คู่มือ ปฏิบัติงาน

การจัดการระบบบริหารบุคลากร และเงินเดือน

นางพรสุภา บุญทศ
เจ้าหน้าที่บริหารงานทั่วไปปฏิบัติการ
สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี

คำนำ

คู่มือการจัดการระบบบริหารงานบุคลากรและเงินเดือน มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี ฉบับนี้ จัดทำขึ้นเพื่อรวบรวมขั้นตอน และแนวทางการปฏิบัติงานต่าง ๆ ที่เกี่ยวข้องกับการทวนสอบประเภทกลุ่มสิทธิ์ การทวนสอบสิทธิ์ของผู้ใช้งาน การกำหนดสิทธิ์ของบุคลากรใหม่ รวมไปถึงยกเลิกสิทธิ์ของบุคลากรที่มีการโยกย้ายงาน เปลี่ยนแปลงหน่วยงาน หรือลาออก เพื่อให้ผู้ปฏิบัติงานสามารถปฏิบัติงานตามขั้นตอนได้อย่างถูกต้องเหมาะสม ให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ในคู่มือฉบับนี้ประกอบไปด้วยหลักการและเหตุผล วัตถุประสงค์ ขอบเขต คำจำกัดความ หลักเกณฑ์การปฏิบัติงาน วิธีการปฏิบัติงาน แนวปฏิบัติที่สำคัญ ตลอดจนข้อปฏิบัติโดยนำเสนอในลักษณะของแผนภูมิ (Flowchart) พร้อมทั้งอธิบายขั้นตอนและรายละเอียด ที่บุคลากรในส่วนงานฝ่ายบริการศูนย์ข้อมูลและสารสนเทศควรทราบ เพื่อช่วยลดข้อผิดพลาดในการทำงาน และเป็นแนวทางในการปฏิบัติงานของผู้ที่จะมาปฏิบัติงานแทนได้อย่างมีประสิทธิภาพ

ผู้จัดทำหวังเป็นอย่างยิ่งว่า คู่มือฉบับนี้ จะเป็นประโยชน์แก่บุคลากรที่ปฏิบัติงานในฝ่ายบริการศูนย์ข้อมูลและสารสนเทศ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ เพื่อนำข้อความรู้ที่ได้ไปปฏิบัติงานให้เกิดประสิทธิผลอย่างแท้จริง พร้อมกันนี้ผู้จัดทำขอขอบคุณทุกท่านที่ให้ที่ให้ความร่วมมือในการรวบรวมเอกสารที่เกี่ยวข้องเพื่อประกอบการเขียนคู่มือในครั้งนี้ หากมีข้อบกพร่องประการใด ผู้จัดทำต้องขออภัย ไว้ ณ ที่นี้

นางพรสุภา บุญทศ

สารบัญ

สารบัญ (ต่อ)

สารบัญภาพ

หน้า

สารบัญภาพ (ต่อ)

หน้า

สารบัญภาพ (ต่อ)

หน้า

สารบัญภาพ (ต่อ)

หน้า

สารบัญภาพ (ต่อ)

สารบัญตาราง

หน้า

บทที่ 1

บทนำ

1.1 ความเป็นมาและความสำคัญ

ในปัจจุบันทุกองค์กรทั้งภาครัฐและเอกชน ต่างก็นำเทคโนโลยีสารสนเทศ มาประยุกต์ใช้ในองค์กร ซึ่งถือได้ว่าเทคโนโลยีมีความจำเป็นต่อทุกองค์กรและเป็นปัจจัยในการดำเนินธุรกิจในยุคที่เทคโนโลยีมีความเจริญก้าวหน้าอย่างไม่หยุดยั้ง ทั้งนี้เนื่องจากการดำเนินงานขององค์กรทุกประเภท ต้องนำเทคโนโลยีสารสนเทศมาประยุกต์ใช้เพื่อเป็นสิ่งที่ช่วยสร้างความสามารถในการแข่งขันและเติบโตขององค์กร องค์กรใดมีการพัฒนาด้านเทคโนโลยีสารสนเทศที่ทันต่อโลกยุคปัจจุบันองค์กรนั้นก็มักจะเป็นผู้นำในอุตสาหกรรมนั้น ๆ ก็ว่าได้ อย่างไรก็ตาม ถึงจะมีข้อดีแต่ก็ยังมีข้อเสียได้เช่นกัน หากนำเทคโนโลยีสารสนเทศมาใช้อย่างไม่รอบคอบนั้น ก็ก่อให้เกิดผลเสียต่อองค์กรได้ ดังนั้น เพื่อความปลอดภัย องค์กรจึงจำเป็นต้องมีหน่วยงานที่ดูแลรับผิดชอบในด้านเทคโนโลยีสารสนเทศ โดยมีบุคลากร นั้นเป็นส่วนประกอบที่สำคัญ เพราะบุคลากรที่มีความรู้ ความสามารถ และเข้าใจวิธีการให้ได้มาซึ่งสารสนเทศ จะเป็นผู้ดำเนินการในการปฏิบัติงานทั้งหมด บุคลากรจึงต้องเป็นผู้มีความรู้ความเข้าใจในการใช้เทคโนโลยีสารสนเทศ บุคลากรภายในองค์กรก็เป็นส่วนประกอบที่ทำให้เกิดระบบสารสนเทศด้วยกันทุกคนและนำมาซึ่งประสิทธิภาพในการดำเนินงานต่าง ๆ ด้วยการประยุกต์ใช้ระบบสารสนเทศ (ไกรทพนธ์ เติมวิย์ขจร ,ศิริชัย นามบุรี,นิมานูนี หะยีวาเงาะ,2559) ให้มีการปฏิบัติงานอย่างมีระบบ ขั้นตอน และแนวทางการปฏิบัติงานต่าง ๆ ที่ถูกต้อง

เทคโนโลยีสารสนเทศที่จะกล่าวถึงในคู่มือนี้ คือ ระบบบริหารงานบุคลากรและเงินเดือน เกี่ยวเนื่องกับการกำหนดสิทธิ์ของบุคลากรใหม่รวมไปถึงยกเลิกสิทธิ์ของบุคลากรที่มีการโยกย้ายงาน เปลี่ยนแปลงหน่วยงาน หรือลาออก ซึ่งในระบบสารสนเทศมีข้อมูลที่เป็นข้อมูลส่วนบุคคลที่มีความลับความละเอียดอ่อน (Sensitive) จึงต้องมีนโยบายการรักษาความลับ (Confidentiality) ข้อมูลที่อยู่ในระบบสารสนเทศผู้บริหารจัดการระบบต้องควบคุมให้ใช้งานได้เฉพาะบุคคลที่ได้รับอนุญาตเท่านั้น เพื่อไม่ให้เกิดข้อมูลรั่วไหล ไม่เปิดเผยหรือเกิดการลักลอบข้อมูลที่ไม่ได้รับอนุญาต โดยจะเชื่อมโยงไปถึงความสำคัญของการกำหนดสิทธิ์การเข้าถึงข้อมูลของเจ้าหน้าที่บุคลากร จะเป็นวิธีที่ช่วยขจัดปัญหาความยุ่งยากที่เกิดจากการปฏิบัติงาน คือกล่าวได้ว่า "การกำหนดสิทธิ์" การเข้าถึงข้อมูล เป็นวิธีช่วยลดขั้นตอนการปฏิบัติงานของเจ้าหน้าที่บุคลากรและทำให้การปฏิบัติงานเป็นระบบ มีหลักเกณฑ์ที่มีมาตรฐานเดียวกัน อีกทั้งยังทำให้การเข้าถึงข้อมูลมีความปลอดภัยมากขึ้น อีกด้วย

ดังนั้น บุคลากรที่จะปฏิบัติงานจะต้องมีความรู้ความเข้าใจในขั้นตอน และแนวทางการปฏิบัติงาน รวมทั้งการจัดการระบบเพื่อให้สามารถดูแลและบริหารจัดการได้อย่างถูกต้อง ซึ่งในปัจจุบันยังไม่มีการจัดทำ

คู่มือการจัดการระบบบริหารงานบุคลากรและเงินเดือน หากบุคลากรที่บริหารจัดการระบบหลักไม่สามารถมาปฏิบัติงาน หรือหากมีการเปลี่ยนหน้าที่การปฏิบัติงาน โดยคู่มือนี้ จะทำให้ผู้ปฏิบัติงานแทนศึกษาขั้นตอนการปฏิบัติงานจากคู่มือนี้ ให้สามารถทำงานทดแทนกันได้

จากเหตุผลข้างต้น ผู้จัดทำคู่มือการจัดการระบบบริหารงานบุคลากรและเงินเดือน มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรีขึ้น ซึ่งสำนักวิทยบริการและเทคโนโลยีสารสนเทศเป็นดูแลและรับผิดชอบ เพื่อให้ผู้ปฏิบัติงานแทนได้รู้ถึงบทบาทหน้าที่ ความรับผิดชอบ และลักษณะงานที่ทำ รวมทั้งขั้นตอน แนวปฏิบัติในการจัดการระบบ โดยผู้เขียนนำความรู้และประสบการณ์ในการปฏิบัติงานในลักษณะเดียวกัน เพื่อเป็นเครื่องมือที่สามารถนำไปใช้ในการพัฒนาปรับปรุงการปฏิบัติงานให้มีประสิทธิภาพยิ่งขึ้นต่อไป

1.2 วัตถุประสงค์

1.2.1 เพื่อให้สามารถปฏิบัติงานเป็นมาตรฐานเดียวกัน

1.2.2 เพื่อให้ทราบถึงขั้นตอนการปฏิบัติงาน เทคนิค แนวปฏิบัติ ขั้นตอนและวิธีการดำเนินการที่ถูกต้อง

1.3 ขอบเขตของคู่มือ

คู่มือการจัดการระบบบริหารงานบุคลากรและเงินเดือน มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี มีขอบเขตเนื้อหาครอบคลุมวิธีการปฏิบัติงาน ที่มีขั้นตอน ข้อปฏิบัติ และแนวปฏิบัติ ในการควบคุม การเข้าถึงและใช้งานระบบสารสนเทศ ทั้งในการทวนสอบประเภทกลุ่มสิทธิ์ การทวนสอบสิทธิ์ของผู้ใช้งาน การกำหนดสิทธิ์ของระบบบริหารงานบุคลากรและเงินเดือน และการยกเลิกสิทธิ์ของระบบบริหารงานบุคลากรและเงินเดือน

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีบทบัญญัติบางประการเกี่ยวกับการจำกัดสิทธิและเสรีภาพของบุคคล ซึ่งเจ้าหน้าที่ที่ปฏิบัติงานด้านบุคลากรของแต่ละหน่วยงาน/คณะ และบุคลากรของกองบริหารงานบุคคลต้องขออนุญาตจากเจ้าของระบบ โดยเป็นไปตามหน้าที่ภาระงานและตามหลักปฏิบัติในการเข้าถึงข้อมูลในระบบ ที่ต้องผ่านการอนุมัติในแต่ละขั้นบังคับบัญชา ไปจนถึงผู้ดูแลระบบและผู้บริหารจัดการระบบ

โดยมีขอบเขตระยะเวลาการดำเนินงานหลังจากได้รับเรื่องจากทางกองบริหารงานบุคคลประมาณ 2-3 วัน และผู้บริหารจัดการระบบจะดำเนินการภายใน 15-30 นาที เพื่อให้ผู้ใช้งานเข้าถึงข้อมูลในระบบบริหารบุคลากรและเงินเดือน

1.4 ประโยชน์ที่คาดว่าจะได้รับ

1.4.1 ทำให้มีความรู้ความเข้าใจในวิธีการ ขั้นตอนและหลักเกณฑ์ของการจัดการระบบบริหารงานบุคลากรและเงินเดือน ได้อย่างถูกต้องโดยสามารถปฏิบัติงานให้เป็นไปในแนวทางเดียวกัน

1.4.2 ทำให้ทราบถึงสาเหตุ เพื่อนำไปแก้ไขปัญหา และเพิ่มความรวดเร็วในการปฏิบัติงานของผู้บริหารจัดการระบบบริหารงานบุคลากรและเงินเดือน

1.4.3 ใช้เป็นคู่มือในการถ่ายทอดการปฏิบัติงานให้บุคลากรที่มาปฏิบัติหน้าที่แทนได้

1.5 นิยามศัพท์เฉพาะ/คำจำกัดความ

เทคโนโลยีสารสนเทศ (Information Technology) คือ การนำเอาเทคโนโลยีมาใช้สร้างมูลค่าเพิ่มให้กับสารสนเทศ ทำให้สารสนเทศมีประโยชน์ และใช้งานได้กว้างขวางมากขึ้น เทคโนโลยีสารสนเทศรวมไปถึงการใช้เทคโนโลยีด้านต่าง ๆ ที่จะรวบรวม จัดเก็บ ใช้งาน ส่งต่อ หรือสื่อสารระหว่างกัน

ระบบบริหารงานบุคลากรและเงินเดือน คือ หนึ่งในระบบสารสนเทศเพื่อการบริหารที่เกี่ยวข้องกับข้อมูลบุคลากรของมหาวิทยาลัย ไม่ครอบคลุมระบบเงินเดือน เพื่อสนับสนุนการบริหารทรัพยากรบุคลของทางมหาวิทยาลัย ผู้ปฏิบัติงานในระดับต่าง ๆ ทำให้การบริหารจัดการทางด้านงานบุคคล มีประสิทธิภาพและช่วยให้ผู้บริหารได้รับข้อมูลเพื่อใช้ในการตัดสินใจได้ทันตามความต้องการ

ระบบบริหารงานบุคลากร คือ ระบบที่ทำหน้าที่ในการบริหารจัดการข้อมูลบุคลากรในเรื่องต่าง ๆ ไม่ว่าจะเป็นข้อมูลทะเบียนประวัติ การลงเวลา/บันทึกเวลา งานพัฒนาบุคลากร งานเครื่องราชอิสริยาภรณ์ งานเลื่อนขั้นค่าจ้างและเงินเดือน โดยจัดเก็บไว้เป็นฐานข้อมูลของบุคลากรภายในองค์กรเดียวกัน

ผู้บริหารจัดการระบบ หมายถึง ผู้ดูแลระบบและทำหน้าที่ประสานงานในการบริหารจัดการระบบบริหารงานบุคลากรและเงินเดือน

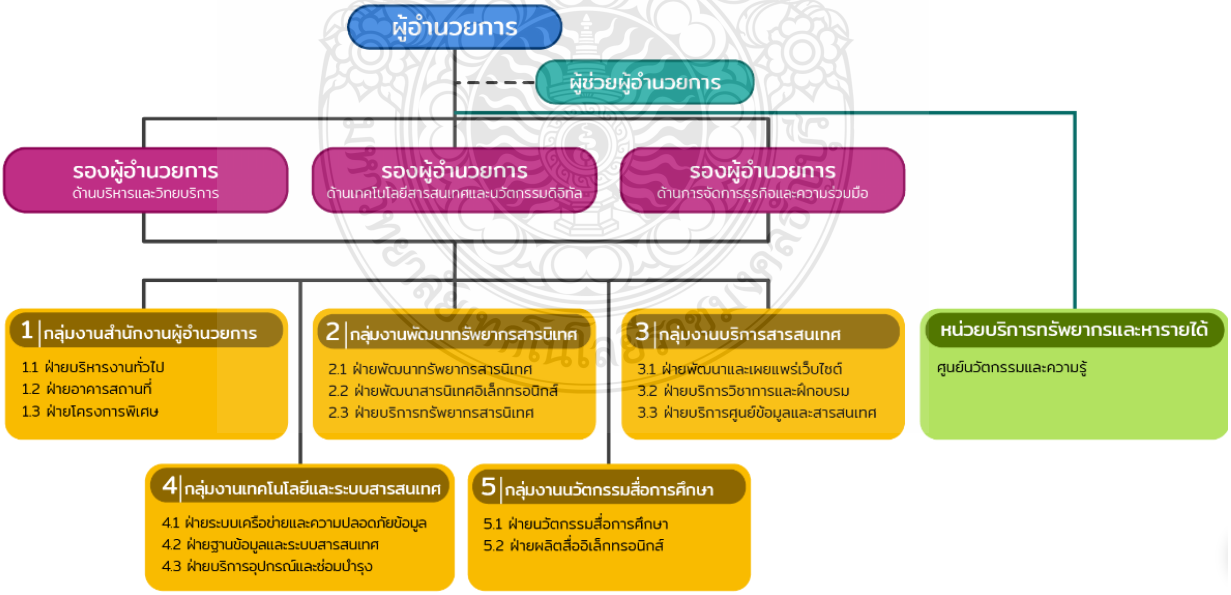
บทที่ 2
บทบาทหน้าที่ความรับผิดชอบ

2.1 โครงสร้างบริหารจัดการ

เมื่อวันที่ 28 พฤศจิกายน 2549 สำนักวิทยบริการและเทคโนโลยีสารสนเทศ เป็นหน่วยงานในสังกัดมหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี ได้รับการจัดตั้งขึ้นให้เป็นหน่วยงานเทียบเท่าคณะของมหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรีตามโครงสร้างการจัดตั้งมหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี โดยการรวมสองหน่วยงานเข้าด้วยกันคือ สถาบันวิทยบริการและสำนักเทคโนโลยีสารสนเทศ

โครงสร้างการแบ่งกลุ่มงานและภาระงานภายในสำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี ประกอบด้วย 5 กลุ่มงาน และ 1 ศูนย์ ได้แก่

- กลุ่มงานสำนักงานผู้อำนวยการ
- กลุ่มงานพัฒนาทรัพยากรสารนิเทศ
- กลุ่มงานบริการสารสนเทศ
- กลุ่มงานเทคโนโลยีและระบบสารสนเทศ
- กลุ่มงานนวัตกรรมสื่อการศึกษา
- หน่วยบริการทรัพยากรและหารายได้



ภาพที่ 2-1 แสดงโครงสร้างสำนักวิทยบริการและเทคโนโลยีสารสนเทศ[1]

[1] อ้างอิงจาก https://www.arit.rmutt.ac.th/ceo-arit/ : เมื่อวันที่ 8/3/2566

2.2 ขอบข่ายภาระงานของหน่วยงาน

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ได้เปิดให้บริการต่าง ๆ ที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศและทรัพยากรการเรียนรู้อย่างเป็นทางการ เมื่อวันที่ 18 กุมภาพันธ์ 2550 ภายใต้วิสัยทัศน์หลักที่จะตอบสนองความต้องการด้านเทคโนโลยีการเรียนรู้ให้กับผู้รับบริการ “For Your ILT (Information Learning Technology) Inspiration” สำนักฯ ได้มีการขยายและปรับเปลี่ยนรูปแบบบริการต่าง ๆ ให้ทันกับความเปลี่ยนแปลงก้าวหน้าด้านเทคโนโลยี และตอบสนองความต้องการของผู้ใช้บริการ ภารกิจหลักสามารถสรุปได้ดังนี้ก้าวหน้าด้านเทคโนโลยี และตอบสนองความต้องการของผู้ใช้บริการ ภารกิจหลักสามารถสรุปได้ดังนี้

(1) การให้บริการที่ใช้เทคโนโลยี สารสนเทศเป็นพื้นฐาน (e-Services) ที่ทันสมัยและเป็นสากล ปัจจุบันสำนักได้ริเริ่มที่จะจัดทำมาตรฐาน ITIL (Information Technology Infrastructure Library) ซึ่งเป็นมาตรฐานด้านการให้บริการเทคโนโลยีสารสนเทศที่ได้รับความนิยมในระดับสากล

(2) ดำเนินการจัดหา ผลิตและพัฒนาทรัพยากรสารนิเทศเพื่อการเรียนรู้ตามความต้องการของผู้ใช้บริการ

(3) พัฒนาและจัดหาระบบงาน ฐานข้อมูลต่าง ๆ ที่ช่วยสนับสนุนการเรียนการสอน และการบริหารจัดการ

(4) นำเทคโนโลยีสารสนเทศเข้ามาดำเนิน งานเพื่อส่งเสริมระบบการจัดการและเพื่อให้ผู้ใช้บริการเข้าถึงแหล่งทรัพยากร สารนิเทศอย่างสะดวกและรวดเร็ว

(5) พัฒนาสำนักวิทยบริการและเทคโนโลยี สารสนเทศให้เป็นศูนย์กลางการให้การศึกษาค้นคว้าการวิจัยและการเรียนรู้ด้วยตนเองแก่บุคลากรของมหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรีและบุคคลทั่วไป

(6) ผลิตสื่อการศึกษา และพัฒนาการจัดการศึกษาทางไกล

(7) บริการระบบเครือข่ายให้สามารถเชื่อมโยงแลกเปลี่ยนข้อมูลเพื่อใช้สนับสนุนด้านการเรียนการสอนและการบริหารงานของมหาวิทยาลัยฯ

(8) กำหนดมาตรฐานและจัดหาคอมพิวเตอร์ อุปกรณ์รวมทั้งสื่อและซอฟต์แวร์ เพื่อใช้สนับสนุนการเรียนการสอน และการบริหารงานของมหาวิทยาลัยฯ

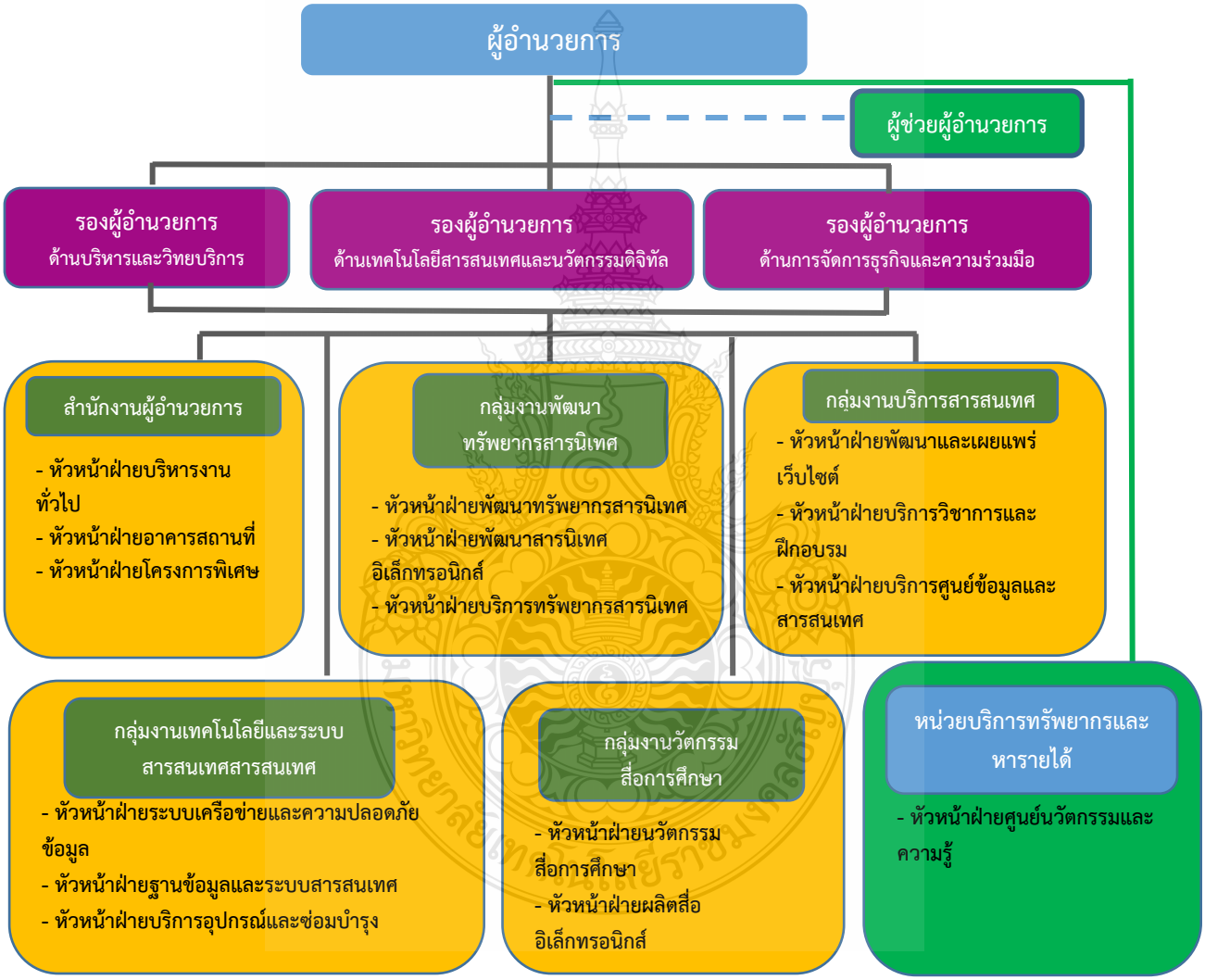
(9)ให้บริการข้อมูลพื้นฐานผ่านสื่ออิเล็กทรอนิกส์ สำหรับนักศึกษา คณาจารย์ ผู้บริหาร และบุคคลภายนอก

(10) ยกระดับบุคลากรของมหาวิทยาลัยฯ ให้มีความรู้ด้านเทคโนโลยีสารสนเทศและการสื่อสาร

(11) สนับสนุนและสร้างผลงานวิจัย สิ่งประดิษฐ์ นวัตกรรมที่เป็นประโยชน์ต่องานด้านระบบสารสนเทศและการพัฒนาโปรแกรม

โดยสำนักฯ มีส่วนช่วยในการสนับสนุนและผลักดันตามนโยบายของมหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี ตามแผนพัฒนามหาวิทยาลัยต่าง ๆ โดยใช้เทคโนโลยีสารสนเทศให้บรรลุตามแผนงานของมหาวิทยาลัยฯ

2.3 โครงสร้างการปฏิบัติงาน



ภาพที่ 2-2 แสดงโครงสร้างการบริหารภายใน ของสำนักวิทยบริการและเทคโนโลยีสารสนเทศ

2.4 โครงสร้างฝ่ายบริการและศูนย์ข้อมูลและสารสนเทศ

ฝ่ายบริการศูนย์ข้อมูกลาง (Information Center) อยู่ภายใต้การกำกับดูแล ของสำนักวิทยบริการและเทคโนโลยีสารสนเทศ ต่อมาในปี 2562 ได้มีการเปลี่ยนชื่อเป็นฝ่ายบริการศูนย์ข้อมูลและสารสนเทศ (Information Center)

ภาพที่ 2-3 แสดงโครงสร้างฝ่ายบริการศูนย์ข้อมูลและสารสนเทศ

2.5 บทบาทหน้าที่ความรับผิดชอบของตำแหน่ง

ปัจจุบันดำรงตำแหน่ง เจ้าหน้าที่บริหารงานทั่วไปปฏิบัติการ ปฏิบัติงานฝ่ายบริการศูนย์ข้อมูลและสารสนเทศ (Information Center) สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี โดยบทบาทหน้าที่ความรับผิดชอบของตำแหน่งมีดังนี้

- พัฒนาระบบฐานข้อมูลเพื่อการบริหารจัดการและการตัดสินใจ
- ให้บริการพื้นที่ศูนย์ข้อมูลและสารสนเทศ (Information Center)

- จัดทำเว็บไซต์ข้อมูลกลาง www.information.rmutt.ac.th
- ดูแลประสานงาน รับแจ้งปัญหาและแนะนำวิธีการใช้งานระบบบริหารบุคลากรและเงินเดือน ระบบสารบรรณอิเล็กทรอนิกส์ (e-office) ระบบบริหารทรัพยากรองค์กร (ERP) ระบบบริการ SMS Marketing
- ประสานงานระบบจัดการงานวิทยานิพนธ์ (i-Thesis)
- จัดทำรูปเล่มรายงานเสนอผู้บริหาร
- สรุปสถิติและรายงานผลการดำเนินงานบริการศูนย์ข้อมูลและสารสนเทศ
- ตรวจสอบและปรับปรุงข้อมูลให้เป็นปัจจุบัน
- จัดเก็บและเผยแพร่องค์ความรู้ และแนวปฏิบัติงานบริการศูนย์ข้อมูลและสารสนเทศ
- วิเคราะห์จัดการความเสี่ยงของงานบริการศูนย์ข้อมูลและสารสนเทศ
- คณะกรรมการเตรียมการเพื่อดำเนินการให้สอดคล้องกับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล
- ผู้ประสานงานโครงการและเจ้าหน้าที่ควบคุมเอกสารระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ (ISMS Working Committee ISOIEC 27001:2013)
- พัฒนาทักษะด้านดิจิทัล และเทคโนโลยีสารสนเทศให้กับนักศึกษา บุคลากรและศิษย์เก่าตามมาตรฐานสากล เช่น IC3, MOs และอื่น ๆ เป็นต้น
- ปฏิบัติหน้าที่อื่น ตามที่ได้รับมอบหมาย

2.6 ลักษณะงานที่ปฏิบัติ

ลักษณะของงานที่ปฏิบัติในปัจจุบัน ได้รับมอบหมายให้ปฏิบัติหน้าที่ดูแลฝ่ายบริการศูนย์ข้อมูลและสารสนเทศ (Information Center) โดยมีหน้าที่รับผิดชอบด้านต่าง ๆ ดังนี้

2.6.1 ดำเนินการติดตามการดำเนินงานของฝ่าย สรุปผลการดำเนินงานได้อย่างมีประสิทธิภาพตรงตามวัตถุประสงค์

2.6.2 สนับสนุนการวางแผนพัฒนาระบบบุคลากรและเงินเดือน (HR) ระบบบริหารทรัพยากรองค์กร (ERP) ในส่วนของความต้องการของผู้ใช้งานโดยประสานงานกับทางผู้ใช้งานและบริษัทผู้พัฒนาระบบ

2.6.3 ปฏิบัติงานด้านการจัดการ ประสานงาน ให้คำปรึกษา ให้คำแนะนำ และให้ข้อมูลแก่ผู้ใช้งานระบบบริหารงานบุคลากรและเงินเดือน ระบบสารบรรณอิเล็กทรอนิกส์ (e-office) ระบบบริหารทรัพยากรองค์กร (ERP) และระบบบริการ SMS Marketing ทั้งในส่วนของผู้ดูแลระบบและผู้ใช้งานทั่วไป

2.6.4 จัดเก็บองค์ความรู้จากปัญหาที่เกิดจากการใช้งานโดยเป็นปัญหาที่เกิดขึ้นใหม่หรือปัญหาที่พบบ่อยนำไปพัฒนารูปแบบการจัดเก็บ เป็นคู่มือการใช้งานของระบบต่าง ๆ

2.6.5 บริการด้าน IT ให้กับบุคลากรและบุคลากรใหม่ โดยสามารถรับบริการครบถ้วน ณ จุดเดียว ได้อย่างสะดวก รวดเร็ว และประหยัดเวลารูปในรูปแบบ One Stop Service

2.6.6 ปฏิบัติงานด้านการเผยแพร่ประชาสัมพันธ์เกี่ยวกับบริการต่าง ๆ ของห้อง Information center

โดยสรุป ในบทที่ 2 นี้ ผู้เขียนได้กล่าวถึงภาพรวมของสำนักวิทยบริการและเทคโนโลยีสารสนเทศและภาพรวมของส่วนงานบริหาร โดยเริ่มตั้งแต่โครงสร้างองค์กร โครงสร้างการบริหาร โครงสร้างการปฏิบัติงาน บทบาทหน้าที่ความรับผิดชอบของตำแหน่ง และลักษณะงานที่ปฏิบัติ ส่วนรายละเอียดของภาระงานหลักที่เขียนเป็นคู่มือการปฏิบัติงานเล่มนี้จะเริ่มเขียนในบทที่ 3 เป็นต้นไป

บทที่ 3

หลักเกณฑ์ วิธีการปฏิบัติงานและเงื่อนไข

การจัดทำคู่มือเรื่อง การจัดการระบบบริหารงานบุคลากรและเงินเดือน มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี มีวัตถุประสงค์เพื่อให้ผู้บริหารจัดการระบบทราบถึงบทบาทหน้าที่ความรับผิดชอบและลักษณะงานที่ปฏิบัติ ขั้นตอนการปฏิบัติงาน เทคนิค แนวปฏิบัติ ขั้นตอนและวิธีการดำเนินการต่าง ๆ เพื่อเป็นเครื่องมือในการการทวนสอบประเภทกลุ่มสิทธิ์ การทวนสอบสิทธิ์ของผู้ใช้งานการกำหนดสิทธิ์และยกเลิกสิทธิ์ของระบบบริหารงานบุคลากรและเงินเดือน ซึ่งในบทที่ 3 เป็นการนำหลักเกณฑ์ วิธีการปฏิบัติงานและเงื่อนไขต่าง ๆ โดยมีรายละเอียดดังต่อไปนี้

3.1 หลักเกณฑ์การปฏิบัติงาน

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี ได้นำระบบบริหารบุคลากรและเงินเดือน มาเริ่มใช้ตั้งแต่ปี 2550 ซึ่งระบบนี้เป็นหนึ่งในระบบสารสนเทศเพื่อการบริหาร เพื่อสนับสนุนการบริหารทรัพยากรบุคคลของทางมหาวิทยาลัย ผู้ปฏิบัติงานในระดับต่าง ๆ ทำให้การบริหารจัดการทางด้านงานบุคคล มีประสิทธิภาพและช่วยให้ผู้บริหารได้รับข้อมูลเพื่อใช้ในการตัดสินใจได้ทันตามความต้องการ โดยสำนักฯ มีหน้าที่สนับสนุนให้ความสำคัญในการสนับสนุนข้อมูลของหน่วยงานเพื่อให้มหาวิทยาลัย สามารถนำข้อมูลไปใช้ประโยชนในการบริหารจัดการด้านต่าง ๆ ได้อย่างมีคุณภาพและบรรลุผลสัมฤทธิ์ตามเป้าหมายที่กำหนดไว้ ตามเกณฑ์มาตรฐาน ซึ่งต้องมีระบบฐานข้อมูลหรือระบบสารสนเทศเพื่อสนับสนุนพันธกิจของหน่วยงานอย่างครบถ้วน ให้ตอบโจทย์การจัดทำรายงานการประเมินตนเอง (Salf Assessment Report : SAR) ของมหาวิทยาลัย องค์ประกอบที่ 2 : การจัดการฐานข้อมูลหรือระบบสารสนเทศตามโครงสร้างของหน่วยงานเพื่อสนับสนุนพันธกิจที่เกี่ยวข้องในตัวบ่งชี้กระบวนการหัวข้อ 2.2.9 ระบบบริหารงานบุคลากรและเงินเดือน มอบหมายให้ฝ่ายบริการศูนย์ข้อมูลและสารสนเทศดำเนินงานร่วมกับกองบริหารงานบุคคล ดูแลระบบและดำเนินการแจ้งปัญหาการใช้งานให้บริษัทปรับแก้ไขพร้อมทั้งตรวจสอบข้อมูลให้ใช้งานได้อยู่เสมอและมีข้อมูลที่เป็นปัจจุบัน (สำนักวิทยบริการและเทคโนโลยีสารสนเทศ,รายงานประเมินตนเองประจำปีงบประมาณ :2562) สามารถเข้าใช้งานได้ผ่านทางเว็บไซต์ httpss://hr.rmutt.ac.th/vncaller/applications.aspx ซึ่งระบบแบ่งออกเป็น 2 ส่วน ดังนี้

1. ระบบบริหารงานบุคลากร สนับสนุนการบริหารทรัพยากรบุคลของทางมหาวิทยาลัย เพื่อช่วยอำนวยความสะดวกให้แก่ผู้ปฏิบัติงานในระดับต่าง ๆ ทำให้การบริหารจัดการทางด้านงานบุคคล มีประสิทธิภาพและช่วยให้ผู้บริหารได้รับข้อมูลเพื่อใช้ในการตัดสินใจได้ทันตามความต้องการ อีกทั้งช่วยจัดรูปแบบการส่งข้อมูลให้กับ อว. หรือส่งข้อมูลให้หน่วยงานภายนอกต่าง ๆ ได้

2. ระบบเงินเดือน เป็นระบบการคำนวณเงินรายได้และรายการหักของบุคลากรในแต่ละงวดเงินเดือน การทำงานของระบบเงินเดือนจะเริ่มต้นจากการประมาณการเงินรายได้, รายการหัก และการสรุปผลการคำนวณรายการได้ และภาษี (เว็บไซต์บริษัท วิชั่นเน็ต จำกัด,HR & Payroll :2553)

การปฏิบัติงานของผู้บริหารจัดการในระบบบริหารงานบุคลากรและเงินเดือน จะมีการเก็บรวบรวมข้อมูลต่าง ๆ ของบุคลากรทั้งมหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี ล้วนเป็นข้อมูลส่วนบุคคล ซึ่งในปี 2562 ได้มีพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 เป็นกฎหมายคุ้มครองข้อมูลส่วนบุคคลตามประกาศพระราชกฤษฎีกาให้มีผลบังคับใช้วันที่ 1 มิถุนายน 2565 โดยมีข้อกำหนดให้องค์กรต่าง ๆ ที่มีธุรกรรมหรือการดำเนินการบนอินเทอร์เน็ตที่มีข้อมูลส่วนบุคคลของผู้บริโภคต้องปฏิบัติตามมาตรการต่าง ๆ ที่เข้มงวดขึ้น เพื่อเพิ่มความคุ้มครองข้อมูลส่วนตัวของบุคคล สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี เห็นความสำคัญและความจำเป็นที่ควรมีแนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลเพื่อรองรับการมีผลบังคับใช้

คู่มือการปฏิบัติงานที่จะกล่าวถึงนี้ มีบทบัญญัติบางประการเกี่ยวกับการจำกัดสิทธิและเสรีภาพของบุคคลโดยมีความเชื่อมโยงกับข้อมูลข้างต้น ครอบคลุมพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลมีประสิทธิภาพและเพื่อให้มีการเยียวยาเจ้าของข้อมูลส่วนบุคคลจากการถูกละเมิดสิทธิในข้อมูลส่วนบุคคล

ข้อมูลบุคคล เป็นข้อมูลเกี่ยวกับบุคคล ซึ่งสามารถระบุถึงตัวเจ้าของข้อมูลได้ ไม่ว่าจะทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ (พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล :2562) ถือเป็น "ข้อมูลส่วนบุคคล" โดยเจ้าของข้อมูลเท่านั้นที่มีสิทธิเข้าถึงและนำข้อมูลไปใช้งาน ข้อมูลเหล่านี้ผู้ควบคุมข้อมูลส่วนบุคคลสามารถนำไปใช้หรือเปิดเผยข้อมูลส่วนบุคคลได้ โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล จึงต้องมีการควบคุมการเข้าถึงระบบ ทางผู้เขียนจึงจัดทำคู่มือนี้ขึ้นเพื่อเป็นแนวปฏิบัติสำหรับการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศภายในมหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรีได้อย่างเหมาะสมและเป็นมาตรฐานในการปฏิบัติเดียวกัน ดังต่อไปนี้

3.1.1 การควบคุมการเข้าถึงข้อมูลและสารสนเทศของมหาวิทยาลัย (Information Access Control)

3.1.1.1 จำแนกกลุ่มทรัพยากรของระบบหรือการปฏิบัติงาน โดยกำหนดกลุ่มผู้ใช้งานและสิทธิ์ของกลุ่มของผู้ใช้งาน

3.1.1.2 กำหนดการอนุญาตให้เข้าถึงการใช้สารสนเทศ ดังนี้

1) กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่ม ให้สามารถสร้างข้อมูล ป้อนข้อมูล แก้ไขข้อมูล ลบข้อมูล อ่านได้อย่างเดียวหรือไม่มีสิทธิเข้าถึงข้อมูลได้เลย

2) กำหนดการระงับสิทธิ์ โดยมอบอำนาจให้เป็นไปตามการบริหารจัดการที่ได้กำหนดไว้

3) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศ จะต้องขออนุญาตจากเจ้าของระบบ โดยผ่านการอนุมัติในแต่ละขั้นบังคับบัญชาเป็นลายลักษณ์อักษร หรือมีหลักฐานในการขอข้อมูล

3.1.1.3 จัดแบ่งประเภทข้อมูลออกเป็น ข้อมูลที่มีความจำเพาะ ข้อมูลภายใน และข้อมูลที่เปิดเผยสาธารณะ

3.1.1.4 จัดแบ่งความสำคัญของข้อมูล โดยระดับความสำคัญมากที่สุดไปถึงความสำคัญที่น้อยที่สุด

3.1.1.5 จัดแบ่งลำดับชั้นความลับของข้อมูล เช่น ลับ ลับมาก และลับที่สุด

3.1.1.6 จัดแบ่งลำดับการเข้าถึงข้อมูลและสารสนเทศของมหาวิทยาลัย

1) ผู้บริหาร เข้าถึงได้ตามอำนาจหน้าที่และลำดับชั้นการบังคับบัญชาในหน่วยงานที่ดูแล

2) ผู้ปฏิบัติงาน เข้าถึงตามอำนาจหน้าที่ที่ได้รับมอบหมาย เช่น เจ้าหน้าที่บุคลากร

3) ผู้ดูแลระบบ (Admin) มีสิทธิ์ในการบริหารจัดการระบบและเข้าถึงข้อมูลที่ได้รับอนุญาตให้เข้าถึงได้

4) ผู้ใช้งานทั่วไป เข้าถึงได้เฉพาะข้อมูลที่ได้รับอนุญาตให้เข้าถึงได้ และสามารถดู เขียน แก้ไข และลบข้อมูลเฉพาะที่ตนเองสร้างขึ้นเท่านั้น

3.1.1.7 มีข้อกำหนดการใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึง โดยให้กำหนดแนวทางการควบคุมการเข้าถึงระบบสารสนเทศ และสิทธิที่เกี่ยวข้องกับระบบสารสนเทศ และมีการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่งคงปลอดภัย

3.1.1.8 กำหนดให้มีหน่วยงานที่ดูแลรับผิดชอบหลักในการอนุญาตการเข้าถึงข้อมูลสานสนเทศของมหาวิทยาลัยในแต่ละประเภท ดังนี้

1) ข้อมูลบุคลากร หน่วยงานหลักคือ กองบริหารงานบุคคล

2) ข้อมูลนักศึกษา หน่วยงานหลักคือ สำนักส่งเสริมวิชาการและงานทะเบียน

3) ข้อมูลการเงินและบัญชี หน่วยงานหลัก คือ กองคลัง

3.1.1.9 การกำหนดการใช้งานตามภารกิจ

1) เจ้าหน้าที่บุคลากร จะให้สิทธิ์เข้าตามภาระหน้าที่ที่ได้รับมอบหมายและหมดสิทธิ์เมื่อพ้นสภาพการเป็นบุคลากร

2) บุคลากร เข้าถึงได้ตามสิทธิ์ของภารกิจที่ได้มอบหมาย

3.1.1.10 การหมดสิทธิ์การเข้าถึงและใช้งานข้อมูลสารสนเทศและระบบสารสนเทศ ต่อเมื่อมีการเปลี่ยนแปลงสิทธิ์ หรือถูกระงับสิทธิ์

3.1.1.11 ช่องทางการเข้าถึง

1) เครือข่ายภายในมหาวิทยาลัย

2) เครือข่ายภายนอกมหาวิทยาลัย

3) เข้าถึงโดยผ่านระบบบริหารงานบุคลากรและเงินเดือน

3.1.2 การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

3.1.2.1 การสร้างความรู้ความเข้าใจให้แก่ผู้ใช้งาน

1) ต้องจัดทำหลักสูตรการฝึกอบรมเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยด้านสารสนเทศ

2) อบรมผู้ใช้งานเพื่อให้สามารถใช้งานข้อมูลและสารสนเทศได้อย่างถูกต้อง รวมถึงตระหนักถึงภัยและผลกระทบที่เกิดจากการใช้งานข้อมูลและสารสนเทศและระบบสารสนเทศโดยไม่ระมัดระวัง

3.1.2.2 การจัดการสิทธิ์ของผู้ใช้งาน

1) เมื่อเจ้าหน้าที่ของหน่วยงาน ลาออก หรือเปลี่ยนแปลงหน้าที่ความรับผิดชอบในระบบที่เคยขอสิทธิ์ ต้องรีบแจ้งเปลี่ยนสิทธิ์หรือถอนสิทธิ์ออกจากระบบทันที

2) การแจ้งขอสิทธิ์/เปลี่ยนแปลงสิทธิ์ในการเข้าถึงและใช้งานข้อมูลสารสนเทศและระบบสารสนเทศจะต้องทำเป็นลายลักษณ์อักษร ระบุเหตุผล และความจำเป็น ดังนี้

2.1) ลงชื่อโดยผู้บริหารของหน่วยงานที่ขอใช้

2.2) ส่งถึงผู้บริหารของหน่วยงานหลัก หรือ เจ้าของระบบ

2.3) เก็บเอกสารไว้เป็นหลักฐานอ้างอิงทั้งฝ่ายผู้ขอและผู้อนุญาต

2.4) หน่วยงานหลักสำเนาเอกสารหรือเก็บเป็นรูปแบบอิเล็กทรอนิกส์ ของการอนุญาตให้ผู้ดูแลระบบเพื่อดำเนินการ

3) ให้อำนาจกับผู้ดูแลระบบในการระงับสิทธิ์ ในกรณีตรวจพบว่ามีการกระทำผิดตามนโยบายเข้าถึงและควบคุมการใช้งานสารสนเทศ

4) กรณีที่มีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานต้องพิจารณาการควบคุมผู้ใช้งานที่มีสิทธิ์พิเศษนั้นอย่างรัดกุมเพียงพอ

3.1.2.3 การทบทวนสิทธิ์การเข้าถึง

1) ต้องมีกระบวนการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานระบบสารสนเทศและปรับปรุงบัญชีผู้ใช้อย่างน้อยปีละ 1 ครั้ง

2) บัญชีผู้ใช้จะหมดอายุ ดังนี้

2.1) กรณีบุคลากร หมดอายุเมื่อพ้นสภาพการเป็นบุคลากรของมหาวิทยาลัย ยกเว้นผู้เกษียณอายุราชการซึ่งสามารถใช้ชื่อบัญชีและรหัสผ่านสำหรับเข้าอินเทอร์เน็ตเท่านั้น

2.2) กรณีที่ไม่ใช่บุคลากรของมหาวิทยาลัย หมดอายุตามวันที่ระบุในเอกสารขอเปิดบัญชีหรือเมื่อไม่มีการเข้าใช้งานติดต่อกันเกิน 3 เดือน

3.1.3 การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

3.1.3.1 การใช้งานบัญชีผู้ใช้งานและรหัสผ่าน

1) ผู้ใช้งานต้องทำการป้องกัน ดูแล รักษาข้อมูลบัญชีและรหัสผ่าน โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งานของตนเอง และห้ามทำการเผยแพร่แจกจ่ายหรือทำให้ผู้อื่นล่วงรู้รหัสผ่าน

3.1.3.2 การใช้งานรหัสผ่าน

1) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

2) เก็บบัญชีและรหัสผ่านของตนเองไว้เป็นความลับ

3.1.4 การควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control)

3.1.4.1 การเข้าใช้งานระบบเครือข่ายของมหาวิทยาลัย

1) การเข้าใช้งานระบบบุคลากรและเงินเดือน มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรีจะต้องพิสูจน์ตัวตนผู้ใช้งานด้วยบัญชีผู้ใช้งานมหาวิทยาลัยออกให้

2) การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกมหาวิทยาลัย (User Authentication for External Connections)

2.1) ผู้ใช้งานที่จะเข้าใช้งานระบบต้องแสดงตัวตนด้วยชื่อผู้ใช้งานทุกครั้ง

2.2) ผู้ใช้งานที่อยู่ภายนอกหน่วยงาน ต้องเป็นผู้ที่ได้รับสิทธิ์ในการเข้าใช้บริการแล้วเท่านั้น

2.3) ต้องมีระบบตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบสารสนเทศของมหาวิทยาลัย โดยจะต้องมีวิธีการยืนยันตัวตนด้วยการป้อนชื่อผู้ใช้งานและรหัสผ่าน เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริง

