน้ากลุ่มมีความพึงพอใจอยู่ในระดับมากที่สุด(4.42) และผู้ปฏิบัติงานมีความพึงพอใจอยู่ในระดับมากที่สุด(4.41) ประเด็นด้านความสำคัญของการป้องกันระบบผู้บริหารและหัวหน้ากลุ่มมีความพึงพอใจอยู่ในระดับมากที่สุด(4.78) และผู้ปฏิบัติงานมีความพึงพอใจอยู่ในระดับมากที่สุด(4.38) ประเด็นด้านความน่าเชื่อถือผู้บริหารและหัวหน้ากลุ่มมีความพึงพอใจอยู่ในระดับมากที่สุด(4.30) และผู้ปฏิบัติงานมีความพึงพอใจอยู่ในระดับมากที่สุด(4.20) และประเด็นด้านคุณภาพการบริการผู้บริหารและหัวหน้ากลุ่มมีความพึงพอใจอยู่ในระดับ

มากที่สุด(4.52) และผู้ปฏิบัติงานมีความพึงพอใจอยู่ในระดับมากที่สุด(4.37) โดยกลุ่มผู้บริหารและหัวหน้ากลุ่มมีความพึงพอใจมากกว่าผู้ปฏิบัติงานในทุกด้าน

## 5.2 การนำไปใช้ประโยชน์/ผลกระทบ

5.2.1 สำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราชเป็นหน่วยงานที่ดำเนินการด้านการป้องกันควบคุมโรคในเขตสุขภาพที่ 11 โดยบุคลากรในหน่วยมีการใช้งาน ถีอครอง ประมวลผลข้อมูลเพื่อภารกิจของหน่วยงาน โดยมีการจัดเก็บข้อมูลบางส่วน หรือทั้งหมดไว้ในเครื่องคอมพิวเตอร์ภายในหน่วยงาน และที่ตั้งของหน่วยงานอยู่ในเขตชุมชน จึงได้ได้ตระหนักถึงความสำคัญของการควบคุมการเข้าถึงระบบเครือข่ายเพื่อเป็นการป้องกันปัญหาที่อาจจะเกิดขึ้นจากการให้บริหารเครือข่ายทั้งทางตรงและทางอ้อม ผลที่เกิดจากการใช้งานระบบคือหน่วยงานมีความมั่นคงปลอดภัยด้านการใช้งานระบบเครือข่ายจากการควบคุมการเข้าถึงโดยไม่ได้รับอนุญาตจากบุคคลภายนอกได้มากยิ่งขึ้น

5.2.2 สามารถยืนยันตัวบุคคลที่เข้าใช้งานระบบเครือข่ายและอินเทอร์เน็ตของหน่วยงานได้ และสามารถตรวจสอบข้อมูลการจราจรทางคอมพิวเตอร์ได้

5.2.3 ระบบการยืนยันตัวบุคคลเพื่อเข้าใช้งานระบบเครือข่ายอินเทอร์เน็ต ของสำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช ทำให้บุคลากรภายในหน่วยงานจำเป็นต้องมีการใช้ Username และ Password ในการเข้าใช้งานทำให้มีขั้นตอนในการทำงานที่เพิ่มขึ้น

5.2.4 สามารถนำข้อมูลการจราจรทางคอมพิวเตอร์ที่ได้จัดเก็บมาใช้เป็นเครื่องมือในการวิเคราะห์ตรวจจับภัยคุกคามทางไซเบอร์ เพื่อให้มีความพร้อมในการรับมือกับภัยคุกคามไซเบอร์ รวมถึงยกระดับความสามารถในการป้องกันการโจมตีให้กับหน่วยงานได้

## 5.3 ความยุ่งยากและซับซ้อนในการดำเนินงาน

5.3.1 ต้องประยุกต์ใช้ความรู้ ทักษะและประสบการณ์เพื่อปรับเปลี่ยนวิธีการปฏิบัติงานให้เหมาะสมกับครุภัณฑ์ Watchguard Firebox M 4600

5.3.2 ต้องพัฒนาระบบให้ง่ายต่อการบำรุงรักษาหรือพัฒนาในอนาคตเนื่องจาก ครุภัณฑ์และเทคโนโลยีมีการเปลี่ยนแปลงอย่างต่อเนื่อง

## 5.4 ปัญหาและอุปสรรคในการดำเนินงาน

5.4.1 มีข้อจำกัดด้านทรัพยากรที่เป็นเวอร์ชันเก่า จำเป็นต้องหาวิธีการในการอัปเดตระบบต่อไปในอนาคต

5.4.2 พื้นที่ในการจัดเก็บ Log Files ใช้พื้นที่เยอะกว่าที่วางแผนไว้ และได้ดำเนินการปรับเพิ่มเพื่อความเหมาะสมแล้ว

## 5.5 ข้อเสนอแนะ

สำนักงานป้องกันควบคุมโรคที่ 11 จังหวัดนครศรีธรรมราช ควรสนับสนุนให้บุคลากรภายในหน่วยงานมีความรู้ความเข้าใจเกี่ยวกับพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 รวมถึงกฎหมายที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศเพื่อเป็นประโยชน์ต่อบุคลากรภายในหน่วยงานและหน่วยงานต่อไปในอนาคต