ตัวอย่างข้อมูลที่เป็นข้อมูลส่วนบุคคล

1. ชื่อ-นามสกุล หรือชื่อเล่น

2. เลขประจำตัวประชาชน เลขหนังสือเดินทาง เลขบัตรประกันสังคม เลขใบอนุญาตขับขี่ เลขประจำตัวผู้เสียภาษี เลขบัญชีธนาคาร และเลขบัตรเครดิต (การเก็บเป็นภาพสำเนา บัตรประชาชนหรือสำเนาบัตรอื่น ๆ ที่มีข้อมูลส่วนบุคคลที่กล่าวมาย่อมสามารถใช้ระบุตัวบุคคลได้โดยตัวมันเอง จึงถือเป็นข้อมูลส่วนบุคคล)

3. ที่อยู่ e-mail เลขโทรศัพท์

4. ข้อมูลอุปกรณ์หรือเครื่องมือ เช่น IP address, MAC address, Cookie ID

5. ข้อมูลทางชีวมิติ (Biometric) เช่น รูปภาพใบหน้า ลายนิ้วมือ ฟิล์มเอกซเรย์ ข้อมูลสแกนม่านตา ข้อมูลอัตลักษณ์เสียง และข้อมูลพันธุกรรม

6. ข้อมูลระบุทรัพย์สินของบุคคล เช่น ทะเบียนรถยนต์ โฉนดที่ดิน

7. ข้อมูลที่สามารถเชื่อมโยงไปยังข้อมูลข้างต้นได้ เช่น วันเกิดและสถานที่เกิด เชื้อชาติ สัญชาติ น้ำหนัก ส่วนสูง ข้อมูลตำแหน่งที่อยู่ (Location) ข้อมูลการแพทย์ ข้อมูลการศึกษา ข้อมูลทางการเงิน และข้อมูลการจ้างงาน

8. ข้อมูลการประเมินผลการทำงานหรือความเห็นของนายจ้างต่อการทำงานของลูกจ้าง

9. ข้อมูลบันทึกต่าง ๆ ที่ใช้ติดตามตรวจสอบกิจกรรมต่าง ๆ ของบุคคล เช่น log file

10. ข้อมูลที่สามารถใช้ในการค้นหาข้อมูลส่วนบุคคลขึ้นในอินเทอร์เน็ต

ตัวอย่างข้อมูลที่ไม่เป็นข้อมูลส่วนบุคคล

1. เลขทะเบียนบริษัท

2. ข้อมูลสำหรับการติดต่อทางธุรกิจที่ไม่ได้ระบุถึงตัวบุคคล เช่น หมายเลขโทรศัพท์ หรือแฟกซ์ที่ทำงาน ที่อยู่สำนักงาน e-mail ที่ใช้ในการทำงาน และ e-mail ของบริษัท

3. ข้อมูลนิรนาม (Anonymous Data) หรือข้อมูลแฝง (Pseudonymous Data) หมายถึงข้อมูลหรือชุดข้อมูลที่ถูกทำให้ไม่สามารถระบุตัวบุคคลได้อีกโดยวิธีการทางเทคนิค

4. ข้อมูลผู้ตาย

ข้อมูลส่วนบุคคลที่เป็นข้อมูลอ่อนไหว

1. เชื้อชาติ

2. เผ่าพันธุ์

3. ความคิดเห็นทางการเมือง

4. ความเชื่อในลัทธิ ศาสนาหรือปรัชญา

5. พฤติกรรมทางเพศ

6. ประวัติอาชญากรรม

7. ข้อมูลสุขภาพ ความพิการ หรือข้อมูลสุขภาพจิต

8. ข้อมูลสหภาพแรงงาน

9. ข้อมูลพันธุกรรม

10. ข้อมูลชีวภาพ

11. ข้อมูลอื่นใดซึ่งกระทบต่อเจ้าของข้อมูลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด (ราชกิจจานุเบกษา,พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 มาตรา 26 :2562)

3.2 วิธีการปฏิบัติงาน

3.2.1 การติดตั้งและเข้าใช้งานระบบ

เนื่องจากระบบสารสนเทศในมหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรีมีหลายระบบงาน ซึ่งผู้ใช้งานต้องจดจำชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) หลายชุด ฝ่ายบริการศูนย์ข้อมูลและสารสนเทศจึงพัฒนาระบบ Single Sign On มาใช้งาน ซึ่งจะทำให้ผู้ใช้งานสามารถใช้ ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพียงหนึ่งบัญชี ผู้ใช้สามารถเข้าถึงระบบสารสนเทศของมหาวิทยาลัยได้ทุกระบบ โดยสำนักวิทยบริการและเทคโนโลยีสารสนเทศ ได้ประกาศเริ่มใช้งานระบบ RMUTT Single Sign On เมื่อวันที่ 1 กรกฎาคม 2562 เป็นต้นไป

การเข้าใช้งานระบบใหม่ในครั้งแรก ผู้ใช้งานต้องแจ้งผู้บริหารจัดการระบบ เพื่อให้กำหนดค่าการใช้งานดังต่อไปนี้

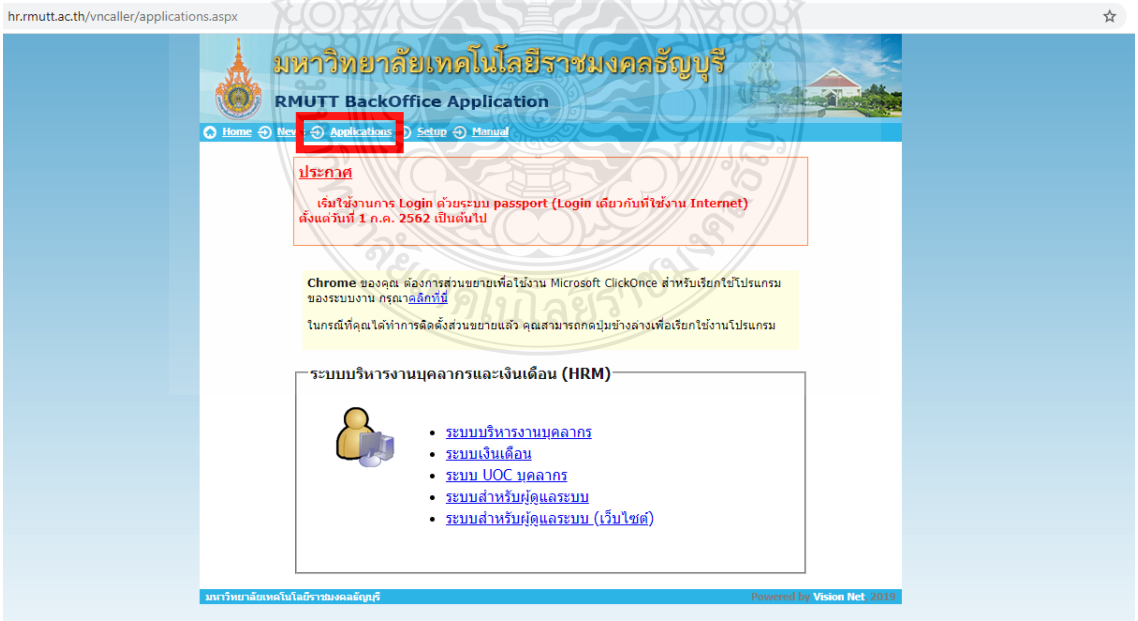
1) ติดตั้ง Application Client

2) เรียกใช้งาน https://hr.rmutt.ac.th/vncaller และคลิกที่ Applications

3) คลิกเลือกระบบงานที่ใช้งาน

4) ทำการ Logon เข้าสู่ระบบด้วย Username/Password ที่ได้รับซึ่งเป็นรหัสเดียวกับที่ใช้เพื่อเข้าใช้งาน Internet

5) รหัสผ่านเพื่อเข้าใช้งานอินเทอร์เน็ตตามข้อมูลที่ฝ่ายบริการศูนย์ข้อมูลและสารสนเทศ แจ้งให้ทราบ กรณีลืมรหัสผ่าน กรุณาติดต่อผู้บริหารจัดการระบบ



ภาพที่ 3-1 แสดงหน้าจอระบบบริหารงานบุคลากรและเงินเดือน

ภาพที่ 3-2 แสดงหน้าจอ Logon

การแจ้งปัญหาการใช้งาน

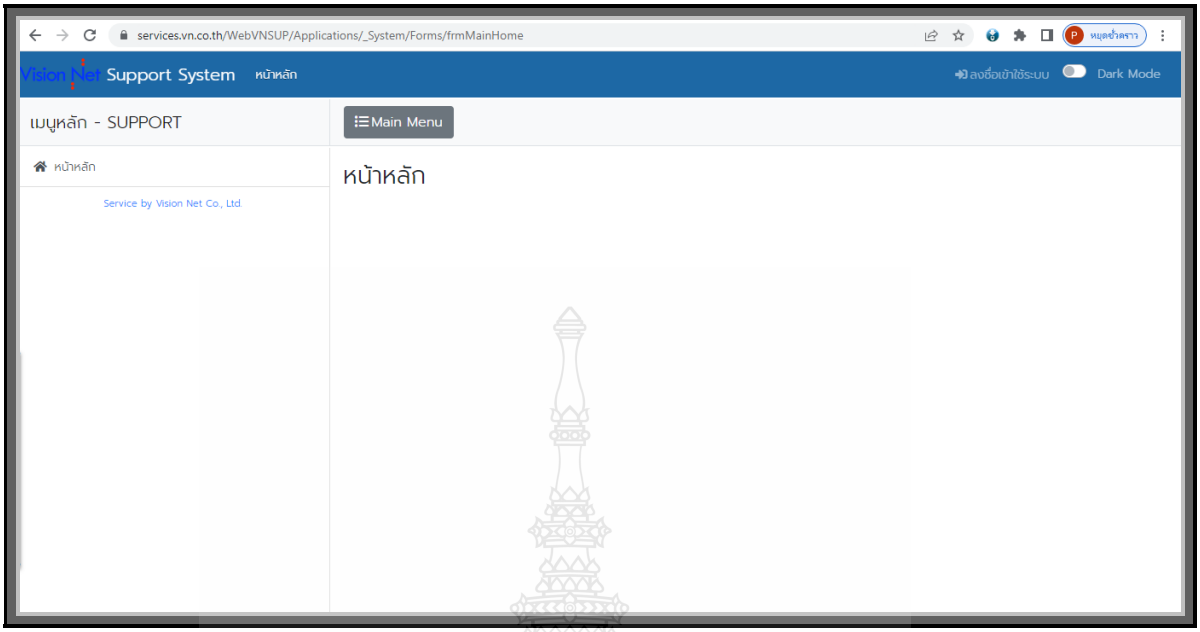
หากพบปัญหาการใช้งานกรณีลืมชื่อผู้ใช้งาน/รหัสผ่าน และแจ้งปัญหาการใช้งานระบบ หรือต้องการติดตั้งระบบสามารถแจ้งปัญหาผ่านช่องทาง ดังนี้

1) ผ่านระบบแจ้งซ่อมออนไลน์ https://helpdesk.rmutt.ac.th โดยเลือกประเภทบริการ “แจ้งปัญหาเกี่ยวกับระบบ HR” หากดำเนินการเสร็จสิ้นแล้ว รายการการแจ้งปัญหาในระบบแจ้งซ่อมออนไลน์ผู้บริหารจัดการระบบจะต้องเข้ามาดำเนินการกรอกสถานะการให้บริการ

2) ผ่าน e-mail :isc@rmutt.ac.th ผู้บริหารจัดการระบบจะส่ง e-mail แจ้งกลับในดำเนินการแก้ไขไปถึงผู้รับผิดชอบตอบกลับไปทาง e-mail

3) ผ่านเบอร์โทรศัพท์ 02549-4442

เมื่อผู้บริหารจัดการระบบได้รับแจ้งปัญหาแล้วจะประเมินปัญหานั้นว่าสามารถแก้ไขได้เองหรือไม่ หรือหากไม่สามารถดำเนินการแก้ไขเองได้ ผู้บริหารจัดการระบบจะต้องส่งปัญหาดังกล่าวให้บริษัทดำเนินการ โดยแจ้งผ่านระบบรับแจ้งปัญหา VN Support System ทางเว็บไซต์ https://services.vn.co.th/WebVNSUP/Applications เบอร์โทรศัพท์ 02641-5310 e-mail: support@vn.co.th หลังจากนั้นจึงดำเนินการแจ้งถึงสถานะของปัญหาให้แก่ผู้ใช้งานได้ทราบต่อไป



ภาพที่ 3-3 แสดงหน้าจอระบบรับแจ้งปัญหา VN Support System

3.2.2 ผู้ใช้งานระบบ

3.2.2.1 กองบริหารงานบุคคล

กองบริหารงานบุคคล เป็นองค์กรการบริหารงานบุคคล เพื่อการสรรหา การรักษาและพัฒนาบุคลากร โดยพัฒนางานสวัสดิการและให้บริหารอย่างมีคุณภาพ พัฒนาศักยภาพของบุคลากรทุกระดับ รักษาบุคลากรที่มีคุณภาพของมหาวิทยาลัยฯ และพัฒนาปรับปรุง แก้ไข ระเบียบที่เกี่ยวข้องกับการบริหารงานบุคคล ให้เอื้อต่อการปฏิบัติงาน โดยยึดตามหลักธรรมาภิบาล ที่จริงแล้วนั้น ส่วนงานนี้มีความจำเป็นต่อองค์กรหรือมหาวิทยาลัยฯ อย่างมาก เพราะทุกภาคส่วนล้วนต้องขับเคลื่อนด้วยพนักงานหรือบุคลากร ดังนั้นความสำคัญของการรวบรวมข้อมูลด้านทรัพยากรบุคคลและความสามารถในการวิเคราะห์ความแตกต่างของแต่ละบุคลากรได้นั้น ทำให้เราสามารถช่วยปรับปรุงหรือเปลี่ยนแปลงบุคลากรได้อย่างรวดเร็ว หากไม่มีกองบริหารงานบุคคลอยู่ ข้อมูลต่าง ๆ อาจกระจัดกระจาย อาจทำให้มีปัญหาต่อการจัดการบุคลากร ตลอดจนปรับปรุงเปลี่ยนแปลงไม่ทันกับปัญหาที่เกิดขึ้น จึงกล่าวได้ว่าการจัดเก็บข้อมูลในระบบบริหารจัดการและเงินเดือนนั้น นับว่าเป็นเครื่องมือที่มีส่วนช่วยในการส่งเสริมสนับสนุนการปฏิบัติงานให้แก่กองบริหารงานบุคคล กล่าวถึงในการดำเนินงานนั้น กองบริหารงานบุคคลจะประสานงานส่งระดับสิทธิ์การเข้าถึงข้อมูลมายังผู้บริหารจัดการระบบ ดำเนินการกำหนดสิทธิ์การเข้าถึงข้อมูลตามภาระงาน และตามหลักปฏิบัติงานของแต่ละบุคคล ต้องกำหนดสิทธิ์กลุ่มกองบริหารงานบุคคลโดยกำหนดแยกสิทธิ์ ในแต่ละแถบหน้าจอตามกลุ่มกองบริหารงานบุคคล ทั้ง 4 กลุ่ม ดังนี้

1. เมนู กองบริหารงานบุคคล (กลุ่ม 1)
2. เมนู กองบริหารงานบุคคล (กลุ่ม 2)
3. เมนู กองบริหารงานบุคคล (กลุ่ม 3)
4. เมนู กองบริหารงานบุคคล (กลุ่ม 4)

ขอเปิดสิทธิการเข้าถึงข้อมูลระบบบุคลากร (MIS)

ที่	ชื่อ - สกุลสกุล	กลุ่มสิทธิ์	ทะเบียนประวัติ									กพ.7	งานเครื่องราชย์	กองทุนฯ	งานพัฒนาบุคลากร	ตรวจสอบผู้สมควรเสนอตำแหน่งทางวิชาการ	ตำแหน่งวิชาการ/วิชาการ, บริหาร
			ตำแหน่งปัจจุบัน	รายได้	ข้อมูลทั่วไป	ข้อมูลอื่น ๆ	ที่อยู่	ผู้เกี่ยวข้อง	การศึกษา/สกอ.	ข้อมูลส่วนบุคคล	ตำแหน่งบริหาร						
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	**นางสุรีพร เป็งเงิน**	1															
2	**นายอุทัย เห็มภูมิ**	1															
3	นางสาวพเก้า จันทร์ทุ่งใหญ่	1															
4	นางสาวอรวรรณ ดันสิงหา	1															
5	นายมงคลชัย โพลังศิริ	3															
6	นางสาสุภารัตน์ เมืองโสภา	3															
7	คนใหม่	3															
8	**นายคมกริช พุ่มเกิด**	1															
9	นางสาวศุภานัน พุดเดาล	1															
10	นายสุรชัย แดผู้เจริญ	1															
11	นางสาวรุ่งอรุณ ในทัง	1															
12	นางศิริญทิพย์ แก้วแทน	1															
13	คนใหม่	1															
14	**นางสาวนภาพร เจริญสุข**	1															
15	นางมาลี พฤกษชาติ	1															
16	นางสาวเกษรินทร์ เรืองวารี	1															
17	นางสาวจุฑารัตน์ ดอนแดงปิน	1															
18	นางสาววาสนา ผิวผลาผล	1															
19	**นางกัญญาณัฐ สายประสาท**	1															
20	นายรุ่งโรจน์ สุทธิสุข	4															
21	นางสาวฐิตาภา ทองไชย	4															
22	นางสาวพันนิดา เสือจ่าศิล	4															
23	นางสาวธีรวดี ยิ่งมี	2															
24	**นางสาวสุกัญญา คัยกรณ์พิพัฒน์**	1															
25	นางสันทนา วุ่นจุ้ด	3															
26	นายเพิ่มศักดิ์ ทับทิมทอง	3															
27	นายยุทธวิทย์ กองแก้ว	3															
28	**นางสรินยา รักษาบุญ**	1															
29	นายชาลิต กนกพาณิชย์สกุล	3															
30	นายธงรบ ชาตะรัตน์	3															
31	นายเสกขพันธ์ คงพิทักษ์	3															
32	คนใหม่	3															

หมายเหตุ

กลุ่ม 1	1-15	เห็น / แก้ไข
กลุ่ม 2	1-10	เห็น
	14	เห็น / แก้ไข
กลุ่ม 3	1-5	เห็น
	13	เห็น/แก้ไข
กลุ่ม 4	1-10	เห็น
	14-15	เห็น/แก้ไข

แก้ไขเมื่อ 19 กุมภาพันธ์ 2563

ภาพที่ 3-4 แสดงตัวอย่างไฟล์ข้อมูลประเภทสิทธิ์ กลุ่มสิทธิ์และระดับสิทธิ์

3.2.2.2 คณะ/หน่วยงานภายในมหาวิทยาลัยฯ

การกำหนดสิทธิ์การเข้าใช้งานระบบบริหารงานบุคคลและเงินเดือน ของเจ้าหน้าที่บุคลากรหน่วยงาน/คณะ กำหนดได้ไม่เกิน 2-3 คน ต่อคณะและหน่วยงาน ผู้บริหารจัดการระบบ จะดำเนินการกำหนดสิทธิ์การเข้าถึงข้อมูลตามภาระงานหน้าที่ของแต่ละบุคคลของหน่วยงาน/คณะนั้น ๆ โดยทางส่วนงานจะต้องทำหนังสือส่งเรื่องการขอเพิ่มสิทธิ์ ยกเลิกสิทธิ์ และเปลี่ยนแปลงชื่อเจ้าหน้าที่บุคลากรมาทางกองบริหารงานบุคคล เพื่อมอบหมายให้ทางสำนักวิทยบริการและเทคโนโลยีสารสนเทศ ดำเนินการต่อไป

ซึ่งระดับสิทธิ์ของเจ้าหน้าที่บุคลากรหน่วยงาน/คณะนั้น จะสามารถเข้าถึงข้อมูลของบุคลากรภายในหน่วยงาน/คณะ ของตนได้เท่านั้น โดยสรุป ดังต่อไปนี้

งานทะเบียนประวัติบุคลากร (เฉพาะตำแหน่งปัจจุบัน)

- ข้อมูลพนักงาน บรรจุแต่งตั้ง ประเภทบุคลากร ตำแหน่ง สังกัด การเกษียณอายุ
- ประวัติการเปลี่ยนตำแหน่ง เลื่อนตำแหน่ง โอนย้ายหน่วยงาน แหล่งเงินเดือน
- ประวัติการเปลี่ยนสถานะ ทดลองงาน ปฏิบัติงาน พ้นสภาพ (ลาออก เกษียณ)
- ข้อมูลพนักงานสัญญาจ้าง และการต่ออายุสัญญาจ้าง
- ประวัติการดำรงตำแหน่งทางวิชาการ ตำแหน่งบริหาร

งานลงเวลา/บันทึกเวลา

- ข้อมูลเวลาเข้า-ออก สถานการณ์ลงเวลา เช่น ขาดงาน ลา มาสาย
- สามารถนำเข้าข้อมูลเวลาเข้า-ออกงาน จากไฟล์ข้อมูลของเครื่องลงเวลา รูปแบบ Text File, Microsoft Excel
- สิทธิ์การลา สถิติการลา วันลาคงเหลือ และวันลาสะสม
- บุคลากรสามารถบันทึกวันใบลา เพื่อขออนุมัติจากผู้บังคับบัญชา และแนบเอกสารประกอบ
- ผู้บังคับบัญชา สามารถตรวจสอบและอนุมัติ/ไม่อนุมัติ ใบลา
- ผู้บังคับบัญชา สามารถตรวจสอบการมาทำงาน ขาดลา มาสาย ของผู้ใต้บังคับบัญชา

งานพัฒนาบุคลากร

- ข้อมูลประวัติการฝึกอบรม ประชุม และสัมมนา
- รายละเอียดของหลักสูตรฝึกอบรม หัวข้อการประชุม หัวข้อการสัมมนา ผู้ร่วมกิจกรรม

งานเครื่องราชอิสริยาภรณ์

- ประวัติการรับเครื่องราชอิสริยาภรณ์

รายงาน/สอบถามข้อมูล 1

- จำนวนบุคลากรจำแนกตามประเภทบุคลากร
- บัญชีรายชื่อบุคลากรที่ดำรงตำแหน่งทางวิชาการ
- ประวัติส่วนตัวและประวัติการทำงาน

รายงาน/สอบถามข้อมูล 2

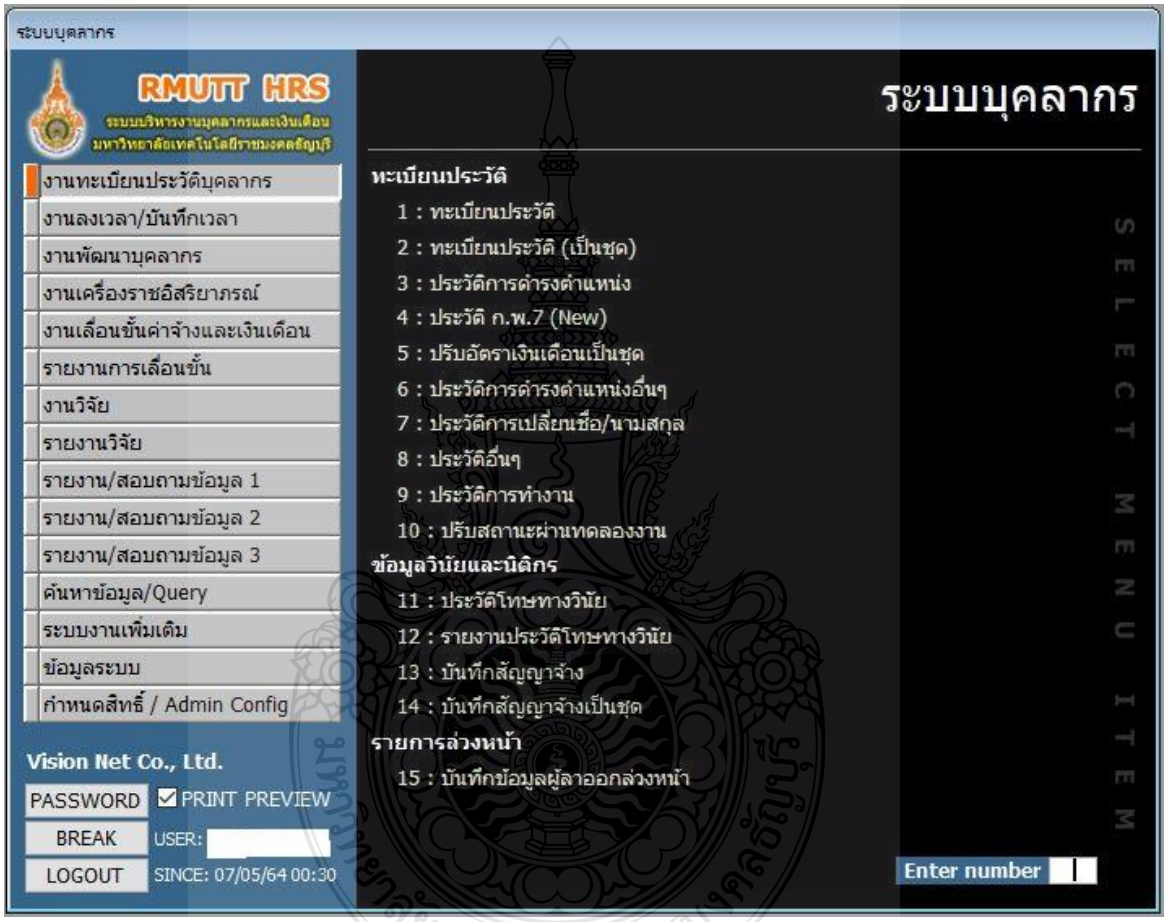
- รายงานข้อมูลบุคลากร
- รายงานจำนวนบุคลากรแยกตามเพศ
- รายชื่อบุคลากรตามสายงาน
- รายงานประวัติการลาศึกษาต่อ ฝึกอบรม ดูงาน วิจัย

รายงาน/สอบถามข้อมูล 3

- Query รายชื่อบุคลากรตามอายุงาน-อายุตัว

ค้นหาข้อมูล/Query

- ข้อมูลบุคลากร จำแนกตามสายงาน



ภาพที่ 3-5 แสดงหน้าจอการใช้งานระบบบริหารงานบุคลากรและเงินเดือน

3.2.2.3 ผู้ดูแลระบบ

การขอชื่อผู้ใช้และรหัสผ่านในการเข้าสู่ระบบบริหารงานบุคลากรและเงินเดือน ของผู้บริหารจัดการระบบ สำหรับผู้บริหารจัดการระบบที่ได้รับมอบหมายตามภาระงาน ต้องติดต่อประสานงานกับทางบริษัทแจ้งชื่อผู้ใช้ (Username) ทางบริษัทจะดำเนินการกำหนดสิทธิ์การเข้าถึงระบบ โดยสามารถใช้ชื่อผู้ใช้และรหัสผ่านเดียวกันกับ AD Wifi ของมหาวิทยาลัยฯ

การขอชื่อผู้ใช้และรหัสผ่านในการเข้าสู่ระบบรับแจ้งปัญหา VN Support System กรณีที่ผู้บริหารจัดการระบบยังไม่มีรหัสประจำตัวสำหรับเข้าใช้งาน ต้องติดต่อ IT Support Department โดยแจ้งชื่อ-นามสกุล ไปยัง e-mail: support@vn.co.th ทางบริษัทจะดำเนินการกำหนดรหัสประจำตัว (Username) และรหัสผ่าน (Password) ระบบจะแจ้งให้เปลี่ยนรหัสผ่านทันทีที่ท่านเข้าใช้งานระบบในครั้งแรก

3.3 แนวคิด/ทฤษฎีที่เกี่ยวข้อง

3.3.1 แนวคิดเกี่ยวกับการกำหนดสิทธิ์

การกำหนดสิทธิ์ เป็นองค์ประกอบหนึ่งที่จะทำให้ผู้ใช้งานสามารถเข้าใช้งานและเข้าถึงข้อมูลต่าง ๆ ในระบบได้ เกิดจากผู้บริหารจัดการระบบ (System Administrators) เป็นผู้กำหนดสิทธิ์ หรือยกเลิกสิทธิ์ในการใช้งานของระบบนั้น ๆ โดยกำหนดว่าแต่ละคนมีสิทธิ์เข้าใช้งานในระบบหรือไม่ และเข้าใช้งานในฟังก์ชั่นไหนบ้าง รวมถึงการยกเลิกสิทธิ์ไม่ให้เข้าใช้งานระบบ และไม่สามารถเข้าถึงข้อมูลในระบบได้เลย จากการศึกษาแนวคิด ผู้เขียนพบว่ามีแนวคิดที่เกี่ยวกับการกำหนดสิทธิ์และยกเลิกสิทธิ์ ดังต่อไปนี้

1. ความหมายของการกำหนดสิทธิ์

การกำหนดสิทธิ์การเข้าถึงข้อมูล หมายถึง การควบคุมการเข้าถึงข้อมูลของผู้ใช้งานผ่านการกำหนดรหัสผ่าน หรือการปิดสิทธิ์ไม่ให้ผู้ใช้งานเห็นข้อมูลนั้น ๆ การกำหนดขึ้นอยู่กับระดับความสำคัญและหน้าที่การทำงานของแต่ละบุคคล (https://www.mangoconsultant.com/en/news-knowledge/knowledge/317, ความสำคัญของการกำหนดสิทธิ์การเข้าถึงข้อมูลของพนักงาน :2551)

2. ความสำคัญและความจำเป็นต่อการกำหนดสิทธิ์

ในการสร้างผู้ใช้และการกำหนดสิทธิการใช้งานระบบฐานข้อมูลถือว่ามีความจำเป็นมากในปัจจุบันโดยเฉพาะหน่วยงานที่เก็บข้อมูลระบบใหญ่ ข้อมูลที่มีความสำคัญ และข้อมูลที่มีการเปลี่ยนแปลงตลอดเวลา ผู้ดูแลระบบจะต้องมีการกำหนดสิทธิในการใช้งานให้กับผู้ใช้ หรือผู้ดูแลระบบย่อย เพื่อป้องกันปัญหาที่จะเกิดขึ้น เช่นถ้าผู้เข้าดูข้อมูล ไม่ควรจะให้มีการแก้ไขโครงสร้างระบบฐานข้อมูล ไม่ควรให้แก้ไขข้อมูลในตารางได้ ผู้ที่ทำหน้าที่ปรับปรุงข้อมูลในตารางก็ควรจะให้สิทธิในเรื่องการปรับปรุง แก้ไขข้อมูลในตารางไม่ควรให้แก้ไขข้อมูลทั้งระบบ จึงควรศึกษาการสร้างผู้ใช้และการกำหนดสิทธิการใช้งาน

3. ผู้ใช้งานต้องการเข้าถึงระบบได้ต้องมีการกำหนดสิทธิ์ (Authorization) คือ การจำกัดสิทธิ์ในการกระทำใด ๆ ต่อระบบและข้อมูลในระบบของผู้ใช้งานที่ผ่านการพิสูจน์ตัวตนมาแล้ว (พีระพล รัตนาไพบูลย์, การบริหารความมั่นคงสารสนเทศ :2560) ประเภทของการกำหนดสิทธิ์ แบ่งออกเป็น 3 ส่วน ดังนี้

3.1 กำหนดสิทธิ์ผู้ใช้งานรายบุคคล โดยระบบจะพิสูจน์ตัวตนของผู้ใช้งานแต่ละรายว่าเป็นผู้ใช้งานที่ได้รับอนุญาตที่แท้จริงหรือไม่ จากนั้นก็จะอนุญาตให้ผู้ใช้งานที่แท้จริงเข้าสู่ระบบได้ เมื่อเข้าสู่ระบบผู้ใช้งานจะสามารถใช้ทรัพยากรเฉพาะส่วนที่อนุญาตให้ใช้ได้เท่านั้น

3.2 กำหนดสิทธิ์สมาชิกของกลุ่ม ระบบจะเปรียบเทียบหลักฐานการยืนยันตัวตน ของสมาชิกกับบัญชีรายชื่อของสมาชิกในกลุ่มใด ๆ ที่จัดเก็บไว้ หากถูกต้องจะอนุญาตให้เข้าใช้ระบบได้ตามสิทธิ์ที่กลุ่มนั้นได้รับ

3.3 กำหนดสิทธิ์การใช้งานเข้าระบบ จะตรวจสอบหลักฐานการยืนยันตัวตนของผู้ใช้งานที่ศูนย์กลางของระบบ ซึ่งหลักฐานดังกล่าวจะเป็นชุดของข้อมูลที่ทุกระบบสามารถตรวจสอบได้เหมือนกัน บางครั้งเรียกระบบดังกล่าวว่า “Single Sign-on” ที่ต้องอาศัยโปรโตคอลชนิดพิเศษที่เรียกว่า “LDAP” จึงจะสามารถทำได้

4. ประโยชน์ของการกำหนดสิทธิ์โดยมีความสำคัญต่อการทำงาน ดังนี้

4.1 เกิดการปฏิบัติงานอย่างเป็นระบบ โดยกำหนดหน้าที่การทำงานของแต่ละฝ่ายแต่ละบุคคลชัดเจน

4.2 ควบคุมทิศทางและจัดระเบียบการทำงานให้ตรงตามวัตถุประสงค์

4.3 รักษาความปลอดภัยของฐานข้อมูล และป้องกันข้อมูลที่เป็นความลับ

4.4 ช่วยให้ผู้บริหารสามารถติดตามผลการทำงานและเห็นภาพการทำงานชัดเจนยิ่งขึ้น

4.5 เพิ่มความสะดวก รวดเร็วในการทำงาน

3.3.2 ทฤษฎีที่เกี่ยวข้อง

ในส่วนของทฤษฎีที่เกี่ยวข้อง ผู้เขียนได้พยายามศึกษาข้อมูลที่เกี่ยวข้องกับการกำหนดสิทธิ์และยกเลิกสิทธิ์ ซึ่งมีความสัมพันธ์ในการควบคุมการเข้าถึง (Access Control) หมายถึง การทำให้มั่นใจว่าทรัพยากรต่าง ๆ ของระบบจะได้รับอนุญาตให้ถูกใช้โดยผู้ที่มีสิทธิ์เท่านั้น (พีระพล รัตนาไพบูลย์, การบริหารความมั่นคงสารสนเทศ :2560) ซึ่งต้องอาศัยเทคโนโลยีต่าง ๆ เป็นกลไกการทำงาน ประกอบด้วย 4 กลไก ได้แก่

1. การระบุตัวตน (Identification) เป็นกลไกที่ได้จัดเตรียมสารสนเทศของบุคคลที่จะเข้าใช้ระบบเรียกว่า Identifies ซึ่งผู้ใช้งานแต่ละคนต้องมีค่าไม่ซ้ำกัน ใช้ร่วมกับกลไกการพิสูจน์ตัวตน

2. การพิสูจน์ทราบตัวตน (Authentication) เป็นกลไกการตรวจสอบว่าผู้ใช้งานเป็นใครและเป็นผู้ได้รับอนุญาตหรือไม่ โดยพิจารณาจาก Identifier ของผู้ใช้งาน

3. การกำาหนดลิขสิทธิ์ (Authorization) เป็นกลไกการอนุญาตหรือให้สิทธิ์ในการเข้าถึงระบบหรือการเข้าใช้ข้อมูลของผู้ใช้งานที่ที่ผ่านการพิสูจน์ทราบตัวตนมาแล้ว โดยพิจารณาว่าผู้ใช้งานแต่ละคนได้รับอนุญาตในระดับไหน และใช้ข้อมูลส่วนใดได้บ้าง

4. การจัดทำประวัติการเข้าใช้ระบบ (Accountability) เป็นส่วนที่ใช้การเข้าบันทึกระบบของผู้ใช้งาน (System Logs) เพื่อจัดทำหลักฐานการตรวจสอบ และเพื่อติดตามพฤติกรรมที่น่าสงสัยได้

การพิสูจน์ทราบตัวตน (Authentication) กระบวนการยืนยันความถูกต้องของตัวบุคคล โดยพิสูจน์ความถูกต้องของตัวบุคคล อาศัยสิ่งที่เป็น Identifier ของบุคคลเป็นหลักฐานในการระบุตัวตน ก่อนที่จะดำเนินการตรวจสอบความถูกต้องของตัวบุคคล

รหัสผ่าน (Password) คือ ค่ากลุ่มหรือตัวอักษรมีเพียงผู้ใช้งานคนเดียวที่ทราบ ซึ่งกลไกการพิสูจน์ตัวตนแบบนี้จะมีความเสี่ยงต่อการถูกโจมตีมากที่สุด นิยมกำหนดรหัสผ่านให้คาดเดายาก จากการศึกษาทฤษฎีเกี่ยวกับการควบคุมการเข้าถึง (Access Control) ผู้เขียนพบว่า มีผู้ให้แนวคิดที่แตกต่างกันตามทัศนคติและมุมมอง ดังนี้

เพจ Facebook ชื่อ Bc0411 การจัดการความมั่นคงของระบบสารสนเทศ (ก.พ. 2562) ได้ให้ข้อความรู้ของ Authentication การพิสูจน์ตัวตน หนทางสู่ความปลอดภัยของข้อมูล ดังนี้

1. การพิสูจน์ตัวตน (Authentication)

การพิสูจน์ตัวตน คือขั้นตอนการยืนยันความถูกต้องของหลักฐาน (Identity) ที่แสดงว่าเป็นบุคคลที่กล่าวอ้างจริง ในทางปฏิบัติจะแบ่งออกเป็น 2 ขั้นตอน คือ

1.1 การระบุตัวตน (Identification) คือขั้นตอนที่ผู้ใช้งานแสดงหลักฐานว่าตนเองคือใคร เช่น ชื่อผู้ใช้งาน (Username)

1.2 การพิสูจน์ตัวตน (Authentication) คือขั้นตอนที่ตรวจสอบหลักฐานเพื่อแสดงว่าเป็นบุคคลที่กล่าวอ้างจริง

การแสดงกระบวนการพิสูจน์ตัวตน ในขั้นแรกผู้ใช้งานจะทำการแสดงหลักฐานที่ใช้ในการพิสูจน์ตัวตนต่อระบบ ซึ่งในขั้นนี้คือการระบุตัวตน และในขั้นตอนต่อมาระบบจะทำการตรวจสอบหลักฐาน ที่ผู้ใช้งานนำมากล่าวอ้างซึ่งก็คือการพิสูจน์ตัวตน หลังจากระบบได้ทำการตรวจสอบหลักฐานเรียบร้อยแล้วถ้าหลักฐานที่นำมากล่าวอ้างถูกต้องจึงอนุญาตให้เข้าสู่ระบบได้ หากหลักฐานที่นำมากล่าวอ้างไม่ถูกต้องผู้ใช้งานจะถูกปฏิเสธจากระบบ

หลักฐานที่ผู้ใช้งานนำมากล่าวอ้างที่เกี่ยวกับเรื่องของความปลอดภัยนั้นสามารถจำแนกได้ 2 ชนิด

1. Actual Identity คือ หลักฐานที่สามารถบ่งบอกได้ว่าในความเป็นจริงบุคคลที่กล่าวอ้างนั้นเป็นใคร

2. Electronic Identity คือ หลักฐานทางอิเล็กทรอนิกส์ซึ่งสามารถบ่งบอกข้อมูลของบุคคลนั้นได้ แต่ละบุคคลอาจมีหลักฐานทางอิเล็กทรอนิกส์ได้มากกว่า 1 หลักฐาน ตัวอย่างเช่น บัญชีชื่อผู้ใช้งาน

ลักษณะของการพิสูจน์ตัวตน การพิสูจน์ตัวตนในปัจจุบันมีอยู่ 3 ลักษณะ ได้แก่

1. สิ่งที่คุณรู้ (Something you know) หมายถึง การใช้ Username และ Password ในการเข้าสู่ระบบโดยทั่วไป เช่น การใช้อินเทอร์เน็ตด้วยการหมุน Modem จากบ้านเข้าสู่ ISP หรือการทำงานในบริษัทที่ต้องมีการ Logon โดยใช้ Username และ Password ซึ่งการพิสูจน์ตัวตนในลักษณะนี้ถือเป็นแบบที่ระดับความปลอดภัยน้อยที่สุด เพราะถ้าใครรู้ Username และ Password ของเราก็สามารถเข้าใช้งาน

ระบบได้ทันที นอกจากนี้เรายังตรวจสอบตัวตน (Authenticity/Accountability) ของผู้ใช้งานระบบไม่ได้ว่าใครเป็นใครอีกด้วย

2. สิ่งที่คุณมี (Something you have) เป็นการพิสูจน์ตัวตนในลักษณะที่เรียกว่า Multi Factor กล่าวคือ นอกจากจะมี Password ที่ต้องจำแล้วยังต้องใช้อุปกรณ์เสริมเข้ามาใช้ในการเข้าระบบด้วย เช่น บัตร ATM, RSA Token, Swipe Card, Access Card และ Smart Card เป็นต้น การตรวจสอบผู้ใช้งานระบบโดยใช้สมาร์ทการ์ดเข้ามาช่วยนั้นจะช่วยตรวจสอบตัวตนของผู้ใช้งานระบบได้คล้าย ๆ กับที่ธนาคารตรวจสอบผู้ใช้งานบัตร ATM ของธนาคารว่าเป็นเจ้าของบัตรหรือไม่ เพราะบัตรควรจะต้องอยู่กับเจ้าของบัตรเท่านั้น และเจ้าของบัตรเท่านั้นที่ทราบรหัสของตน ผู้อื่นถึงแม้จะขโมยบัตรไปแต่ก็ไม่ทราบรหัสที่อยู่ในบัตร ทำให้ยากไปอีกขั้นหนึ่งในการเจาะเข้าสู่ระบบ

3. สิ่งที่คุณเป็น (Something you are) ก็คือการนำเทคโนโลยี Biometric เข้ามาใช้ในการตรวจสอบตัวตนโดยอาศัยอวัยวะที่คนเรามีอยู่ และมีลักษณะที่เป็นหนึ่งเดียวคือ ไม่ซ้ำกัน ได้แก่ ลายนิ้วมือ, ม่านตา หรือเสียง เป็นต้น การใช้งานสมาร์ทการ์ดสามารถร่วมกับระบบ Biometric ได้ กล่าวคือ เราสามารถเก็บลายนิ้วมือของคนลงไปใน Microchip ที่อยู่ในสมาร์ทการ์ดได้ด้วย ซึ่งจะเพิ่มระดับของความปลอดภัยมากขึ้น แต่ค่าใช้จ่ายก็จะสูงขึ้นเช่นกัน

กระบวนการพิสูจน์ตัวตนนั้นจะนำ 3 ลักษณะข้างต้นมาใช้ในการยืนยันหลักฐานที่นำมากล่าวอ้าง ทั้งนี้ขึ้นอยู่กับระบบ วิธีการที่นำมาใช้เพียงลักษณะอย่างใดอย่าง หนึ่ง (Single-factor Authentication) นั้นมีข้อจำกัดในการใช้ ตัวอย่างเช่น สิ่งที่คุณมี (Possession Factor) นั้นอาจจะสูญหายหรือถูกขโมยได้ สิ่งที่คุณรู้ (Knowledge Factor) อาจจะถูกดักฟัง เดา หรือขโมยจากเครื่องคอมพิวเตอร์ สิ่งที่คุณเป็น (Biometric Factor) จัดได้ว่าเป็นวิธีที่มีความปลอดภัยสูงอย่างไรก็ตามการที่จะใช้เทคโนโลยีนี้ได้นั้นจำเป็นต้องมีการลงทุนที่สูง เป็นต้น

ดังนั้น จึงได้มีการนำแต่ละคุณลักษณะมาใช้ร่วมกัน (Multi-factor Authentication) ตัวอย่างเช่น ใช้สิ่งที่คุณมีกับสิ่งที่คุณรู้มาใช้ร่วมกัน เช่น การใช้ลายมือชื่อร่วมกับการใช้บัตรเครดิตหรือการใช้รหัสผ่านร่วมกับการใช้บัตร ATM เป็นต้น การนำแต่ละลักษณะของการพิสูจน์ตัวตนมาใช้ร่วมกันมากกว่า 1 ลักษณะจะช่วยเพิ่มประสิทธิภาพในการรักษาความปลอดภัยของข้อมูล

2. การกำหนดสิทธิ์ (Authorization)

การกำหนดสิทธิ์ คือขั้นตอนในการอนุญาตให้แต่ละบุคคลสามารถเข้าถึงข้อมูลหรือระบบใดได้บ้าง ก่อนอื่นต้องทราบก่อนว่าบุคคลที่กล่าวอ้างนั้นคือใครตามขั้นตอนการพิสูจน์ตัวตนและต้องให้แน่ใจด้วยว่าการพิสูจน์ตัวตนนั้นถูกต้อง

3. การเข้ารหัส (Encryption)

การเข้ารหัส คือการเก็บข้อมูลให้เป็นส่วนบุคคลจากบุคคลอื่นที่ไม่ได้รับอนุญาต ส่วนประกอบ 2 ส่วน ที่สำคัญที่จะช่วยทำให้ข้อมูลนั้นเป็นความลับได้ก็คือ การกำหนดสิทธิ์และการพิสูจน์ตัวตนเพราะว่าก่อนการอนุญาตให้บุคคลที่กล่าวอ้างเข้าถึงข้อมูลหรือถอดรหัสข้อมูลนั้นต้องสามารถแน่ใจได้ว่าบุคคลที่กล่าวอ้างนั้นเป็นใครและได้รับอนุญาตให้สามารถเข้ามาดูข้อมูลได้หรือไม่ ในการเข้ารหัสนั้นวิธีการหนึ่ง

ที่ทำได้คือการเข้ารหัสในรูปแบบของกุญแจลับ (Secret Key) ซึ่งในการใช้คีย์รูปแบบนี้ต้องเฉพาะผู้ที่มีกุญแจลับนี้เท่านั้นที่สามารถรับข้อมูลที่เข้ารหัสแล้วได้

4. การรักษาความสมบูรณ์ (Integrity)

การรักษาความสมบูรณ์ คือการรับรองว่าข้อมูลจะไม่ถูกเปลี่ยนแปลงหรือทำลายไปจากต้นฉบับ (source) ไม่ว่าจะเป็นโดยบังเอิญหรือดัดแปลงโดยเจตนาที่อาจส่งผลเสียต่อข้อมูล การคุกคามความสมบูรณ์ของข้อมูลคือการที่บุคคลที่ไม่ได้รับอนุญาตสามารถที่จะเข้าควบคุมการจัดการของข้อมูลได้

5. การตรวจสอบ (Audit)

การตรวจสอบ คือการตรวจสอบหลักฐานทางอิเล็กทรอนิกส์ ซึ่งสามารถใช้ในการติดตามการดำเนินการเพื่อตรวจสอบความถูกต้องและแม่นยำ ตัวอย่างเช่น การตรวจสอบบัญชีชื่อผู้ใช้งานโดยผู้ตรวจบัญชี ซึ่งการตรวจสอบความถูกต้องของการดำเนินการเพื่อให้แน่ใจว่าหลักฐานทางอิเล็กทรอนิกส์นั้นได้ถูกสร้างและสั่งให้ทำงานโดยบุคคลที่ได้รับอนุญาต และในการเชื่อมต่อเหตุการณ์เข้ากับบุคคลจะต้องทำการตรวจสอบหลักฐานของบุคคลนั้นด้วย ซึ่งถือเป็นหลักการพื้นฐานของขั้นตอนการทำงานของการพิสูจน์ตัวตนด้วย

การพิสูจน์ตัวตนจัดเป็นการตรวจสอบหลักฐานขั้นพื้นฐานที่สำคัญที่สุดใน 5 ระดับชั้นของการควบคุมความปลอดภัย ดังนั้นการพิสูจน์ตัวตนดีจะช่วยเพิ่มความมั่นคงปลอดภัยขั้นพื้นฐานให้กับระบบมากยิ่งขึ้น

ประเภทของการพิสูจน์ตัวตน (Authentication Types) ส่วนประกอบพื้นฐานของการพิสูจน์ตัวตนสมบูรณ์แบ่งได้เป็น 3 ส่วน คือ

1. การพิสูจน์ตัวตน (Authentication) คือ ส่วนที่สำคัญที่สุดเพราะเป็นขั้นตอนแรกของการเข้าใช้ระบบ ผู้เข้าใช้ระบบต้องถูกยอมรับจากระบบว่าสามารถเข้าสู่ระบบได้ การพิสูจน์ตัวตนเป็นการตรวจสอบหลักฐานเพื่อแสดงว่าเป็นบุคคลนั้นจริง

2. การกำหนดสิทธิ์ (Authorization) คือ ข้อจำกัดของบุคคลที่เข้ามาในระบบ ว่าบุคคลคนนั้นสามารถทำอะไรกับระบบได้บ้าง

3. การบันทึกการใช้งาน (Accountability) คือ การบันทึกรายละเอียดของการใช้ระบบและรวมถึงข้อมูลต่าง ๆ ที่ผู้ใช้งานกระทำลงไปในระบบ เพื่อผู้ตรวจสอบจะได้ตรวจสอบได้ว่า ผู้ใช้งานที่เข้ามาใช้บริการได้เปลี่ยนแปลงหรือแก้ไขข้อมูลในส่วนใดบ้าง

การพิสูจน์ตัวตนมีความสำคัญที่สุดกับการเข้าใช้ระบบ มีการแจกแจงชนิดของการพิสูจน์ตัวตนใช้กันอยู่ในปัจจุบันว่ามีอะไรบ้างและแต่ละชนิดมีลักษณะอย่างไร ดังนี้

1. ไม่มีการพิสูจน์ตัวตน (No Authentication) ตามหลักการแล้วการพิสูจน์ตัวตนไม่มีความจำเป็น ถ้าเงื่อนไขต่อไปนี้เป็นจริง ข้อมูลเหล่านั้นเป็นข้อมูลสาธารณะ ที่อนุญาตให้ทุกคนเข้าใช้บริการและเปลี่ยนแปลงได้ หรือข้อมูลข่าวสารหรือแหล่งของข้อมูลนั้น ๆ สามารถเข้าถึงได้เฉพาะบุคคลที่ได้รับอนุญาตเท่านั้น

ข้อดี :ง่ายต่อการใช้งานและค่าใช้จ่ายต่ำ

ข้อเสีย : ความปลอดภัยของข้อมูลจะขึ้นอยู่กับผู้ใช้งานว่าจะนำข้อมูลเหล่านั้นไปใช้ในทางที่ควรหรือไม่

2. การพิสูจน์ตัวตนโดยใช้รหัสผ่าน(Authentication by Passwords) รหัสผ่านเป็นวิธีการที่ใช้มานานและนิยมใช้กันแพร่หลาย รหัสผ่านควรจำกัดให้เฉพาะผู้ใช้งานที่มีสิทธิเท่านั้นที่ทราบ แต่ว่าในปัจจุบันนี้ การใช้แค่รหัสผ่านไม่มีประสิทธิภาพมากพอที่จะรักษาความมั่นคงปลอดภัยให้กับระบบคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ เนื่องจากการตั้งรหัสผ่านที่ง่ายเกินไป และวิทยาการและความรู้ที่ก้าวหน้าทำให้รหัสผ่านอาจจะถูกขโมยโดยระหว่างการสื่อสารผ่านเครือข่ายได้

ข้อดี : สามารถใช้ได้กับทุกระบบ

ข้อเสีย : จะไม่ปลอดภัยเมื่อมีการส่งข้ามระบบเครือข่ายที่เป็นสาธารณะหรือไม่มีการเข้ารหัสข้อมูล

3. การพิสูจน์ตัวตนโดยใช้ PIN (Personal Identification Number) เป็นรหัสลับส่วนบุคคลที่ใช้เป็นรหัสผ่านเพื่อเข้าสู่ระบบ ซึ่ง PIN ใช้อย่างแพร่หลายโดยเฉพาะการทำธุรกรรมทางด้านธนาคาร เช่น บัตร ATM และเครดิตการ์ดต่าง ๆ การใช้ PIN ทำให้มีความปลอดภัยในการสื่อสารข้ามระบบเครือข่ายสาธารณะมากขึ้น เนื่องจาก PIN จะถูกเข้ารหัสเอาไว้และจำเป็นต้องมีเครื่องมือที่สามารถถอดรหัสนี้ออกมาได้ เช่น ฮาร์ดแวร์ที่ออกแบบมาโดยเฉพาะ และถูกติดตั้งไว้ในเครื่องของผู้รับและผู้ส่งเท่านั้น

ข้อดี : ง่ายต่อการจำและความปลอดภัยค่อนข้างดีบัตร ATM) และสามารถสื่อสารข้ามเครือข่ายสาธารณะได้อย่าง

ข้อเสีย : ต้องใช้ฮาร์ดแวร์เฉพาะในการอ่าน PIN ไม่สามารถใช้กับต่างระบบกันได้ และราคาแพง

4. การพิสูจน์ตัวตนโดยใช้ Password Authenticators หรือ Tokens Authenticator หรือ Token เป็นฮาร์ดแวร์พิเศษที่ใช้สร้าง รหัสผ่านซึ่งเปลี่ยนแปลงได้ (Dynamic Password) ในขณะที่กำลังเข้าสู่ระบบเครือข่าย มี 2 วิธี คือ ซิงโครนัสและอะซิงโครนัส

การพิสูจน์ตัวตนแบบซิงโครนัส แบ่งออกเป็น 2 ประเภทตามลักษณะของการใช้งาน คือ

การพิสูจน์ตัวตนแบบซิงโครนัสโดยขึ้นอยู่กับสถานการณ์ (Event-synchronous Authentication) เมื่อผู้ใช้งานต้องการที่จะเข้าสู่ระบบ ผู้ใช้งานจะต้องกด Token เพื่อให้ Token สร้างรหัสผ่านให้ จากนั้นผู้ใช้งานนำรหัสผ่านที่แสดงหลังจากกด Token ใส่ลงในฟอร์ม เพื่อเข้าสู่ระบบ ระบบจะทำการตรวจสอบกับเซิร์ฟเวอร์ก่อนว่ารหัสผ่านที่ใส่มีอยู่ในเซิร์ฟเวอร์จริงจึงจะยินยอมให้ผู้ใช้งานเข้าสู่ระบบ การพิสูจน์ตัวตนแบบซิงโครนัสโดยขึ้นอยู่กับเวลา (Time-synchronous Authentication) เป็นวิธีการที่สร้างรหัสผ่านโดยมีการกำหนดช่วงระยะเวลาการใช้งาน โดยปกติแล้วรหัสผ่านจะถูกเปลี่ยนทุก ๆ หนึ่งนาที การสร้างรหัสผ่าน จะเป็นไปอย่างต่อเนื่อง ทำให้บางครั้งรหัสผ่านที่สร้างออกมาอาจจะซ้ำกันกับรหัสผ่านตัวอื่นที่เคยสร้างมาแล้วก็ได้ เมื่อผู้ใช้งานต้องการเข้าสู่ระบบก็ใส่รหัสผ่านและเวลาที่รหัสผ่านตัวนั้นถูกสร้างขึ้นมา (รหัสผ่านจะถูกสร้างขึ้นมาจาก Token) ลงในฟอร์ม เพื่อเข้าสู่ระบบ ระบบจะทำการตรวจสอบเวลาและรหัสผ่านที่ผู้ใช้งานใส่ลงไป กับเซิร์ฟเวอร์ว่ารหัสผ่านที่ใส่ตรงกับเวลาที่ Token สร้าง และมีอยู่ในเซิร์ฟเวอร์จริงจึงยินยอมให้ผู้ใช้งานเข้าสู่ระบบ

ข้อดี : มีความปลอดภัยมากกว่าการใช้การจำรหัสผ่านแบบธรรมดา ไม่ต้องใช้เครื่องอ่านการ์ด และผู้ที่ละเมิดเข้ามาไม่สามารถจะเข้ามาจู่โจมได้

ข้อเสีย : การใช้งานยุ่งยากกว่าแบบจำรหัสผ่าน และAuthenticator เป็นวัตถุจึงง่ายต่อการสูญหาย และการถูกขโมยได้

การพิสูจน์ตัวตนแบบอะซิงโครนัส หรือเรียกอีกอย่างหนึ่ง ว่า Challenge-response ถูกพัฒนาขึ้นเป็นลำดับแรก ๆ ของระบบการใช้รหัสผ่านซึ่งเปลี่ยนแปลงได้ ซึ่งถือได้ว่าเป็นการป้องกันการจู่โจมที่ปลอดภัยที่สุด เพราะเนื่องจากว่าเมื่อผู้ใช้งานต้องการจะเข้าสู่ระบบ ผู้ใช้งานจะต้องทำการร้องของไปยังเซิร์ฟเวอร์ จากนั้นเซิร์ฟเวอร์ก็จะส่ง Challenge String มาให้ผู้ใช้งาน เพื่อให้ผู้ใช้งานใส่ลงใน Token ที่ผู้ใช้งานถืออยู่ จากนั้น Token จะทำการคำนวณรหัสผ่านออกมาให้ผู้ใช้งาน ผู้ใช้งานจึงสามารถนำรหัสผ่านนั้นใส่ลงในฟอร์มเพื่อเข้าสู่ระบบได้

ข้อดี : มีความปลอดภัยมากกว่าการใช้การจำรหัสผ่านแบบธรรมดา ไม่ต้องใช้เครื่องอ่านการ์ด และเป็นวิธีการป้องกันที่ดีที่สุดเมื่อเปรียบเทียบกับวิธีการใช้การพิสูจน์ตัวตนโดยใช้ Password Authenticators หรือ Tokens

ข้อเสีย : การใช้งานยุ่งยากกว่าแบบจำรหัสผ่าน Authenticator เป็นวัตถุจึงง่ายต่อการสูญหาย และการถูกขโมยได้ไม่สามารถป้องกันผู้ที่ละเมิดเข้ามาในระบบได้ และการใช้งานค่อนข้างยุ่งยากกว่าวิธีการใช้รหัสผ่านซึ่งเปลี่ยนแปลงได้ (Dynamic Password) วิธีอื่น

การพิสูจน์ตัวตนแบบซิงโครนัสทั้งไคลเอ็นต์และเซิร์ฟเวอร์จะมีรหัสผ่านเก็บเอาไว้ แต่แบบอะซิงโครนัส ไคลเอ็นต์จะต้องติดต่อเซิร์ฟเวอร์ก่อน ก่อนจะได้รับรหัสผ่านจริง ทำให้การพิสูจน์ตัวตนแบบอะซิงโครนัสมีขั้นตอนที่ซับซ้อนกว่าแบบซิงโคนัส

5. การพิสูจน์ตัวตนโดยใช้ลักษณะเฉพาะทางชีวภาพของแต่ละบุคคล (Authentication by Biometric Traits) ลักษณะทางชีวภาพของแต่ละบุคคลเป็นลักษณะเฉพาะและลอกเลียนแบบกันไม่ได้ การนำมาใช้ในการพิสูจน์ตัวตนจะเพิ่มความน่าเชื่อถือได้มากขึ้นเช่นการใช้ลายนิ้วมือ เสียง ม่านตา เป็นต้น จึงมีการนำเทคโนโลยีนี้มาช่วยในการพิสูจน์ตัวตน เพื่อเพิ่มความปลอดภัยก่อนเข้าสู่ระบบ เช่น การใช้ควบคู่กับการใช้รหัสผ่านในขั้นตอนของการเก็บหลักฐานทางชีวภาพ ในขั้นแรกระบบจะทำการเก็บภาพของเรตินาจากบุคคลที่ถือ Token การ์ดหรือสมาร์ทการ์ด จากนั้นจะนำภาพเรตินาที่ได้มาแยกแยะเพื่อหาลักษณะเด่นของแต่ละบุคคลเพื่อไม่ให้ซ้ำกับบุคคลอื่น แล้วเก็บไว้เป็น Template ซึ่ง Template ที่ได้จะถูกบันทึกเป็นกุญแจคู่กับรหัสผ่านที่มีอยู่ใน Token การ์ด หรือสมาร์ทการ์ดของแต่ละบุคคล ในขั้นตอนของการตรวจสอบหลักฐานผู้ใช้งานที่ถือ Token การ์ด หรือสมาร์ทการ์ด จะนำบัตรมาผ่านเครื่องอ่านบัตรและแสดงเรตินาให้เครื่องเก็บภาพ เมื่อเครื่องอ่านบัตร อ่านค่าเลขที่ได้จากบัตรแล้ว ก็จะนำไปหากุญแจ ซึ่งในขณะเดียวกันภาพเรตินาที่เครื่องเก็บไว้ได้ ก็จะนำไปแยกแยะเพื่อหาลักษณะเด่น แล้วเก็บค่าไว้เป็น Template และนำ Template ที่ได้ไปตรวจสอบกับ Template ที่เก็บไว้เพื่อหากุญแจ และนำกุญแจที่ได้มาเปรียบเทียบกันว่าตรงกันหรือไม่ ถ้าตรงกันก็แสดงว่าผู้ที่ถือบัตรกับผู้ใช้งานเป็นคนเดียวกัน จึงอนุญาตให้เข้าสู่ระบบ

ข้อดี : มีความปลอดภัยสูงเพราะเลียนแบบกันได้ยาก

ข้อเสีย : ระบบมีความซับซ้อนสูง ยังไม่ได้รับความนิยมกันอย่างแพร่หลาย และค่าใช้จ่ายสูง

6. การพิสูจน์ตัวตนโดยใช้รหัสผ่านที่ใช้เพียงครั้งเดียว One-time Password (OTP) ถูกพัฒนาขึ้นเพื่อหลีกเลี่ยงปัญหาที่เกิดจากการใช้รหัสผ่านเพียงตัวเดียวซ้ำ ๆ กัน OTP จะทำให้ระบบมีความปลอดภัยมากขึ้น เพราะรหัสผ่านจะถูกเปลี่ยนทุกครั้งก่อนที่ผู้ใช้งานจะเข้าสู่ระบบ การทำงานของ OTP คือเมื่อผู้ใช้งานต้องการจะเข้าใช้ระบบ ผู้ใช้งานจะทำการร้องขอไปยังเซิร์ฟเวอร์ จากนั้นเซิร์ฟเวอร์จะส่ง Challenge String กลับมาให้ผู้ใช้งาน จากนั้นผู้ใช้งานจะนำ Challenge String และรหัสลับที่มีอยู่กับตัวของผู้ใช้งานนำไปเข้าแฮชฟังก์ชันแล้วออกมาเป็นค่า Response ผู้ใช้งานก็จะส่งค่านั้นกลับไปยังเซิร์ฟเวอร์ เซิร์ฟเวอร์จะทำการตรวจสอบค่าที่ผู้ใช้งานส่งมาเปรียบเทียบกับค่าที่เซิร์ฟเวอร์เองคำนวณได้ โดยเซิร์ฟเวอร์ก็ใช้วิธีการคำนวณเดียวกันกับผู้ใช้งาน เมื่อได้ค่าที่ตรงกันเซิร์ฟเวอร์ก็จะยอมรับให้ผู้ใช้งานเข้าสู่ระบบ

ข้อดี : ทำให้การเดาหรือขโมยรหัสผ่านเป็นไปได้ยาก

ข้อเสีย : ไม่สะดวกต่อการใช้งาน เพราะผู้ใช้งานต้องจำรหัสผ่านหลายตัว และถ้าผู้ใช้งานจำรหัสผ่านไม่ได้ หรือทำรหัสผ่านสูญหายก็ไม่สามารถเข้าใช้ระบบได้

7. การพิสูจน์ตัวตนโดยการเข้ารหัสโดยใช้กุญแจสาธารณะ (Public-key Cryptography) เป็นการรักษาความปลอดภัยของข้อมูลระหว่างการส่งข้ามเครือข่ายวิธีหนึ่งที่นิยมใช้กันอยู่ในปัจจุบัน การเข้ารหัสแบบคู่รหัสกุญแจนี้จะมีความปลอดภัยมากกว่าการเข้ารหัสข้อมูลแบบธรรมดา แต่ก็ไม่ได้หมายความว่าการเข้ารหัสแบบคู่รหัสกุญแจนี้จะเป็นวิธีที่เหมาะสมที่สุดของวิธีการเข้ารหัส ทั้งนี้ขึ้นอยู่กับประเภทงานของแต่ละองค์กรหรือบุคคล

การเข้ารหัสโดยใช้กุญแจสาธารณะ ประกอบไปด้วยกุญแจ 2 ชนิด ที่ต้องใช้คู่กันเสมอในการเข้ารหัสและถอดรหัส คือ

1. กุญแจสาธารณะ (Public Key) เป็นกุญแจที่ผู้สร้างจะส่งออกไปให้ผู้ใช้งานอื่น ๆ ทราบหรือเปิดเผยได้

2. กุญแจส่วนตัว (Private Key) เป็นกุญแจที่ผู้สร้างจะเก็บไว้ โดยไม่เปิดเผยให้คนอื่นรู้

กระบวนการของการเข้ารหัสแบบคู่รหัสกุญแจ มีดังนี้

2.1) ผู้ใช้งานแต่ละคนจะสร้างคู่รหัสกุญแจของตัวเองขึ้นมา เพื่อใช้สำหรับการเข้ารหัสและการถอดรหัส

2.2) กุญแจสาธารณะจะถูกส่งออกไปยังผู้ใช้งานคนอื่นๆ แต่กุญแจส่วนตัวจะถูกเก็บที่ตนเอง

2.3) เมื่อจะส่งข้อมูลออกไปหาผู้ใช้งานคนใด ข้อมูลที่ส่งจะถูกเข้ารหัสด้วยกุญแจสาธารณะก่อนถูกส่งออกไป

2.4) เมื่อผู้รับได้รับข้อความแล้วจะใช้กุญแจส่วนตัวซึ่งเป็นคู่รหัสกันถอดรหัสออกมา การเข้ารหัสโดยใช้กุญแจสาธารณะสามารถใช้ได้ทั้งในการเข้ารหัส (Encryption) และการพิสูจน์ตัวตน (Authentication)

การประยุกต์ใช้ในการเข้ารหัสข้อมูล (Encryption) เป็นการนำข้อมูลที่จะส่งไปยังผู้รับมาเข้ารหัสด้วยกุญแจสาธารณะของผู้รับ และเมื่อผู้รับได้รับข้อความนั้นแล้วจะถอดรหัสออกมาด้วยกุญแจส่วนตัว จึงจะเห็นได้ว่ามีเพียงผู้รับเท่านั้นที่จะสามารถถอดรหัสออกมาได้

การประยุกต์ใช้ในการพิสูจน์ตัวตน (Authentication) เป็นการนำข้อมูลที่ผู้ส่งต้องการส่งมาเข้ารหัสด้วยกุญแจส่วนตัวของผู้ส่ง แล้วนำข้อมูลนั้นส่งไปยังผู้รับ ซึ่งผู้รับจะใช้กุญแจสาธารณะซึ่งเป็นคู่รหัสกันถอดรหัสออกมา ผู้รับก็สามารถรู้ได้ว่าข้อความนั้นถูกส่งมาจากผู้ส่งคนนั้นจริง ถ้าสามารถถอดรหัสข้อมูลได้อย่างถูกต้อง

ข้อดี : การจัดการกุญแจทำได้ปลอดภัย เพราะใช้กุญแจในการเข้ารหัสและถอดรหัสต่างกัน สามารถระบุผู้ใช้งานโดยการใช้ร่วมกับลายมือชื่ออิเล็กทรอนิกส์

ข้อเสีย :ใช้เวลาในการเข้าและถอดรหัสค่อนข้างนานเพราะต้องใช้การคำนวณอย่างมาก และต้องใช้ระบบที่สนับสนุนการทำงาน

8. การพิสูจน์ตัวตนโดยการใช้ลายเซ็นอิเล็กทรอนิกส์ (Digital Signature) เป็นการนำหลักการของการทำงานของระบบการเข้ารหัสแบบใช้คู่รหัสกุญแจเพื่อการพิสูจน์ตัวตนมาประยุกต์ใช้ระบบของลายเซ็นดิจิตอลสามารถแบ่งเป็นขั้นตอนได้ ดังนี้

เมื่อผู้ใช้งานต้องการจะส่งข้อมูลไปยังผู้รับ ข้อมูลนั้นจะถูกนำไปเข้าฟังก์ชันทางคณิตศาสตร์ที่เรียกว่า แฮชฟังก์ชัน ได้เมสเซจไดเจสต์ (Message Digest) ออกมา

การใช้กุญแจส่วนตัวเข้ารหัสข้อมูล หมายถึงว่าผู้ส่งได้ลงลายเซ็นดิจิตอล ยินยอมที่จะให้ผู้รับสามารถทำการตรวจสอบด้วยกุญแจสาธารณะของผู้ส่งเพื่อพิสูจน์ตัวตนของผู้ส่งได้

การตรวจสอบข้อมูลว่าถูกส่งมาจากผู้ส่งคนนั้นจริงในด้านผู้รับ โดยการนำข้อมูลมาผ่านแฮชฟังก์ชันเพื่อคำนวณหาค่าเมสเซจไดเจสต์ และถอดรหัสลายเซ็นอิเล็กทรอนิกส์ด้วยกุญแจสาธารณะของผู้ส่ง ถ้าสามารถถอดได้อย่างถูกต้อง จะเป็นการยืนยันข้อมูลจากผู้ส่งคนนั้นจริง และถ้าข้อมูลเมสเซจไดเจสต์ที่ได้จากการถอดรหัสเท่ากันกับค่าเมสเซจไดเจสต์ในตอนต้นที่ทำการคำนวณได้ จะถือว่าข้อมูลดังกล่าวนั้นถูกต้อง

ลายเซ็นอิเล็กทรอนิกส์นิยมนำไปใช้ในระบบรักษาความปลอดภัยในการชำระเงินผ่านระบบอินเทอร์เน็ต ซึ่งในปัจจุบันนี้การทำธุรกรรมการเงินอิเล็กทรอนิกส์ได้รับความนิยมเป็นอย่างมาก

ข้อดี : สามารถระบุตัวผู้ส่งได้ชัดเจน ป้องกันข้อมูลถูกแก้ไขระหว่างการส่งได้ หรือสามารถตรวจสอบข้อมูลได้ว่าผ่านการแก้ไขมาหรือไม่

ข้อเสีย : ใช้เวลาในการเข้าและถอดรหัสค่อนข้างนาน เพราะต้องใช้การคำนวณอย่างมาก

9. การพิสูจน์ตัวตนโดยใช้การถาม-ตอบ (Zero-knowledge Proofs) เป็นวิธีการพิสูจน์ตัวตนโดยใช้การถาม-ตอบ เมื่อผู้ใช้งานเข้ามาในระบบแล้ว ระบบจะแน่ใจได้อย่างไรว่าผู้ใช้งานคนนั้น เป็นคนที่ได้รับอนุญาตให้เข้ามาใช้ระบบได้จริง การใช้ชื่อผู้ใช้งานและรหัสผ่านในปัจจุบันนี้ไม่มีความปลอดภัยเพียงพอต่อการเข้าใช้ระบบ เนื่องจากความรู้และวิทยาการที่ก้าวหน้า ทำให้เกิดผู้ที่ต้องการจะเข้ามาละเมิดระบบต่าง ๆ มีมากขึ้น ทำให้ชื่อผู้ใช้งานและรหัสผ่าน อาจจะถูกลักลอบดักข้อมูลระหว่างการสื่อสารกันได้ การที่จะทำให้ระบบมั่นใจได้ว่า ผู้ที่เข้าไปในระบบผู้นั้นเป็นผู้ที่ได้รับอนุญาตจริง นั่นก็คือระบบจะใช้การถาม-ตอบ

ซึ่งคำถามและคำตอบเหล่านี้ ผู้ใช้งานจะเป็นคนสร้างคำถามและคำตอบขึ้นมาเอง จากนั้นจะส่งให้กับเซิร์ฟเวอร์ ซึ่งคำถาม-คำตอบที่ผู้ใช้งานสร้างขึ้นมา ผู้ใช้งานเท่านั้นจะเป็นคนที่ทราบคำตอบของแต่ละคำถามที่ถูกสร้าง และเมื่อผู้ใช้งานคนนั้น ๆ เข้าสู่ระบบได้ ระบบจะถามสุ่มคำถามเหล่านั้นที่ผู้ใช้งานคนนั้น ๆ สร้างขึ้นมา ถามผู้ใช้งานคนนั้น ๆ ก่อนที่จะยอมให้เข้าใช้ระบบได้จริง การให้ใช้ระบบได้จริงจะได้รับการยินยอมก็ต่อเมื่อการตอบคำตอบที่ผู้ใช้งานตอบนั้นสัมพันธ์กับคำตอบที่มีอยู่ในเซิร์ฟเวอร์ วิธีการพิสูจน์ตัวตนวิธีนี้ เป็นวิธีการที่ต้องใช้ความรู้ขั้นสูงในการนำมาใช้ เนื่องจากระบบจะใช้การเรียนรู้จากข้อมูลที่ได้รับ อาจจะเรียกระบบนี้ได้ว่าเป็นการนำความรู้ด้าน AI (Artificial Intelligence) มาใช้

ข้อดี : ความปลอดภัยค่อนข้างสูง เพราะคำถามและคำตอบจะมีเพียงผู้ใช้งาน และเซิร์ฟเวอร์เท่านั้นที่ทราบ

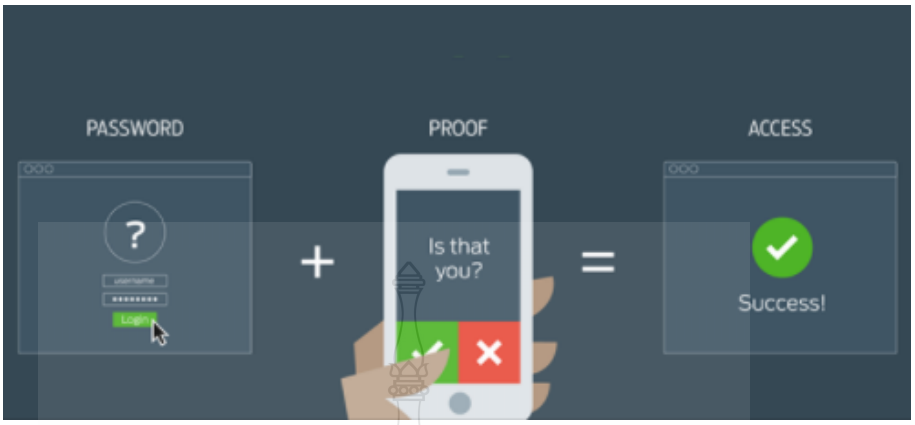
ข้อเสีย : ความปลอดภัยค่อนข้างสูง เพราะคำถามและคำตอบจะมีเพียงผู้ใช้งานและเซิร์ฟเวอร์เท่านั้นที่ทราบ และความซับซ้อนของระบบเพิ่มขึ้นตามความฉลาดของระบบโพรโตคอลในการพิสูจน์ตัวตน (Authentication Protocol) ในระบบเครือข่ายแบบเปิดหรืออินเตอร์เน็ต การพิสูจน์ตัวตนถือได้ว่าเป็นกระบวนการเริ่มต้นและมีความสำคัญที่สุดในการปกป้องเครือข่ายให้ปลอดภัย โพรโตคอลในการพิสูจน์ตัวตนคือโพรโตคอลการสื่อสารที่มีกระบวนการพิสูจน์ตัวตนรวมอยู่ในชุดโพรโตคอล โพรโตคอลหลักของการพิสูจน์ตัวตนที่นิยมใช้อย่างแพร่หลายบนอินเตอร์เน็ตในปัจจุบัน ประกอบไปด้วย

- Secure Socket Layer (SSL)
- Secure Shell (SSH)
- Internet Security (IPSEC)
- Kerberos

การรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ หรือ ระบบเครือข่ายคอมพิวเตอร์เป็นสิ่งที่ควรตระหนักเป็นอย่างยิ่งในปัจจุบัน เพราะโลกในยุคปัจจุบันเป็นโลกแห่งข้อมูลข่าวสาร การเก็บรักษาข้อมูลให้ปลอดภัยจึงเป็นสิ่งสำคัญกับตัวบุคคลและองค์กร เพราะฉะนั้นการที่จะอนุญาตให้บุคคลใดบุคคลหนึ่งสามารถเข้าถึงข้อมูลจึงเป็นสิ่งที่ควรระมัดระวัง เพราะข้อมูลบางอย่างของบุคคลและองค์กรมีความสำคัญและไม่สามารถเปิดเผยต่อบุคคลภายนอกได้

การพิสูจน์ตัวตนจึงมีความสำคัญ เนื่องจากว่าการที่บุคคลใดบุคคลหนึ่งจะเข้าสู่ระบบได้จะต้องได้รับการยอมรับว่าได้รับอนุญาตจริง การตรวจสอบหลักฐานจึงเป็นขั้นตอนแรกก่อนอนุญาตให้เข้าสู่ระบบ การยืนยันตัวตนยิ่งมีความซับซ้อนมาก นั่นก็หมายถึงว่าความปลอดภัยของข้อมูลก็มีมากขึ้นด้วย องค์กรต่าง ๆ จะต้องกระทำสิ่งที่จะเป็นในการปกป้องข้อมูลที่สำคัญ ไม่เพียงแค่ป้องกันการบุกรุกเท่านั้น แต่จะต้องหลีกเลี่ยงผลกระทบที่อาจตามมา

ดังนั้นถ้าหากว่าข้อมูลได้รับการป้องกันนั้นมีความสำคัญอย่างยิ่งต่อความสำเร็จขององค์กรหรือมหาวิทยาลัย ระบบในการตรวจสอบผู้ใช้งานที่มีประสิทธิภาพเป็นสิ่งที่จะต้องพิจารณาอย่างยิ่ง โดยที่มีอยู่หลายวิธีให้เลือกใช้กันในปัจจุบัน ดังนั้นการเลือกวิธีที่นำมาใช้นั้นจะต้องเป็นวิธีที่ให้ความมั่นใจได้เป็นอย่างดี การพิจารณาจะต้องไม่เพียงแค่จะต้องสามารถทำงานได้ในปัจจุบันเท่านั้น แต่วิธีการที่เลือกระบบรักษาความปลอดภัยจะต้องสามารถทำงานได้ดีในอนาคตอีกด้วย



ภาพที่ 3-6 แสดงการพิสูจน์ทราบตัวตน (Authentication) เพื่อขออนุญาตเข้าใช้งานระบบ

สมาคมธนาคารไทย (ก.ค. 2562) ได้ให้ความหมายการพิสูจน์และยืนยันตัวตนด้วยหลายปัจจัย ดังนี้ การพิสูจน์และยืนยันตัวตน (Authentication) เป็นกระบวนการที่ใช้ในการตรวจสอบผู้มีสิทธิ์เข้าใช้บริการทำธุรกรรม หรือใช้ทรัพยากรที่บุคคลนั้นเป็นเจ้าของจริง ซึ่งโดยทั่วไปมักพบกระบวนการพิสูจน์และยืนยันตัวตนในบริการต่าง ๆ ผ่านระบบเครือข่ายอินเทอร์เน็ต เช่นการเข้าถึงบัญชี e-mail หรือบัญชีเครือข่ายสังคมออนไลน์ ส่วนมากจะนิยมใช้ชื่อบัญชีและรหัสผ่าน โดยที่รหัสผ่านที่ตั้งนั้นบางครั้งอาจจะสั้นเกินไป ง่ายเกินไป ใช้รหัสผ่านเดิมเป็นระยะเวลานานเกินไป รวมถึงผู้ประสงค์ร้ายอาจจะล่วงรู้หรือเดารหัสผ่านได้ ทำให้บัญชีผู้ใช้ถูกขโมยได้ ดังนั้นการใช้รหัสผ่านเพียงอย่างเดียวในการพิสูจน์และยืนยันตัวตนจึงไม่เพียงพอในการป้องกันบัญชีผู้ใช้ได้

ประเภทของวิธีการพิสูจน์และยืนยันตัวตน วิธีการพิสูจน์และยืนยันตัวตนแบ่งได้ 3 ประเภท ดังนี้

1. สิ่งที่คุณรู้ (Something you know) เช่น ชื่อบัญชี รหัสผ่าน รหัส PIN เลขที่บัตรประชาชน หรือคำถามคำตอบ ความลับ เป็นต้น

2. สิ่งที่คุณมี (Something you have) เช่น โทรศัพท์มือถือที่ใช้คู่กับ One-time Password (OTP) หรือ Authenticator App รวมถึง Token และ บัตรต่าง ๆ เป็นต้น

3. สิ่งที่คุณเป็น (Something you are) หรืออัตชีวมิติ (Biometric) เช่น ลายนิ้วมือ ฝ่ามือ ม่านตา ใบหน้า เสียง และรวมถึงพฤติกรรมที่ทำประจำด้วย เป็นต้น

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (ส.ค. 2563) ได้ให้ข้อมูลการยืนยันตัวตนทางดิจิทัล (Authentication) ดังนี้

ข้อกำหนดการยืนยันตัวตนทางดิจิทัล (Authentication Requirements)

ข้อกำหนดของการยืนยันตัวตนทางดิจิทัลสำหรับบริการภาครัฐ ให้เป็นไปตามข้อเสนอแนะมาตรฐาน ด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ว่าด้วยแนวทาง

การใช้ดิจิทัลไอดีสำหรับประเทศไทย การยืนยันตัวตนระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (Authenticator Assurance Level) โดยปัจจัยของการยืนยันตัวตน (Authentication Factor) มีรายละเอียดตามแนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัล เรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ สิ่งที่ใช้ยืนยันตัวตน (Authenticator)

ระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน (Authenticator Assurance Level: AAL) ระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน คือ ระดับความเข้มงวดในกระบวนการยืนยันตัวตนของผู้ใช้บริการ ซึ่งการกำหนดระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตนที่เหมาะสมจะช่วยลดโอกาสของการยืนยันตัวตนผิดพลาด แบ่งออกเป็น 3 ระดับ ดังนี้

(1) ระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน ระดับที่ 1 (AAL1) กำหนดให้ผู้ใช้บริการต้องยืนยันตัวตนแบบปัจจัยเดียว (Single-factor Authentication) เป็นอย่างน้อย หรือหากต้องการความมั่นคงปลอดภัยที่สูงขึ้น สามารถยืนยันตัวตนแบบหลายปัจจัยได้ (Multi-factor Authentication) และต้องเป็นโพรโทคอลที่มีความปลอดภัย (Secure Authentication Protocol) เหมาะสำหรับบริการภาครัฐที่มีความเสี่ยงต่ำ

(2) ระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน ระดับที่ 2 (AAL2) กำหนดให้ผู้ใช้บริการต้องยืนยันตัวตนแบบ 2 ปัจจัยที่แตกต่างกัน ซึ่งอาจเป็นสิ่งที่ใช้ยืนยันตัวตนหลายปัจจัย (Multi-factor Authenticator) เช่น อุปกรณ์ OTP แบบหลายปัจจัย (Multi-factor OTP Device) ซึ่งจะสร้างรหัสผ่านแบบใช้ครั้งเดียว หลังจากตรวจสอบลายนิ้วมือของผู้ใช้บริการ หรือสิ่งที่ใช้ ยืนยันตัวตนแบบปัจจัยเดียว (Single-factor Authenticator) อย่างน้อย 2 สิ่งที่เป็นปัจจัยต่างกัน โดยที่ต้องเป็นรหัสลับจดจำ (Something you know) และเป็นสิ่งที่ผู้ใช้บริการครอบครอง (Something you have) เช่น การใช้รหัสผ่านควบคู่กับการใช้ OTP ผ่านหมายเลขโทรศัพท์ โดยโพรโทคอลที่ใช้รับส่งข้อมูลระหว่าง ผู้ใช้บริการและผู้พิสูจน์และยืนยันตัวตนต้องเป็นโพรโทคอลที่มีความปลอดภัย เหมาะสำหรับบริการภาครัฐที่มีความเสี่ยงปานกลางถึงความเสี่ยงสูง

(3) ระดับความน่าเชื่อถือของสิ่งที่ใช้ยืนยันตัวตน ระดับที่ 3 (AAL3) กำหนดให้ผู้ใช้บริการต้องยืนยันตัวตนแบบ 2 ปัจจัยขึ้นไปที่แตกต่างกัน โดยมีปัจจัยหนึ่งเป็น กุญแจ (Key) ที่ผ่านเกณฑ์วิธีการเข้ารหัสลับ (Cryptographic Protocol) ซึ่งผู้ใช้บริการต้องพิสูจน์ว่าตนครอบครองกุญแจนั้น และต้องพิสูจน์ว่าตนครอบครองปัจจัยของการยืนยันตัวตนดังกล่าวผ่านโพรโทคอลที่มีความปลอดภัยในการใช้รับส่งข้อมูลระหว่างผู้ใช้บริการและผู้พิสูจน์และยืนยันตัวตน และต้องมีการเข้ารหัสข้อมูลส่วนบุคคลหรือข้อมูลอ่อนไหว รวมถึงสิ่งที่ใช้ยืนยันตัวตนเพื่อป้องกันการปลอมแปลงเหมาะสำหรับบริการภาครัฐที่มีความเสี่ยงสูง

กล่าวโดยสรุป การกำหนดสิทธิ์การเข้าถึงข้อมูล คือ การควบคุมการเข้าถึงข้อมูลของผู้ใช้งานผ่านการกำหนดรหัสผ่าน หรือการปิดสิทธิ์ไม่ให้ผู้ใช้งานเห็นข้อมูลนั้น ๆ การกำหนดขึ้นอยู่กับระดับความสำคัญและหน้าที่การทำงานของแต่ละบุคคล หนึ่งวิธีที่ช่วยลดปัญหาความยุ่งยากที่เกิดจากการทำงาน คือ "การกำหนดสิทธิ์" การเข้าถึงข้อมูลเป็นวิธีช่วยลดขั้นตอนการทำงานของพนักงานและทำให้การทำงานเป็นระบบ อีกทั้งยังทำให้การเข้าถึงข้อมูลมีความปลอดภัยมากยิ่งขึ้น

3.4 วิธีการให้บริการกับผู้รับบริการมีความพึงพอใจ

ความพึงพอใจเป็นปัจจัยที่สำคัญประการหนึ่งที่มีผลต่อความสำเร็จของงานให้บรรลุเป้าหมาย ที่วางไว้อย่างมีประสิทธิภาพ อันเป็นผลจากการได้รับการตอบสนองต่อแรงจูงใจหรือความต้องการของแต่ละบุคคลในการใช้บริการ

ความพึงพอใจ (Satisfaction) หมายถึง ระดับความรู้สึกของผู้ใช้งานที่มีผลมาจากการเปรียบเทียบระหว่างสิ่งที่ได้รับกับสิ่งที่คาดหวัง ระดับความพึงพอใจของผู้ใช้งานเกิดจากความแตกต่างระหว่างสิ่งที่ได้รับกับสิ่งที่คาดหวัง (รัตนาภรณ์ ศรีหาพล, รอปี มิง แมะเราะ:2556) ซึ่งหากพิจารณาถึง ความพึงพอใจ ของการบริการว่าจะเกิดความพึงพอใจมากน้อยเพียงใดถ้าได้รับการบริการต่ำกว่าความคาดหวัง ทำให้เกิดความไม่พอใจ แต่ถ้าระดับผลของการบริการเท่ากับความคาดหวังก็จะทำให้เกิดความพึงพอใจ แต่ถ้าผลที่ได้รับจากบริการสูงกว่าความคาดหวังผู้ใช้งานก็จะเกิดความประทับใจก็จะส่งผลให้ผู้ใช้งาน กลับไปใช้บริการซ้ำอีก

จึงกล่าวได้ว่าความพึงพอใจในบริการ หมายความถึง ภาวะการแสดงออกถึงความรู้สึกในทางบวกของบุคคลอันเป็นผลมาจากการเปรียบเทียบการรับรู้สิ่งที่ได้รับจากการบริการ ไม่ว่าจะเป็นการรับบริการหรือการให้บริการในระดับที่ตรงกับการรับรู้สิ่งที่คาดหวังเกี่ยวกับการบริการนั้น ซึ่งจะเกี่ยวข้องกับความพึงพอใจของผู้รับบริการและความพึงพอใจในงานของผู้ให้บริการ

ระดับความพึงพอใจของผู้รับบริการ สามารถแบ่งออกเป็น 2 ระดับ คือ

ระดับที่ 1 ความพึงพอใจที่ตรงกับความคาดหวังเป็นการแสดงความรู้สึกยินดี มีความสุขของผู้รับบริการเมื่อได้รับการบริการที่ตรงกับความคาดหวังที่มีอยู่

ระดับที่ 2 ความพึงพอใจที่เกินความคาดหวังเป็นการแสดงความรู้สึกปลาบปลื้มใจหรือประทับใจของผู้รับบริการเมื่อได้รับการบริการที่เกินความคาดหวังที่มีอยู่

จากความหมายที่กล่าวมาข้างต้นสรุปได้ว่า “ความพึงพอใจ” หมายถึง ความรู้สึก หรือทัศนคติของบุคคลที่มีต่อสิ่งหนึ่งหรือปัจจัยใดปัจจัยหนึ่งที่เกี่ยวข้องกับความรู้สึกพอใจ ที่เป็น การยอมรับ ความรู้สึกชอบ เกิดความสบายใจความรู้สึกที่ยินดีกับการปฏิบัติงาน ทั้งการให้บริการและการรับบริการในทุกสถานการณ์ทุกสถานที่ซึ่งความรู้สึกนี้จะเกิดขึ้นเมื่อความต้องการของบุคคลได้รับการตอบสนองตามที่ตนคาดหวังหรือบรรลุตามจุดมุ่งหมายระดับใดระดับหนึ่ง

สำหรับวิธีการให้บริการกับผู้รับบริการเกิดความพึงพอใจในการปฏิบัติงานของผู้เขียน ในฐานะที่เป็นบุคลากรของมหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี มีวิธีการให้ผู้รับบริการมีความพึงพอใจ โดยยึดหลักความพอใจของผู้ใช้งาน (User Satisfaction) ดังต่อไปนี้

1. ผู้ปฏิบัติงานต้องปฏิบัติงานให้เป็นไปตามหลักเกณฑ์และวิธีการปฏิบัติงาน ของมหาวิทยาลัย

2. ผู้ปฏิบัติงานต้องปฏิบัติงานด้วยความตั้งใจอุตสาหะ รอบคอบ ซื่อสัตย์ รักษาผลประโยชน์ รวมทั้งรักษาความลับของมหาวิทยาลัยและสำนักฯ โดยไม่ให้เกิดข้อมูลรั่วไหลที่จะส่งผลทางด้านลบให้แก่มหาวิทยาลัยและสำนักฯ

3. ผู้ปฏิบัติงานต้องปฏิบัติงานด้วยทัศนคติเชิงบวก มีความสมัครสมานสามัคคี ช่วยเหลือระหว่างบุคลากร เจ้าหน้าที่บุคลากร และผู้ปฏิบัติงานอื่นที่ไม่ใช่หน่วยงานของตน

4. ผู้ปฏิบัติงานต้องให้การต้อนรับแก่ผู้มาติดต่องานที่เกี่ยวกับหน้าที่ของตน โดยให้ความสะดวก ให้ความเป็นธรรมไม่โอนเอียงฝักใฝ่ฝ่ายใด หรือพวกพ้องของตนเอง

5. ผู้ปฏิบัติงานต้องให้คำปรึกษา แนะนำ และให้ข้อมูลด้วยความเต็มใจที่แสดงผ่านทางกิริยาท่าทาง การเปล่งเสียง คำพูด สีหน้า ทั้งภาษากาย (Nonverbal Communication) และภาษาพูด (Verbal Communication)

6. ผู้ปฏิบัติงานต้องมีความเชี่ยวชาญในงานของตน เพื่อสามารถให้ข้อมูล คำปรึกษาแนะนำได้อย่างถูกต้อง ข้อมูลที่ดีจะต้องมีความถูกต้องและปราศจากความคลาดเคลื่อน โดยที่ความถูกต้องจะช่วยส่งเสริมให้สารสนเทศที่ได้มาเกิดความน่าเชื่อถือมากขึ้น เช่น ข้อมูลที่ถูกป้อนเข้าไปในระบบสารสนเทศเกิดความผิดพลาดหรือมีข้อบกพร่อง อาจจะส่งผลให้สารสนเทศที่ได้มีความผิดพลาด หรือไม่สามารถนำไปใช้ประโยชน์ได้อย่างสมบูรณ์

7. ผู้ปฏิบัติงานต้องมีความรวดเร็วในการให้บริการ ทันต่อเวลา ข้อมูลจะต้องทันต่อเหตุการณ์และไม่ล้าสมัย ความล้าสมัยของข้อมูลทำให้สารสนเทศที่ได้มีประโยชน์ต่อผู้ใช้งานน้อยลง หรือไม่เป็นประโยชน์ต่อการใช้งานเลย แต่ความทันต่อเวลาจะมีความสำคัญต่อผู้ใช้งานมากหรือน้อยขึ้นอยู่กับประเภทหรือปัญหาของหน่วยงานและคณะ

8. ผู้ปฏิบัติงานต้องแน่ใจได้ว่าในระบบที่ดูแลมีข้อมูลที่สอดคล้องกับงานของผู้รับบริการ เช่น สารสนเทศที่เป็นประโยชน์ต่อผู้บริหารต้องได้มาจากการประมวลผลของข้อมูลที่มีสาระตรงกัน หรือสัมพันธ์กับปัญหาของงาน ข้อมูลที่ไม่มีความสัมพันธ์กับงาน ถึงแม้จะเป็นข้อมูลที่มีความถูกต้อง เชื่อถือได้ และทันต่อเหตุการณ์แต่ก็จัดว่าไม่มีคุณภาพ เนื่องจากไม่สามารถนำไปประกอบการตัดสินใจหรือไม่สอดคล้องกับความต้องการของงาน

9. ผู้ปฏิบัติงานต้องตรวจสอบความถูกต้อง และความน่าเชื่อถือได้ของสารสนเทศก่อนการนำมาใช้งาน มิเช่นนั้น อาจก่อให้เกิดผลเสียขึ้นกับมหาวิทยาลัยโดยข้อมูลที่ได้ไปต้องสามารถตรวจสอบได้ ข้อมูลบางประเภทอาจมาจากแหล่งข้อมูลที่ซับซ้อนและหลากหลาย ทั้งจากภายนอกและภายในมหาวิทยาลัย

10. ผู้ปฏิบัติงานต้องเป็นผู้ที่สามารถเก็บรักษาความลับของข้อมูลบุคลากรได้เป็นอย่างดี เพื่อรักษาไว้ซึ่งชื่อเสียงและผลประโยชน์ของบุคลากรและผู้รับบริการ เช่น รหัสบัตรประชาชน เงือนเดือน เชื้อชาติ ฯลฯ

11. ผู้ปฏิบัติงานต้องมีทักษะการเจรจาต่อรองในการประสานงาน ลดความขัดแย้งที่อาจจะเกิดขึ้นในการปฏิบัติงาน และต้องเป็นผู้ที่สามารถแก้ไขปัญหาให้กับผู้รับบริการให้เกิดความพึงพอใจได้

12. ผู้ปฏิบัติงานควรรับฟังความคิดเห็นและข้อเสนอแนะจากผู้รับบริการ เพื่อนำมาแก้ไขปรับปรุงและพัฒนาในการปฏิบัติงานที่ดียิ่งขึ้น

ทั้งนี้ วิธีการให้บริการกับผู้รับบริการมีความพึงพอใจข้างต้น สอดคล้องกับจรรยาบรรณของบุคลากรมหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี ตามข้อบังคับมหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี ว่าด้วยจรรยาบรรณของข้าราชการและบุคลากรของมหาวิทยาลัย พ.ศ. 2552 ซึ่งจะกล่าวในหัวข้อต่อไป