## บรรณานุกรม

- 1.ประกาศกระทรวงสาธารณสุข เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงสาธารณสุข พ.ศ. 2565 ประกาศ ณ วันที่ 23 มีนาคม พ.ศ. 2565.สืบค้นเมื่อ 24 สิงหาคม พ.ศ. 2566. จาก [https://ict.moph.go.th/upload\\_file/files/bfa2dfae9c3c2ff79e12cb0faa09d8c7.pdf](https://ict.moph.go.th/upload_file/files/bfa2dfae9c3c2ff79e12cb0faa09d8c7.pdf)
- 2.พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ฉบับที่ 2 พ.ศ. 2560. สืบค้นเมื่อ 24 สิงหาคม พ.ศ. 2566. จาก [Slide 1 \(dga.or.th\) พ.ร.บ. คอมพิวเตอร์ พ.ศ. ๒๕๖๐ – KM \(prd.go.th\)](#)
3. PDCA : ความหมาย ประโยชน์ และตัวอย่างใช้ 4 ขั้นตอนเพื่อพัฒนาองค์กรอย่างต่อเนื่อง. สืบค้นเมื่อ 24 สิงหาคม พ.ศ. 2566. จาก [PDCA : ความหมาย ประโยชน์ และตัวอย่างใช้ 4 ขั้นตอนเพื่อพัฒนาองค์กรอย่างต่อเนื่อง | HREX.asia \(hrnote.asia\)](#)
4. Action Plan คืออะไร?. สืบค้นเมื่อ 24 สิงหาคม พ.ศ. 2566. จาก [Action Plan คืออะไร? สำคัญอย่างไรต่อการทำงาน - Thai Winner](#)
- 5.แนวคิดการระบุตัวตน การพิสูจน์ตัวตน และการให้สิทธิ์. สืบค้นเมื่อ 25 พฤษภาคม พ.ศ. 2566. จาก <https://www.acisonline.net/?p=9723>
6. ทำความรู้จักกับ The CIA Triad. สืบค้นเมื่อ 25 สิงหาคม พ.ศ. 2566. จาก <https://www.cyberdrive.in.th/%E0%B8%97%E0%B8%B3%E0%B8%84%E0%B8%A7%E0%B8%B2%E0%B8%A1%E0%B8%A3%E0%B8%B9%E0%B9%89%E0%B8%88%E0%B8%B1%E0%B8%81%E0%B8%81%E0%B8%B1%E0%B8%9A-the-cia-triad/>
7. Active Directory คือ. สืบค้นเมื่อ 25 พฤษภาคม พ.ศ. 2566. จาก <https://www.mvpskill.com/kb/active-directory-%E0%B8%84%E0%B8%B7%E0%B8%AD.html>
- 8.เจาะลึกการใช้ Group Policy Object (GPO)แบบเข้าใจง่าย EP1 (ปี2022). สืบค้นเมื่อ 25 พฤษภาคม พ.ศ. 2566. จาก <https://www.youtube.com/watch?v=qOsKijZ2egA>
9. Lightweight Directory Access Protocol. สืบค้นเมื่อ 18 พฤษภาคม พ.ศ. 2566. จาก <https://saixiii.com/what-is-ldap/>
10. 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)

## บรรณานุกรม

11. 7 สิทธิ PDPA พนักงานควรรู้ ก่อนบริษัทเก็บข้อมูลส่วนตัว. สืบค้นเมื่อ 25 สิงหาคม พ.ศ. 2566. จาก 7 สิทธิ PDPA พนักงานควรรู้ ก่อนบริษัทเก็บข้อมูลส่วนตัว - SO PEOPLE
12. ทฤษฎีการประเมิน (Evaluation Theory) อ.ดร.จตุภูมิ เขตจัตุรัส. สืบค้นเมื่อ วันที่ 31 สิงหาคม พ.ศ. 2566. จาก [https://home.kku.ac.th/sompo\\_pu/spweb/evaluation/evaluation-theory.pptx](https://home.kku.ac.th/sompo_pu/spweb/evaluation/evaluation-theory.pptx)
13. คำนวณกลุ่มตัวอย่างสูตร "ทาโร่ ยามาเน่" Taro Yamane. สืบค้นเมื่อ 24 ตุลาคม 2566. จาก <https://digi.data.go.th/blog/method-of-controlling-the-sample/>

## ภาคผนวก ก

ประกาศใช้แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ



## บันทึกข้อความ

ส่วนราชการ สำนักงานป้องกันควบคุมโรคที่ ๑๑ จังหวัดนครศรีธรรมราช โทร. ๐ ๗๕๓๔ ๑๑๕๑ ต่อ ๑๔  
ที่ สธ 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  
รักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานป้องกันควบคุมโรคที่ ๑๑ จังหวัดนครศรีธรรมราช  
เพื่อให้ระบบเทคโนโลยีสารสนเทศของหน่วยงานเป็นไปอย่างเหมาะสม 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/ว๑๕๕ วันที่ ๒๖ กุมภาพันธ์ ๒๕๖๖

เรื่อง ประกาศการใช้งานระบบพิสูจน์ยืนยันตัวตนในการเข้าใช้อินเตอร์เน็ตของหน่วยงาน

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 จะดำเนินการใช้งานระบบพิสูจน์ยืนยันตัวตนในการเข้าใช้อินเตอร์เน็ตของหน่วยงาน โดยเปิดใช้งานระบบดังกล่าวในวันที่ ๒๗ กุมภาพันธ์ ๒๕๖๖ และขอแจ้งรหัสผู้ใช้งาน (User) และรหัสผ่าน (Password) ให้กับเจ้าหน้าที่ทุกท่านสำหรับใช้งานอินเทอร์เน็ต โดยติดต่อขอรับรหัสผู้ใช้งาน (User) และรหัสผ่าน (Password) เป็นรายกลุ่มได้ที่งานเทคโนโลยีสารสนเทศ กลุ่มยุทธศาสตร์ แผนงาน และเครือข่าย

จึงเรียนมาเพื่อทราบ และแจ้งผู้เกี่ยวข้องดำเนินการต่อไปด้วย

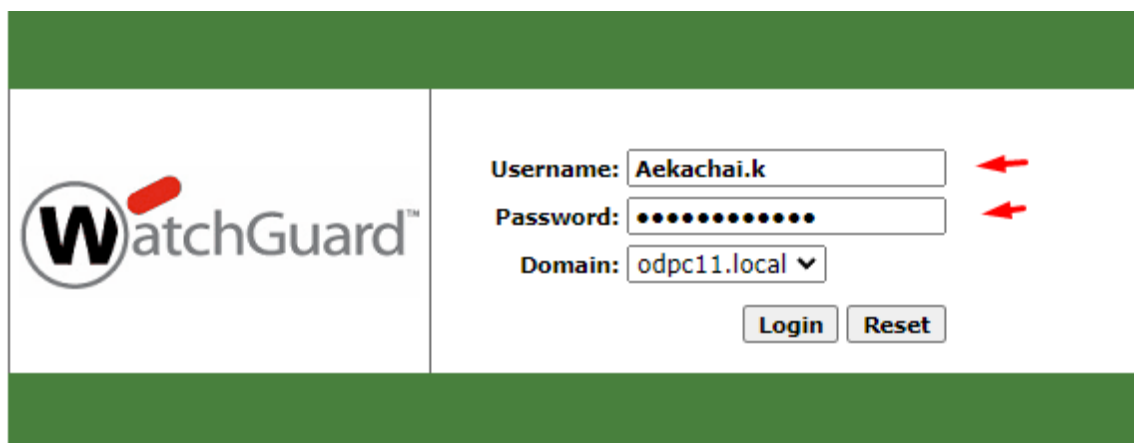
(นายไกรสร โตทับเที่ยง)  
นายแพทย์เชี่ยวชาญ (ด้านเวชกรรมป้องกัน) ปฏิบัติหน้าที่  
ผู้อำนวยการสำนักงานป้องกันควบคุมโรคที่ ๑๑  
จังหวัดนครศรีธรรมราช