3.5 วิธีการติดตามและประเมินผลการปฏิบัติงาน

วิธีการติดตามการปฏิบัติงาน กำหนดสิทธิ์และยกเลิกสิทธิ์การเข้าใช้งานระบบบริหารงานบุคลากรและเงินเดือน มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี มีวิธีการติดตามและประเมินผลการปฏิบัติงาน 3 ระดับ ดังนี้

1. ระดับส่วนงานภายในมหาวิทยาลัย ซึ่งหมายถึง หน่วยงาน/คณะ ทั้งในส่วนของการกำหนดสิทธิ์ และยกเลิกสิทธิ์ในระบบบริหารงานบุคลากรและเงินเดือน ผู้เขียนจะทำหนังสือแจ้งผลเปลี่ยนแปลง ตอบกลับไปยังหน่วยงาน/คณะทราบ และตรวจสอบการเข้าใช้งานระบบได้ที่ https://hr.rmutt.ac.th/vncaller/applications.aspx หากติดปัญหาสามารถสอบถามรายละเอียดเพิ่มเติมได้ที่ ฝ่ายบริการศูนย์ข้อมูลและสารสนเทศ โทร. 02 549 4442

2. ระดับหน่วยงาน ซึ่งหมายถึง กองบริหารงานบุคคล หากมีการแก้ไขหรือเปลี่ยนแปลงสิทธิ์ผู้ดูแลระบบบริหารงานบุคลากรและเงินเดือน สามารถแจ้งผ่านทางช่องทาง e-mail: isc@rmutt.ac.th หรือ ระบบแจ้งซ่อมออนไลน์ https://helpdesk.rmutt.ac.th โดยเลือกประเภทการให้บริการ “แจ้งปัญหาเกี่ยวกับระบบ HR” หากดำเนินการเสร็จแล้วผู้เขียนจะส่ง e-mail แจ้งผลการดำเนินกลับพร้อมแนบลิงค์แบบประเมินความพึงพอใจของผู้ขอใช้บริการ และแบบประเมินความพึงพอใจการใช้งานระบบสารสนเทศ ผ่านช่องทาง e-mail: isc@rmutt.ac.th หรือ ผู้ใช้งานสามารถเข้าไปประเมินออนไลน์ผ่านหน้าระบบบริหารงานบุคลากรและเงินเดือน

3. ระดับบุคคล ซึ่งหมายถึง เจ้าหน้าที่บุคลากรหน่วยงาน/คณะ หากมีการดำเนินการกำหนดสิทธิ์ยกเลิกสิทธิ์ และติดตั้งระบบบริหารงานบุคลากรและเงินเดือน เสร็จแล้วผู้เขียนจะส่งคู่มือการใช้งานพร้อมแนบลิงค์แบบประเมินความพึงพอใจของผู้ขอใช้บริการ และแบบประเมินความพึงพอใจการใช้งาน

ระบบสารสนเทศ ผ่านช่องทาง e-mail: isc@rmutt.ac.th หรือ ผู้ใช้งานสามารถเข้าไปประเมินออนไลน์ผ่านหน้าระบบบริหารงานบุคลากรและเงินเดือน

ทั้งนี้ การติดตามและประเมินผลการปฏิบัติงาน ที่กล่าวมาข้างต้นนี้ ผู้เขียนสามารถติดตามการดำเนินงานโดยมีลายลักษณ์อักษร และสรุปประเมินผลการปฏิบัติงานทั้งทางด้านความพึงพอใจในของผู้ขอใช้บริการและด้านระบบสารสนเทศ เพื่อนำมาแก้ไขปรับปรุงและพัฒนาในการปฏิบัติงานที่ดียิ่งขึ้น

3.6 จริยธรรมและจรรยาบรรณในการปฏิบัติงาน

มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี (2552) ได้กำหนดจรรยาบรรณของข้าราชการและบุคลากรของมหาวิทยาลัยฯ โดยมีรายละเอียดดังนี้

3.6.1 จรรยาบรรณต่อตนเอง

3.6.1.1 มีศีลธรรมอันดีและประพฤติตนให้เหมาะสมกับการเป็นข้าราชการ

3.6.1.2 มีทัศนคติที่ดีและพัฒนาตนเองให้มีคุณธรรมจริยธรรมรวมทั้งเพิ่มพูนความรู้ความสามารถและทักษะในการทำงานเพื่อให้การปฏิบัติหน้าที่มีประสิทธิ์ภาพ ประสิทธิผลยิ่งขึ้น

3.6.1.3 ไม่นำผลงานทางวิชาการของผู้เป็นของตนโดยมิชอบ

3.6.1.4 ไม่ละเมิดทรพย์สินทางปัญญาของผู้อื่น

3.6.2 จรรยาบรรณต่อวิชาชีพ

3.6.2.1 ใช้วิชาชีพในการปฏิบัติหน้าที่ด้วยความซื่อสัตย์สุจริต

3.6.2.2 ปฏิบัติตามจรรยาวิชาชีพที่กำหนดไว้

3.6.3 จรรยาบรรณต่อการปฏิบัติงาน

3.6.3.1 ไม่แสวงหาประโยชน์อันเป็นอามิสสินจ้างจากผู้อื่นในการปฏิบัติหน้าที่ และไม่กระทำการใดอันเป็นการหาประโยชน์ให้แก่ตนโดยมิชอบ

3.6.3.2 ปฏิบัติหน้าที่ด้วยความสุจริต เสมอภาค และปราจากอคติ

3.6.3.3 ไม่ละทิ้งหน้าที่ราชการ ไม่ปฏิบัติหรือละเว้นการปฏิบัติหน้าที่โดยมิชอบ เพื่อให้ตนเองหรือผู้อื่นได้รับประโยชน์ที่มิควรได้

3.6.4 จรรยาบรรณต่อหน่วยงาน

3.6.4 1 ปฏิบัติหน้าที่อย่างเต็มกำลังความสามารถ รอบคอบ รวดเร็ว ขยันหมั่นเพียร ถูกต้อง สมเหตุ สมผล โดยคำนึงถึงประโยชน์ของทางราชการและประชาชนเป็นสำคัญ

3.6.4 2 ประพฤติตนเป็นผู้ตรงต่อเวลาและใช้เวลาในการปฏิบัติหน้าที่ให้เป็นประโยชน์ต่อราชการอย่างเต็มที่

3.6.4.3 ดูแลรักษาและใช้ทรัพย์สินของทางราชกรอย่างประหยัดคุ้มค่า โดยระมัดระวังมิให้เสียหายหรือสิ้นเปลือง

3.6.4.4 รักษาเกียรติภูมิของมหาวิทยาลัยโดยไม่กระทำการใดอันเป็นที่เสื่อมเสียต่อชื่อเสียง และภาพพจน์ของทางมหาวิทยาลัย

3.6.5 จรรยาบรรณต่อผู้บังคับบัญชา ผู้ใต้บังคับบัญชาและผู้ร่วมงาน

3.6.5.1 มีความรับผิดชอบในการปฏิบัติงาน การให้ความร่วมมือกับผู้บังคับบัญชาทั้งในด้านการให้ความคิดเห็น การช่วยทำงานและการแก้ปัญหาร่วมกัน

3.6.5.2 ข้าราชการซึ่งเป็นผู้บังคับบัญชา พึงดูแลเอาใจใส่ผู้ใต้บังคับบัญชา ทั้งในด้านการปฏิบัติงาน ขวัญกำลังใจ และยอมรับฟังความคิดเห็นของผู้อยู่ใต้บังคับบัญชา ตลอดจนบริหารด้วยหลักการและเหตุผลที่ถูกต้องตามทำนองคลองธรรม

3.6.5.3 ช่วยเหลือเกื้อกูลในทางที่ชอบ รวมทั้งส่งเสริมและสนับสนุนให้เกิดความสามัคคีร่วมแรงร่วมใจกับบรรดาเพื่อนร่วมงานในการปฏิบัติหน้าที่เพื่อประโยชน์ส่วนรวม

3.6.5.4 พึงปฏิบัติต่อเพื่อนร่วมงานตลอดจนผู้เกี่ยวข้องด้วยความสุภาพ มีน้ำใจและมนุษย์สัมพันธ์อันดี

3.6.5.5 ไม่ล่วงละเมิดทางเพศ หรือความสัมพันธ์ทางเพศกับผู้ซึ่งมิใช่คู่สมรสของตน

3.6.6 จรรยาบรรณต่อนักศึกษาและผู้รับบริการ

3.6.6.1 ไม่เรียกรับหรือยอมรับทรัพย์สินหรือประโยชน์อื่นใดจักนักศึกษาและผู้รับบริการ เพื่อทำกระทำการหรือไม่กระทำการใด

3.6.6.2 ไม่เปิดเผยความลับของนักศึกษาและผู้รับบริการที่ได้มาจากการปฏิบัติหน้าที่หรือจากความไว้วางใจ และก่อให้เกิดเสียหายแก่นักศึกษาและผู้รับบริการ

3.6.6.3 ไม่สอนหรืออบรมนักศึกษาให้กระทำการที่รู้อยู่ว่าผิดกฎหมาย หรือฝ่าฝืนศีลธรรมอันดีของประชาชน

สำหรับตำแหน่งเจ้าหน้าที่บริหารงานทั่วไป ที่มีหน้าที่ในการจัดการระบบบริหารบุคลากรและเงินเดือน มีส่วนเกี่ยวข้องกับกองบริหารงานบุคคลในการดูแลข้อมูลบุคลากร ในมหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี ซึ่งต้องพึงมีจรรยาบรรณวิชาชีพการบริหารทรัพยากรบุคคล คือประมวลความประพฤติที่ผู้ประกอบวิชาชีพนี้กำหนดขึ้นทั้งที่เป็นและไม่เป็นลายลักษณ์อักษร เพื่อรักษาและส่งเสริมเกียรติคุณ ศักดิ์ศรี ชื่อเสียง และฐานะของสมาชิกและผู้ประกอบวิชาชีพนี้ (กรมสุขภาพจิต, มาตรฐานทางจรรยาบรรณและจรรณยาบรรณทางวิชาชีพบุคลากร: 2562) ประกอบด้วย ดังนี้

1. สุจริต เป็นธรรม ปราศจากอคติ และไม่เลือกปฏิบัติ (Integrity, Legality and Non-Discrimination) ความหมาย ปฏิบัติหน้าที่ด้วยความซื่อสัตย์ สุจริต ไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึง

ข้อมูลของผู้ใช้งานโดยไม่มีเหตุผลอันสมควร โดยนึกถึงประโยชน์ส่วนรวมเหนือประโยชน์ส่วนตน และปฏิบัติตามหน้าที่ตามกฎหมาย กฎระเบียบอย่างตรงไปตรงมา โดยยึดมั่นในหลักวิชาการและหลักคุณธรรมเพื่อผลสัมฤทธิ์ของงาน หรือประโยชน์ที่ดีต่อองค์กรและส่วนรวมรวมทั้งปฏิบัติงาน หรือให้การส่งเสริมการบริหารทรัพยากรบุคคล โดยปราศจากอคติหรือการเลือกปฏิบัติใด ๆ โดยไม่คำนึงถึง เพศ ฐานะ เชื้อชาติ ศาสนา สังคม และการเมือง

2. พัฒนาความรู้ ความสามารถไปสู่ความเป็นเลิศในวิชาชีพ (Self-Development and Proficiency) ความหมาย รอบรู้เท่าทันการเปลี่ยนแปลงเทคโนโลยีหรือการพัฒนาองค์ความรู้ด้านการบริหารจัดการใหม่ ๆ ในวิชาชีพ เพื่อรักษามาตรฐานความสามารถทางวิชาชีพและพัฒนาความรู้ความสามารถ ทักษะและสมรรถนะในการประกอบวิชาชีพ รวมถึงการเพิ่มผลิตภาพของงาน (Productivity) ตลอดจนการสร้างแรงผลักดันและกระตุ้นให้เกิดการเปลี่ยนแปลง

3. เคารพและรักษาความลับและเปิดเผยข้อมูลส่วนบุคคลอย่างเหมาะสม เพื่อประโยชน์ต่อการบริหารทรัพยากรบุคคล (Confidentiality and Information Sharing) ความหมาย ตระหนักและมีวิจารณญาณในการจัดลำดับความสำคัญของข้อมูลรักษาความลับ และแลกเปลี่ยนหรือเปิดเผยข้อมูลให้แก่ผู้ที่จำเป็นต้องได้รับรู้ข้อมูลนั้น เพื่อประโยชน์ในการทำงานและการตัดสินใจ ไม่ใช้หรือเปิดเผยข้อมูลส่วนบุคคลและข้อมูลองค์การโดยมิชอบ ยกเว้นเป็นการปฏิบัติตามหน้าที่หรือได้รับความเห็นชอบ ไม่ใช้หรือแสวงหาประโยชน์อันมิชอบจากการเข้าถึงข้อมูลขององค์การ เนื่องจากการดำรงตำแหน่ง หรือหน้าที่งานของตนเอง และจะต้องพึงระวังและคำนึงถึงลิขสิทธิ์ของข้อมูลก่อนเปิดเผยข้อมูลส่วนบุคคล และองค์กรแก่ผู้อื่น

4. ดำรงตนเป็นแบบอย่างด้านจรรยาบรรณวิชาชีพการบริหารทรัพยากรบุคคล (Ethics Role Model) ความหมาย ประพฤติตนให้เป็นแบบอย่างต่อผู้อื่น รวมทั้งมีบทบาทในการสร้างเสริมและผลักดันให้เกิดวัฒนธรรมหรือค่านิยมจริยธรรมขึ้นในองค์กร

5. บริหารจัดการทรัพยากรบุคคล โดยปราศจากผลประโยชน์แอบแฝง (Conf Lict of Interests and Opportunistic Benefits) ความหมาย การตัดสินใจหรือการปฏิบัติงานในหน้าที่ในด้านของการบริหารทรัพยากรบุคคลจะต้องเป็นไปเพื่อประโยชน์สูงสุดขององค์กรเท่านั้น การบรรลุผลจากการตัดสินใจดังกล่าว จะต้องปลอดจากอิทธิพลของความต้องการส่วนตัวของครอบครัวหรือของพวกพ้อง

6. ความรับผิดชอบเมื่อพ้นสภาพจากองค์การ จะต้องไม่แสวงประโยชน์จากการดำรงตำแหน่งเพื่อวางแผน หรือได้มาซึ่งตำแหน่งที่ดีกว่าในองค์การอื่นที่มีผลประโยชน์ขัดกัน และไม่เปิดเผยความลับและข้อมูลขององค์การเดิมในทางมิชอบ

7. การประพฤติผิดจรรยาบรรณ อาจนำไปสู่การพิจารณาลงโทษสถานเบา หรือสถานหนักได้

และผู้เขียนยังหยิบยกแนวคิดเพื่อการทำงานให้มีความสุขตามวิถีพุทธศาสนาคือ การนำธรรมะหรือหลักธรรมทางพระพุทธศาสนา มาประยุกต์ใช้ในการปฏิบัติงาน สร้างบรรยากาศการทำงานโดยให้แต่ละคนต่างรู้หน้าที่ของตนเอง ซึ่งธรรมะที่เหมาะสำหรับผู้ปฏิบัติงาน นั่นคือ “อิทธิบาท 4” ซึ่งหมายถึง ธรรมแห่งความสำเร็จประกอบด้วย ฉันทะหรือ ความพอใจ หมายถึง ผู้ปฏิบัติงานต้องชอบหรือศรัทธางานที่ทำอยู่ และมีความสุข

กับงานที่ได้รับมอบหมาย วิริยะ หรือ ความพากเพียร ผู้ปฏิบัติงานจะต้องมีความขยันหมั่นเพียรในการทำงานที่ได้รับมอบหมาย รวมทั้งหมั่นฝึกตนเองอย่างต่อเนื่อง เพื่อให้การทำงานมีประสิทธิภาพมากขึ้น จิตตะ หรือ ความเอาใจใส่ หมายถึง ผู้ปฏิบัติงานจะต้องมีจิตใจหรือสมาธิจดจ่อกับงานที่ทำ รวมถึงมีความรอบคอบและความรับผิดชอบในงานที่ทำอย่างเต็มสติกำลัง และ วิมังสา หรือ ความหมั่นตริตรองพิจารณาหาเหตุผลในงานที่ทำ ทำงานด้วยปัญญา ด้วยสมองคิด รวมถึงเข้าใจในงานอย่างลึกซึ้ง ทั้งในแง่ขั้นตอนและผลสำเร็จหรือผลสัมฤทธิ์ของงาน

กล่าวโดยสรุปในภาพรวมบทที่ 3 มีรายละเอียดเกี่ยวกับหลักเกณฑ์วิธีการปฏิบัติงาน วิธีการปฏิบัติงาน แนวปฏิบัติและข้อควรระวังในการปฏิบัติงาน แนวคิด/งายวิจัยที่เกี่ยวข้อง วิธีการให้บริการกับผู้รับบริการมีความพึงพอใจ วิธีการติดตามและประเมินผลการปฏิบัติงาน และจริยธรรมและจรรยาบรรณในการปฏิบัติงาน ในแต่ละหัวข้อที่กล่าวมาผู้เขียนได้พยายามศึกษา รวบรวม และอธิบายรายละเอียดเกี่ยวกับหลักเกณฑ์วิธีการปฏิบัติงานและเงื่อนไขต่าง ๆ ในการกำหนดสิทธิ์ และยกเลิกสิทธิ์การเข้าใช้งานระบบบริหารงานบุคลากรและเงินเดือน ซึ่งเกิดจากการเรียนรู้ และประสบการณ์ในการปฏิบัติงานสำหรับกระบวนการและขั้นตอนกำหนดสิทธิ์ และยกเลิกสิทธิ์การเข้าใช้งานระบบบริหารงานบุคลากรและเงินเดือน ผู้เขียนจะกล่าวถึงในบทที่ 4 ต่อไป

บทที่ 4

กระบวนการและขั้นตอนการปฏิบัติงาน

เนื้อหาในบทที่ 4 กระบวนการและขั้นตอนการปฏิบัติงาน ประกอบด้วย แผนผังการปฏิบัติงาน (Work Flow) รายละเอียดของกระบวนการและขั้นตอนการปฏิบัติงาน กิจกรรม แผนการปฏิบัติงาน และกลยุทธ์ในการปฏิบัติงาน ที่แสดงให้เห็นถึงความชัดเจนของกระบวนการและขั้นตอนของการกำหนดสิทธิ์และยกเลิกสิทธิ์ของระบบบริหารงานบุคลากรและเงินเดือน สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี

4.1 ขั้นตอนการปฏิบัติงาน

กระบวนการปฏิบัติงานในการกำหนดสิทธิ์ และยกเลิกสิทธิ์ ของระบบบริหารงานบุคลากรและเงินเดือน สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี ผู้จัดทำคู่มือจะอธิบายโดยจะเขียนรายละเอียดของแต่ละแผนผังการปฏิบัติงาน (Work Flow) ในลำดับถัดไป และให้ผู้ปฏิบัติงานสามารถเข้าใจแผนผังการปฏิบัติงาน (Work Flow) ได้ดียิ่งขึ้น เพื่อให้เกิดความเข้าใจตรงกันและถูกต้องตามขั้นตอนที่ก่อให้เกิดความสะดวกรวดเร็วในการปฏิบัติงาน ผู้จัดทำคู่มือจึงกำหนดกระบวนการการปฏิบัติงาน ดังนี้

4.1.1 การทวนสอบประเภทกลุ่มสิทธิ์

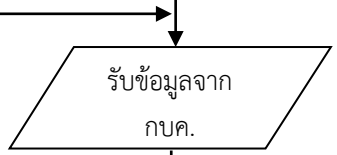
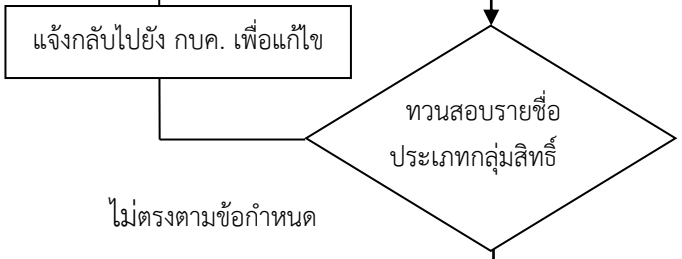
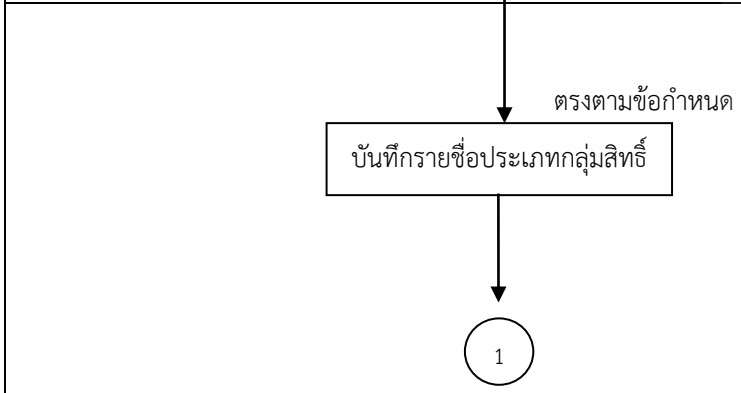
4.1.2 การทวนสอบสิทธิ์ของผู้ใช้งาน

4.1.3 การกำหนดสิทธิ์ของระบบบริหารงานบุคลากรและเงินเดือน

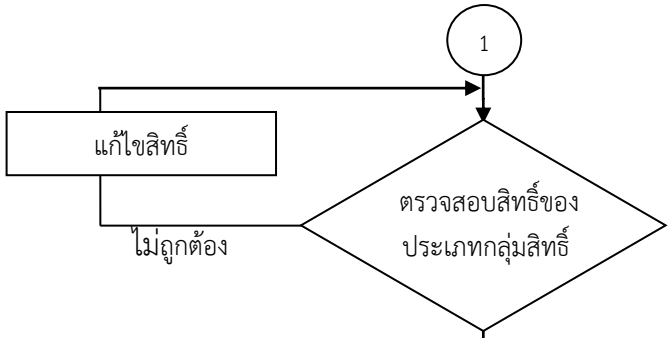
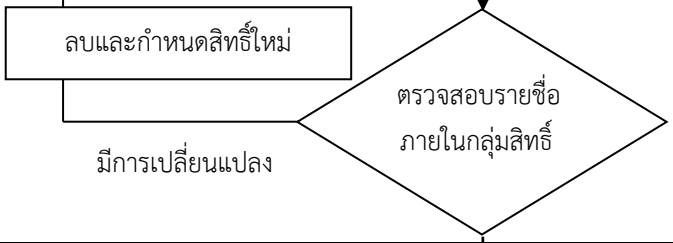
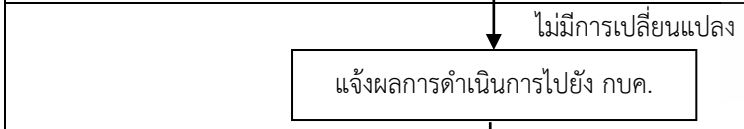
4.1.4 การยกเลิกสิทธิ์ของระบบบริหารงานบุคลากรและเงินเดือน

4.1.1 การทวนสอบประเภทกลุ่มสิทธิ์ สามารถแสดงได้ ดังตารางที่ 4.1

ตารางที่ 4.1 การทวนสอบประเภทกลุ่มสิทธิ์

ผังกระบวนการ	รายละเอียดงาน	ผู้รับผิดชอบ	เอกสารที่เกี่ยวข้อง	ระยะเวลา
	-	-	-	-
	**ขั้นตอนที่ 1** รับข้อมูลประเภทสิทธิ์/กลุ่มสิทธิ์จากกองบริหารงานบุคคล	ผู้บริหารจัดการระบบ	e-mail	ไม่แน่นอนตามกระบวนการ
	**ขั้นตอนที่ 2** ผู้บริหารจัดการระบบทวนสอบรายชื่อประเภทกลุ่มสิทธิ์ในระบบว่าตรงตามข้อกำหนดหรือไม่ กรณีไม่ตรงตามข้อกำหนดให้แจ้งกลับไปยัง กบค. เพื่อแก้ไขชื่อประเภทกลุ่มสิทธิ์	ผู้บริหารจัดการระบบ	ระบบบริหารงานบุคลากรและเงินเดือน	1-2 นาที
	**ขั้นตอนที่ 3** เมื่อทำการทวนสอบรายชื่อประเภทกลุ่มสิทธิ์แล้วตรงตามข้อกำหนด ให้ทำการบันทึกรายชื่อประเภทกลุ่มสิทธิ์	ผู้บริหารจัดการระบบ	ระบบบริหารงานบุคลากรและเงินเดือน	3 นาที

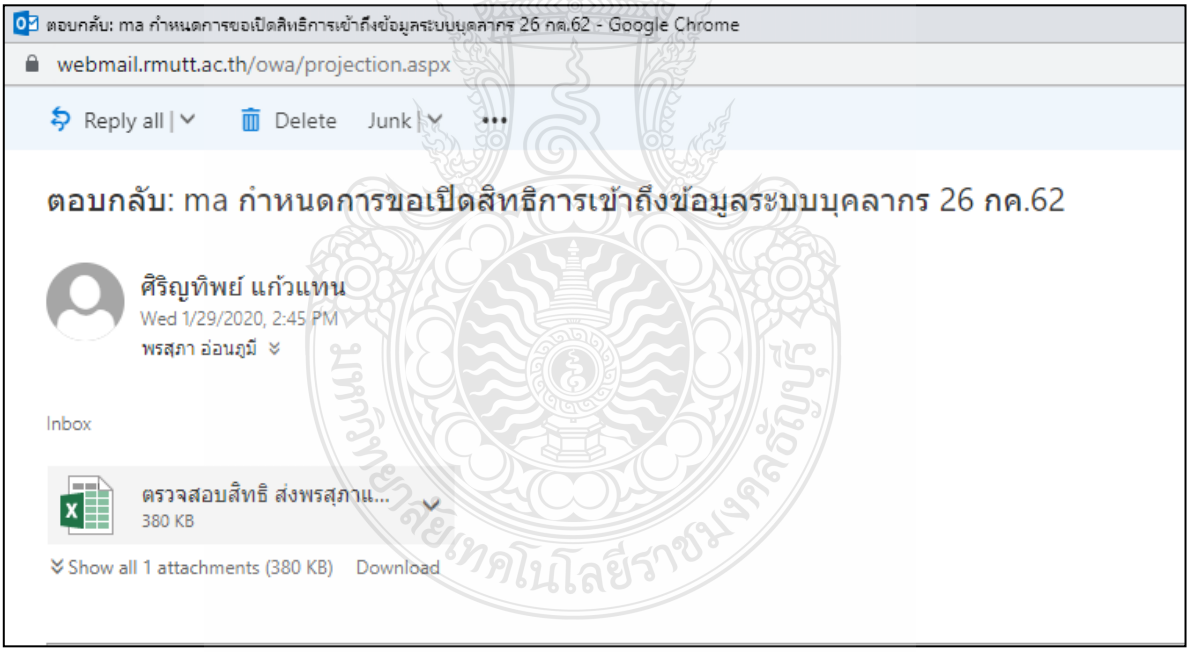
ตารางที่ 4.1 การทวนสอบประเภทกลุ่มสิทธิ์ (ต่อ)

ผังกระบวนการ	รายละเอียดงาน	ผู้รับผิดชอบ	เอกสารที่เกี่ยวข้อง	ระยะเวลา
	**ขั้นตอนที่ 4** ตรวจสอบสิทธิ์ของประเภทกลุ่มสิทธิ์ สิทธิ์แก้ไข :สามารถดูเท่านั้น หรือ ดูและแก้ไขได้ สิทธิ์หน่วยงาน :สามารถดูได้ทั้งหมด หรือ ดูภายในหน่วยงานเท่านั้น สิทธิ์การเข้าถึง :สามารถเข้าถึงแถบข้อมูลไหนได้บ้าง กรณีไม่ถูกต้องให้ทำการแก้ไขสิทธิ์การเข้าถึงแต่ละประเภทกลุ่มสิทธิ์	ผู้บริหารจัดการระบบ	ระบบบริหารงานบุคลากรและเงินเดือน	2 นาที
	**ขั้นตอนที่ 5** เมื่อทำการตรวจสอบประเภทกลุ่มสิทธิ์ถูกต้องแล้ว ให้ทำการบันทึกรายชื่อประเภทกลุ่มสิทธิ์	ผู้บริหารจัดการระบบ	ระบบบริหารงานบุคลากรและเงินเดือน	5 นาที
	**ขั้นตอนที่ 6** ตรวจสอบรายชื่อภายในกลุ่มสิทธิ์ กรณีมีการแก้ไขหรือเปลี่ยนแปลงเจ้าหน้าที่บุคลากรของคณะ/หน่วยงาน ให้ทำการลบและกำหนดสิทธิ์ของชื่อผู้ใช้งาน (User) ใหม่	ผู้บริหารจัดการระบบ	ระบบบริหารงานบุคลากรและเงินเดือน	5-10 นาที
	**ขั้นตอนที่ 7** ดำเนินการแจ้งผลการดำเนินการไปยัง กบค.	ผู้บริหารจัดการระบบ	e-mail	20-30 นาที
				

รายละเอียดของกระบวนการและขั้นตอนการปฏิบัติงาน

การทวนสอบ เป็นกระบวนการในการตรวจสอบ เพื่อยืนยันความถูกต้องของการกระทำสิ่งใดสิ่งหนึ่ง เพื่อไม่ให้เกิดการผิดพลาด การทวนสอบเป็นกระบวนการที่เกิดขึ้นควบคู่ไปกับการดำเนินการหรือดำเนินกิจกรรมใด ๆ ตลอดเวลา เพื่อเป็นการตรวจสอบ ตรวจทาน หรือยืนยันให้มั่นใจว่า สิ่งต่าง ๆ ที่ได้ดำเนินไปมีความถูกต้องเหมาะสม ในการทวนสอบจึงควรมีระบบและกระบวนการอย่างเป็นขั้นตอน โดยมีระบบในการทวนสอบเพื่อความถูกต้อง ความครบถ้วน และความเหมาะสมกับบริบทของหน่วยงาน และตัวหลักฐานเองที่เป็นสิ่งพิสูจน์หรือยืนยันได้ว่าการกระทำนั้น ๆ มีความถูกต้อง การทวนสอบจึงมีความสัมพันธ์เกี่ยวข้องกับองค์ประกอบอื่น ๆ ในระบบ หรือในหน่วยงานหนึ่ง

ขั้นตอนที่ 1 ผู้บริหารจัดการระบบรับข้อมูลประเภทสิทธิ์/กลุ่มสิทธิ์ ในส่วนของบุคลากรของกองบริหารงานบุคคลจะประสานงานส่งประเภทสิทธิ์ กลุ่มสิทธิ์และระดับสิทธิ์การเข้าถึงข้อมูลมาทาง e-mail : isc@rmutt.ac.th ที่ใช้ติดต่อภายในและภายนอกมหาวิทยาลัยฯ ที่ได้กล่าวถึงในบทที่ 3



ภาพที่ 4-1 แสดงตัวอย่างหน้าจอการส่งข้อมูลประเภทสิทธิ์ กลุ่มสิทธิ์และระดับสิทธิ์

***ข้อควรระวัง** จากการปฏิบัติงานพบว่า กรณีกองบริหารงานบุคคลมีการส่ง e-mail แล้ว CC Mail ผู้เกี่ยวข้อง ผู้บริหารจัดการระบบจะต้อง Reply All ทั้งหมดเพื่อให้ผู้เกี่ยวข้องทราบ เพราะจากประสบการณ์ที่พบผู้บริหารจัดการระบบส่ง e-mail แจ้งกลับไปยังผู้แจ้งเพียงผู้เดียว ซึ่งผู้ที่เกี่ยวข้องอาจจะเป็นผู้รับผิดชอบโดยตรงในการดำเนินการต่าง ๆ ภายในกลุ่มสิทธิ์ที่ทางผู้บริหารจัดการระบบนั้นได้มีการตรวจสอบและแก้ไข จึงจำเป็นเพื่อให้ผู้เกี่ยวข้องนั้นทราบด้วย

ขอเปิดสิทธิการเข้าถึงข้อมูลระบบบุคลากร (MIS)

ที่	ชื่อ - สกุลสกุล	กลุ่มสิทธิ์	ทะเบียนประวัติ									กพ.7	งานเครื่องราชย์	กองทุนฯ	งานพัฒนาบุคลากร	ตรวจสอบผู้สมควรเสนอตำแหน่งทางวิชาการ	ตำแหน่งวิชาการ/วิชาการ, บริหาร
			ตำแหน่งปัจจุบัน	รายได้	ข้อมูลทั่วไป	ข้อมูลอื่น ๆ	ที่อยู่	ผู้เกี่ยวข้อง	การศึกษา/สกอ.	ข้อมูลส่วนบุคคล	ตำแหน่งบริหาร						
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	**นางสุริพร เป็งเงิน**	1															
2	**นายอุทัย เห็มภูมิ**	1															
3	นางสาวพเก้า จันทร์ทุ่งใหญ่	1															
4	นางสาวอรารรถ ดันสิงหา	1															
5	นายมงคลชัย โพสังศิริ	3															
6	นางสาวสุภารัตน์ เมืองโสภา	3															
7	คนใหม่	3															
8	**นายคมกริช พุ่มเกิด**	1															
9	นางสาวศุภานัน พุดเดาล	1															
10	นายสุรชัย แดผู้เจริญ	1															
11	นางสาวรุ่งอรุณ โนทัง	1															
12	นางศิริญทิพย์ แก้วแทน	1															
13	คนใหม่	1															
14	**นางสาวนภาพร เจริญสุข**	1															
15	นางมาลี พฤกษชาติ	1															
16	นางสาวเกษรินทร์ เรืองวารี	1															
17	นางสาวจุฑารัตน์ ดอนแดงบึน	1															
18	นางสาววาสนา ผิวผลาผล	1															
19	**นางกัญญาณัฐ สายประสาท**	1															
20	นายรังโรจน์ สุทธิสุข	4															
21	นางสาวจิตาภา ทองไชย	4															
22	นางสาวพันนิดา เสือจ่าศิล	4															
23	นางสาวธีรวดี ยิ่งมี	2															
24	นางสาวสุกัญญา คัยกรณ์พัฒน์	1															
25	นางสันทนา วุนจุ้ด	3															
26	นายเพิ่มศักดิ์ ทับทิมทอง	3															
27	นายยุทธวิทย์ กองแก้ว	3															
28	**นางสรินยา รักษาบุญ**	1															
29	นายชวลิต กนกพาณิชย์สกุล	3															
30	นายธงรบ ชาตะรัตน์	3															
31	นายเสกขพันธ์ คงฟักษ์	3															
32	คนใหม่	3															

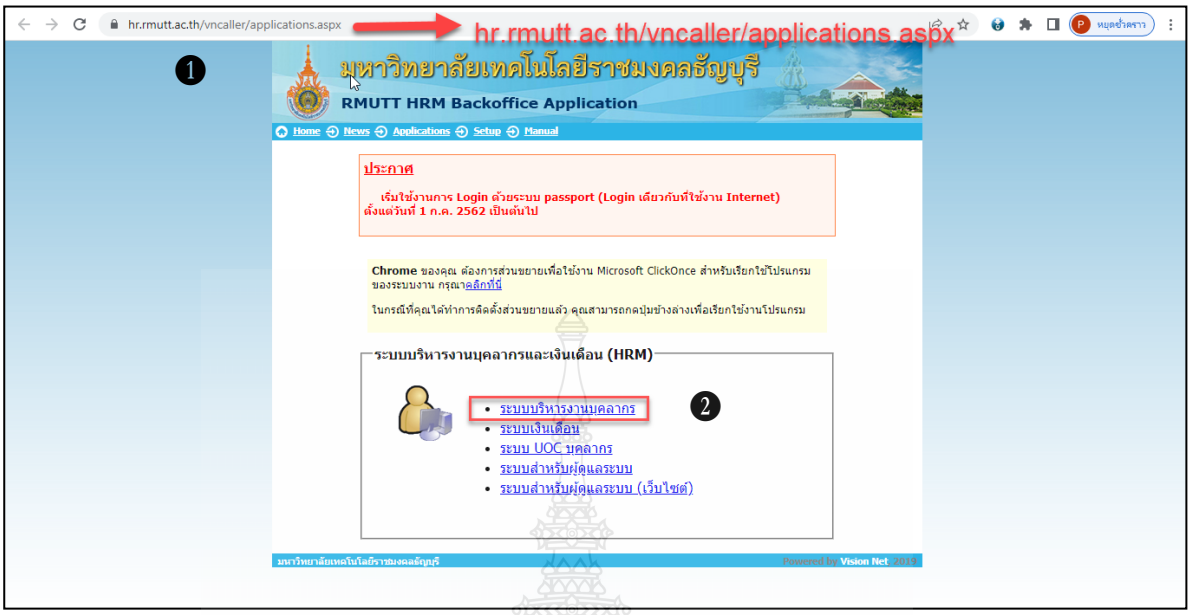
หมายเหตุ

กลุ่ม 1	1-15	เห็น / แก้ไข
กลุ่ม 2	1-10	เห็น
	14	เห็น / แก้ไข
กลุ่ม 3	1-5	เห็น
	13	เห็น/แก้ไข
กลุ่ม 4	1-10	เห็น
	14-15	เห็น/แก้ไข

แก้ไขเมื่อ 19 กุมภาพันธ์ 2563

ภาพที่ 4-2 แสดงตัวอย่างไฟล์ข้อมูลประเภทสิทธิ์ กลุ่มสิทธิ์และระดับสิทธิ์

ขั้นตอนที่ 2 ผู้บริหารจัดการระบบทวนสอบรายชื่อประเภทกลุ่มสิทธิ์ในระบบว่าตรงตามข้อกำหนดหรือไม่ สามารถดำเนินการได้ดังต่อไปนี้



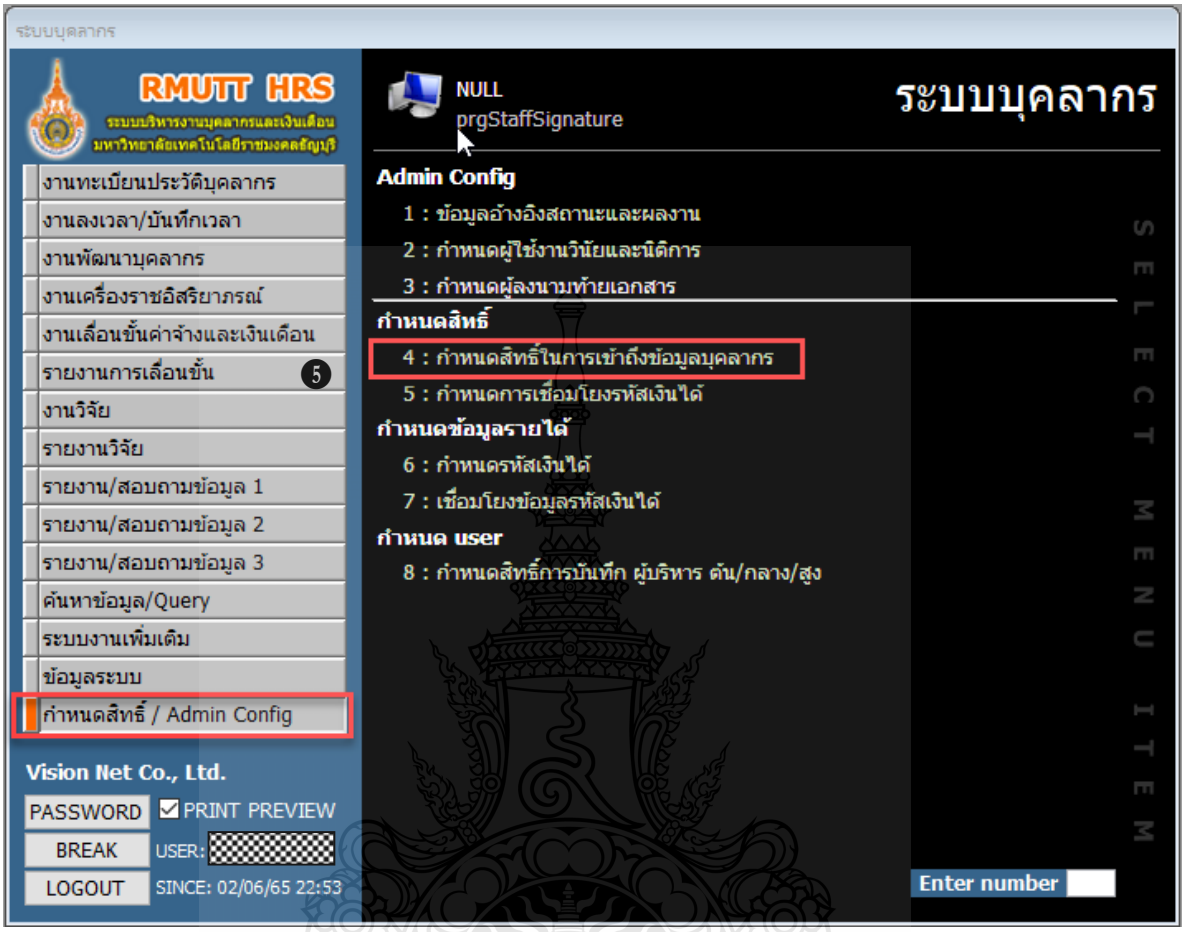
ภาพที่ 4-3 แสดงตัวอย่างหน้าจอระบบบริหารงานบุคลากรและเงินเดือน

ภาพที่ 4-4 แสดงตัวอย่างหน้าจอการเข้าสู่ระบบ (Logon)

หมายเลข 1 เข้าสู่หน้าเว็บ https://hr.rmutt.ac.th/vncaller/applications.aspx

หมายเลข 2 เรียกเมนู >>ระบบบริหารงานบุคลากร

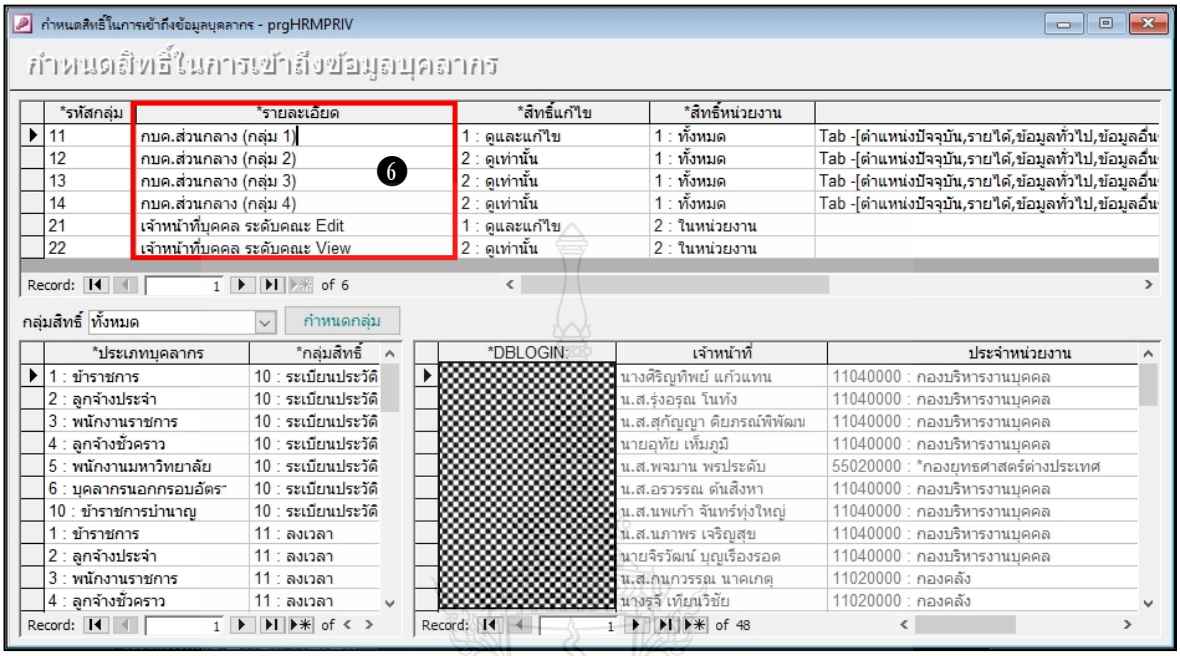
หมายเลข 3 กรอกชื่อและรหัสผู้ใช้งาน และกดปุ่ม OK



ภาพที่ 4-5 แสดงตัวอย่างหน้าจอกำหนดสิทธิ์ / Admin Config

หมายเลข 4 คลิกกำหนดสิทธิ์/Admin Config เพื่อไปทำการกำหนดสิทธิ์ในการเข้าถึงข้อมูลบุคลากร

หมายเลข 5 คลิก 4: กำหนดสิทธิ์ในการเข้าถึงข้อมูลบุคลากร เพื่อไปตรวจสอบชื่อประเภทกลุ่มสิทธิ์



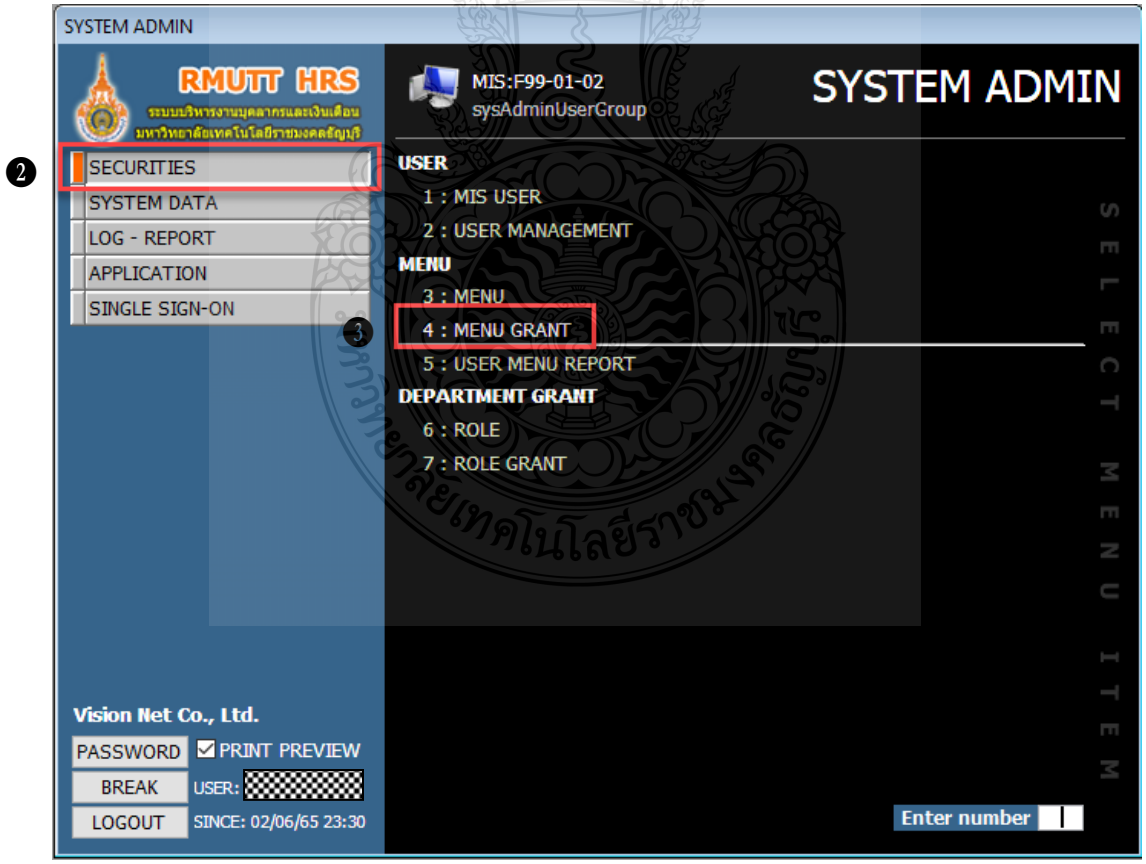
ภาพที่ 4-6 แสดงตัวอย่างหน้าจอกำหนดสิทธิ์ในการเข้าถึงข้อมูลบุคลากร

หมายเลข 6 จะปรากฏหน้าต่างกำหนดสิทธิ์ในการเข้าถึงข้อมูลบุคลากร ในคอลัมน์ *รายละเอียด จะแสดงรายชื่อประเภทกลุ่มสิทธิ์ สามารถตรวจสอบได้ว่าตรงตามข้อกำหนดหรือไม่

กรณีไม่ตรงตามข้อกำหนดให้แจ้งกลับไปยังกองบริหารงานบุคคล โดยผู้บริหารจัดการระบบกลับไปดำเนินการใหม่ในขั้นตอนที่ 1

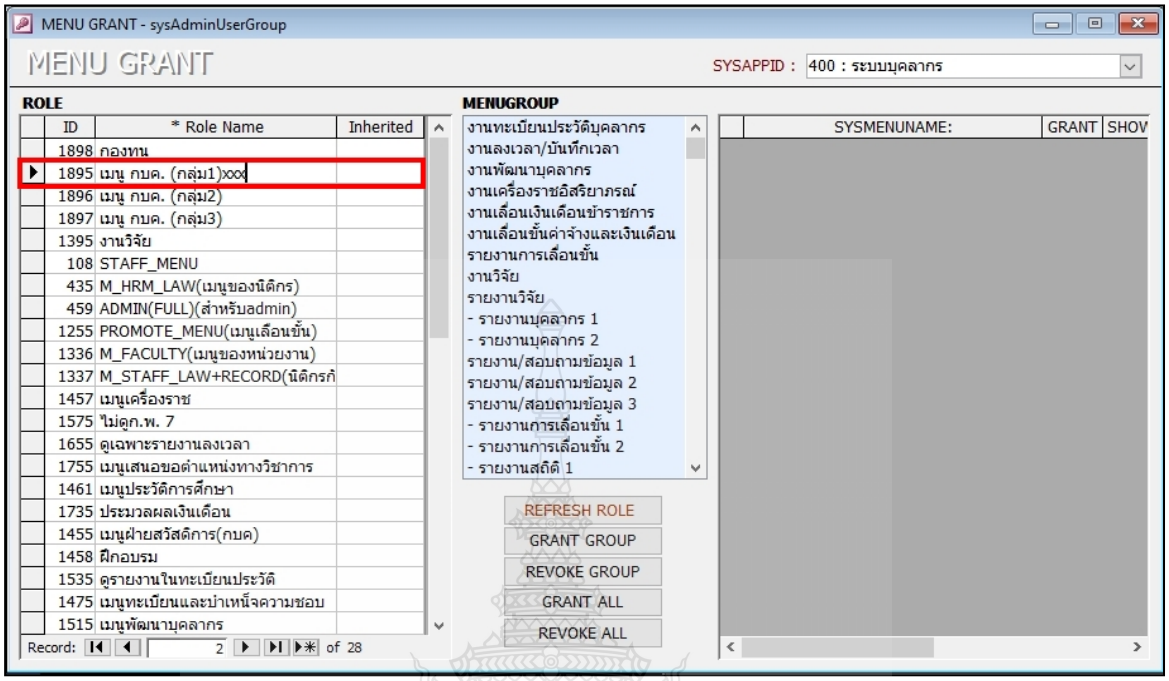
ขั้นตอนที่ 3 เมื่อทำการทวนสอบรายชื่อประเภทกลุ่มสิทธิ์แล้วตรงตามข้อกำหนด ให้ทำการบันทึกรายชื่อประเภทกลุ่มสิทธิ์ สามารถดำเนินการ ได้ดังต่อไปนี้

ภาพที่ 4-7 แสดงตัวอย่างหน้าจอระบบสำหรับผู้ดูแลระบบ



ภาพที่ 4-8 แสดงตัวอย่างหน้าจอการเข้า MENU GRANT

❹



ภาพที่ 4-9 แสดงตัวอย่างหน้าจอแก้ไขชื่อประเภทกลุ่มสิทธิ์

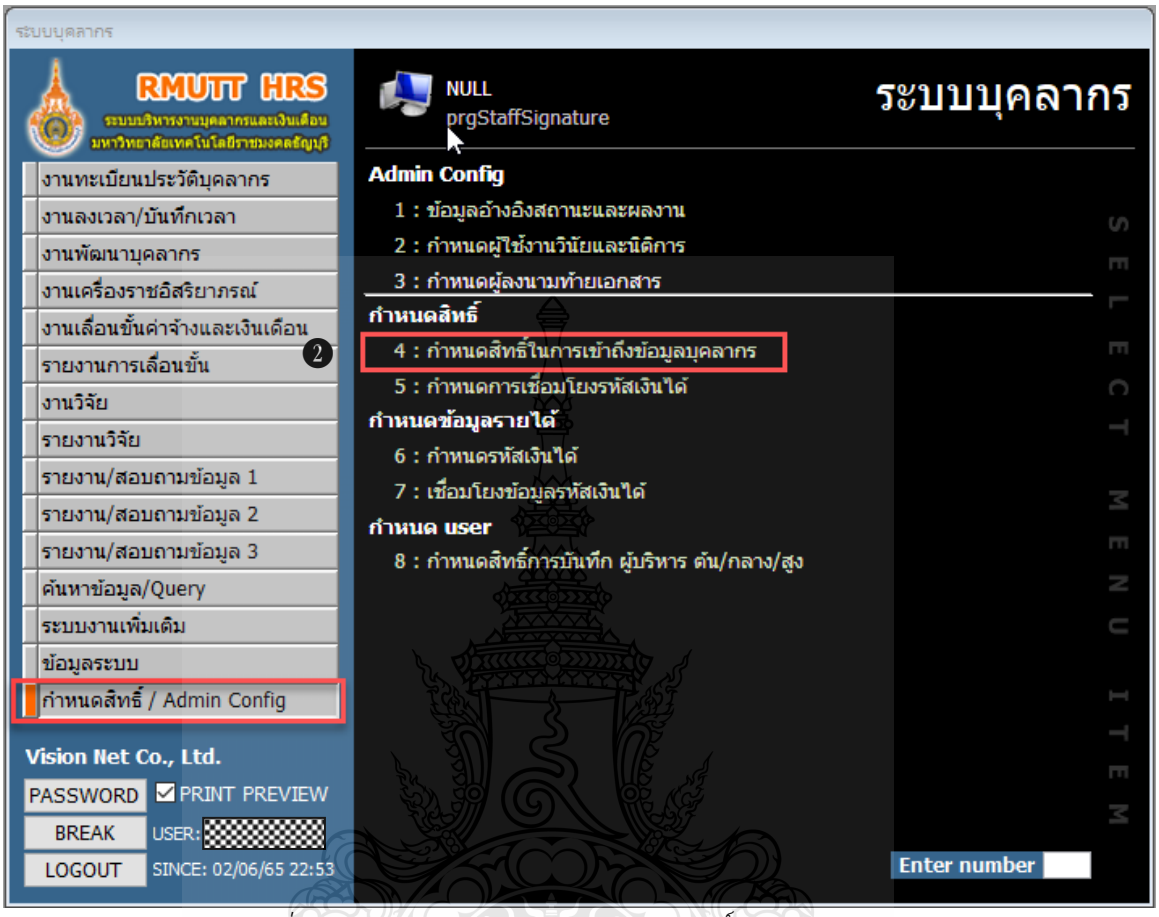
หมายเลข 1 เรียกเมนู >>ระบบสำหรับผู้ดูแลระบบ

หมายเลข 2 คลิก SECURITIES >>> MENU GRANT

หมายเลข 3 จะปรากฏหน้าจอ MENU GRANT ที่แสดงชื่อประเภทกลุ่มสิทธิ์ทั้งหมด

หมายเลข 4 คลิกที่คอลัมน์ Role Name สามารถแก้ไขชื่อประเภทกลุ่มสิทธิ์ และคลิกปุ่ม ▶ เพื่อบันทึก

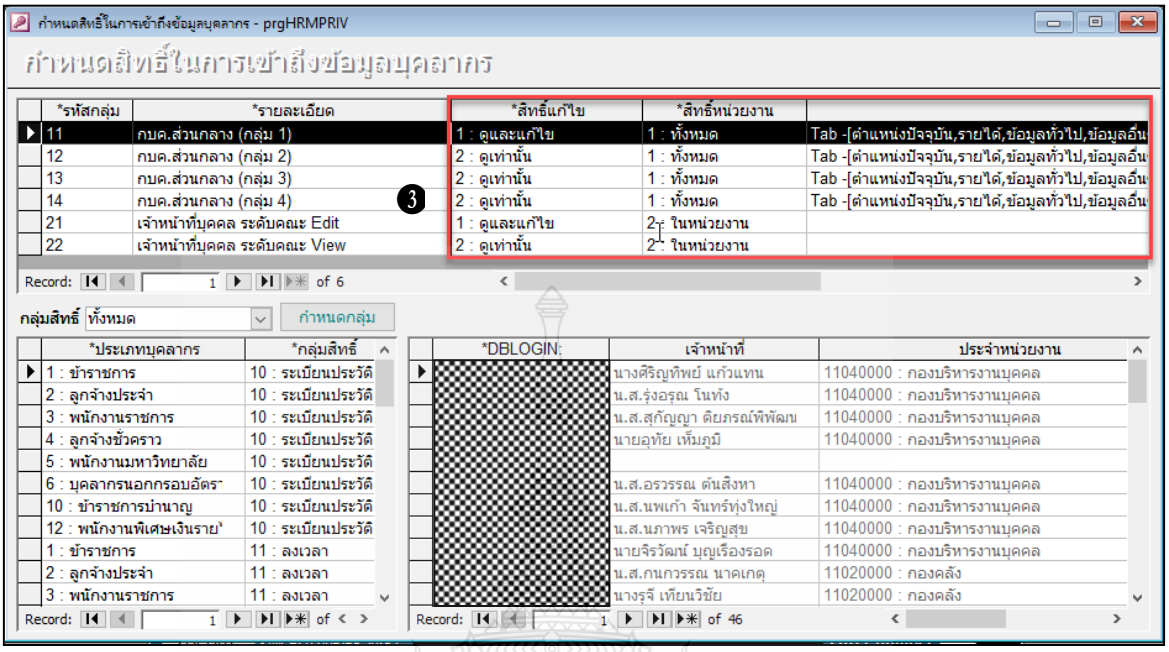
ขั้นตอนที่ 4 ตรวจสอบสิทธิ์ของประเภทกลุ่มสิทธิ์ ผู้บริหารจัดการระบบทวนสอบสิทธิ์ของประเภทกลุ่มสิทธิ์ได้ ดังต่อไปนี้



ภาพที่ 4-10 แสดงตัวอย่างหน้าจอกำหนดสิทธิ์ / Admin Config

หมายเลข 1 เรียกเมนู ระบบบริหารงานบุคลากร >> กำหนดสิทธิ์/Admin Config >>> กำหนดสิทธิ์ ในการเข้าถึงข้อมูลบุคลากร เพื่อไปทำการกำหนดสิทธิ์ในการเข้าถึงข้อมูลบุคลากร

หมายเลข 2 คลิก 4: กำหนดสิทธิ์ในการเข้าถึงข้อมูลบุคลากร เพื่อไปตรวจสอบสิทธิ์ของประเภทกลุ่มสิทธิ์



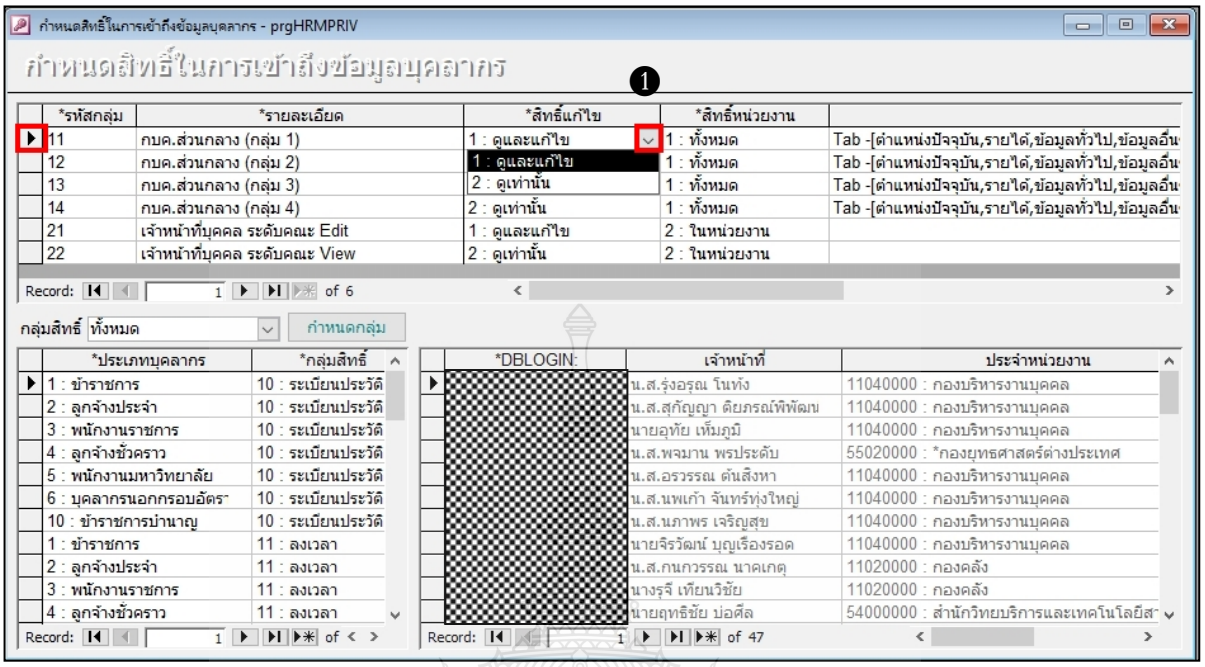
ภาพที่ 4-11 แสดงตัวอย่างหน้าจอตรวจสอบสิทธิ์ของประเภทกลุ่มสิทธิ์

หมายเลข 3 จะแสดงหน้าจอตรวจสอบสิทธิ์ของประเภทกลุ่มสิทธิ์ ดังนี้

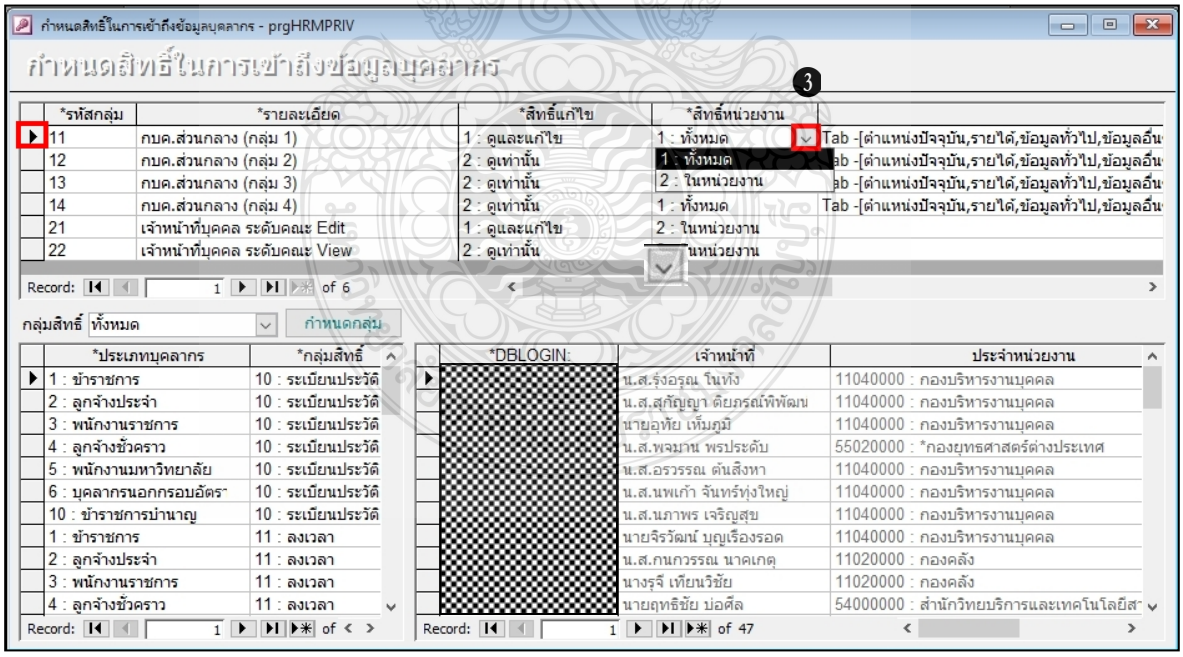
- สิทธิ์แก้ไข :สามารดดูเท่านั้นหรือดูและแก้ไขได้
- สิทธิ์หน่วยงาน :สามารถดูได้ทั้งหมดหรือดูภายในหน่วยงานเท่านั้น
- สิทธิ์การเข้าถึง :สามารถเข้าถึงแถบข้อมูลไหนได้บ้าง

จะปรากฏหน้าต่างกำหนดสิทธิ์ในการเข้าถึงข้อมูลบุคลากร ในคอลัมน์ *สิทธิ์แก้ไข *สิทธิ์หน่วยงาน และคอลัมน์สุดท้ายจะแสดงรายละเอียดประเภทกลุ่มสิทธิ์ สามารถตรวจสอบได้ว่าสิทธิ์ การเข้าถึงแต่ละประเภทกลุ่มสิทธิ์กำหนดไว้ถูกต้องหรือไม่ กรณีไม่ถูกต้องให้ทำการแก้ไขสิทธิ์การเข้าถึงแต่ละประเภทกลุ่มสิทธิ์

ขั้นตอนที่ 5 เมื่อทำการตรวจสอบประเภทกลุ่มสิทธิ์ถูกต้องแล้ว ให้ทำการบันทึกสิทธิ์ของประเภทกลุ่มสิทธิ์ ดังต่อไปนี้



ภาพที่ 4-12 แสดงตัวอย่างหน้าจอตรวจสอบสิทธิ์การเข้าถึงแต่ละประเภทกลุ่มสิทธิ์



ภาพที่ 4-13 แสดงตัวอย่างหน้าจอแก้ไขสิทธิ์การเข้าถึงแต่ละประเภทกลุ่มสิทธิ์

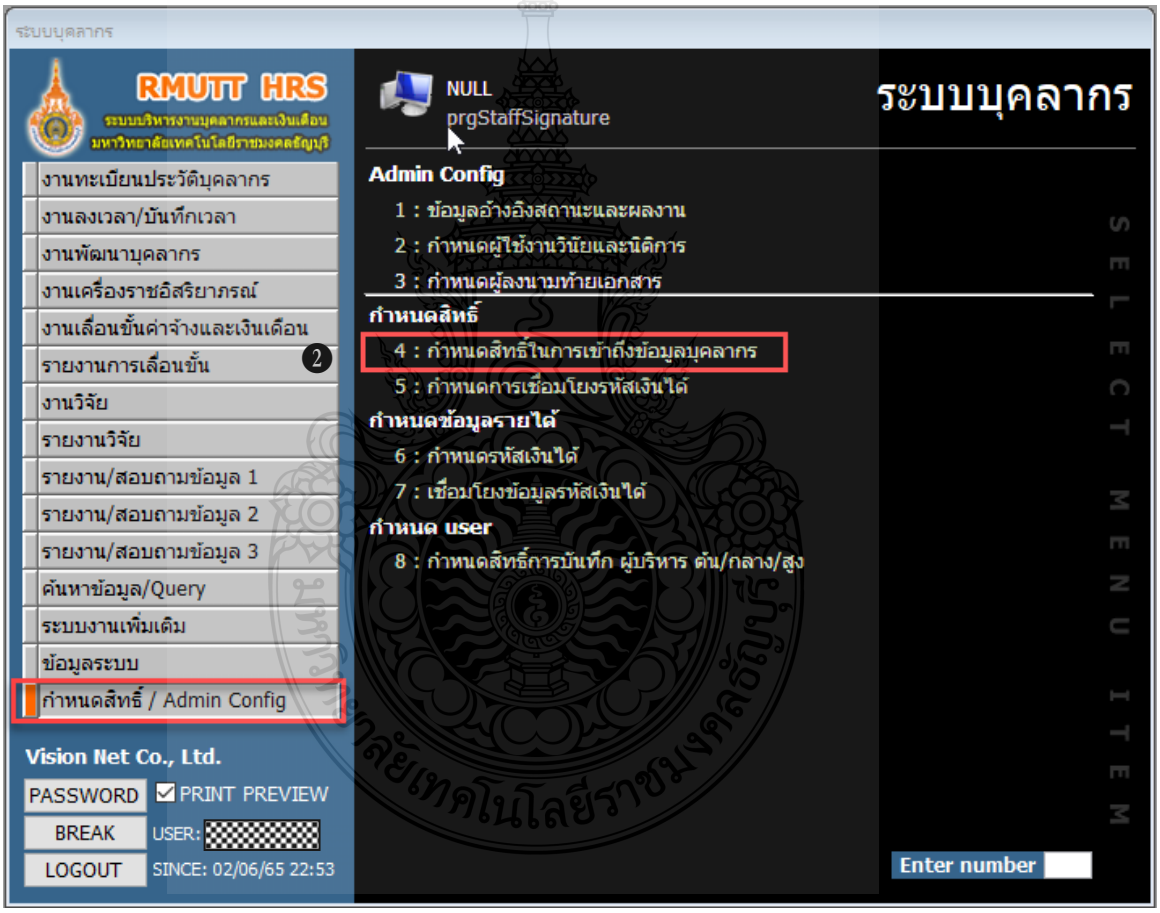
หมายเลข 1 คลิกคอลัมน์ *สิทธิ์แก้ไข กดเลือก Drop Down เลือกสิทธิ์การแก้ไข

หมายเลข 2 กดปุ่ม เพื่อบันทึก

หมายเลข 3 คลิกคอลัมน์ *สิทธิ์หน่วยงาน กดเลือก Drop Down เลือกสิทธิ์ของหน่วยงาน

หมายเลข 4 กดปุ่ม เพื่อบันทึก

ขั้นตอนที่ 6 ตรวจสอบรายชื่อภายในกลุ่มสิทธิ์ ผู้บริหารจัดการระบบตรวจสอบรายชื่อภายในกลุ่มสิทธิ์ได้ ดังต่อไปนี้

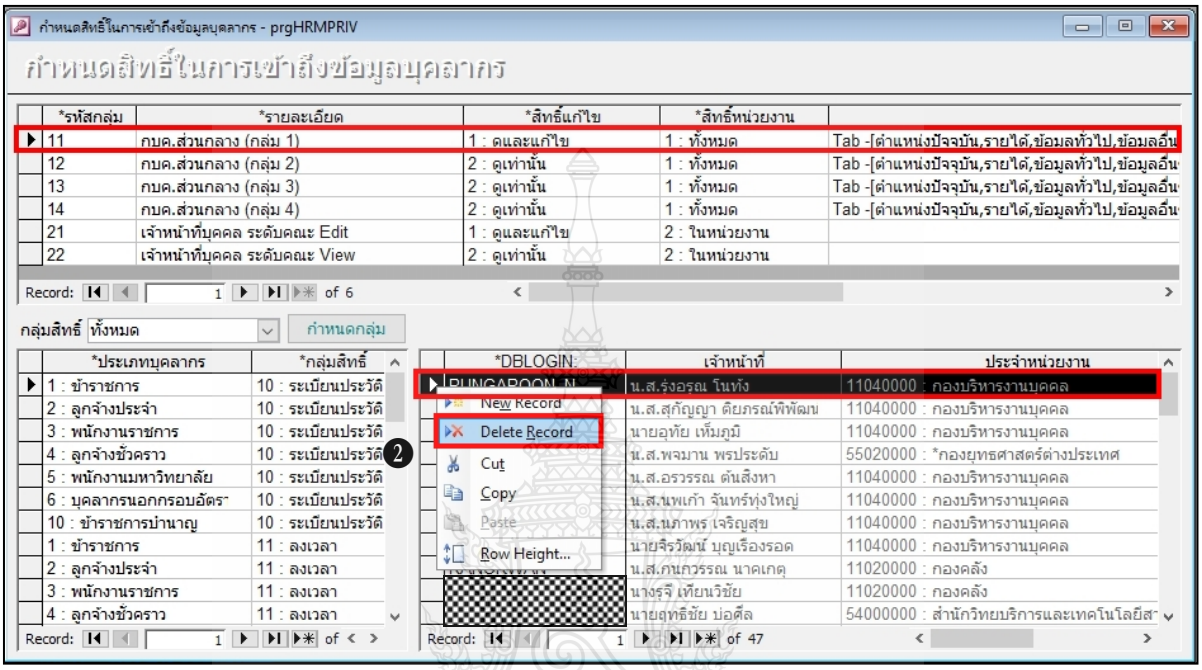


ภาพที่ 4-14 แสดงตัวอย่างหน้าจอกำหนดสิทธิ์ / Admin Config

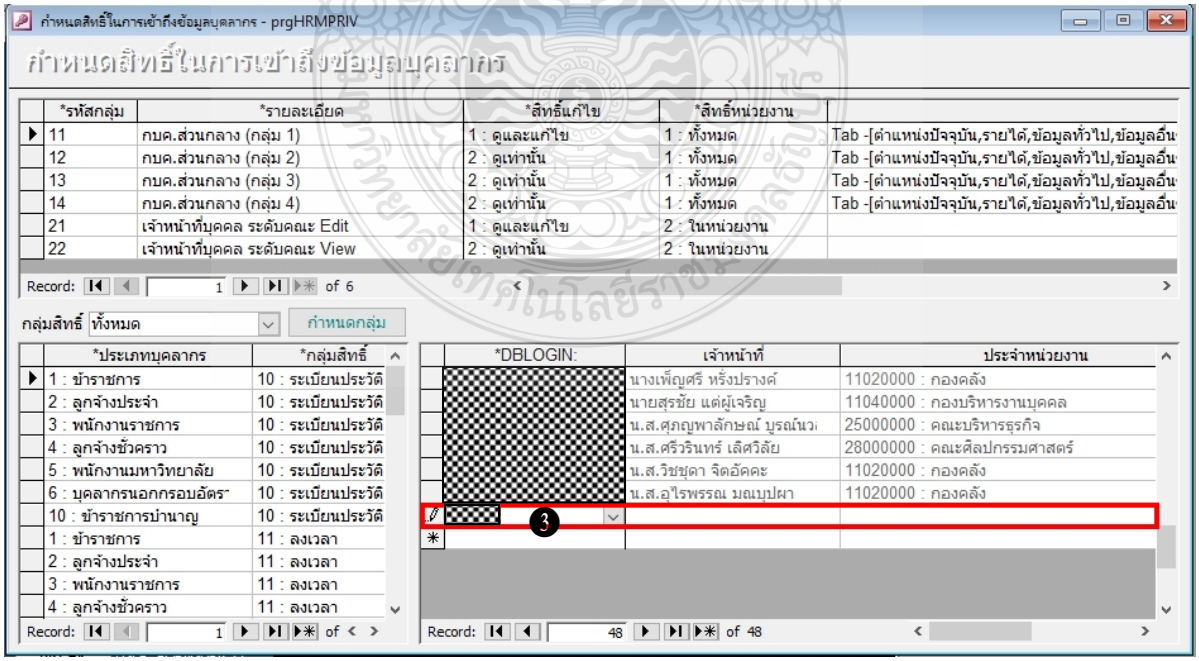
หมายเลข 1 เรียกเมนู ระบบบริหารงานบุคลากร >> กำหนดสิทธิ์/Admin Config >>> กำหนดสิทธิ์ ในการเข้าถึงข้อมูลบุคลากร เพื่อไปทำการกำหนดสิทธิ์ในการเข้าถึงข้อมูลบุคลากร

หมายเลข 2 คลิก 4: กำหนดสิทธิ์ในการเข้าถึงข้อมูลบุคลากร เพื่อไปตรวจสอบรายชื่อภายในกลุ่มสิทธิ์

จะปรากฏหน้าต่างกำหนดสิทธิ์ในการเข้าถึงข้อมูลบุคลากร กรณีมีการแก้ไขหรือเปลี่ยนแปลงเจ้าหน้าที่บุคลากรของคณะ/หน่วยงาน ให้ทำการลบและกำหนดสิทธิ์ของชื่อผู้ใช้งาน (User) ใหม่ ผู้บริหารจัดการระบบสามารถดำเนินการได้ ดังต่อไปนี้



ภาพที่ 4-15 แสดงตัวอย่างหน้าจอแสดงชื่อผู้ใช้งานแต่ละประเภทกลุ่มสิทธิ์



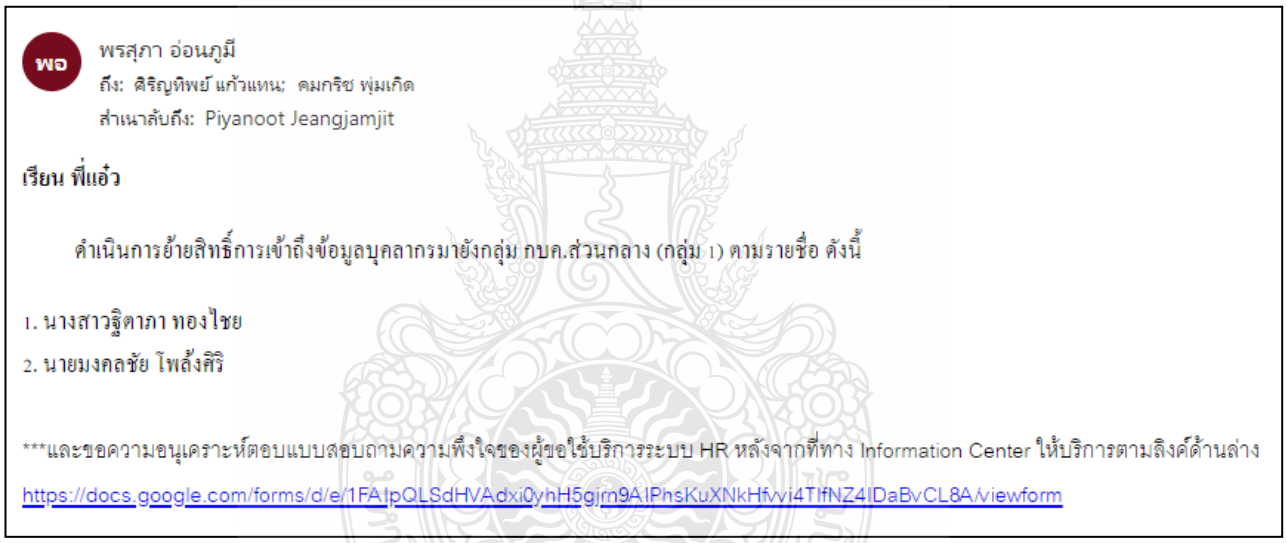
ภาพที่ 4-16 แสดงตัวอย่างหน้าจอแก้ไขชื่อผู้ใช้งานแต่ละประเภทกลุ่มสิทธิ์

หมายเลข 1 คลิกเลือกแถวประเภทกลุ่มสิทธิ์ จะแสดงชื่อผู้ใช้งานแต่ละประเภทกลุ่มสิทธิ์

หมายเลข 2 หากมีการแก้ไขหรือเปลี่ยนแปลงเจ้าหน้าที่บุคลากรของคณะ/หน่วยงาน ให้ทำการลบโดยคลิกขวาที่ชื่อผู้ใช้งาน (User) เลือก Delete Record

หมายเลข 3 กำหนดสิทธิ์ชื่อผู้เข้าใช้งานใหม่โดยการคลิกช่องล่างสุดพิมพ์ชื่อผู้ใช้งานใหม่ ระบบจะ Gen ชื่อ-นามสกุลและหน่วยงานขึ้นมาให้และกดปุ่ม  เพื่อเสร็จสิ้น

ขั้นตอนที่ 7 เมื่อดำเนินการทวนสอบรายชื่อประเภทกลุ่มสิทธิ์ ตรวจสอบสิทธิ์ของประเภทกลุ่มสิทธิ์และตรวจสอบรายชื่อภายในกลุ่มสิทธิ์เรียบร้อยแล้ว ผู้บริหารจัดการระบบแจ้งผลการดำเนินการส่ง e-mail ไปยังกองบริหารงานบุคคล ดังตัวอย่างภาพที่ 4-17



พจ พรสุภา อ่อนภูมี
ถึง: ศิริญทิพย์ แก้วแหน; คมกริช พุ่มเกิด
สำเนาลับถึง: Piyanoot Jeangjamjit

เรียน พี่แอ๋ว

ดำเนินการย้ายสิทธิ์การเข้าถึงข้อมูลบุคลากรมายังกลุ่ม กบค.ส่วนกลาง (กลุ่ม 1) ตามรายชื่อ ดังนี้

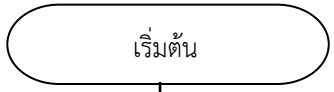
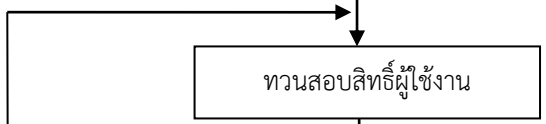
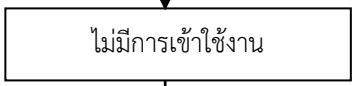
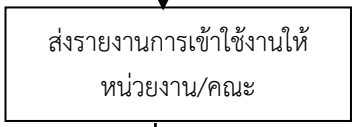
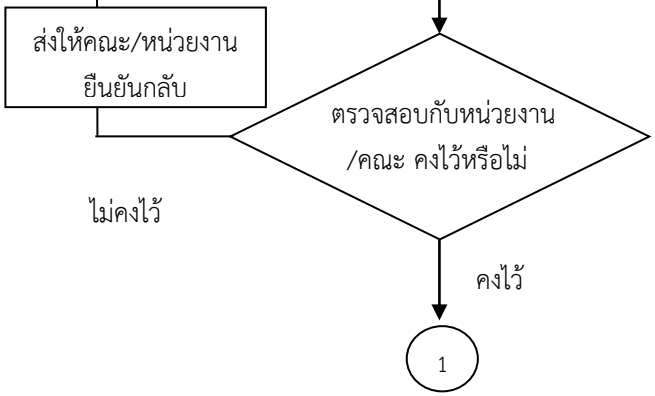
1. นางสาวฐิตาภา ทองไชย
2. นายมงคลชัย โพลิ้งศิริ

***และขอความอนุเคราะห์ตอบแบบสอบถามความพึงใจของผู้ขอใช้บริการระบบ HR หลังจากที่ทาง Information Center ให้บริการตามลิงค์ด้านล่าง
https://docs.google.com/forms/d/e/1FAIpQLSdHVAdxi0yhH5gjrn9AIPhsKuXNkHfvvi4TIfNZ4IDaBvCL8A/viewform

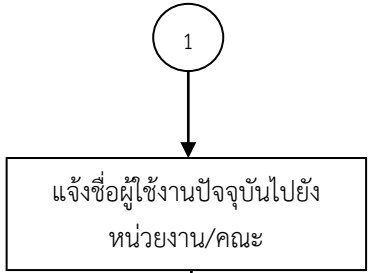
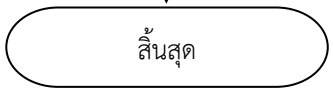
ภาพที่ 4-17 แสดงตัวอย่างหน้าจอแจ้งผลการดำเนินการไปยัง กบค.

ตารางที่ 4.1.2 การทวนสอบสิทธิ์ของผู้ใช้งาน สามาแสดงได้ดังตารางที่ 4.2

4.2 การทวนสอบสิทธิ์ของผู้ใช้งาน

ผังกระบวนการ	รายละเอียดงาน	ผู้รับผิดชอบ	เอกสารที่เกี่ยวข้อง	ระยะเวลา
	-	-	-	-
	**ขั้นตอนที่ 1** ดำเนินการทวนสอบสิทธิ์ประจำปีของผู้ใช้งานระบบ	ผู้บริหารจัดการระบบ	ระบบบริหารงานบุคลากรและเงินเดือน	30 นาที
	**ขั้นตอนที่ 2** พบว่าชื่อผู้ใช้แต่ละหน่วยงาน/คณะ ไม่มีการเข้าใช้งานระบบเกิน 1 ปี	ผู้บริหารจัดการระบบ	ระบบบริหารงานบุคลากรและเงินเดือน	10 นาที
	**ขั้นตอนที่ 3** ดำเนินการส่งรายงานการเข้าใช้งานให้หน่วยงาน/คณะ เพื่อให้ทราบชื่อผู้ใช้ที่ไม่มีสถานะการเข้าใช้งานระบบ	ผู้บริหารจัดการระบบ	รายงานการเข้าใช้งานและบันทึกข้อความ	ไม่แน่นอนตามกระบวนการ
	**ขั้นตอนที่ 4** ตรวจสอบกับทางหน่วยงาน/คณะ ยืนยันจะคงชื่อผู้ใช้งานไว้หรือไม่ กรณีไม่คงไว้ให้ทางคณะ/หน่วยงานยืนยันกลับไปยังขั้นตอนที่ 1 เพื่อดำเนินการตามตารางที่ 4.1.4 การยกเลิกสิทธิ์ของระบบบริหารงานบุคลากรและเงินเดือน กรณีคงไว้จะตรวจสอบว่าคณะ/หน่วยงานมีชื่อผู้เข้าถึงสิทธิ์จำนวนกี่คน	หน่วยงาน/คณะต้นสังกัดและผู้บริหารจัดการระบบ	ระบบบริหารงานบุคลากรและเงินเดือน	ไม่แน่นอนตามกระบวนการ

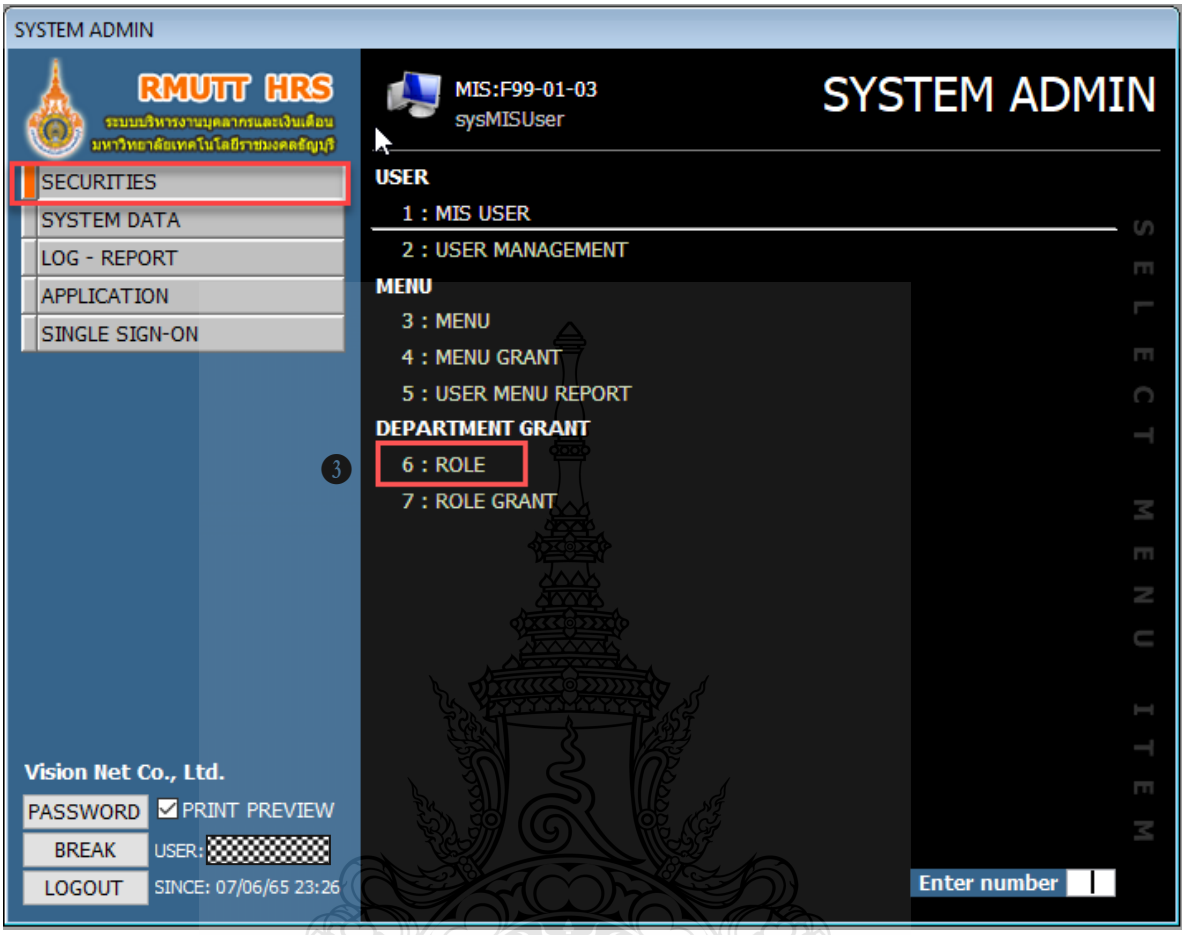
4.2 การทวนสอบสิทธิ์ของผู้ใช้งาน (ต่อ)

ผังกระบวนการ	รายละเอียดงาน	ผู้รับผิดชอบ	เอกสารที่เกี่ยวข้อง	ระยะเวลา
	**ขั้นตอนที่ 5** ผู้บริหารจัดการระบบดำเนินการแจ้งชื่อผู้เข้าถึงสิทธิ์การใช้งานปัจจุบันไปยังหน่วยงาน/คณะ	หน่วยงาน/คณะต้นสังกัดและผู้บริหารจัดการระบบ	ระบบบริหารงานบุคลากรและเงินเดือนและบันทึกข้อความ	ไม่แน่นอนตามกระบวนการ
				

รายละเอียดของกระบวนการและขั้นตอนการปฏิบัติงาน

ขั้นตอนที่ 1 ดำเนินการทวนสอบสิทธิ์ประจำปี ผู้บริหารจัดการระบบตรวจสอบชื่อผู้ใช้งานระบบทั้งหมดอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง กรณีชื่อผู้ใช้งาน (Username) มีการปรับเปลี่ยนงาน โยกย้ายหน่วยงานหรือลาออก เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต สามารถดำเนินการได้ ดังต่อไปนี้

ภาพที่ 4-18 แสดงตัวอย่างหน้าจอระบบสำหรับผู้ดูแลระบบ



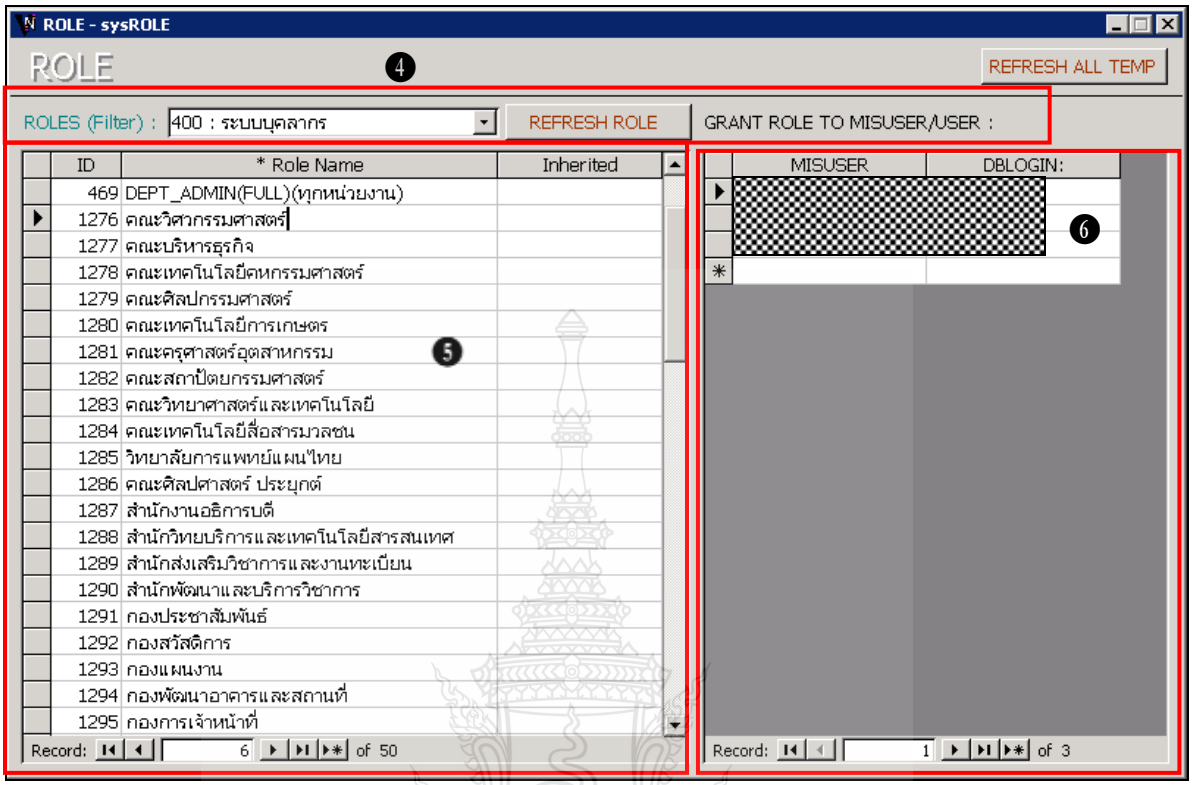
ภาพที่ 4-19 แสดงตัวอย่างหน้าจอ ROLE

การเพิ่ม ROLE

หมายเลข 1 เรียกเมนู >>ระบบสำหรับผู้ดูแลระบบ

หมายเลข 2 คลิก SECURITIES

หมายเลข 3 คลิก ROLE จะปรากฏหน้าจอของสิทธิ์ในการเข้าถึงโดยแสดง USER ทั้งหมดที่ได้สิทธิ์ในแต่ละ Role, สิทธิ์ในการเข้าถึงวิทยาเขต, หน่วยงาน, งบประมาณ,เล่มบัญชี



ภาพที่ 4-20 แสดงตัวอย่างหน้าจอแสดง USER ทั้งหมดที่ได้สิทธิ์ ในแต่ละ Role

หมายเลข 4 เลือกระบบที่ต้องการสร้าง Role

หมายเลข 5 สร้าง Role โดยระบุข้อมูลดังนี้ ดังนี้

ตารางที่ 4.2.1 คำอธิบายข้อมูลในการสร้าง Role

ข้อมูล	คำอธิบาย
ID	เป็นเลขที่ ที่ระบบสร้างขึ้น เพื่ออ้างอิง Role
Role Name	ชื่อ Role Menu
Inherited	คือการถ่ายทอดสิทธิ์ ให้ Role นี้สามารถมีสิทธิ์เท่ากัน Role ที่ให้