ภาคผนวก ค

คู่มือการใช้งานบนคอมพิวเตอร์

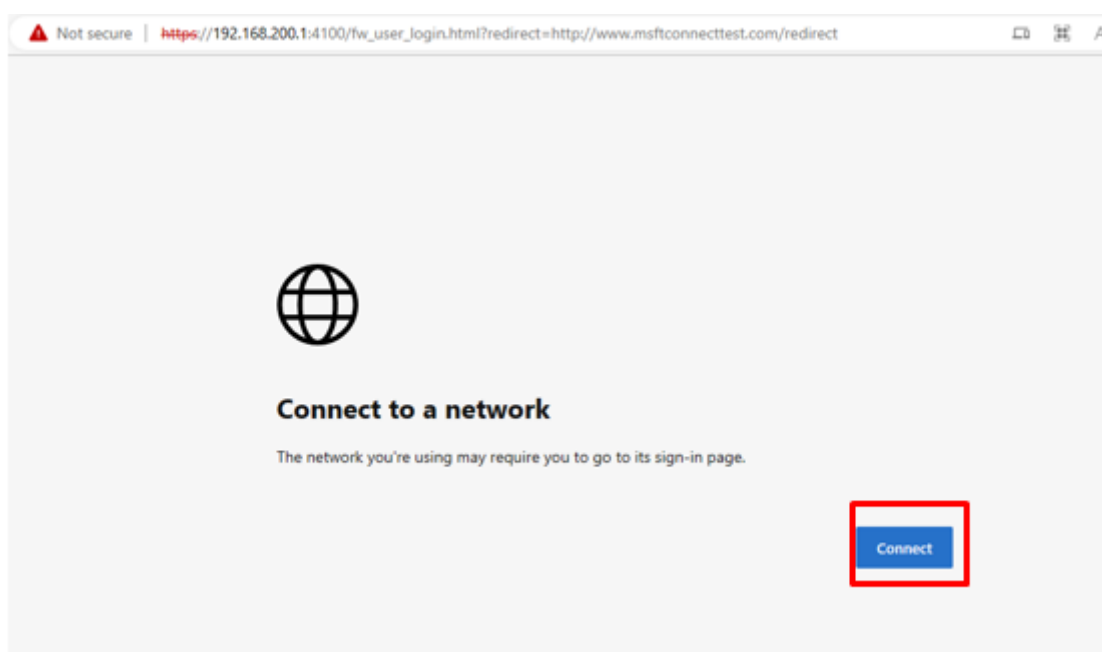
## คู่มือการใช้งานบนคอมพิวเตอร์

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



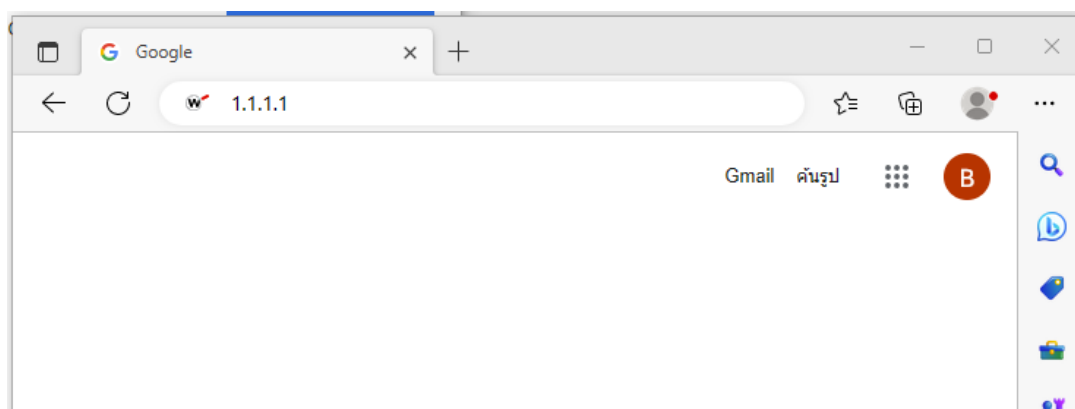
ภาพที่ 1

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



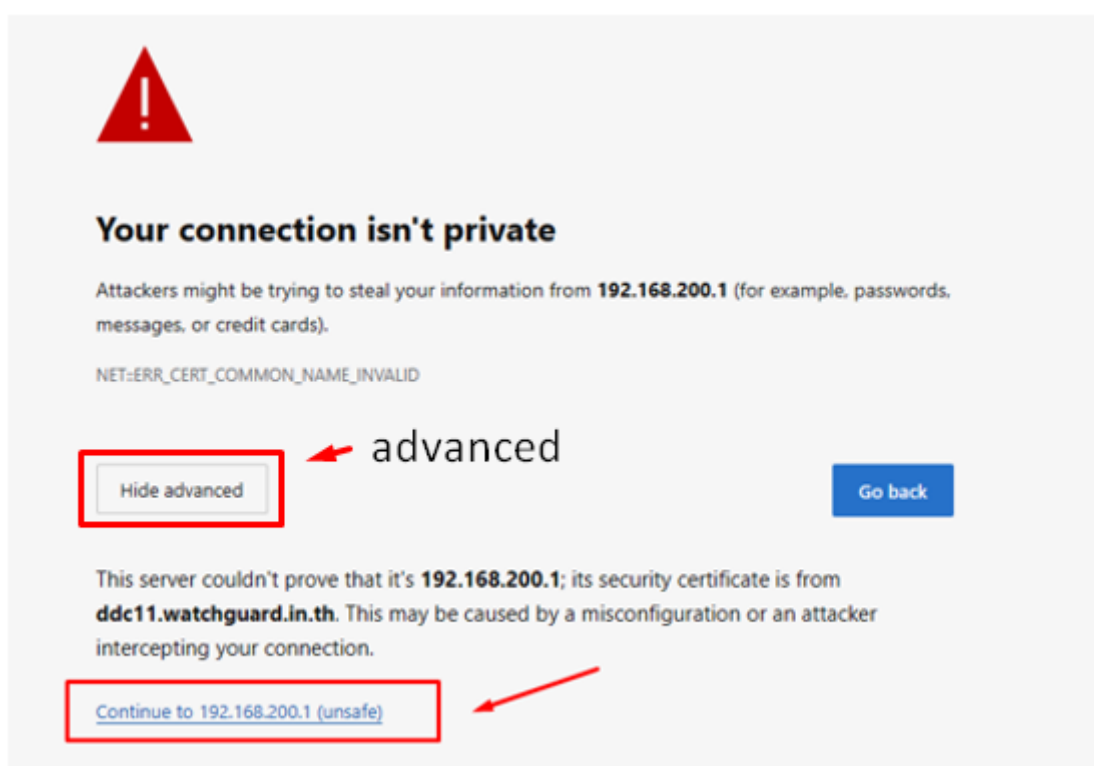
ภาพที่ 2





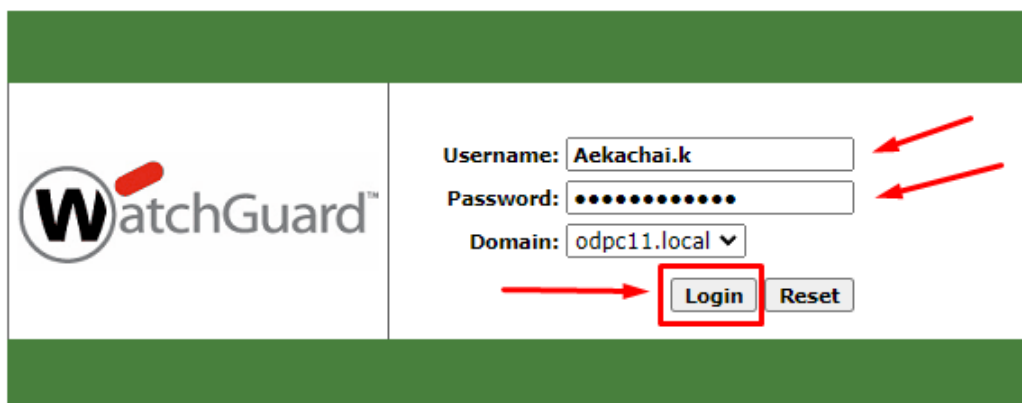