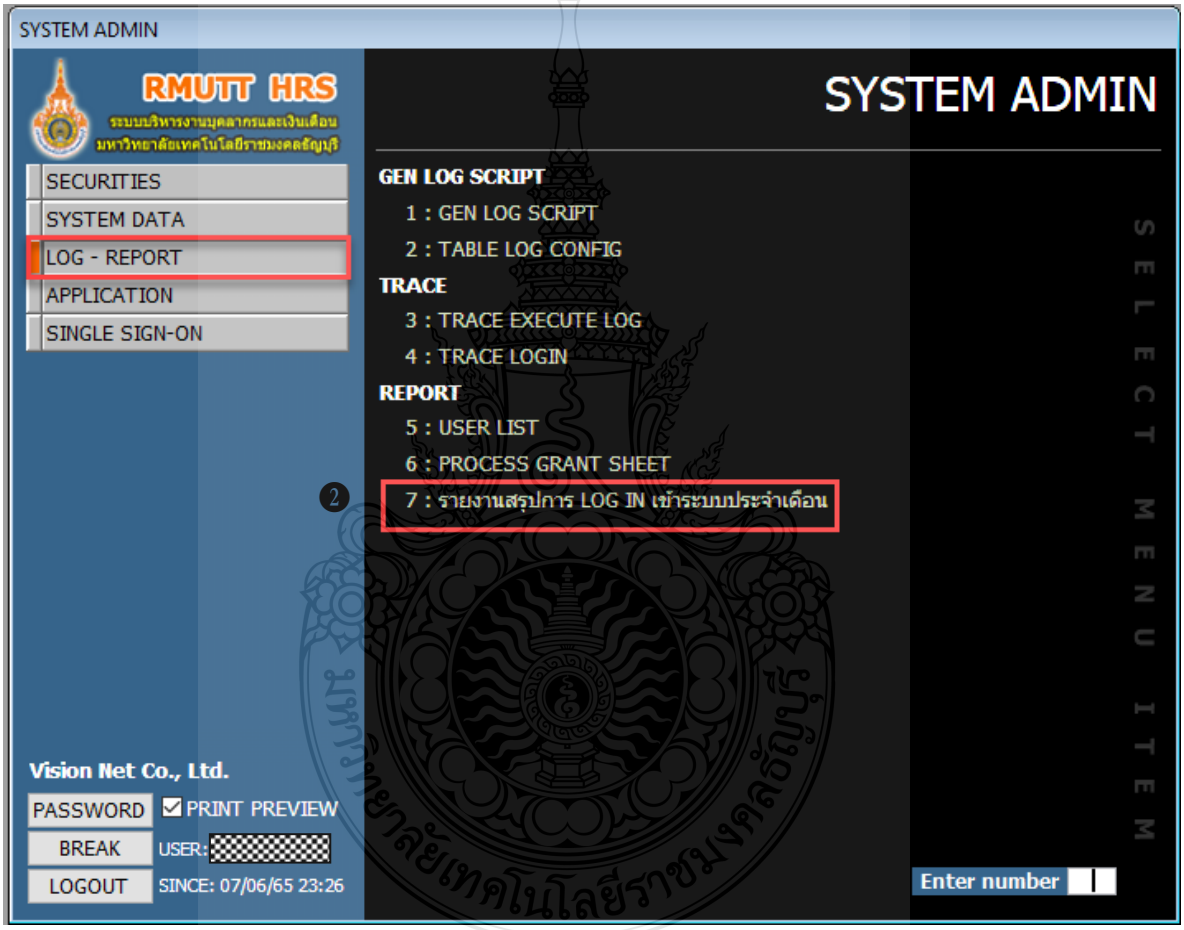
หมายเลข 6 สร้างและแสดง User ที่ได้สิทธิ์ใน Role ที่กำหนด ดังนี้

ตารางที่ 4.2.2 คำอธิบายข้อมูลในการสร้างและแสดง User ที่ได้สิทธิ์ใน Role

ข้อมูล	คำอธิบาย
MISUSER	USER ในระบบบริหารงานบุคลากรและเงินเดือน
DBLOGIN	USER ที่ใช้ LOG IN Oracle

หมายเหตุ : ในกรณีที่มีการเปลี่ยนแปลงสิทธิ์ สามารถ Click ปุ่ม REFRESH ALL TEMP แทนการกดปุ่ม Refresh ตามประเภทสิทธิ์ได้

ขั้นตอนที่ 2 ผู้บริหารจัดการระบบตรวจสอบแล้วพบว่าชื่อผู้ใช้งาน (User) ไม่มีการเข้าใช้งานระบบเกิน 1 ปี การเก็บ Log หรือประวัติการแก้ไขข้อมูล โดยเฉพาะข้อมูลที่สำคัญและจำเป็นต่อการแก้ไขความผิดพลาดหรือตรวจสอบข้อมูลย้อนหลัง นอกจากนั้นยังมีการเก็บประวัติการเข้าใช้ระบบ เพื่อตรวจสอบการใช้งานของผู้ใช้งาน (User) ดังนี้

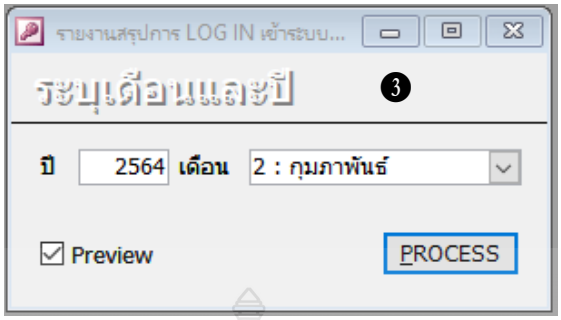


ภาพที่ 4-21 แสดงตัวอย่างหน้าจอ LOG - REPORT

LOG REPORT

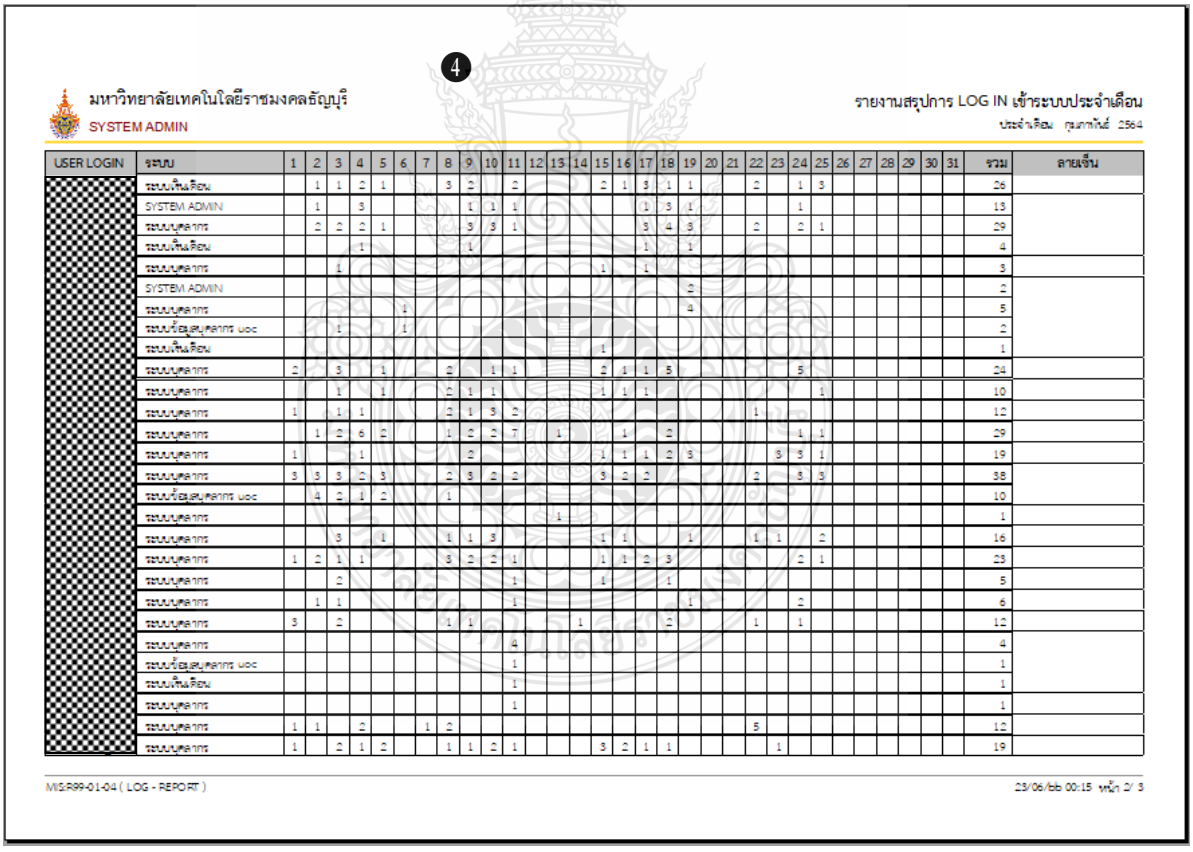
หมายเลข 1 เรียกเมนู >>ระบบสำหรับผู้ดูแลระบบ >>>LOG - REPORT

หมายเลข 2 คลิก 7:รายงานสรุปการ LOG IN เข้าระบบประจำเดือน



ภาพที่ 4-22 แสดงตัวอย่างหน้าจอเลือกเงื่อนการ LOG IN เข้าระบบ

หมายเลข 3 จะปรากฏหน้าจอรายงานสรุปการ LOG IN เข้าระบบประจำเดือน คลิกระบุปี/เดือน และกดปุ่ม PROCESS



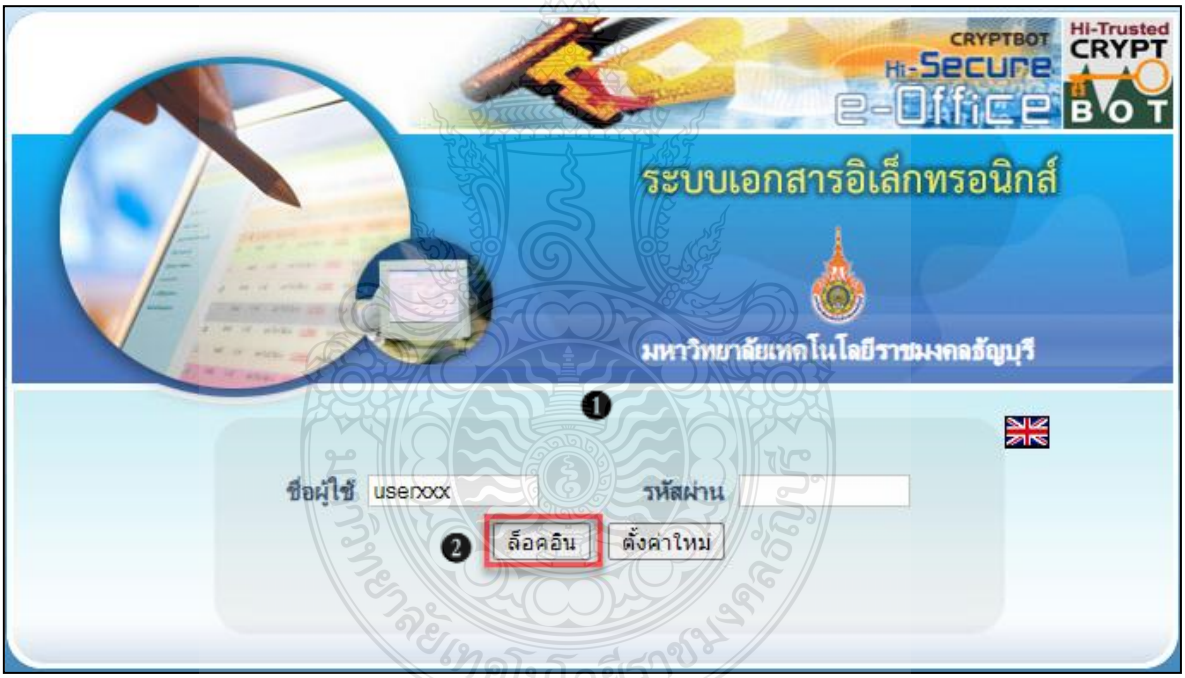
ภาพที่ 4-23 แสดงตัวอย่างหน้าจอรายงานสรุปการใช้ LOG IN เข้าระบบ

หมายเลข 4 จะแสดงรายงานสรุปการใช้ LOG IN เข้าระบบประจำเดือนที่ระบุ

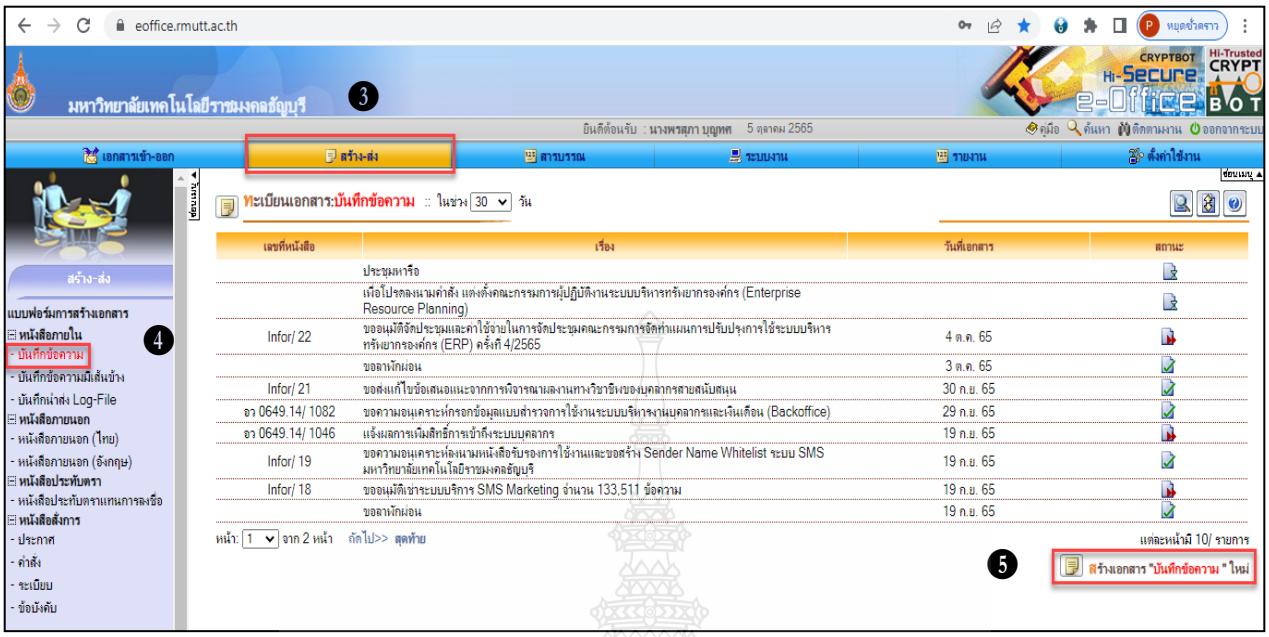
ขั้นตอนที่ 3 ผู้บริหารจัดการระบบทำการส่งรายงานการใช้ LOG IN เข้าระบบตามขั้นตอนที่ 2 ให้กับผู้บังคับบัญชา โดยทำหนังสือแจ้งเวียน เพื่อให้หน่วยงาน/คณะ ทราบชื่อผู้ใช้ที่ไม่มีสถานะการเข้าใช้งานระบบ

*****โดยในขั้นตอนนี้** จากประสบการณ์ของผู้ปฏิบัติงานได้มีการทำหนังสือแจ้งเวียนในระบบสารบรรณอิเล็กทรอนิกส์ (e-office) ให้ทางคณะ/หน่วยงานส่งรายชื่อผู้มีสิทธิ์เข้าใช้งานระบบบริหารงานบุคลากรและเงินเดือน หลังจากที่ได้มีการอบรมหลักสูตรฝึกอบรมระบบบุคลากร เพื่อเป็นการพัฒนาทักษะด้าน ICT เป็นการทวนสอบชื่อผู้ใช้งาน ให้ทางหน่วยงาน/คณะ ยืนยันชื่อผู้ใช้งาน (Username) กลับ เพื่อให้ผู้บริหารจัดการระบบทำการทวนสอบสิทธิ์ผู้ใช้งานได้ ดังตัวอย่างภาพที่ 4-24

หมายเหตุ : ผู้บริหารจัดการระบบสามารถสร้างบันทึกข้อความเพื่อแจ้งเวียนหนังสือ โดยเข้าใช้งานที่ https://eoffice.rmutt.ac.th/ ดังต่อไปนี้



ภาพที่ 4-24 แสดงตัวอย่างหน้าจอเข้าสู่ระบบเอกสารอิเล็กทรอนิกส์ (e-office)



ภาพที่ 4-25 แสดงตัวอย่างหน้าจอการสร้างบันทึกข้อความระบบเอกสารอิเล็กทรอนิกส์ (e-office)

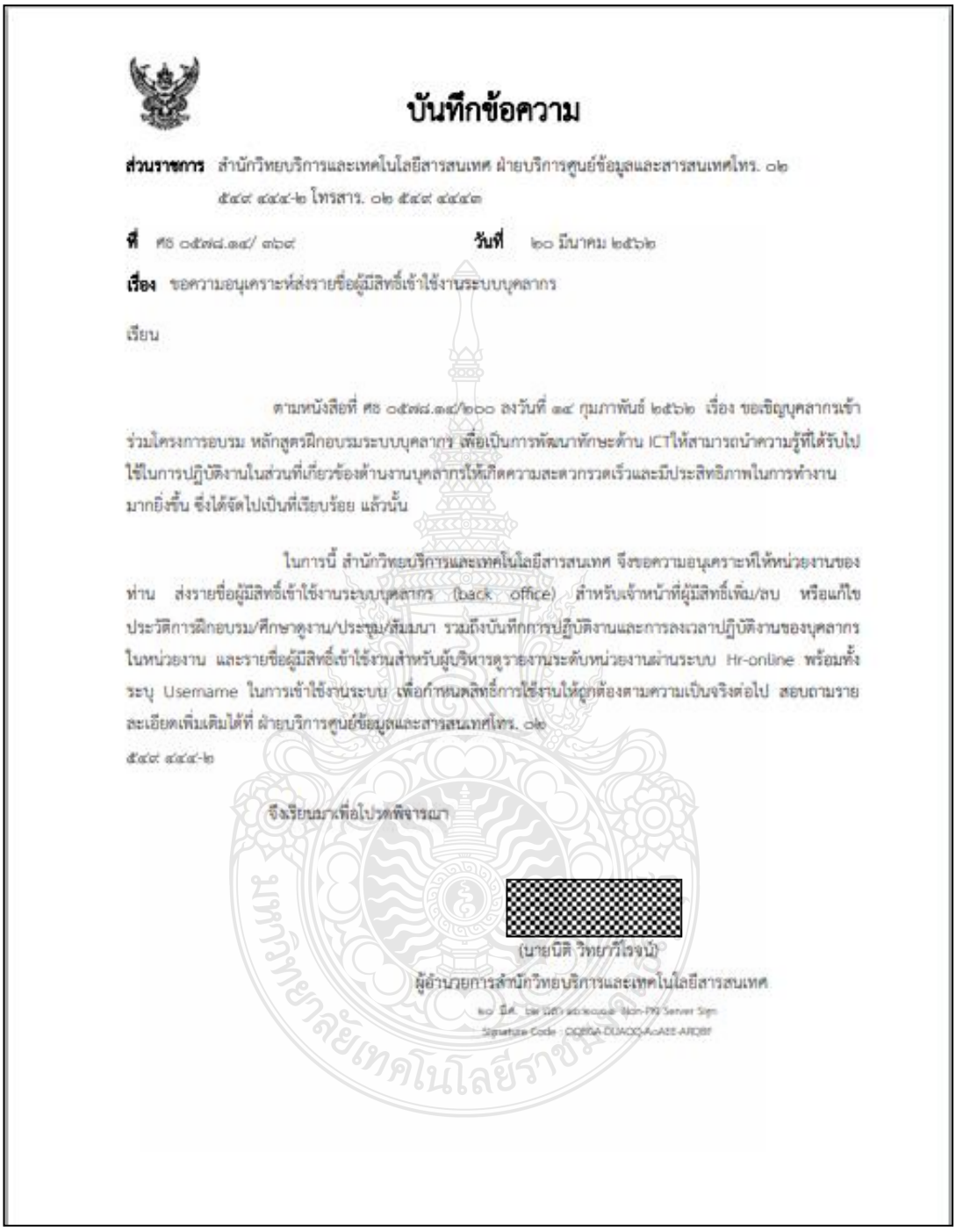
หมายเลข 1 จะปรากฏหน้าจอการเข้าใช้งาน (LOG IN) กรอกชื่อผู้ใช้งาน และรหัสผ่าน โดยใช้ชื่อผู้ใช้งาน (Username) ตัวเดียวกันกับ Account Internet ของมหาวิทยาลัยฯ

หมายเลข 2 คลิกปุ่ม ล็อคอิน เพื่อเข้าสู่ระบบ

หมายเลข 3 คลิกแถบ สร้าง-ส่ง

หมายเลข 4 คลิกบันทึกข้อความ

หมายเลข 5 คลิกสร้างเอกสาร “บันทึกข้อความ” ใหม่ เพื่อสร้างบันทึกข้อความ



บันทึกข้อความ

ส่วนราชการ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ฝ่ายบริการศูนย์ข้อมูลและสารสนเทศโทร. ๐๒ ๕๔๙ ๔๔๔-๒ โทรสาร. ๐๒ ๕๔๙ ๔๔๔๓

ที่ ศธ ๐๕๒๘.๑๔/ ๓๖๙ **วันที่** ๒๐ มีนาคม ๒๕๖๒

เรื่อง ขอความอนุเคราะห์ส่งรายชื่อผู้มีสิทธิ์เข้าใช้งานระบบบุคลากร

เรียน

ตามหนังสือที่ ศธ ๐๕๒๘.๑๔/๒๐๐ ลงวันที่ ๑๔ กุมภาพันธ์ ๒๕๖๒ เรื่อง ขอเชิญบุคลากรเข้าร่วมโครงการอบรม หลักสูตรฝึกอบรมระบบบุคลากร เพื่อเป็นการพัฒนาทักษะด้าน ICTให้สามารถนำความรู้ที่ได้รับไปใช้ในการปฏิบัติงานในส่วนที่เกี่ยวข้องด้านงานบุคลากรให้เกิดความสะดวกรวดเร็วและมีประสิทธิภาพในการทำงานมากยิ่งขึ้น ซึ่งได้จัดไปเป็นที่เรียบร้อย แล้วนั้น

ในการนี้ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ จึงขอความอนุเคราะห์ให้หน่วยงานของท่าน ส่งรายชื่อผู้มีสิทธิ์เข้าใช้งานระบบบุคลากร (back office) สำหรับเจ้าหน้าที่ผู้มีสิทธิ์เพิ่ม/ลบ หรือแก้ไขประวัติการฝึกอบรม/ศึกษาดูงาน/ประชุม/สัมมนา รวมถึงบันทึกการปฏิบัติงานและการลงเวลาปฏิบัติงานของบุคลากรในหน่วยงาน และรายชื่อผู้มีสิทธิ์เข้าใช้งานสำหรับผู้บริหารดูรายงานระดับหน่วยงานผ่านระบบ Hr-online พร้อมทั้งระบุ Username ในการเข้าใช้งานระบบ เพื่อกำหนดสิทธิ์การใช้งานให้ถูกต้องตามความเป็นจริงต่อไป สอบถามรายละเอียดเพิ่มเติมได้ที่ ฝ่ายบริการศูนย์ข้อมูลและสารสนเทศโทร. ๐๒ ๕๔๙ ๔๔๔-๒

จึงเรียนมาเพื่อโปรดพิจารณา

(นายนิติ วิทยาวิโรจน์)

ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ

๒๐ มี.ค. ๒๕๖๒ ๑๓:๑๐:๐๘ Skin-PKI Server Sign

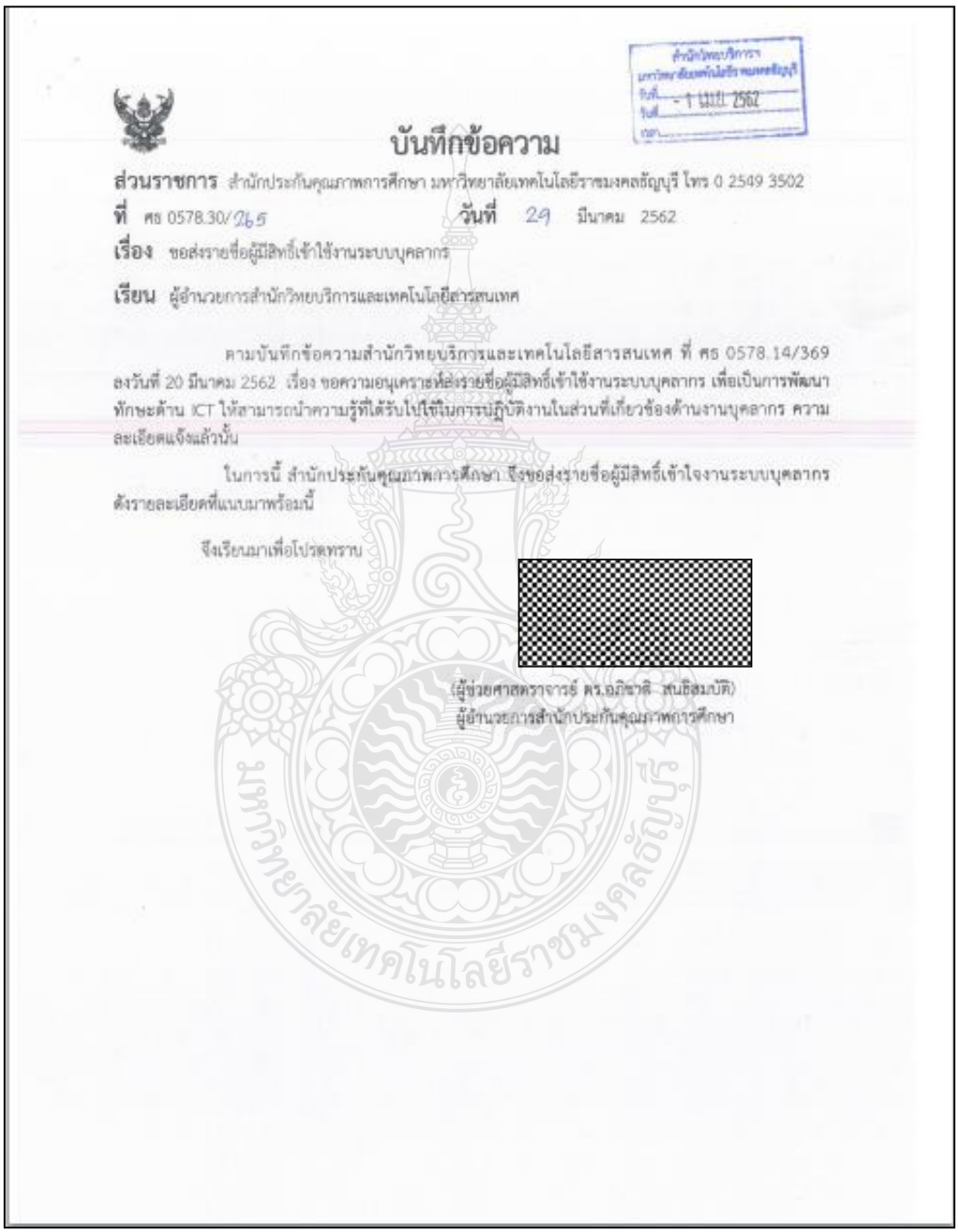
Signature Code : OQRNA-DUAOQ-AcAEE-AIQBF

ภาพที่ 4-26 แสดงตัวอย่างหน้าจอการสร้างบันทึกข้อความเวียนแจ้งหน่วยงาน/คณะ

ขั้นตอนที่ 4 ตรวจสอบกับทางหน่วยงาน/คณะ เพื่อดำเนินการทบทวนว่ามีชื่อผู้ใช้งานที่มีสถานะลาออกหรือมีการเปลี่ยนแปลงโยกย้ายงาน ให้ทางหน่วยงาน/คณะยืนยันว่าจะคงชื่อผู้ใช้งานไว้หรือไม่ ดังตัวอย่างภาพที่ 4-27

กรณีไม่คงไว้ให้ทางคณะ/หน่วยงานยืนยันกลับไปยังขั้นตอนที่ 1 เพื่อดำเนินการตามตารางที่ 4.1.4 การยกเลิกสิทธิ์ของระบบบริหารงานบุคลากรและเงินเดือน

กรณีคงไว้ผู้บริหารจัดการระบบจะดำเนินการตรวจสอบว่าคณะ/หน่วยงานมีชื่อผู้เข้าถึงสิทธิ์จำนวนกี่คน



บันทึกข้อความ

ส่วนราชการ สำนักประกันคุณภาพการศึกษา มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี โทร 0 2549 3502

ที่ ศธ 0578.30/265 **วันที่** 29 มีนาคม 2562

เรื่อง ขอส่งรายชื่อผู้มีสิทธิ์เข้าใช้งานระบบบุคลากร

เรียน ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ

ตามบันทึกข้อความสำนักวิทยบริการและเทคโนโลยีสารสนเทศ ที่ ศธ 0578.14/369 ลงวันที่ 20 มีนาคม 2562 เรื่อง ขอความอนุเคราะห์ส่งรายชื่อผู้มีสิทธิ์เข้าใช้งานระบบบุคลากร เพื่อเป็นการพัฒนาทักษะด้าน ICT ให้สามารถนำความรู้ที่ได้รับไปใช้ในการปฏิบัติงานในส่วนที่เกี่ยวข้องด้านงานบุคลากร ความละเอียดแจ้งแล้วนั้น

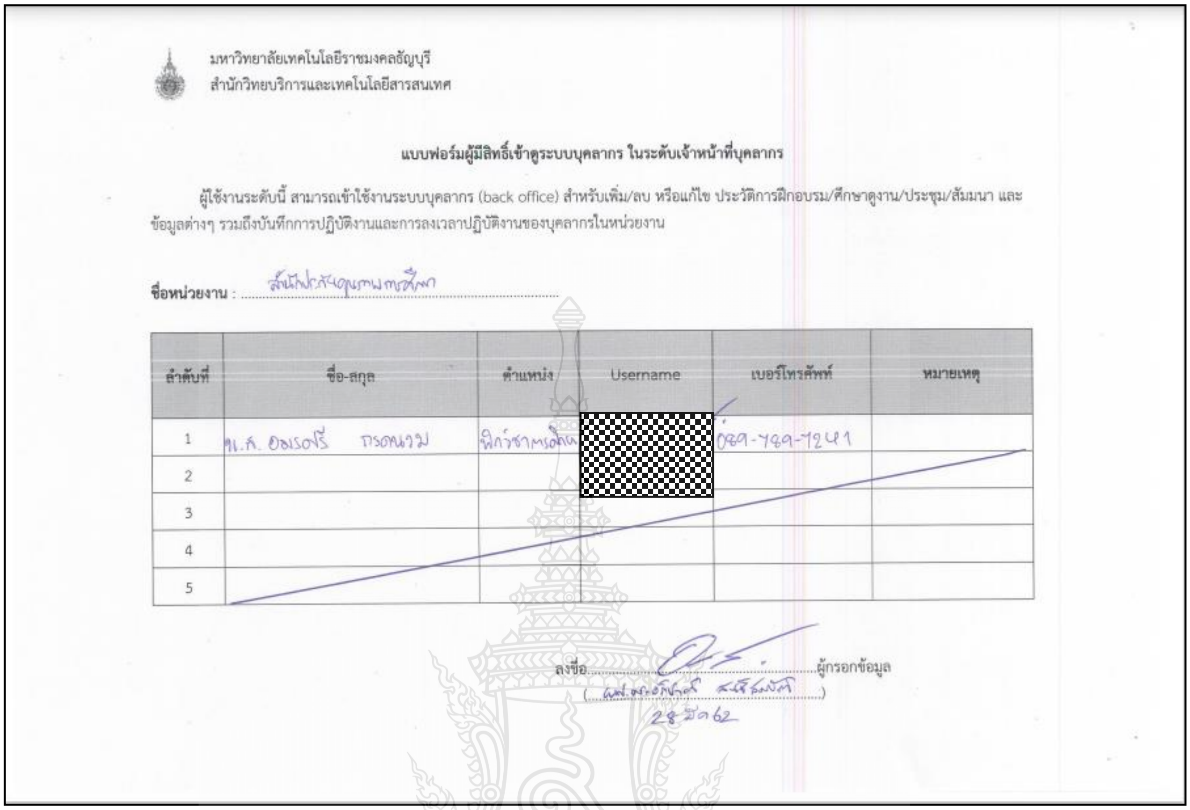
ในการนี้ สำนักประกันคุณภาพการศึกษา จึงขอส่งรายชื่อผู้มีสิทธิ์เข้าใจงานระบบบุคลากร ดังรายละเอียดที่แนบมาพร้อมนี้

จึงเรียนมาเพื่อโปรดทราบ

[redacted]

(ผู้ช่วยศาสตราจารย์ ดร.อภิชาติ สนธิสมบัติ)
ผู้อำนวยการสำนักประกันคุณภาพการศึกษา

ภาพที่ 4-27 แสดงตัวอย่างหน้าจอหน่วยงาน/คณะต้นสังกัดทำหนังสือตอบกลับมาเพื่อยืนยันชื่อผู้เข้าใช้งาน



มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี
สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

แบบฟอร์มผู้มีสิทธิ์เข้าดูระบบบุคลากร ในระดับเจ้าหน้าที่บุคลากร

ผู้ใช้งานระดับนี้ สามารถเข้าใช้งานระบบบุคลากร (back office) สำหรับเพิ่ม/ลบ หรือแก้ไข ประวัติการฝึกอบรม/ศึกษาดูงาน/ประชุม/สัมมนา และข้อมูลต่างๆ รวมถึงบันทึกการปฏิบัติงานและการลงเวลาปฏิบัติงานของบุคลากรในหน่วยงาน

ชื่อหน่วยงาน : สำนักประกันคุณภาพการศึกษา

ลำดับที่	ชื่อ-สกุล	ตำแหน่ง	Username	เบอร์โทรศัพท์	หมายเหตุ
1	น.ส. อมรศรี กรอนงาม	นักวิชาการศึกษา	[redacted]	089-789-7241	
2					
3					
4					
5					

ลงชื่อ..................................ผู้กรอกข้อมูล
(ผศ.ดร.อภิชาติ สนธิสมบัติ)
28 มี.ค. 62

ภาพที่ 4-28 แสดงตัวอย่างแบบฟอร์มที่ทางหน่วยงาน/คณะต้นสังกัดกรอกชื่อผู้ใช้งาน (Username)

ขั้นตอนที่ 5 ผู้บริหารจัดการระบบดำเนินการแจ้งชื่อผู้เข้าถึงสิทธิ์การใช้งานปัจจุบันไปยังหน่วยงาน/คณะ ดังตัวอย่างภาพที่ 4-29

กองประชาสัมพันธ์
มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี
เลขที่รับ 942/2565
วันที่ 21 ก.ย. 65
เวลา 08:33 น.

บันทึกข้อความ

ส่วนราชการ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ฝ่ายบริการศูนย์ข้อมูลและสารสนเทศ โทร.๐๒ ๕๙๙ ๔๔๔๓-๒

ที่ อว ๐๖๔๙.๓๔/ ๓๐๔๖ **วันที่** ๑๙ กันยายน ๒๕๖๕

เรื่อง แจ้งผลการเพิ่มสิทธิ์การเข้าถึงระบบบุคลากร

เรียน ผู้อำนวยการกองประชาสัมพันธ์

ตามหนังสือที่ อว ๐๖๔๙.๒๓/ ๒๓๖ ลงวันที่ ๒๕ พฤษภาคม ๒๕๖๕ เรื่อง ขอเปลี่ยนแปลงผู้ใช้งานระบบบุคลากร ความทราบแล้วนั้น

ในการนี้ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ได้ดำเนินการเพิ่มสิทธิ์การเข้าถึงระบบบุคลากร (back office) ให้เรียบร้อยแล้ว **ปัจจุบันมีผู้เข้าถึงสิทธิ์การใช้งาน จำนวน ๒ ราย คือ**

๑. นางสาวสว่างนภา ด่วนภูษา ตำแหน่ง นักประชาสัมพันธ์
๒. นางสาวณัฏฐ์นารี สุขดี ตำแหน่ง นักประชาสัมพันธ์

หากมีการแก้ไขหรือเปลี่ยนแปลง รบกวนทางหน่วยงานทำหนังสือแจ้งแก้ไขหรือเปลี่ยนแปลงสิทธิ์การเข้าถึงระบบบริหารงานบุคลากรและเงินเดือน (Back office) สอบถามรายละเอียดเพิ่มเติมได้ที่ ฝ่ายบริการศูนย์ข้อมูลและสารสนเทศ โทร. ๐๒ ๕๙๙ ๔๔๔๒

จึงเรียนมาเพื่อโปรดทราบ

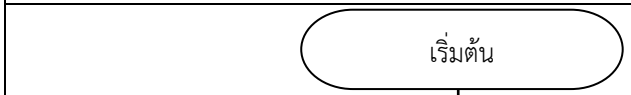
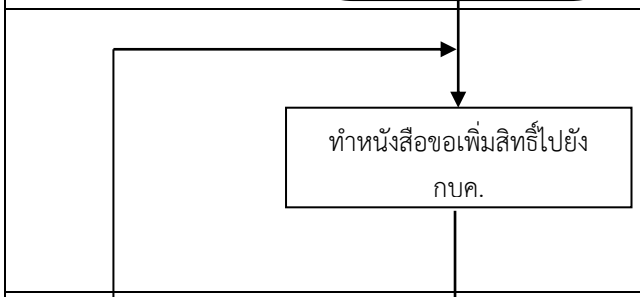
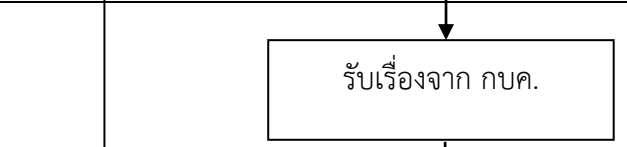
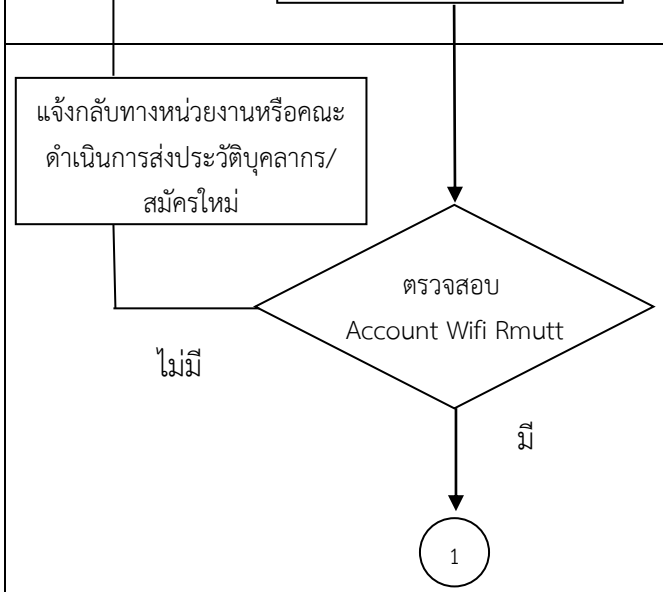
(นายนิติ วิทยาวิโรจน์)
ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ

Non-PKI Server Sign
Signature Code : QqBEA-DIAOA-BBADg-AQqAy

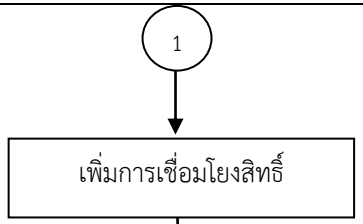
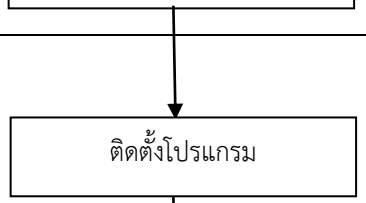
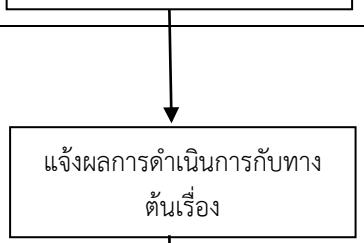
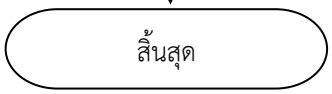
ภาพที่ 4-29 แสดงตัวอย่างหนังสือแจ้งชื่อผู้เข้าถึงสิทธิ์การใช้งานปัจจุบัน

ตารางที่ 4.1.3 การกำหนดสิทธิ์ของระบบบริหารงานบุคลากรและเงินเดือน สามารถแสดงได้ ดังตารางที่ 4.3

4.3 การกำหนดสิทธิ์ของระบบบริหารงานบุคลากรและเงินเดือน

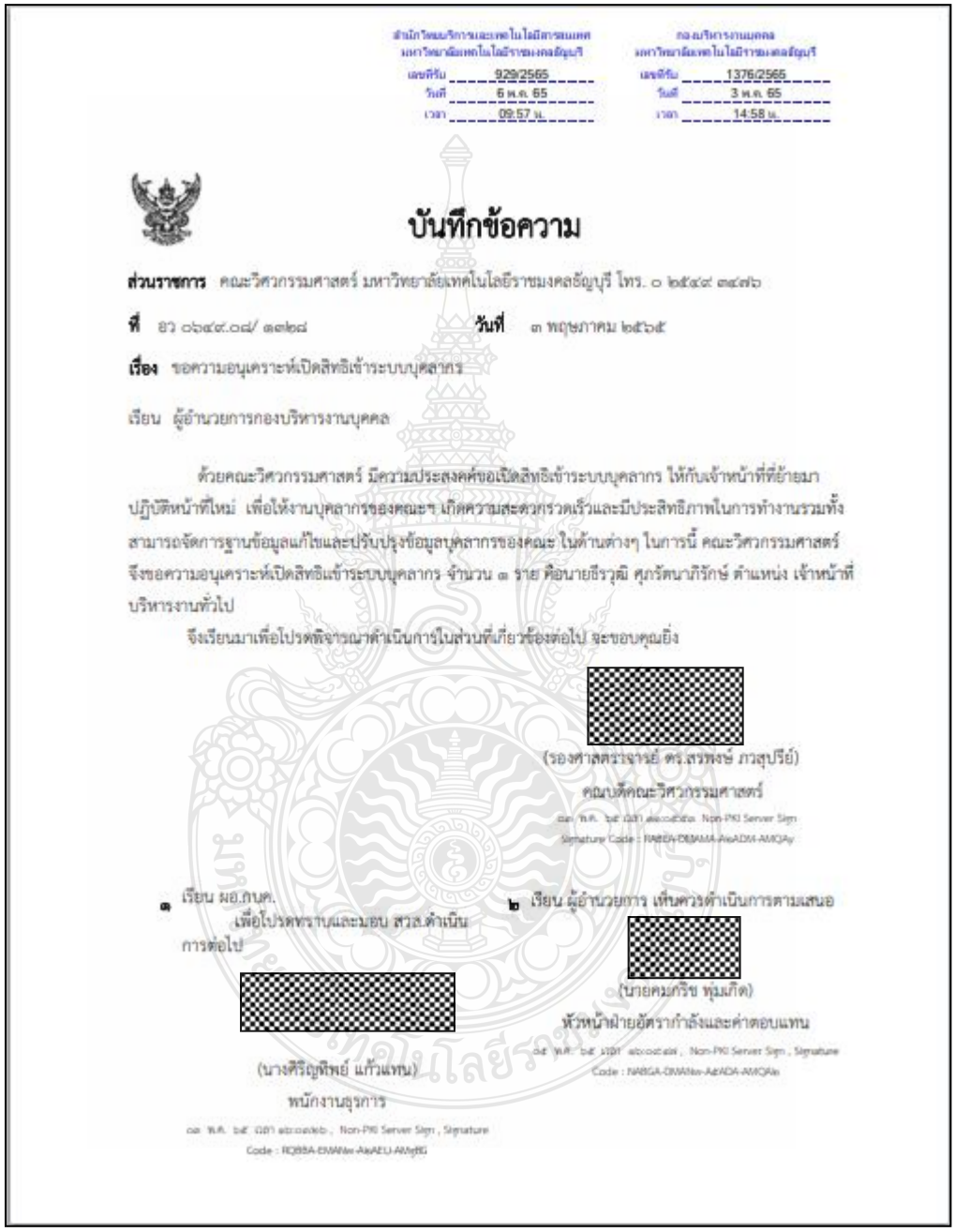
ผังกระบวนการ	รายละเอียดงาน	ผู้รับผิดชอบ	เอกสารที่เกี่ยวข้อง	ระยะเวลา
	-	-	-	-
	**ขั้นตอนที่ 1** หน่วยงาน/คณะต้นสังกัดแจ้งขอเพิ่มสิทธิ์โดยทำบันทึกข้อความส่งในระบบสารบรรณอิเล็กทรอนิกส์ (e-office) ผ่านผู้บังคับบัญชาส่งถึงผู้อำนวยการกองบริหารงานบุคคล	หน่วยงาน/คณะ	บันทึกข้อความจากหน่วยงาน/คณะต้นสังกัด	ไม่แน่นอนตามกระบวนการ
	**ขั้นตอนที่ 2** รับเรื่องจากกองบริหารงานบุคคลเพื่อให้ผู้บริหารจัดการระบบดำเนินการ	ผู้บริหารจัดการระบบ	บันทึกข้อความจากหน่วยงาน/คณะต้นสังกัด	2-3 วัน
	**ขั้นตอนที่ 3** ผู้บริหารจัดการระบบตรวจสอบ Account Wifi กรณีตรวจสอบแล้วไม่มีให้ดำเนินการกลับไปที่ขั้นตอนที่ 1 เพื่อแจ้งกลับทางหน่วยงานหรือคณะดำเนินการส่งประวัติบุคลากรให้กับกองบริหารงานบุคคลเพื่อเพิ่มข้อมูลบุคลากรในระบบ และแจ้งสมัคร Account Wifi สำหรับบุคลากรใหม่ กรณีพบว่ามี Account Wifi ผู้บริหารจัดการระบบจะดำเนินการนำชื่อผู้ใช้ไปเชื่อมโยงสิทธิ์	ผู้บริหารจัดการระบบ	e-mail	ไม่แน่นอนตามกระบวนการ

4.3 การกำหนดสิทธิ์ของระบบบริหารงานบุคลากรและเงินเดือน (ต่อ)

ผังกระบวนการ	รายละเอียดงาน	ผู้รับผิดชอบ	เอกสารที่เกี่ยวข้อง	ระยะเวลา
	**ขั้นตอนที่ 4** ผู้บริหารจัดการระบบเพิ่มการเชื่อมโยงสิทธิ์การเข้าใช้งานกับ Account Wifi Rmutt	ผู้บริหารจัดการระบบ	ระบบบริหารงานบุคลากรและเงินเดือน	5 นาที
	**ขั้นตอนที่ 5** ผู้บริหารจัดการระบบดำเนินการกำหนดสิทธิ์การเข้าถึงเมนูระบบบริหารงานบุคลากรและเงินเดือน	ผู้บริหารจัดการระบบ	ระบบบริหารงานบุคลากรและเงินเดือน	15-30 นาที
	**ขั้นตอนที่ 6** ดำเนินการติดตั้งโปรแกรม	ผู้บริหารจัดการระบบ	ระบบบริหารงานบุคลากรและเงินเดือน	10 นาที
	**ขั้นตอนที่ 7** ผู้บริหารจัดการระบบแจ้งผลการดำเนินการกับทางต้นเรื่อง โดยส่งรายละเอียดไปทาง e-mail พร้อมแนบคู่มือการใช้งานระบบ แนะนำการเข้าใช้งานเบื้องต้น และทำหนังสือตอบกลับเรื่องแจ้งผลการเพิ่มสิทธิ์การเข้าใช้งานระบบ	ผู้บริหารจัดการระบบ	e-mail และบันทึกข้อความ	15-30 นาที
				

รายละเอียดของกระบวนการและขั้นตอนการปฏิบัติงาน

ขั้นตอนที่ 1 หน่วยงาน/คณะต้นสังกัดแจ้งขอเพิ่มสิทธิ์โดยทำบันทึกข้อความส่งในระบบสารบรรณอิเล็กทรอนิกส์ (e-office) ผ่านผู้บังคับบัญชาส่งถึงผู้อำนวยการกองบริหารงานบุคคล ดังตัวอย่างภาพที่ 4-30



สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี
เลขที่รับ 929/2565
วันที่ 6 พ.ค. 65
เวลา 09:57 น.

กองบริหารงานบุคคล
มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี
เลขที่รับ 1376/2565
วันที่ 3 พ.ค. 65
เวลา 14:58 น.

บันทึกข้อความ

ส่วนราชการ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี โทร. ๐ ๒๕๔๙ ๓๔๗๖

ที่ อว ๐๖๔๙.๐๔/ ๑๓๒๘ **วันที่** ๓ พฤษภาคม ๒๕๖๕

เรื่อง ขอความอนุเคราะห์เปิดสิทธิเข้าระบบบุคลากร

เรียน ผู้อำนวยการกองบริหารงานบุคคล

ด้วยคณะวิศวกรรมศาสตร์ มีความประสงค์ขอเปิดสิทธิเข้าระบบบุคลากร ให้กับเจ้าหน้าที่ที่ย้ายมาปฏิบัติหน้าที่ใหม่ เพื่อให้งานบุคลากรของคณะฯ เกิดความสะดวกรวดเร็วและมีประสิทธิภาพในการทำงานรวมทั้งสามารถจัดการฐานข้อมูลแก้ไขและปรับปรุงข้อมูลบุคลากรของคณะ ในด้านต่างๆ ในการนี้ คณะวิศวกรรมศาสตร์ จึงขอความอนุเคราะห์เปิดสิทธิเข้าระบบบุคลากร จำนวน ๓ ราย คือนายธีรวุฒิ ศุภรัตนาภิรักษ์ ตำแหน่ง เจ้าหน้าที่บริหารงานทั่วไป

จึงเรียนมาเพื่อโปรดพิจารณาดำเนินการในส่วนที่เกี่ยวข้องต่อไป จะขอบคุณยิ่ง

(รองศาสตราจารย์ ดร.สรพงษ์ ภาสุปรีย์)
คณบดีคณะวิศวกรรมศาสตร์

๑ เรียน ผอ.กบค.
เพื่อโปรดทราบและมอบ สวส.ดำเนินการต่อไป

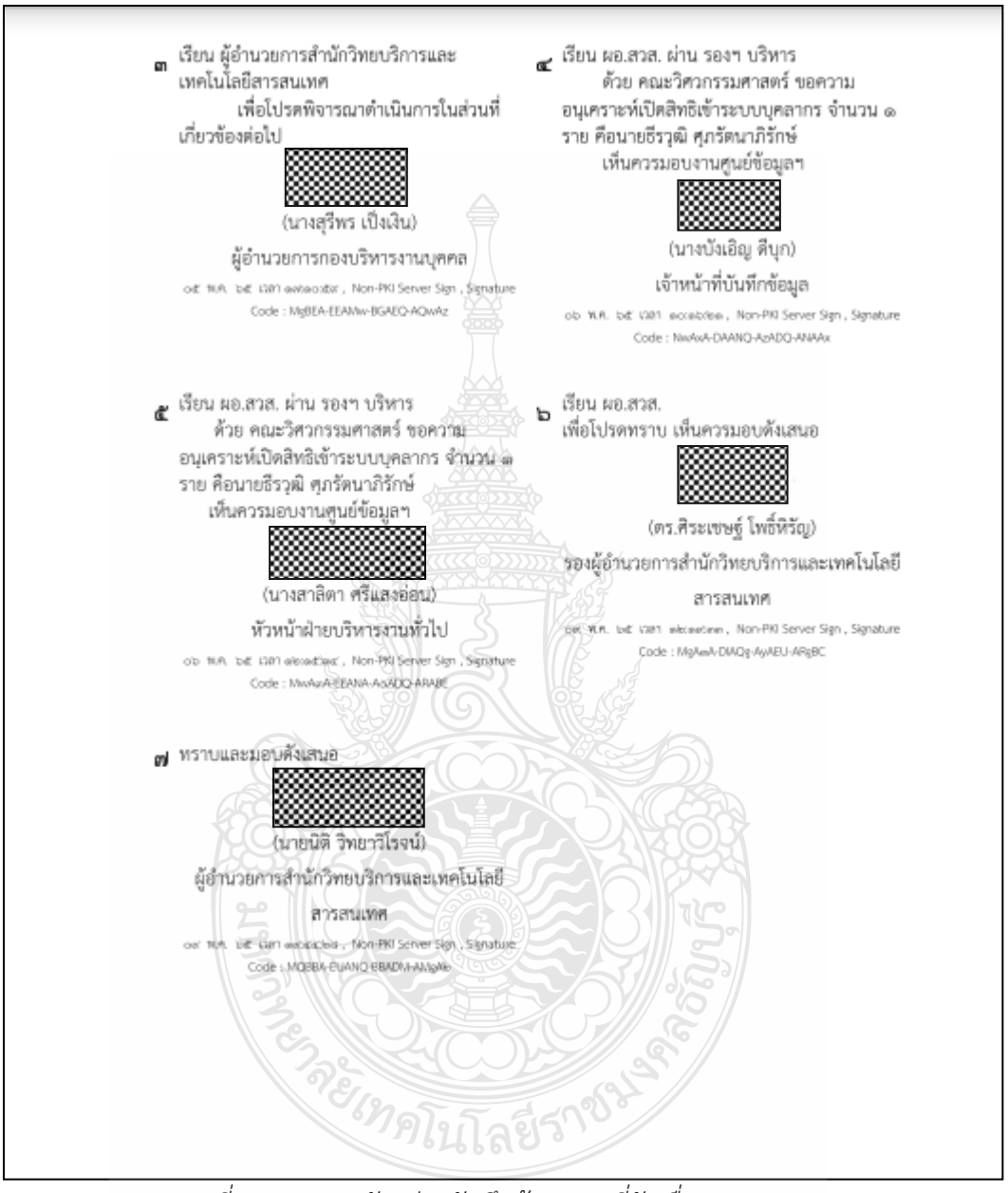
(นางศิริญทิพย์ แก้วแทน)
พนักงานธุรการ

๒ เรียน ผู้อำนวยการ เห็นควรดำเนินการตามเสนอ

(นายคมกริช พุมเกิด)
หัวหน้าฝ่ายอัตรากำลังและค่าตอบแทน

ภาพที่ 4-30 แสดงตัวอย่างบันทึกข้อความหน่วยงาน/คณะต้นสังกัดแจ้งขอเพิ่มสิทธิ์

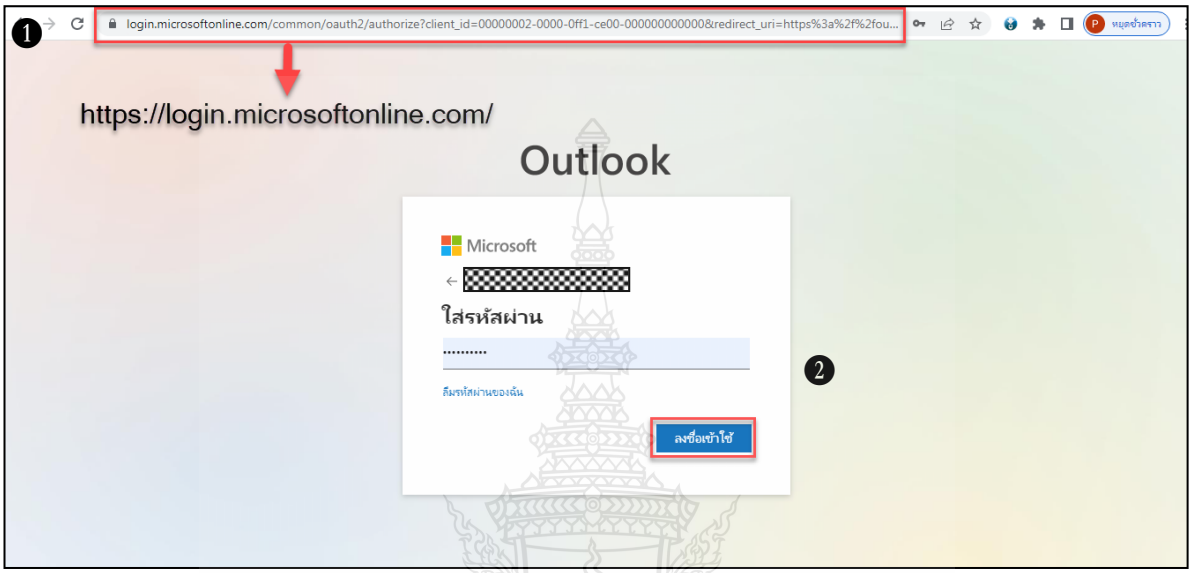
ขั้นตอนที่ 2 รับเรื่องจากกองบริหารงานบุคคล โดยผู้บังคับบัญชาพิจารณามอบหมายงานเพื่อให้ผู้บริหารจัดการระบบดำเนินการกำหนดสิทธิ์การเข้าใช้งาน ดังตัวอย่างภาพที่ 4-31



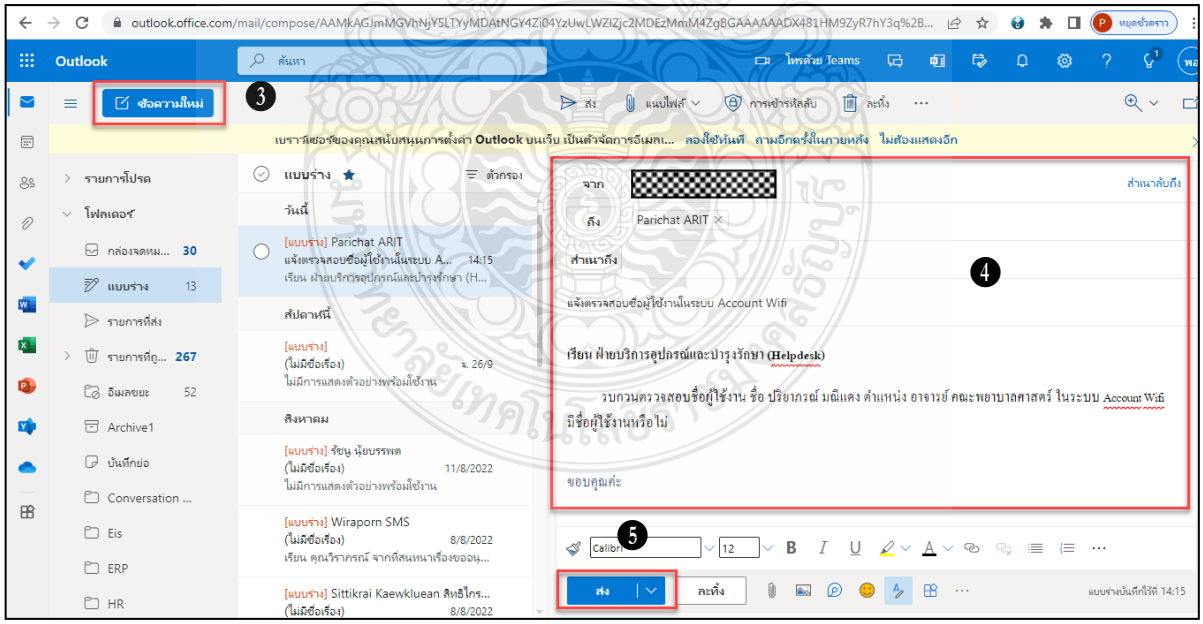
ภาพที่ 4-31 แสดงตัวอย่างบันทึกข้อความ ที่รับเรื่องมาจาก กบค.

***** ข้อควรระวัง** จากการปฏิบัติงานพบว่า ผู้บริหารจัดการระบบจะต้องสอบถามทางเจ้าหน้าที่บุคคลของหน่วยงาน/คณะ ให้แน่ชัดว่าผู้ดูแลระบบคนเดิมยังให้คงชื่อผู้ใช้งาน (Username) ไว้หรือไม่ หรือชื่อผู้ใช้ที่ส่งมาเป็นการช่วยงานต้องคงชื่อผู้ใช้งานเดิมไว้ และดำเนินการเพิ่มสิทธิ์ตามบันทึกข้อความที่ส่งมา

ขั้นตอนที่ 3 ผู้บริหารจัดการระบบตรวจสอบ Account Wifi ของผู้ขอใช้บริการ โดยทำการส่ง e-mail ให้ฝ่ายบริการอุปกรณ์และบำรุงรักษา (Helpdesk) ที่ดูแลรับผิดชอบระบบ AD ของทางมหาวิทยาลัยฯ โดยสามารถดำเนินการได้ ดังนี้



ภาพที่ 4-32 แสดงตัวอย่างหน้าจอเข้าสู่ระบบ Mail@rmutt.ac.th



ภาพที่ 4-33 แสดงตัวอย่างหน้าจอการส่ง e-mail

หมายเลข 1 เข้าไปที่ Mail@rmutt ของมหาวิทยาลัยที่ใช้ในการรับ-ส่งข้อมูลที่ลิงก์ https://Login.microsoftonline.com/ โดยกรอกชื่อผู้ใช้และรหัสผ่าน

หมายเลข 2 คลิกปุ่ม “ลงชื่อเข้าใช้”

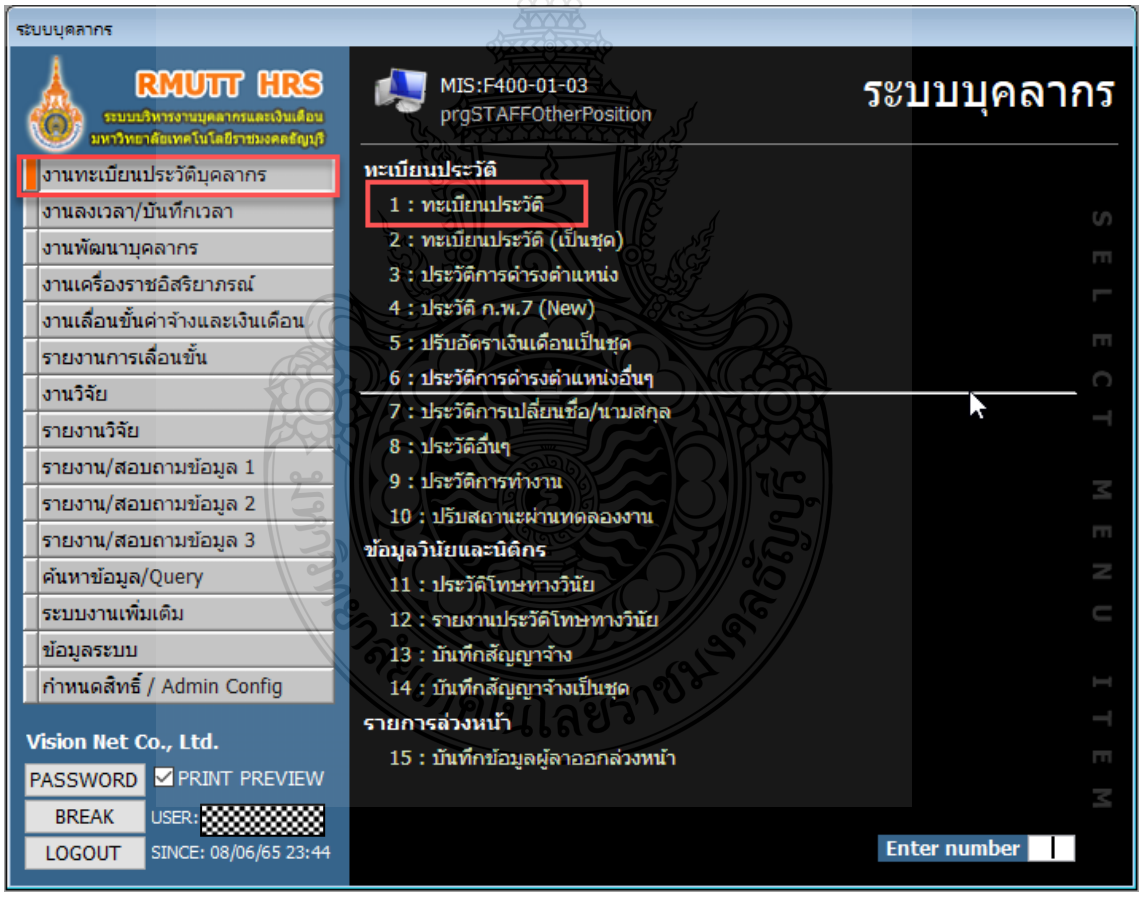
หมายเลข 3 กดปุ่ม “สร้างข้อความใหม่”

หมายเลข 4 ใช่ชื่อ e-mail และเนื้อหา

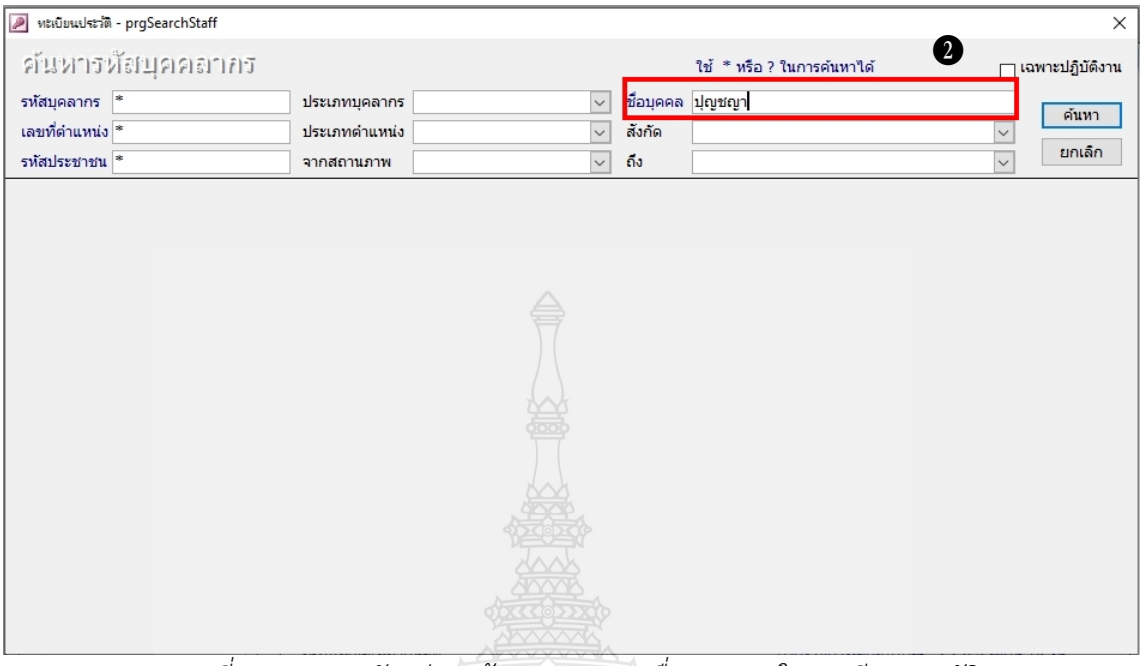
หมายเลข 5 กดปุ่ม “ส่ง”

กรณีตรวจสอบแล้วไม่มีให้ดำเนินการกลับไปที่ขั้นตอนที่ 1 เพื่อแจ้งกลับทางหน่วยงานหรือคณะดำเนินการส่งประวัติบุคลากรให้กับกองบริหารงานบุคคลเพื่อเพิ่มข้อมูลบุคลากรในระบบ และแจ้งสมัคร Account Wifi สำหรับบุคลากรใหม่ที่จุดบริการของสำนักวิทยบริการและเทคโนโลยีสารสนเทศ

กรณีพบว่ามี Account Wifi ผู้บริหารจัดการระบบจะดำเนินการนำชื่อผู้ใช้ไปเชื่อมโยงสิทธิ์ โดยจะต้องตรวจสอบรหัสบุคลากรในทะเบียนประวัติ ดังนี้



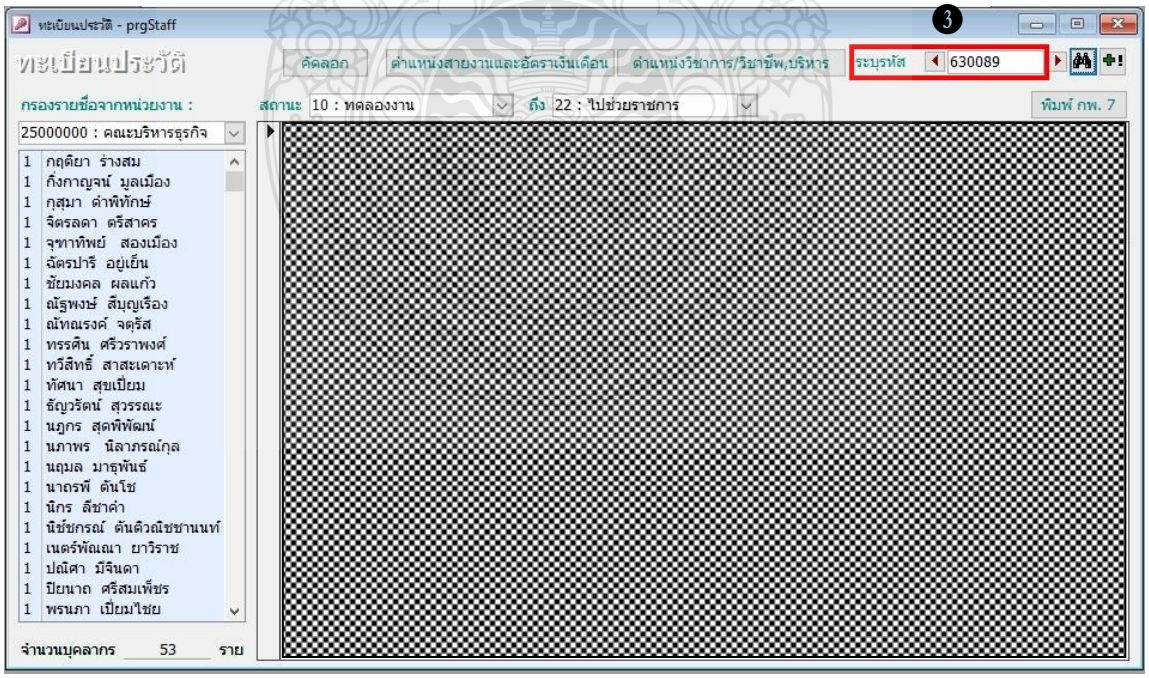
ภาพที่ 4-34 แสดงตัวอย่างหน้าจองานทะเบียนประวัติบุคลากร



ภาพที่ 4-35 แสดงตัวอย่างหน้าจอตรวจสอบชื่อบุคลากรในทะเบียนประวัติ

หมายเลข 1 เรียกเมนู ระบบบริหารงานบุคลากร >งานทะเบียนประวัติบุคลากร >ทะเบียนประวัติ

หมายเลข 2 ค้นหาในช่องชื่อบุคคล และกดปุ่มค้นหา



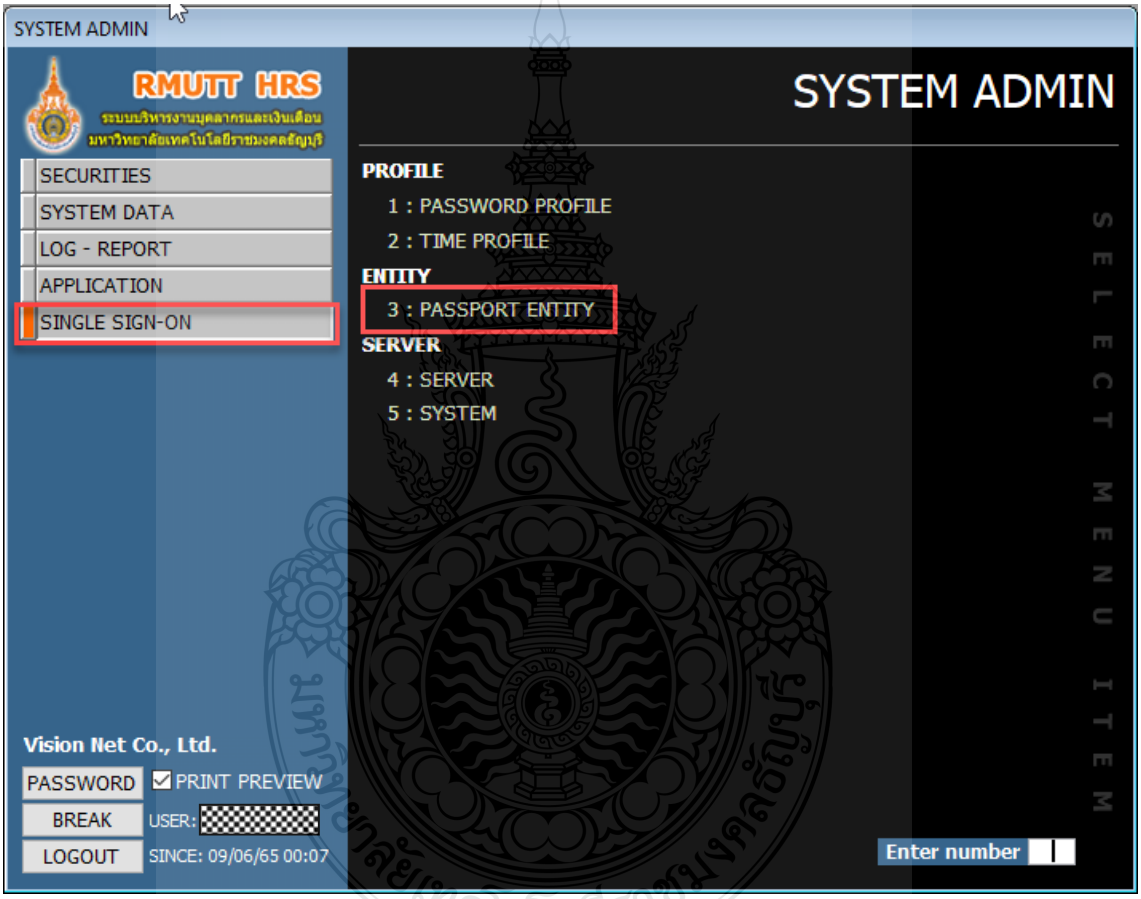
ภาพที่ 4-36 แสดงตัวอย่างหน้าจอทะเบียนประวัติแสดงข้อมูลบุคลากร

หมายเลข 3 จะปรากฏหน้าต่างทะเบียนประวัติแสดงข้อมูลบุคลากร ตรวจสอบรหัสบุคลากรในช่องระบุรหัส ซึ่งจะต้องนำรหัสบุคลากรไปใช้ในการเชื่อมโยงสิทธิ์การเข้าถึงการเข้าใช้งานกับ Account Wifi Rmutt ในขั้นตอนที่ 4 ต่อไป

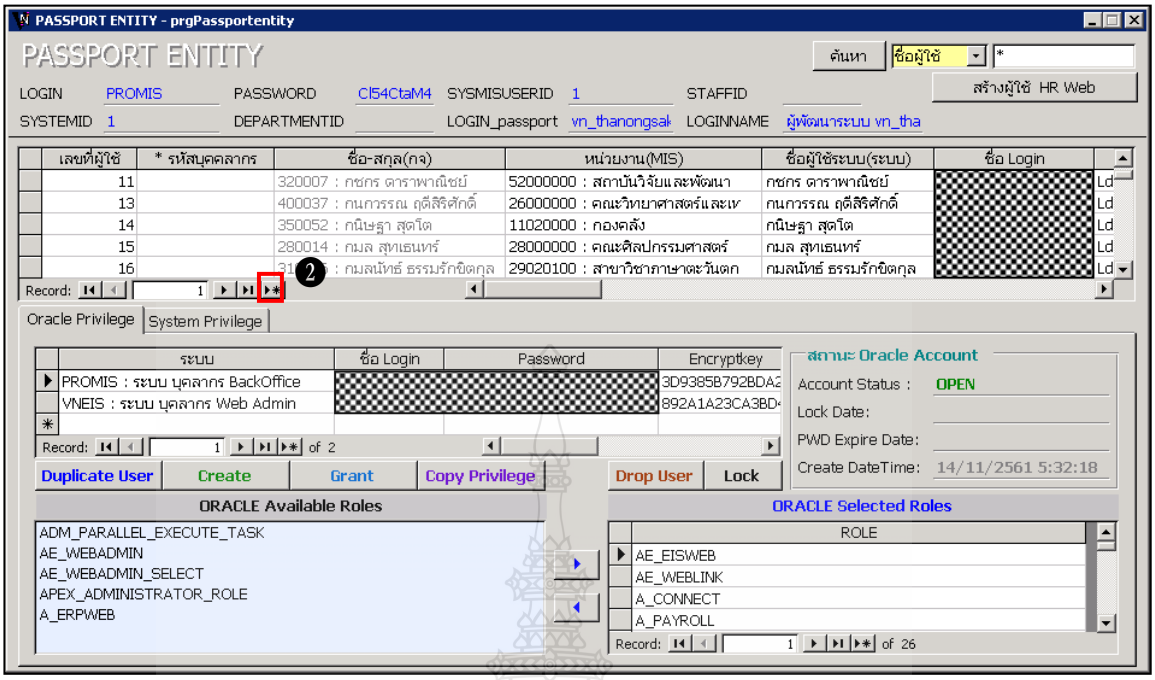
ขั้นตอนที่ 4 ผู้บริหารจัดการระบบเพิ่มการเชื่อมโยงสิทธิ์การเข้าใช้งานกับ Account Wifi Rmutt วิธีกำหนดสิทธิ์การใช้งานระบบ

กำหนดสิทธิ์เข้าใช้งานระบบ ดังนี้

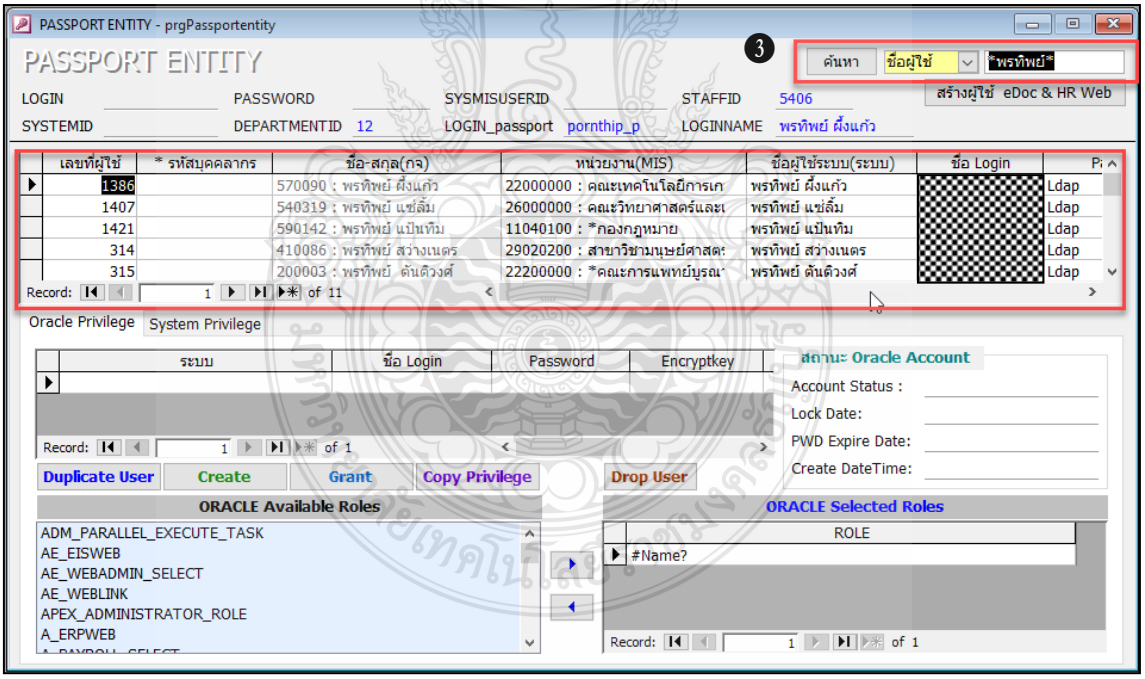
กำหนดสิทธิ์ผู้ใช้ใหม่



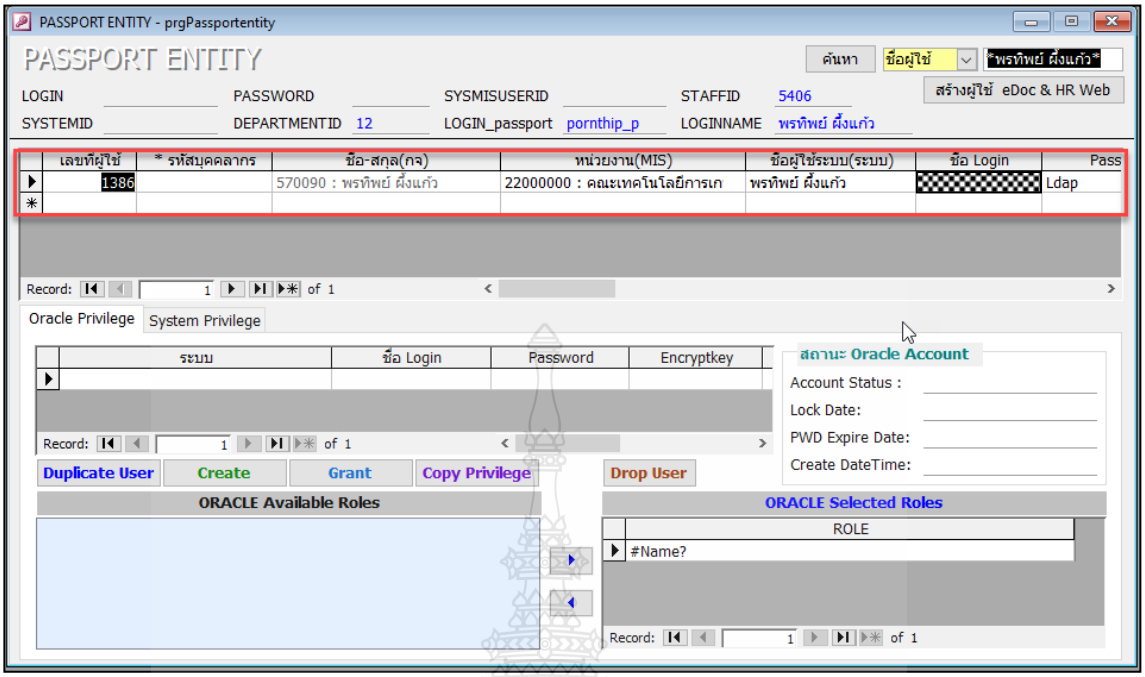
ภาพที่ 4-37 แสดงตัวอย่างหน้าจอ SINGLE SIGN-ON



ภาพที่ 4-38 แสดงตัวอย่างหน้าจอการเพิ่มระเบียนใหม่



ภาพที่ 4-39 แสดงตัวอย่างหน้าจอแสดงรายชื่อบุคลากรซ้ำ



ภาพที่ 4-40 แสดงตัวอย่างหน้าจอเพิ่มการเชื่อมโยงสิทธิ์การเข้าใช้งานกับ Account Wifi Rmutt

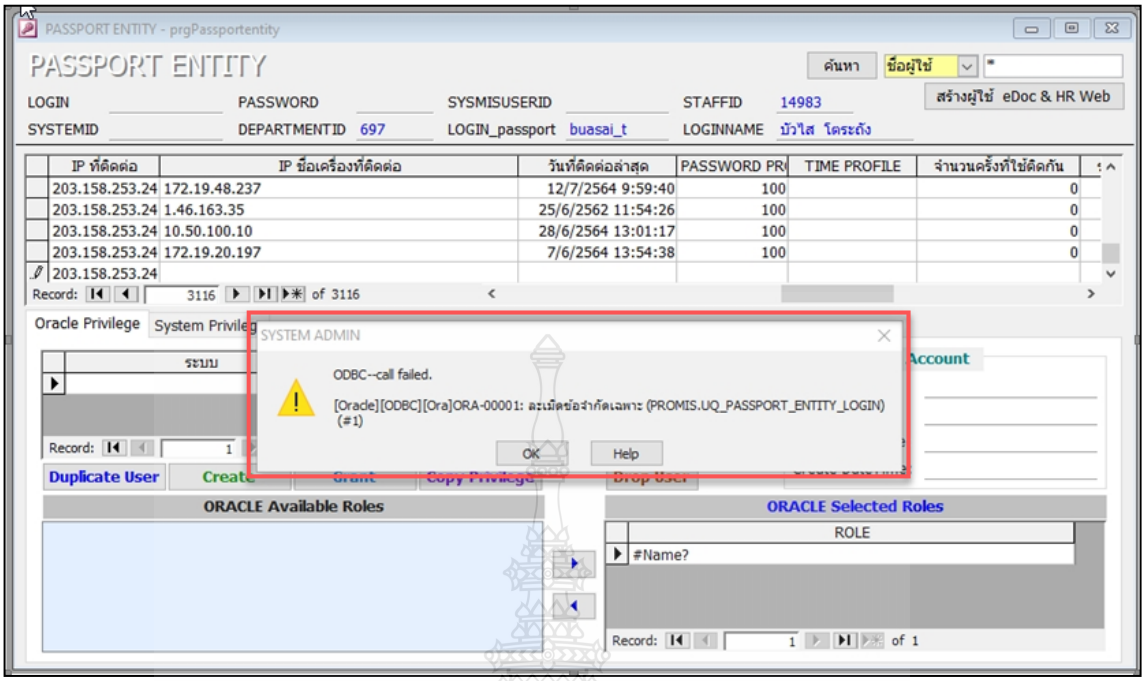
หมายเลข 1 เรียกเมนู ระบบสำหรับผู้ดูแลระบบ> SINGLE SIGN-ON > PASSPORT ENTITY

หมายเลข 2 กดปุ่ม  เพื่อไปที่ระเบียนใหม่

หมายเลข 3 จากนั้นพิมพ์ชื่อบุคลากรที่ต้องการเพิ่มสิทธิ์ให้ใช้งานระบบในช่องชื่อผู้ใช้ ในกรณี ที่ชื่อบุคลากรซ้ำ ระบบจะแสดงหน้าจอค้นหารหัสบุคลากร

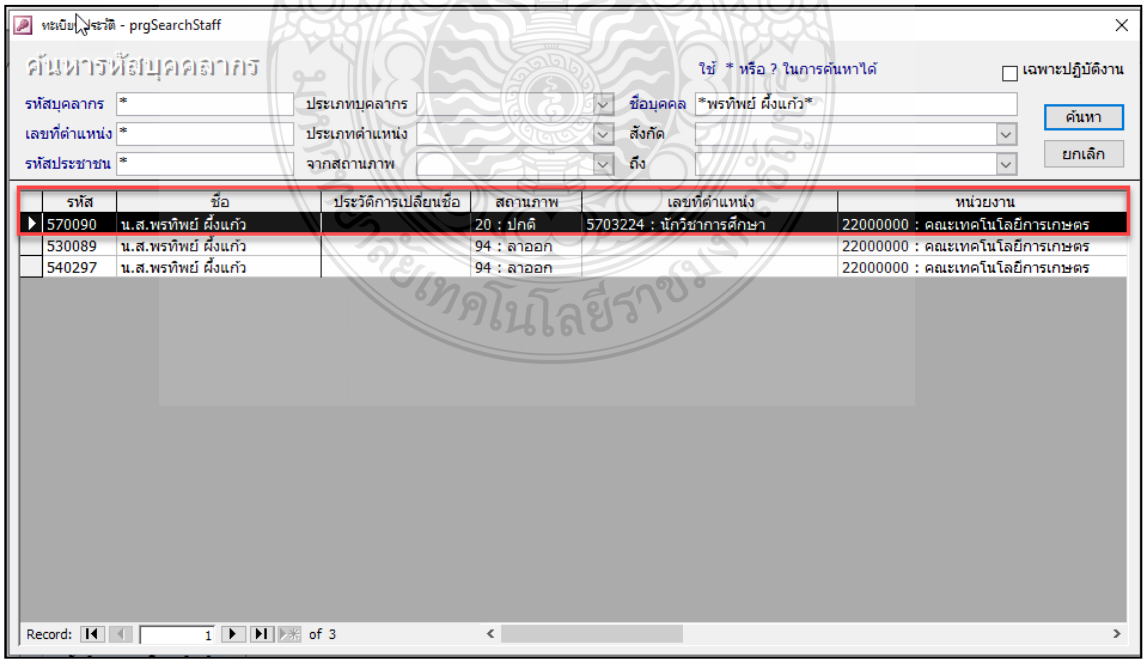
หมายเลข 4 ให้เลือกบุคลากรที่ต้องการกำหนดสิทธิ์ โดยการดับเบิ้ลคลิกปุ่ม  ด้านหน้าเมื่อเพิ่มชื่อบุคลากรแล้วระบบจะแสดงชื่อผู้ใช้งานระบบ , ชื่อผู้ใช้ (ระบบ) และ หน่วยงาน (MIS) ให้ในกรณีที่ต้องการกำหนดสิทธิ์ให้กับบุคลากรที่ไม่มีชื่อหรือทะเบียนประวัติในระบบบุคลากร ให้ระบุชื่อผู้ใช้ (ระบบ) และหน่วยงาน (MIS) เอง จากนั้นระบุชื่อ LOG IN โดยมีรูปแบบคือ ชื่อภาษาอังกฤษ_นามสกุลตัวแรก

***ข้อควรระวัง** จากการปฏิบัติงานพบว่า หากชื่อและนามสกุลตัวแรกซ้ำกับจะขึ้น Error แจ้งเตือนชื่อผู้ใช้งานในการ LOG IN ที่กำหนดซ้ำกับข้อมูลที่มีอยู่ ให้กำหนดชื่อผู้ใช้งานเดิมโดยเพิ่ม _นามสกุลเป็น 2 ตัว และกำหนด Password ให้กับชื่อผู้ใช้งาน ดังตัวอย่างภาพที่ 4-41



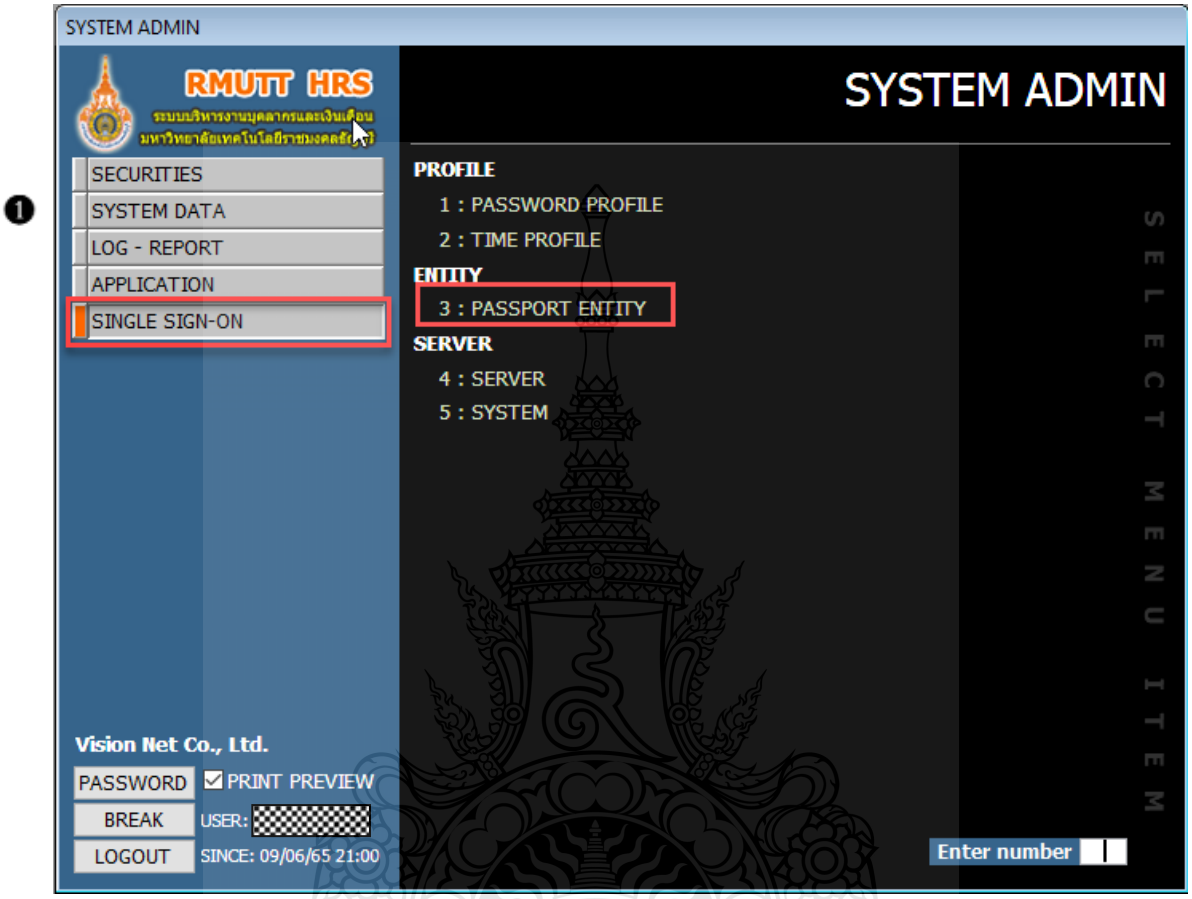
ภาพที่ 4-41 แสดงตัวอย่างหน้าจอแจ้งเตือนชื่อผู้ใช้งานในการ LOG IN ที่กำหนดซ้ำกับข้อมูลที่มีอยู่

*****ข้อควรระวัง** จากการปฏิบัติงานพบว่า ผู้บริหารจัดการระบบต้องตรวจสอบรหัสบุคลากรในทะเบียนประวัติว่า Account Wifi ที่เชื่อมโยงสิทธิ์นั้น ผูกกับรหัสเดิมหรือไม่ เช่น มีการปรับเปลี่ยนตำแหน่งงานในสถานภาพเดิมจะเป็น :ลาออก ให้นำรหัสบุคลากรสถานะ : ปกติ ไปทำการเชื่อมโยงสิทธิ์การเข้าใช้งานกับ Account Wifi Rmutt ดังตัวอย่างภาพที่ 4-42

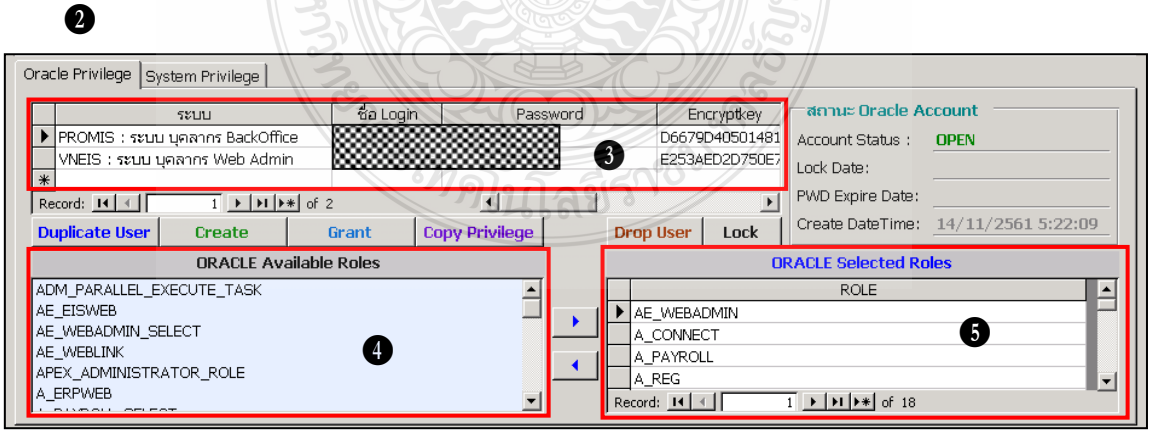


ภาพที่ 4-42 แสดงตัวอย่างหน้าจอชื่อผู้ใช้งานที่มีหลายสถานภาพ

ขั้นตอนที่ 5 ผู้บริหารจัดการระบบดำเนินการกำหนดสิทธิ์การเข้าถึงเมนูระบบบริหารงานบุคลากรและเงินเดือน เพื่อให้ผู้ใช้สามารถเข้าใช้งานระบบได้ สามารถดำเนินการได้ ดังต่อไปนี้



ภาพที่ 4-43 แสดงตัวอย่างหน้าจอ SINGLE SIGN-ON

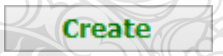


ภาพที่ 4-44 แสดงตัวอย่างหน้าจอกำหนดสิทธิ์การใช้งานระบบ

หมายเลข 1 เรียกเมนู ระบบสำหรับผู้ดูแลระบบ> SINGLE SIGN-ON > PASSPORT ENTITY
หมายเลข 2 คลิกที่ Tab Oracle Privilege
หมายเลข 3 กำหนดสิทธิ์การเชื่อมโยงในการเข้าใช้งานแต่ละระบบ โดยระบุข้อมูลดังนี้