ภาพที่ 3

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



ภาพที่ 4

4. เมื่อกด Continue to 192.168.200.1 (Unsafe) จะเข้าสู่หน้าต่าง ตามภาพที่ 5  
ให้กรอก Username : ที่ได้รับ Password :  
เลือก Domain เป็น : odpc11.local (ปกติจะเป็นค่าเริ่มต้นอยู่แล้ว)



WatchGuard™

Username:

Password:

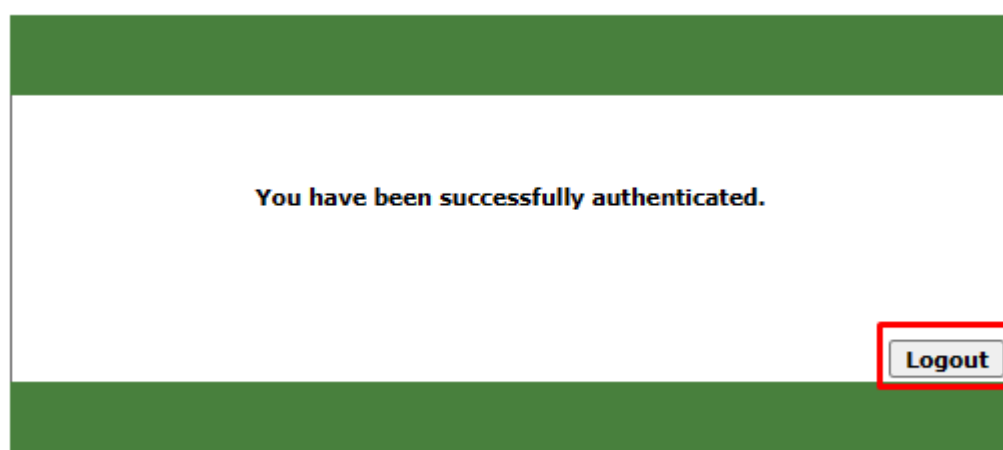
Domain:

ภาพที่ 5

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



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



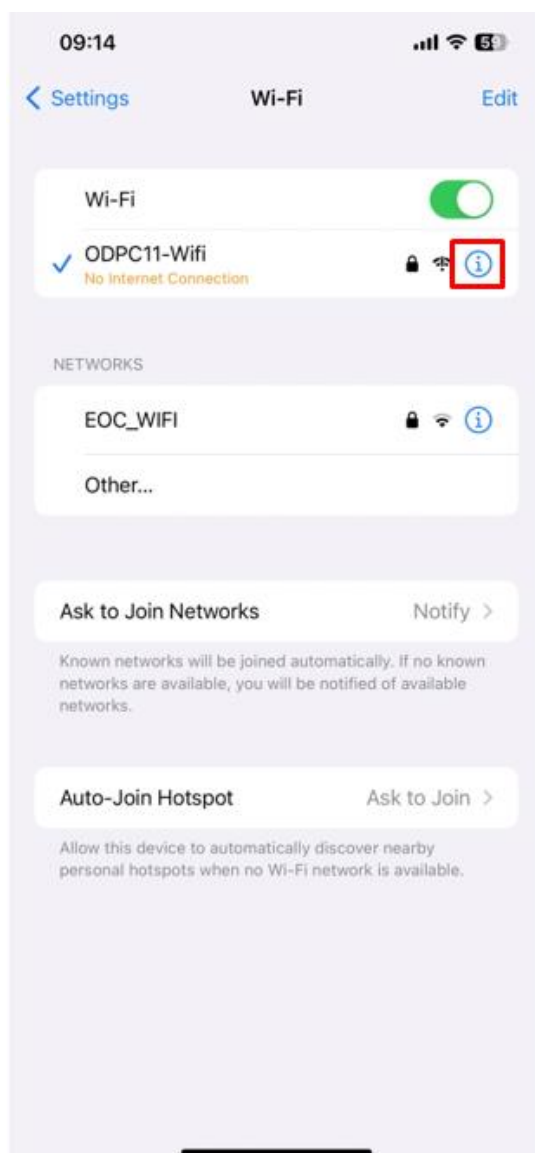
ภาคผนวก ง

คู่มือการใช้งานบนมือถือ

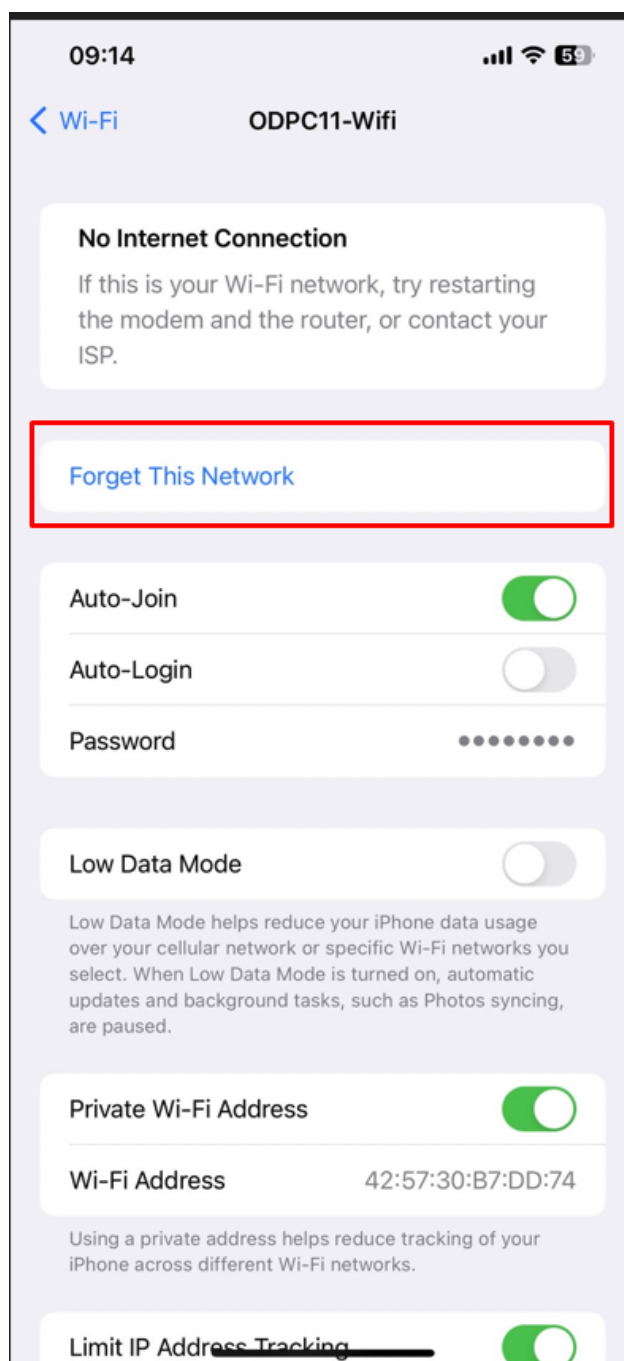
## คู่มือการใช้งานบนมือถือ

### 1. วิธีใช้งานระบบยืนยันตัวตนบน Tablet , Smartphone

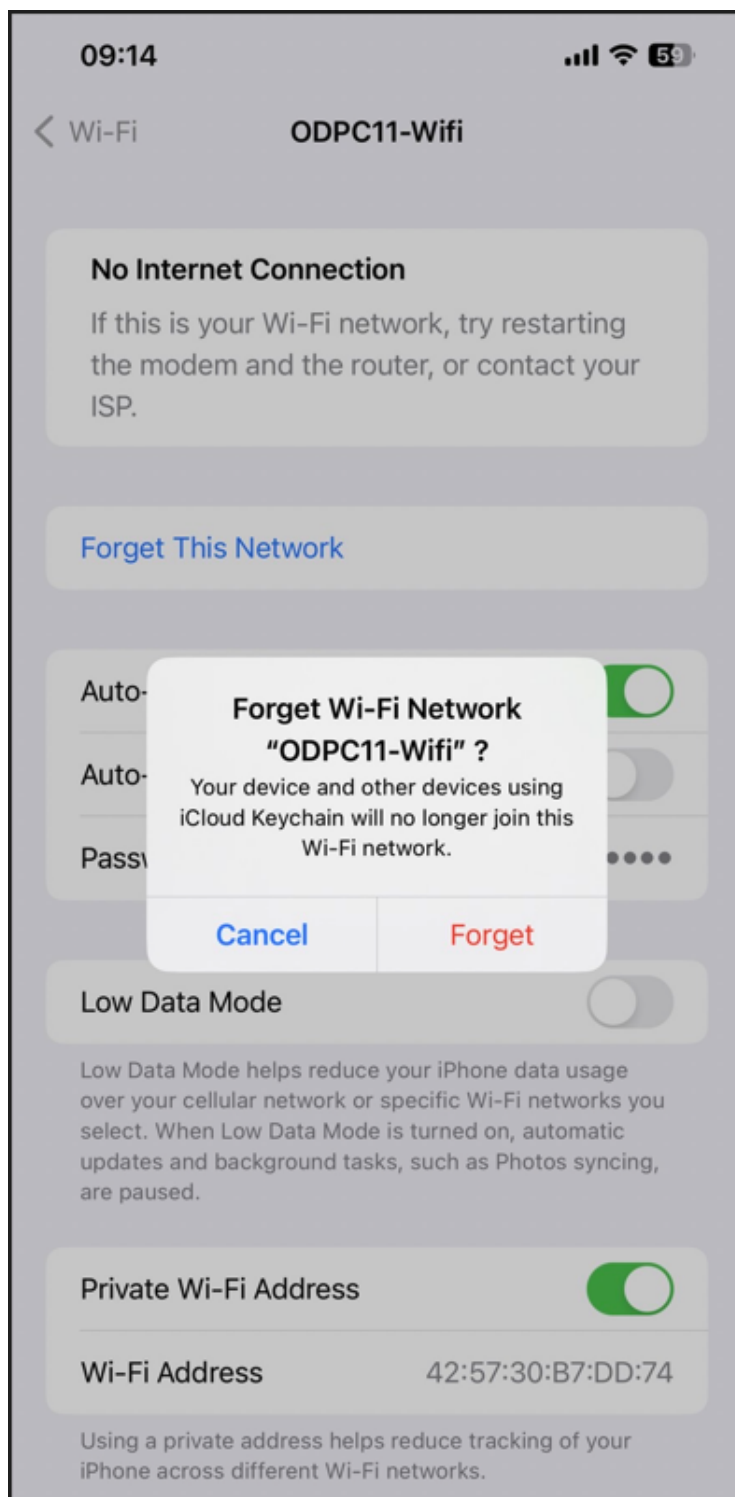
หากเคยเชื่อมต่ออินเทอร์เน็ตอยู่แล้วเข้าใช้งานไม่ได้ ให้กดสัญลักษณ์ ( i ) information icons



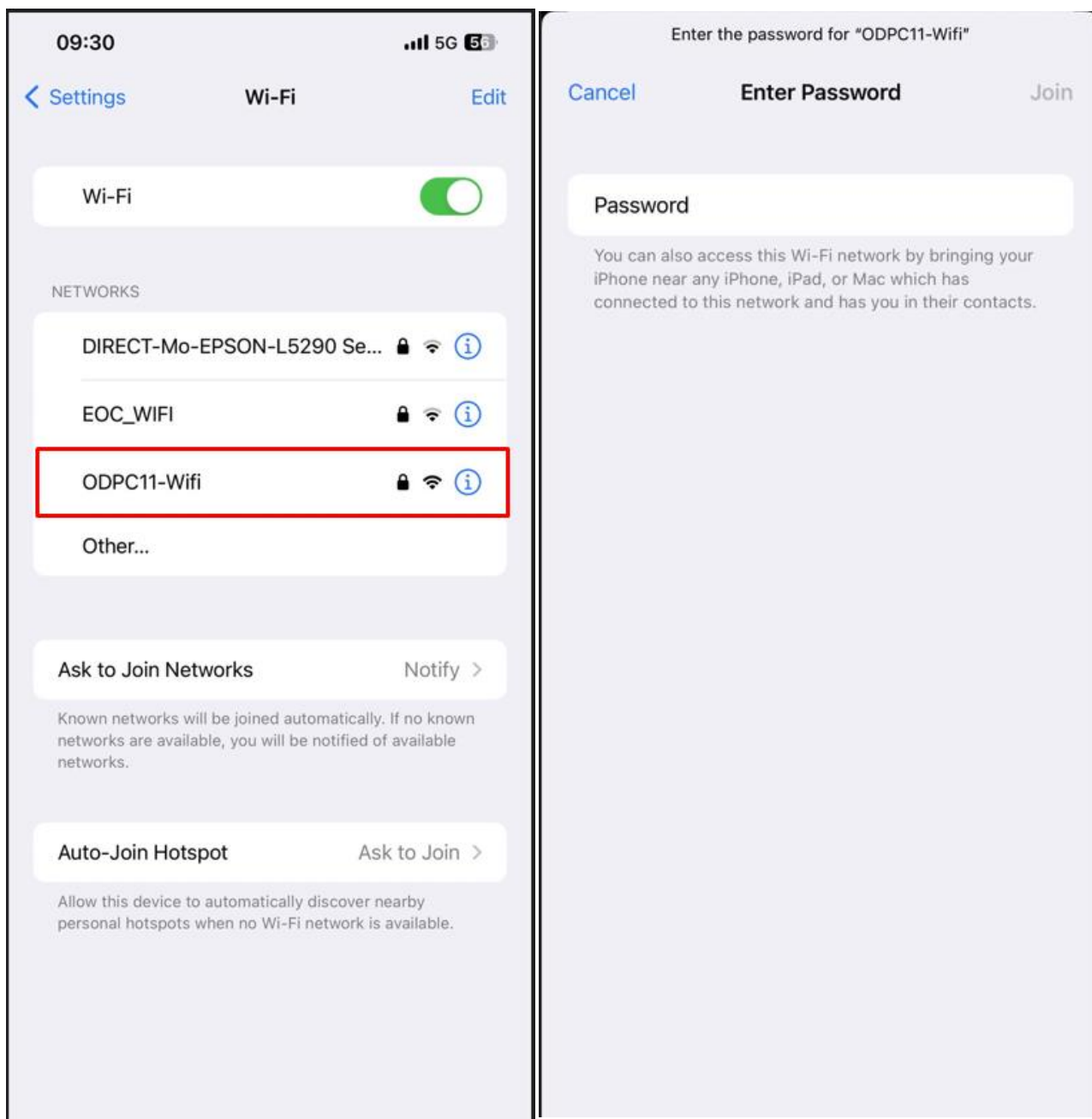
2. เมื่อเข้าสู่หน้า Information ให้กดที่ปุ่ม Forget This Network, หรือคำต่างกันต่างรุ่น ยี่ห้อของอุปกรณ์ เพื่อลืมเครือข่ายนี้



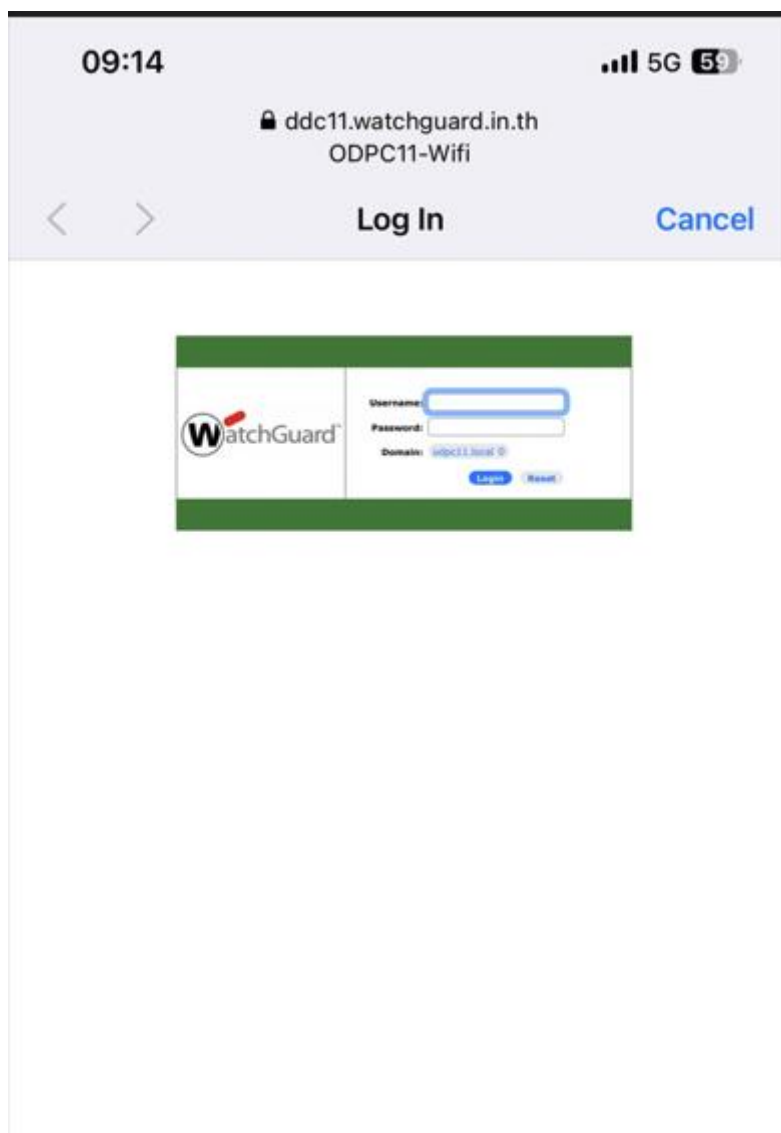
3. กดยืนยันการลืม เพื่อลืมการใช้งานเครือข่ายนี้



4. เมื่อสิ้นการใช้งานเรียบร้อยแล้ว กดเชื่อมต่อเข้าใช้งานเครือข่าย Wireless ที่ต้องการอีกครั้ง ใส่ password ของ Wifi หากมีการถาม



5. เมื่อเชื่อมต่อเรียบร้อยแล้วระบบจะปรากฏหน้าต่างสำหรับยืนยันตัวตนให้ กรอก Username password ที่ได้รับจากงานเทคโนโลยีสารสนเทศ





ภาคผนวก จ

คู่มือการเปลี่ยนรหัสผ่าน

## คู่มือการเปลี่ยนรหัสผ่าน

1. หลังจากได้รับ User log on และ Password แล้ว

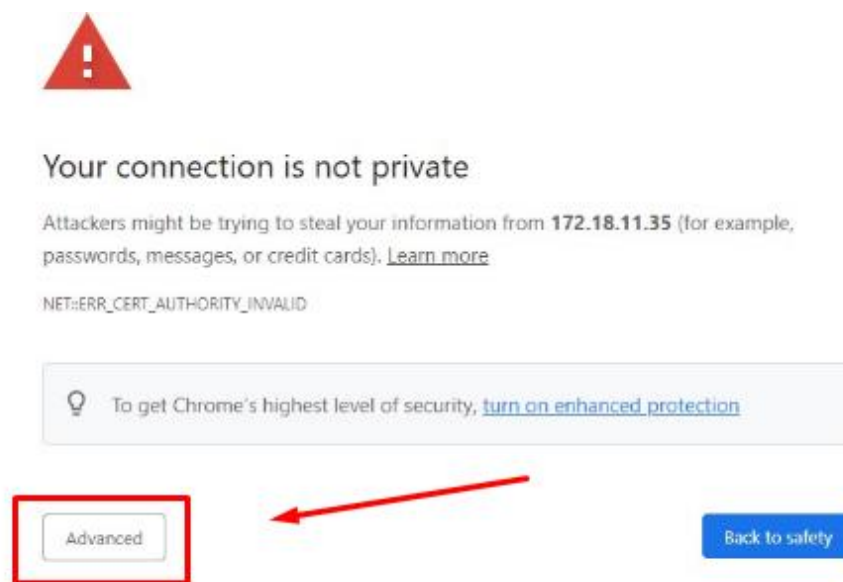
<p>กลุ่มยุทธศาสตร์ แผนงาน และ เครือข่าย นายเอกชัย แก้วเรืองฤทธิ์</p>
<p>User logon: <u>Khem.k</u></p> <p><u>Password</u> : p12s</p>

ตัวอย่าง User และ Password ที่ได้รับ

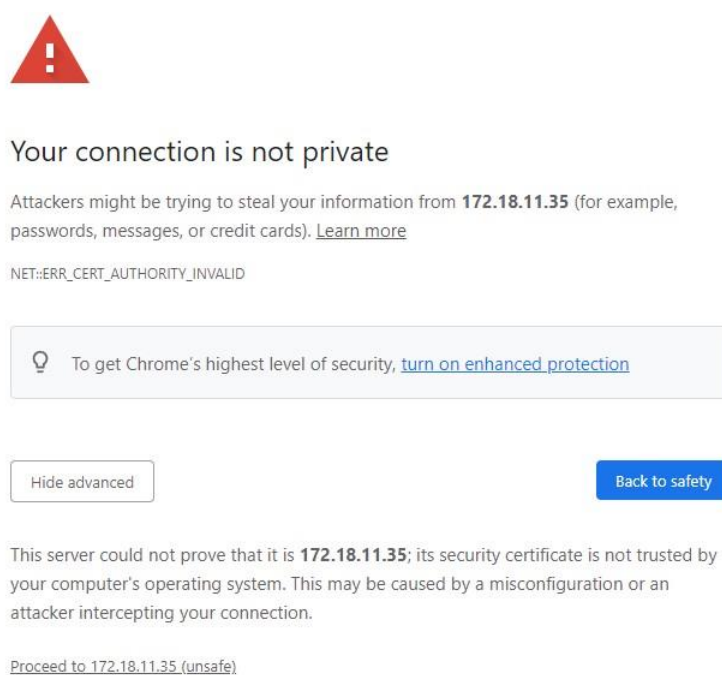
2. ให้ใช้เครื่องคอมพิวเตอร์หรือคอมพิวเตอร์โน้ตบุ๊กเท่านั้น ที่จะเข้าใช้งานอินเทอร์เน็ตของ สคร.11 โดยเข้าไปยังหน้าเว็บไซต์ : [172.18.11.35/RDWeb/Pages/en-US/password.aspx](https://172.18.11.35/RDWeb/Pages/en-US/password.aspx)  
หรือ <https://172.18.11.35/RDWeb/Pages/en-US/password.aspx>  
หรือ QR CODE



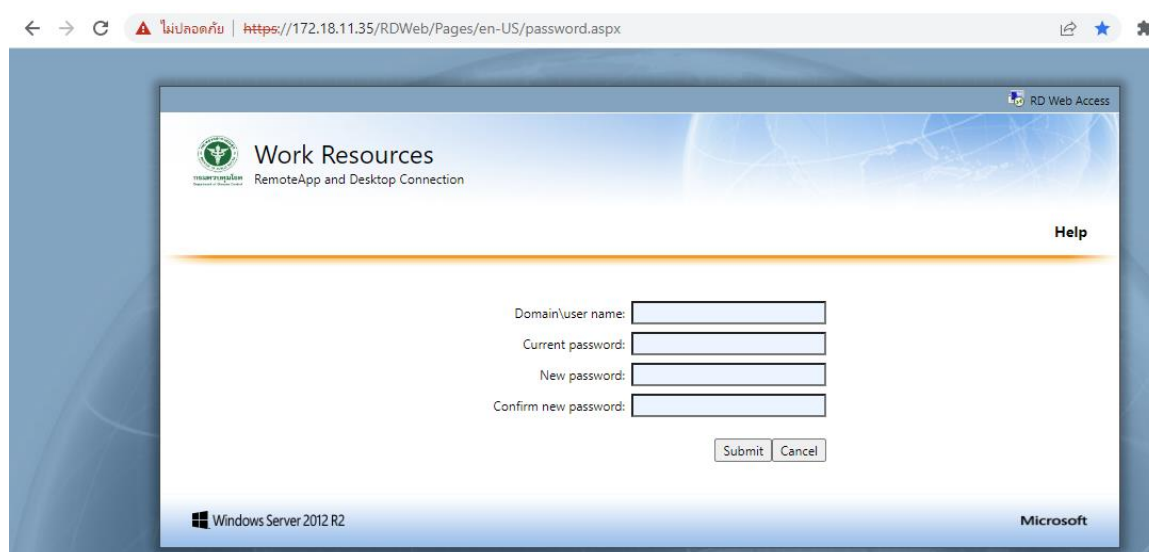
3. เมื่อเข้าไปยังลิงค์ในข้อที่ 2 แล้ว จะปรากฏหน้าเว็บไซต์ ให้กดปุ่ม Advanced หรือขั้นสูง ตามในรูปด้านล่างนี้



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



5. เมื่อเข้ากดลิงค์ Proceed to 172.18.11.35 (unsafe) จะปรากฏหน้าเว็บไซต์ ตามในรูปด้านล่างนี้



#### 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

Work Resources  
RemoteApp and Desktop Connection

Help

Domain\user name:

Current password:

New password:

Confirm new password:

Submit Cancel

Windows Server 2012 R2 Microsoft

## 7. เมื่อกดปุ่ม Summit จะได้หน้าต่างตามภาพ

Work Resources  
RemoteApp and Desktop Connection

Help

Domain\user name:

Current password:

New password:

Confirm new password:

Your password has been successfully changed.

OK

Windows Server 2012 R2 Microsoft

8. กรณีที่มีการลืม ชื่อ ผู้ใช้ หรือ รหัสการเข้าใช้งาน ต้องใช้แบบฟอร์ม ต่อไปนี้เพื่อติดต่อกับ  
เทคโนโลยีสารสนเทศ

แบบฟอร์มแจ้งลืมชื่อผู้ใช้หรือรหัสผ่าน

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

ชื่อ.....สกุล.....(ภาษาอังกฤษ)

กลุ่มงาน.....

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

ทั้งนี้ ก่อนการแสดงผลหน้าจอ ข้าพเจ้าได้ทราบถึงวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วน  
บุคคลดังกล่าว และมีความเข้าใจดีแล้ว

ข้าพเจ้าให้ความยินยอมหรือปฏิเสธไม่ให้ความยินยอมในเอกสารนี้ด้วยความสมัครใจปราศจากการ บังคับ  
หรือขู่ข่ม และข้าพเจ้าทราบว่าข้าพเจ้าสามารถถอนความยินยอมนี้เสียเมื่อใดก็ได้เว้นแต่ในกรณี มีข้อจำกัดสิทธิ  
ตามกฎหมาย

ให้ความยินยอม  ไม่ให้ความยินยอม

ลงชื่อ.....

(.....)

วันที่.....

ส่วนของผู้เจ้าหน้าที่

ดำเนินการเปลี่ยนรหัสผ่านเรียบร้อยแล้ว

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

ลงชื่อ.....

(.....)

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 ต่อการประเมินประสิทธิผลและความสำเร็จของระบบสารสนเทศในด้าน 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 ความเข้าใจเกี่ยวกับข้อกำหนดและเงื่อนไขของการยืนยันตัวตน					
2.2 ความสำคัญของการรักษาความปลอดภัยของข้อมูลและข้อมูลสำคัญขององค์กรขณะใช้งานอินเทอร์เน็ต					
2.3 ความสำคัญของการป้องกันการเข้าถึงที่ไม่ได้รับอนุญาตในการใช้งานอินเทอร์เน็ต.					
<b>3.ความปลอดภัยและความเชื่อถือ</b>					
3.1 ระดับความปลอดภัยของระบบยืนยันตัวตน					
3.2 ความพร้อมที่ระบบยืนยันตัวตนต่อการป้องกันการแฮกเกอร์หรือการละเมิดความปลอดภัย					
3.3 ความเชื่อถือในระบบยืนยันตัวตนจากผู้ใช้					
<b>4. การสนับสนุนด้านการใช้งาน</b>					
4.1 การได้รับความรู้และการสนับสนุนในการใช้งานการยืนยันตัวตน					
4.2 ระบบมีการแจ้งเตือนในกรณีเกิดข้อผิดพลาด					
4.3 การได้รับการแก้ปัญหาในกรณีเกิดข้อผิดพลาด					

**ส่วนที่ 3** ข้อเสนอแนะ/ ข้อคิดเห็นเพิ่มเติม

.....

.....

.....

.....