ตารางที่ 4.3.1 คำอธิบายข้อมูลกำหนดสิทธิ์การเชื่อมโยงในการเข้าใช้งานแต่ละระบบ

ข้อมูล	คำอธิบาย
ระบบ	ระบุระบบที่ต้องการใช้งาน - PROMIS : MIS ระบบบริหารงานบุคลากร - AVSREG : Register ระบบบริการการศึกษา - VNEIS : EIS ระบบแสดงผลข้อมูลบุคลากรออนไลน์
ชื่อ LOG IN	ระบุชื่อ LOG IN สำหรับ Oracle
Password	ระบุ Password สำหรับ Oracle
สถานะการใช้งาน	ระบุสถานะการใช้งานระบบ -Y:Yes อนุญาตเข้าใช้งานระบบ -N:No ไม่อนุญาตให้เข้าใช้งานระบบ

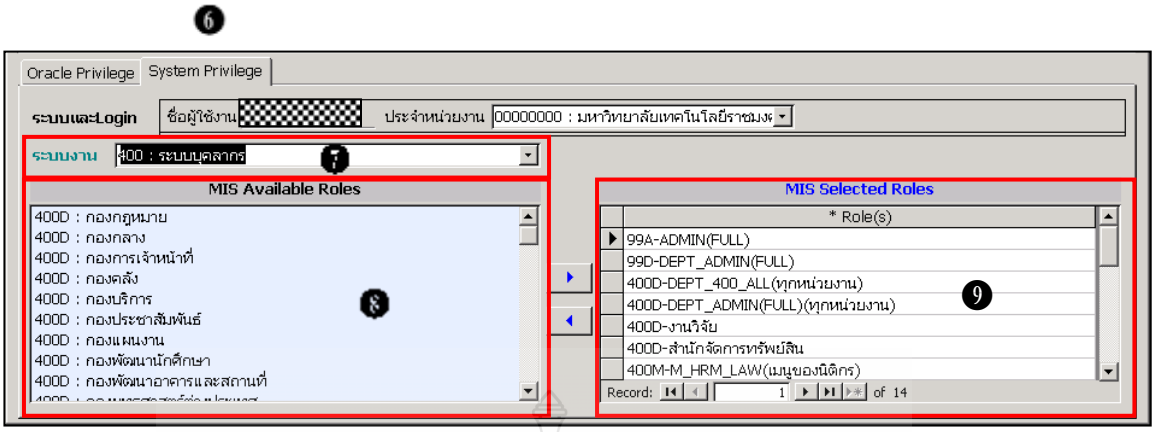
หลังจากระบุข้อมูลเรียบร้อยแล้วให้กดปุ่ม 

เพื่อกำหนด User ของ Oracle

หมายเลข 4 Oracle Available Role เป็นกลุ่มสิทธิ์ที่กำหนดสำหรับการเข้าใช้ฐานข้อมูล Oracle (สิทธิ์ Role ใน Oracle) โดยสิทธิ์ที่อยู่ส่วนของ Oracle Available Role เป็น Role ซึ่งยังไม่ได้อนุญาตให้ User มีสิทธิ์ในการเข้าถึง Oracle ในกรณีที่ต้องการกำหนดสิทธิ์การเข้าถึงของระบบใดให้ดับเบิ้ลคลิกที่สิทธิ์ของระบบนั้น หรือกดปุ่ม  โดยการกำหนดสิทธิ์ของแต่ละระบบต้องกำหนดสิทธิ์ 2 สิทธิ์นี้เป็นหลักคือ A_ชื่อระบบ และ A_ชื่อระบบ_Select โดยสิทธิ์ที่สำคัญคือต้องกำหนด A_Connect ให้กับทุก User สิทธิ์ที่ดับเบิ้ลคลิกจะถูกย้ายไปอยู่ในฝั่งของ Oracle Selected Role จากนั้นให้คลิกปุ่ม 

เพื่อสร้างข้อมูลสิทธิ์ Role ในฐานข้อมูล Oracle ให้กับ User นั้น

หมายเลข 5 Oracle Selected Role แสดงสิทธิ์ในการเข้าใช้ฐานข้อมูลที่ User ได้รับ



ภาพที่ 4-45 แสดงตัวอย่างหน้าจอสร้างข้อมูลสิทธิ์ Role ในฐานข้อมูล Oracle ให้กับ User

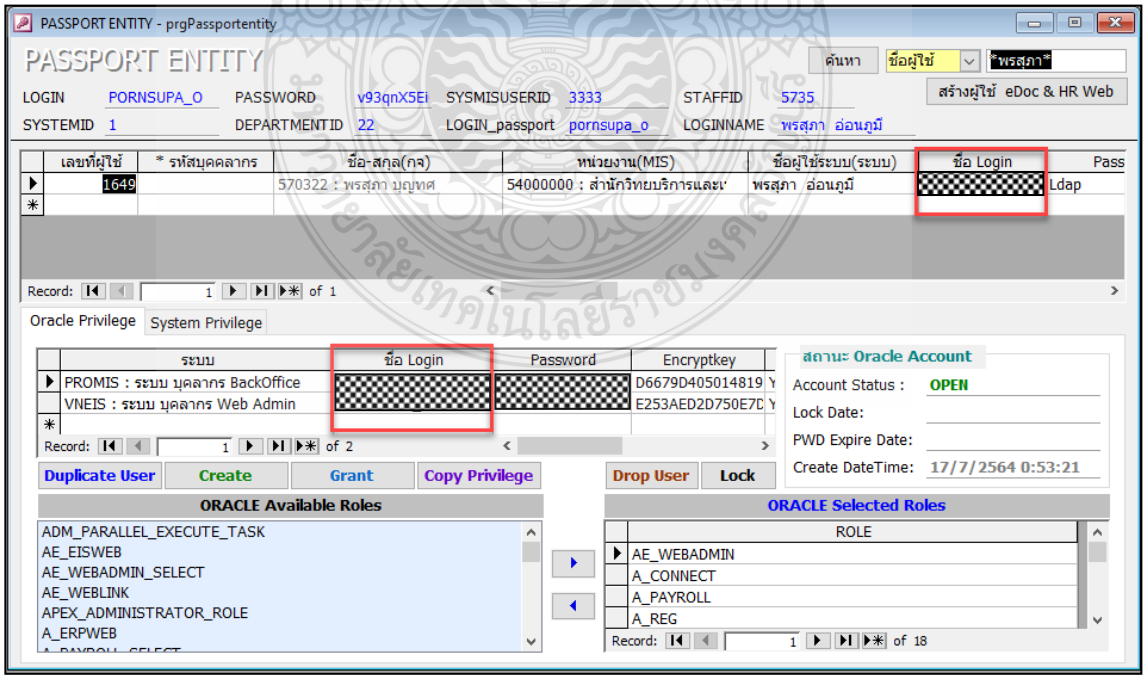
หมายเลข 6 คลิกที่ Tab System Privilege

หมายเลข 7 เลือกระบบงานต้องการกำหนดสิทธิ์

หมายเลข 8 กรอบ MIS Available Role เป็นสิทธิ์ในการเข้าใช้ระบบ หรืออีกอย่างหนึ่งก็คือสิทธิ์ในการเข้าถึง menu ของระบบ รวมถึงรายงานด้วย สำหรับการกำหนดสิทธิ์การเข้าใช้เมนู (Menu) , กำหนดสิทธิ์การเข้าถึงหน่วยงาน (DEP) และแหล่งเงิน (BGROUP) ให้เลือกที่สิทธิ์ที่ต้องการกำหนดให้กับ User จากนั้นดับเบิ้ลคคลิก หรือกดปุ่ม  สิทธิ์ที่ถูกกำหนดจะย้ายไปฝั่ง MIS Selected Roles

หมายเลข 9 MIS Selected Roles แสดงสิทธิ์ที่ User ได้รับ

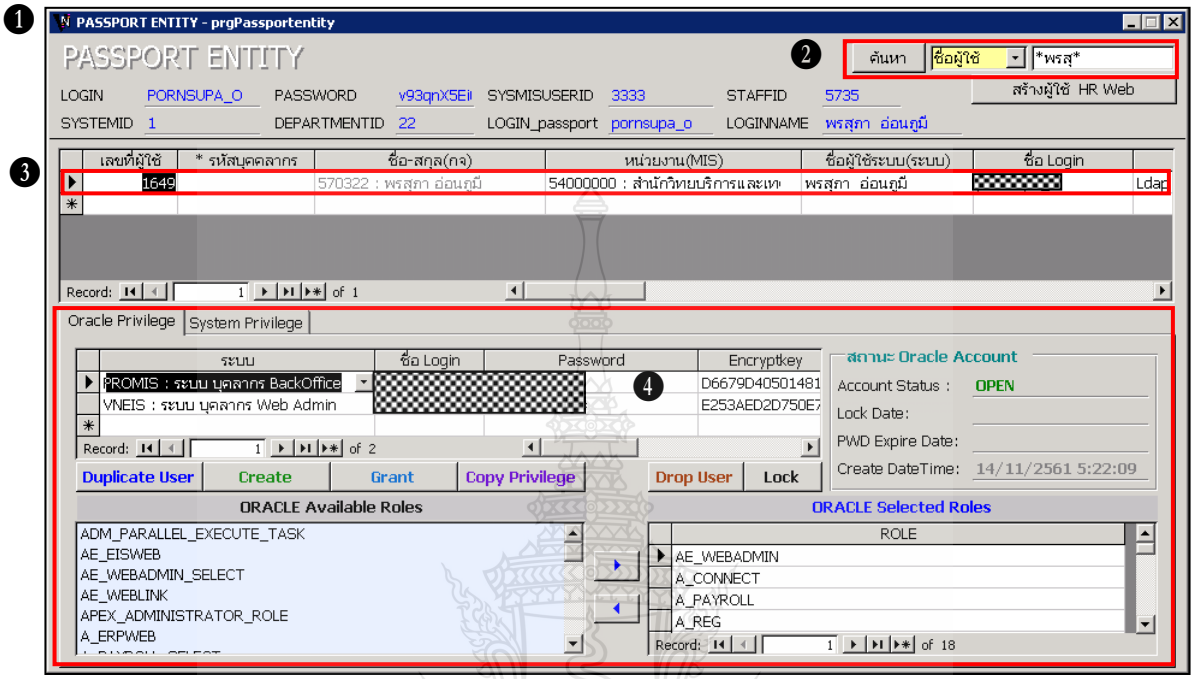
***ข้อควรระวัง** จากการปฏิบัติงานพบว่าหากผู้ใช้งานมีการเปลี่ยน User Account Wifi ผู้บริหารจัดการระบบจะต้องดำเนินการเปลี่ยนในคอลัมน์ชื่อ LOG IN โดยกำหนดเป็นชื่อผู้ใช้งาน (User) ให้ปัจจุบัน



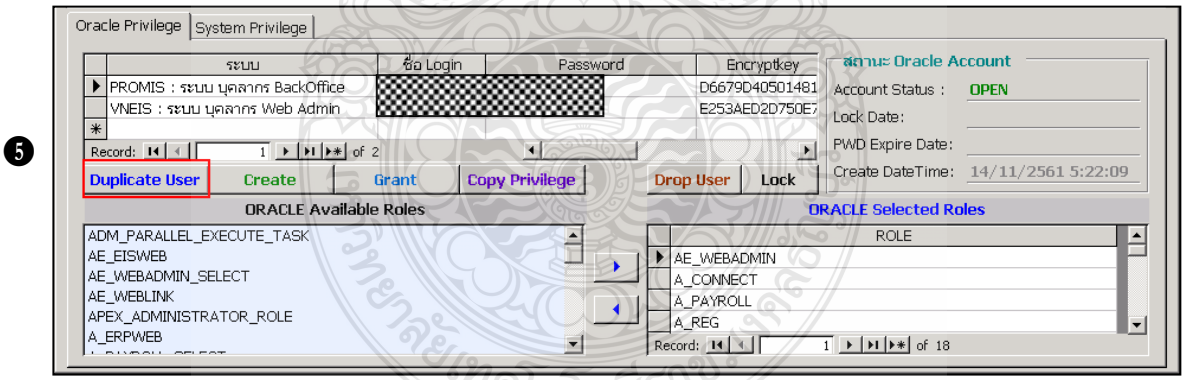
ภาพที่ 4-46 แสดงตัวอย่างหน้าจอแสดงชื่อ LOG IN

กำหนดสิทธิ์ผู้ใช้เหมือน

การกำหนดสิทธิ์ผู้ใช้เหมือน คือการกำหนดสิทธิ์เข้าใช้งาน, สิทธิ์การเข้าถึงหน่วยงานให้เหมือนสิทธิ์ของผู้ใช้อื่น สามารถดำเนินการได้ ดังต่อไปนี้



ภาพที่ 4-47 แสดงตัวอย่างหน้าจอกำหนดสิทธิ์การใช้งานระบบ



ภาพที่ 4-48 แสดงตัวอย่างหน้าจอกำหนดสิทธิ์ผู้ใช้เหมือน

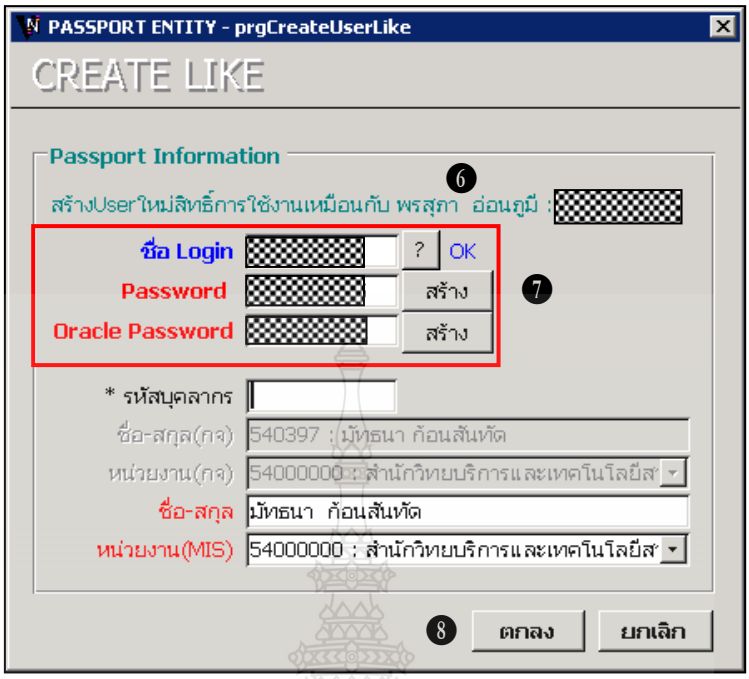
หมายเลข 1 เรียกเมนู ระบบสำหรับผู้ดูแลระบบ> SINGLE SIGN-ON > PASSPORT ENTITY

หมายเลข 2 ค้นหาชื่อผู้ใช้ต้นแบบ โดยการระบุชื่อผู้ใช้ หรือ LOG IN

หมายเลข 3 คลิกเลือกผู้ใช้ที่ต้องการเป็นต้นแบบ

หมายเลข 4 กำหนดสิทธิ์การใช้งานระบบ

หมายเลข 5 กำหนดสิทธิ์การใช้งานระบบคลิกปุ่ม **Duplicate User** ระบบจะแสดงหน้าจอกำหนดข้อมูลผู้ใช้ใหม่



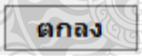
ภาพที่ 4-49 แสดงตัวอย่างหน้าจอกำหนดข้อมูลผู้ใช้ใหม่

หมายเลข 6 กรณีที่กำหนดสิทธิ์เหมือนให้กับบุคลากรของมหาวิทยาลัย ให้ระบุชื่อบุคลากรในส่วนของรหัสบุคลากร จากนั้นระบบจะแสดงข้อมูลของบุคลากร

หมายเลข 7 ระบบแสดงชื่อ LOG IN ตั้งต้นให้ (สามารถตรวจ LOG IN ซ้ำได้ด้วยการ Click ปุ่ม ?

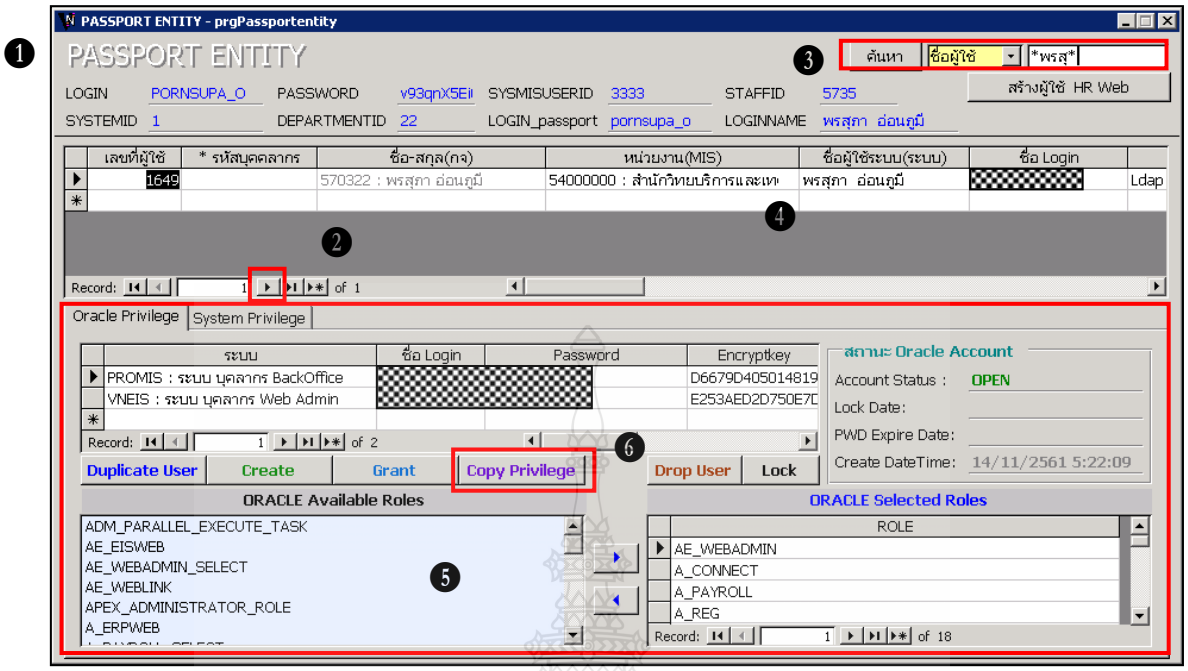
“Password” คือ รหัสผ่านที่กำหนดให้แก่ผู้ใช้งาน

“Oracle Password” คือ รหัสผ่านของชื่อผู้ใช้งานใน Oracle ให้กำหนดใหม่ โดยไม่ควรตรงกันกับช่อง “Password” และเป็นรหัสที่ยากต่อการจดจำ (เพื่อป้องกันการเชื่อมต่อฐานข้อมูลโดยตรง)

หมายเลข 8 คลิกปุ่ม 

การคัดลอกสิทธิ์ผู้ใช้งาน

การคัดลอกสิทธิ์ผู้ใช้งาน คือการทำสำเนาสิทธิ์เข้าใช้งาน, สิทธิ์การเข้าถึงหน่วยงานและแหล่งเงินให้เหมือนสิทธิ์ของผู้ใช้อื่น สามารถดำเนินการได้ ดังต่อไปนี้



ภาพที่ 4-50 แสดงตัวอย่างหน้าจอคัดลอกสิทธิ์ผู้ใช้งาน

หมายเลข 1 เรียกเมนู ระบบสำหรับผู้ดูแลระบบ> SINGLE SIGN-ON > PASSPORT ENTITY

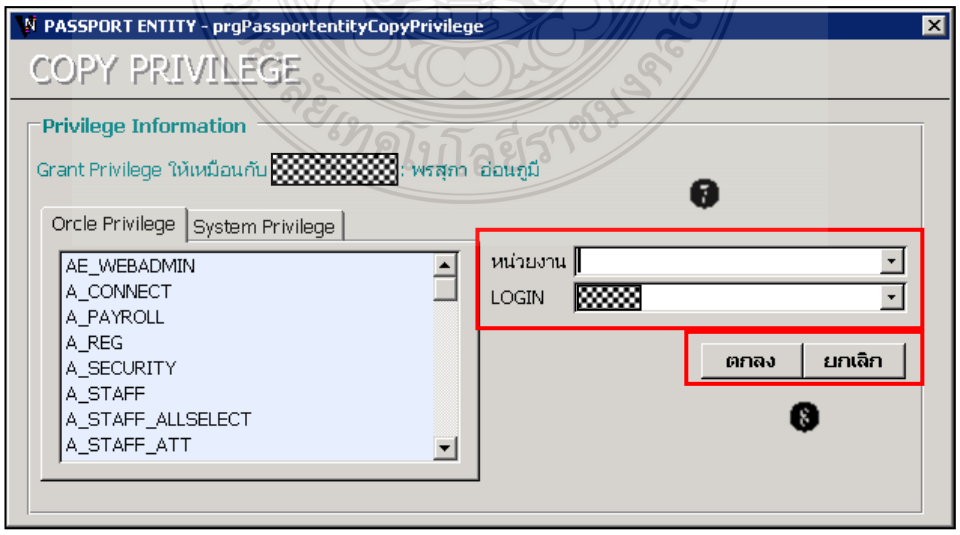
หมายเลข 2 กำหนดชื่อผู้ใช้งานระบบคนใหม่ โดยระบุชื่อบุคลากรในช่องรหัสบุคลากร จากนั้นกำหนดชื่อ LOG IN และ Password

หมายเลข 3 ค้นหาชื่อผู้ใช้ต้นแบบ โดยการระบุชื่อผู้ใช้ หรือ LOG IN

หมายเลข 4 คลิกเลือกผู้ใช้ที่ต้องการเป็นต้นแบบ

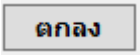
หมายเลข 5 กำหนดสิทธิ์ระบบงาน

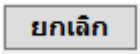
หมายเลข 6 คลิกปุ่ม Copy Privilege ระบบจะแสดง หน้าจอกำหนดข้อมูลผู้ใช้ใหม่



ภาพที่ 4-51 แสดงตัวอย่างหน้าจอกำหนดข้อมูลผู้ใช้ใหม่

หมายเลข 7 ระบุหน่วยงานของผู้ใช้งาน และ LOG IN ของผู้ใช้งานที่ต้องกำหนดสิทธิ์เหมือนผู้ใช้ต้นแบบ

หมายเลข 8 กรณีที่ต้องการกำหนดสิทธิ์ให้คลิกปุ่ม {ตกลง} 

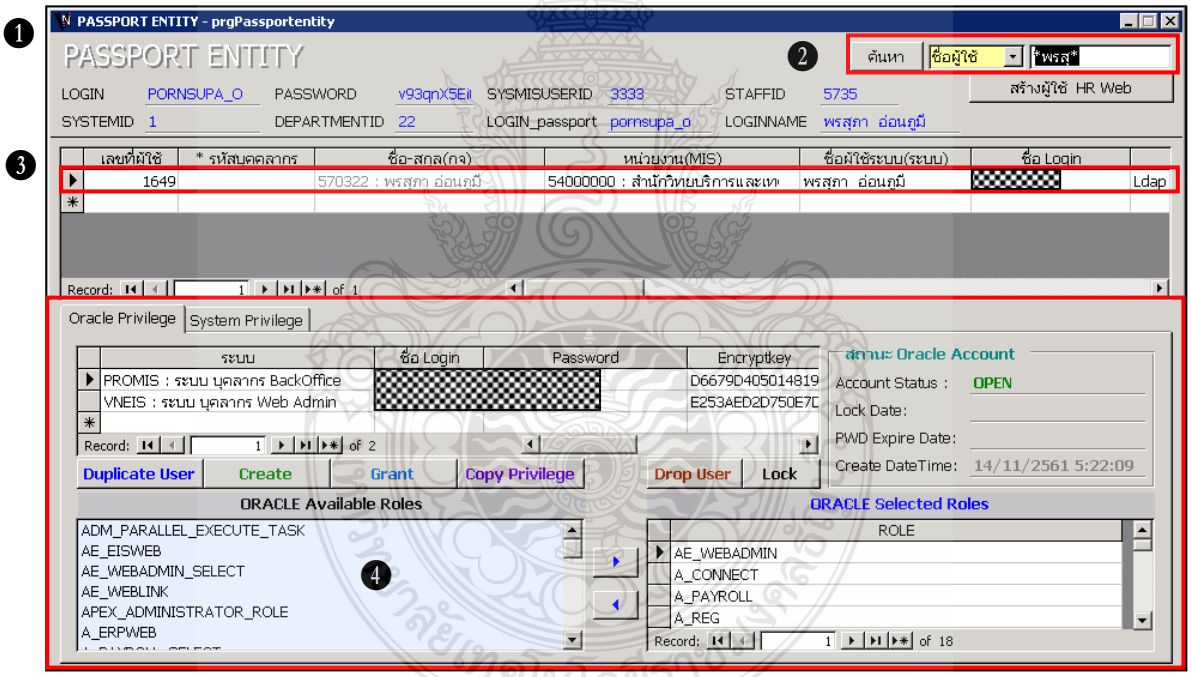
หรือกรณีต้องการยกเลิก การกำหนดสิทธิ์ให้คลิกปุ่ม 

{ยกเลิก}

*****ข้อแนะนำ** จากการปฏิบัติงานพบว่า การกำหนดสิทธิ์โดยการคัดลอกสิทธิ์ผู้ใช้งาน แนะนำให้คัดลอกจากชื่อผู้ใช้งานที่อยู่หน่วยงานเดียวกัน ซึ่งในส่วนของการกำหนดสิทธิ์การเข้าถึงข้อมูลบุคลากรนั้นก็จะอยู่ภายในหน่วยงานเดียวกัน

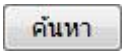
กำหนดสิทธิ์เพิ่มสำหรับผู้ใช้เดิม

การกำหนดสิทธิ์เพิ่มสำหรับผู้ใช้เดิม คือการกำหนดสิทธิ์เข้าใช้งาน, สิทธิ์การเข้าถึงหน่วยงานเพิ่มเติมจากเดิมที่มีอยู่ สามารถดำเนินการได้ดังต่อไปนี้



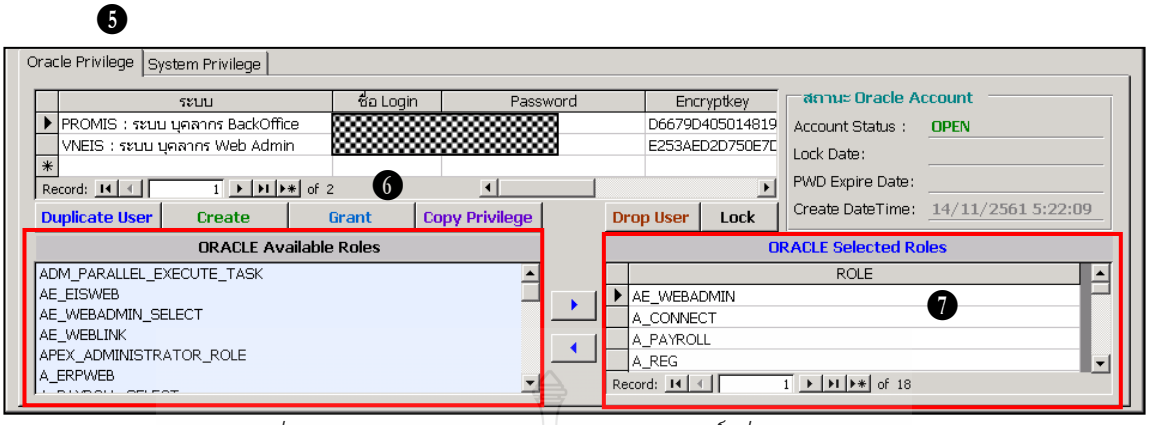
ภาพที่ 4-52 แสดงตัวอย่างหน้าจอกำหนดสิทธิ์การใช้งานระบบ

หมายเลข 1 เรียกเมนู ระบบสำหรับผู้ดูแลระบบ> SINGLE SIGN-ON > PASSPORT ENTITY

หมายเลข 2 ระบุชื่อผู้ใช้ หรือ ชื่อ LOG IN จากนั้นกดปุ่ม 

หมายเลข 3 แสดงชื่อของผู้ใช้ หรือ ชื่อ LOG IN ตามที่ค้นหา จากนั้นเลือกชื่อผู้ใช้ที่ต้องการกำหนดสิทธิ์เพิ่ม

หมายเลข 4 กำหนดสิทธิ์การใช้งานระบบ



ภาพที่ 4-53 แสดงตัวอย่างหน้าจอกำหนดสิทธิ์เพิ่มสำหรับผู้ใช้เดิม

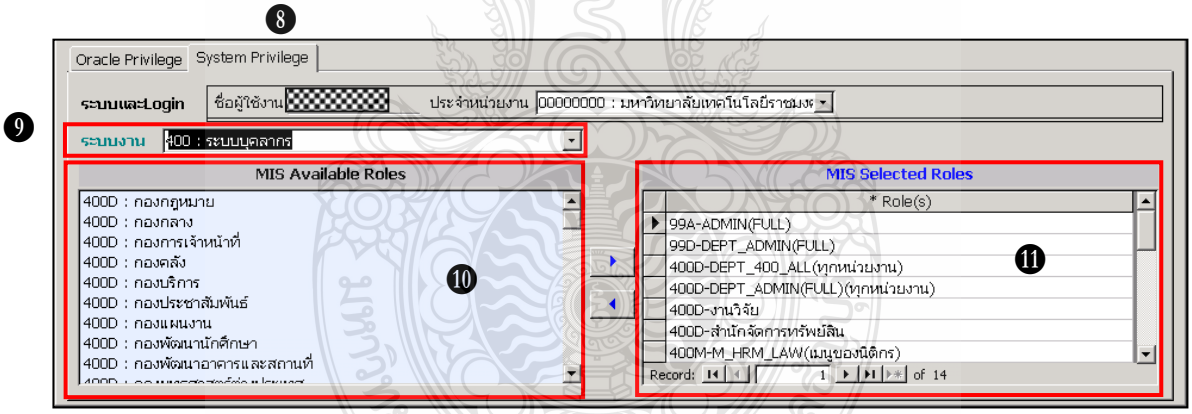
<u>กรณีกำหนดสิทธิ์ระบบอื่นเพิ่ม</u>

หมายเลข 5 คลิกที่ Tab Oracle Privilege

หมายเลข 6 Oracle Available Role ให้ระบุสิทธิ์ของระบบที่ต้องการเพิ่ม จากนั้นให้คลิกปุ่ม 

เพื่อสร้างข้อมูลสิทธิ์ Role ในฐานข้อมูล Oracle ให้กับ User นั้น

หมายเลข 7 กรอบ Oracle Selected Role แสดงสิทธิ์ที่ User



ภาพที่ 4-54 แสดงตัวอย่างหน้าจอกำหนดสิทธิ์ระบบอื่นเพิ่ม

หมายเลข 8 คลิกที่ Tab System Privilege

หมายเลข 9 เลือกระบบงานต้องการกำหนดสิทธิ์

หมายเลข 10 กรอบ (MIS Available Role) เป็นสิทธิ์ในการเข้าใช้ระบบ หรืออีกอย่างหนึ่งก็คือสิทธิ์ในการเข้าถึง menu ของระบบ รวมถึงรายงานด้วย สำหรับการกำหนดสิทธิ์การเข้าใช้เมนู (Menu) กำหนดสิทธิ์การเข้าถึงหน่วยงาน (DEP) และแหล่งเงิน (BGROUP) ให้เลือกที่สิทธิ์ที่ต้องการกำหนดให้กับ User จากนั้นดับเบิ้ลคลิก หรือกด  ปุ่ม สิทธิ์ที่ถูกกำหนดจะย้ายไปฝั่ง MIS Selected Roles

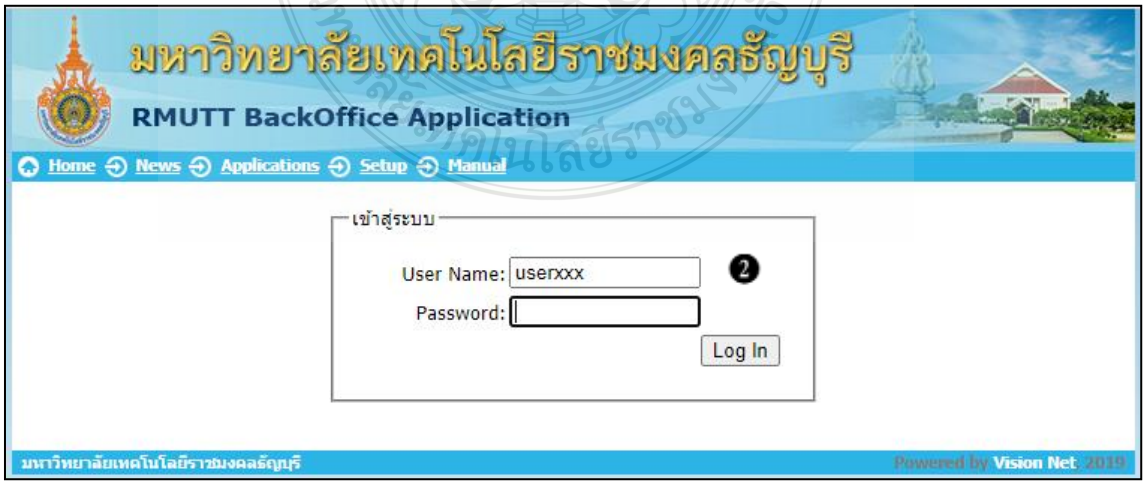
หมายเลข 11 แสดงสิทธิ์ที่ User ได้รับ

ขั้นตอนที่ 6 ผู้บริหารจัดการระบบดำเนินการติดตั้งระบบบริหารงานบุคลากรและเงินเดือน เพื่อให้ผู้ขอบริการเข้าใช้งานระบบ วิธีการเข้าใช้งานระบบครั้งแรกโดยการติดตั้งการใช้งาน ผู้ใช้งานสามารถแจ้งผู้บริหารจัดการระบบให้ดำเนินการติดตั้ง โดยติดตั้งเครื่องผู้ใช้งาน สำหรับ Support Microsoft Window 7 และ Microsoft Window 10 (Version 20H2 ,Version 20H1) ได้ดังนี้

การติดตั้ง VN Application Client

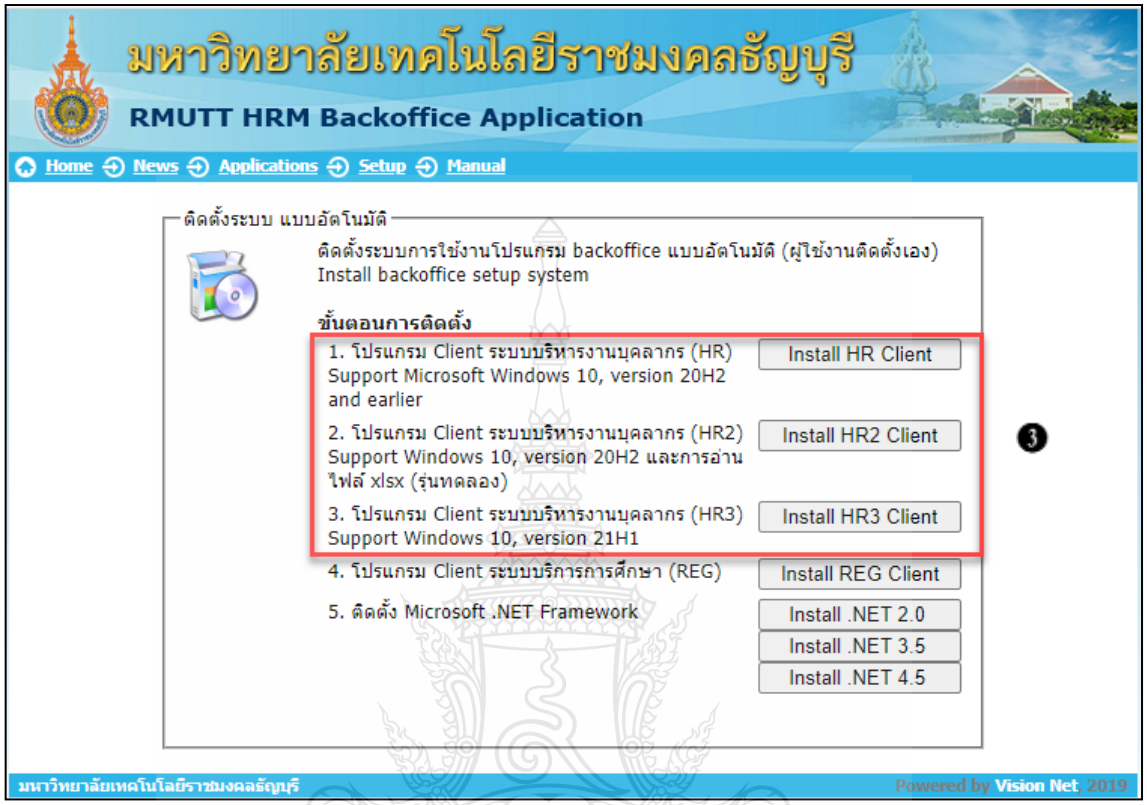
ภาพที่ 4-55 แสดงตัวอย่างหน้าจอการ Setup

หมายเลข 1 เปิด Internet Explore เข้าไปที่ https://hr.rmutt.ac.th/vncaller/applications.aspx จากนั้นคลิก setup ด้านบน



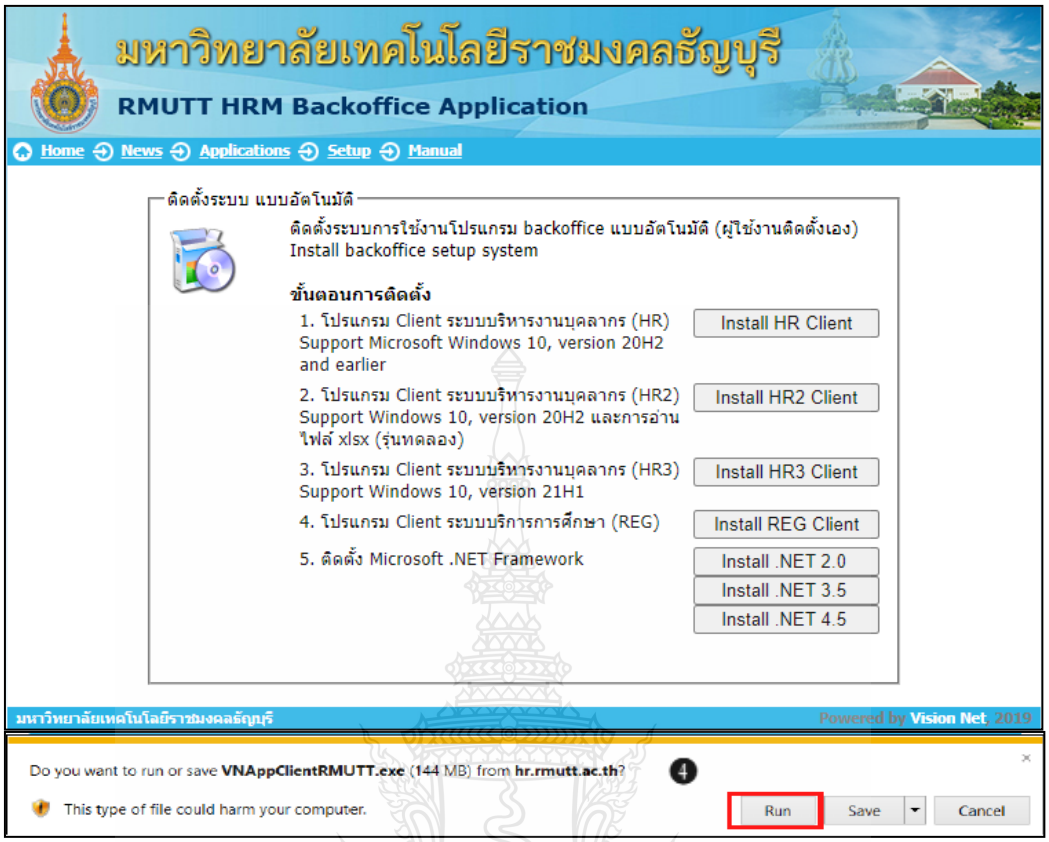
ภาพที่ 4-56 แสดงตัวอย่างหน้าจอการใส่ Username Password Admin

หมายเลข 2 ระบุ Username และ Password (Username และ Password เป็นตัวเดียวกับที่ใช้งานอินเตอร์เน็ตของมหาวิทยาลัยฯ) จากนั้นคลิกปุ่ม (LOG IN) เพื่อเข้าสู่หน้าจอติดตั้ง



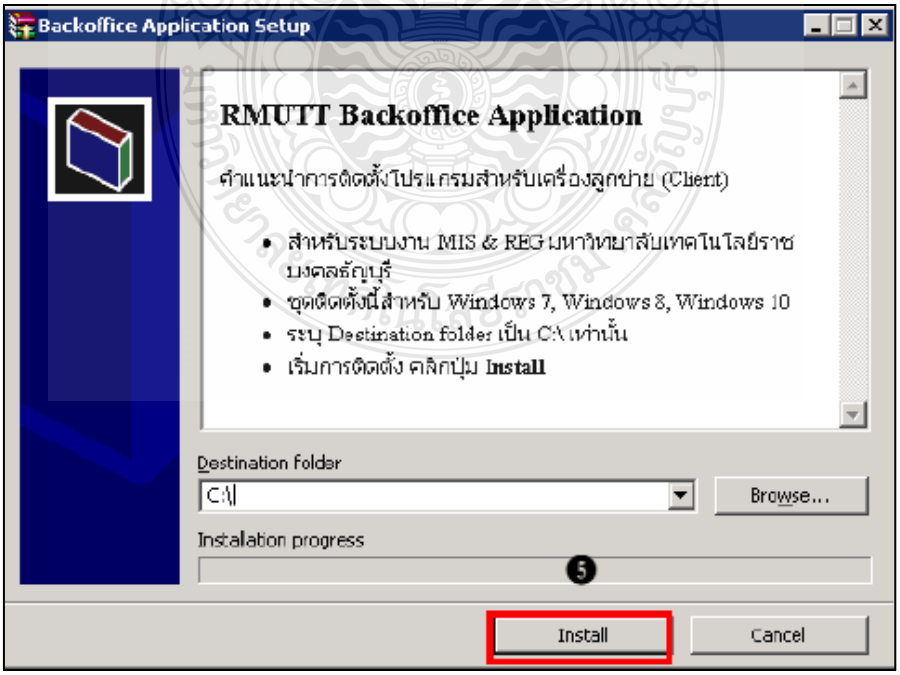
ภาพที่ 4-57 แสดงตัวอย่างหน้าจอติดตั้ง Application Client

หมายเลข 3 ติดตั้ง Application Client ในส่วนการติดตั้งระบบ ให้เลือก 1.Application Client สำหรับ Microsoft Window 10 (Version 20H2 ,Version 20H1)โดยคลิกปุ่ม Install HR Client ขวามือ ดังรูป



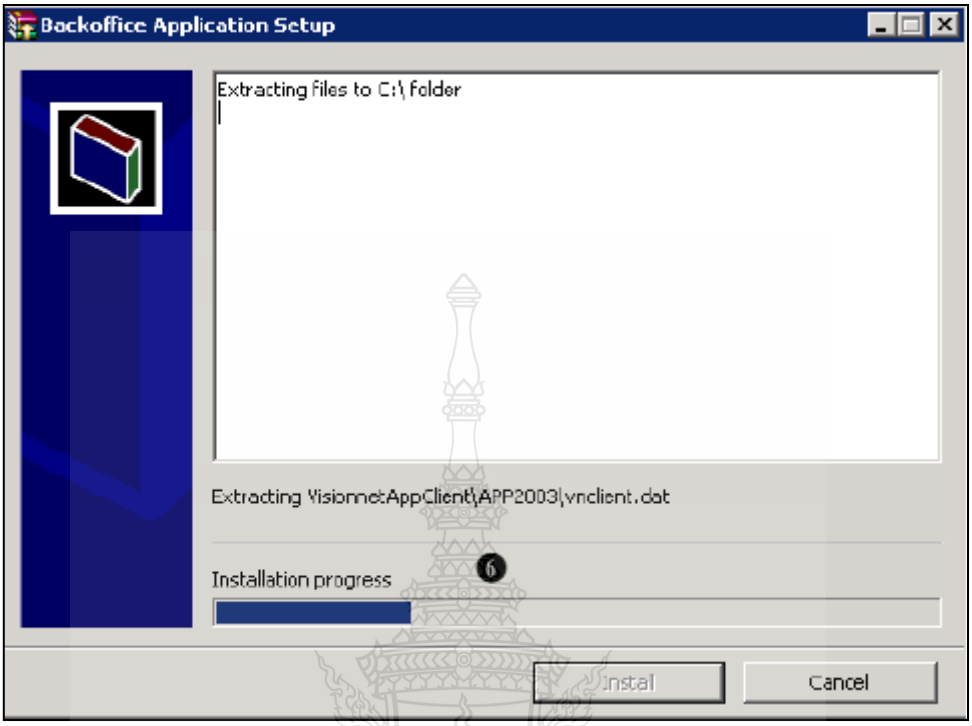
ภาพที่ 4-58 แสดงตัวอย่างหน้าจอกระบวนการติดตั้ง

หมายเลข 4 คลิกปุ่ม Run เพื่อเริ่มกระบวนการติดตั้ง (สามารถเลือก Save เก็บไฟล์ติดตั้งบนฮาร์ดดิสก์ เพื่อ Run ภายหลังได้



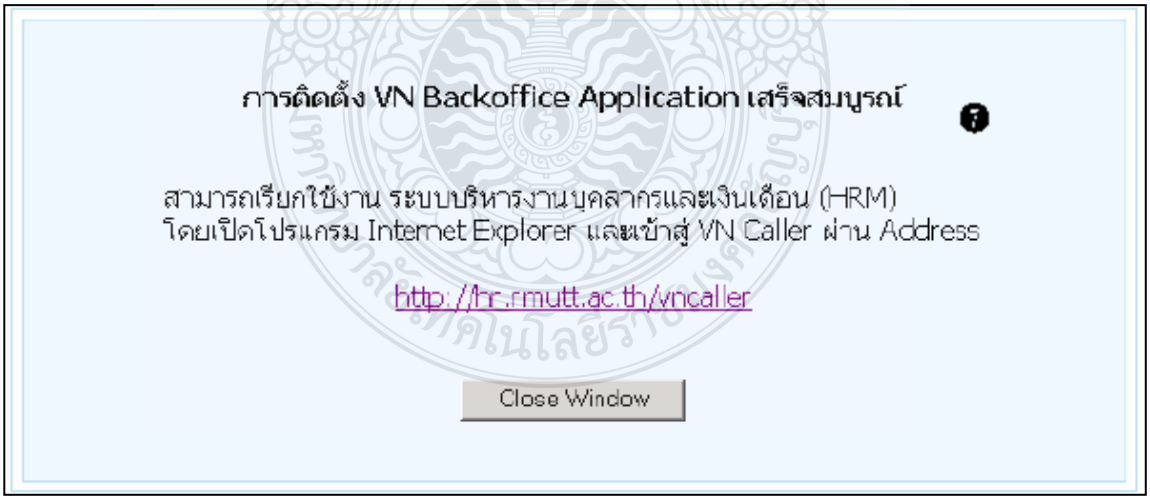
ภาพที่ 4-59 แสดงตัวอย่างหน้าจอ Install เพื่อเริ่มการติดตั้ง

หมายเลข 5 คลิกปุ่ม Install เพื่อเริ่มการติดตั้ง



ภาพที่ 4-60 แสดงตัวอย่างหน้าจอประมวลผลในการติดตั้ง

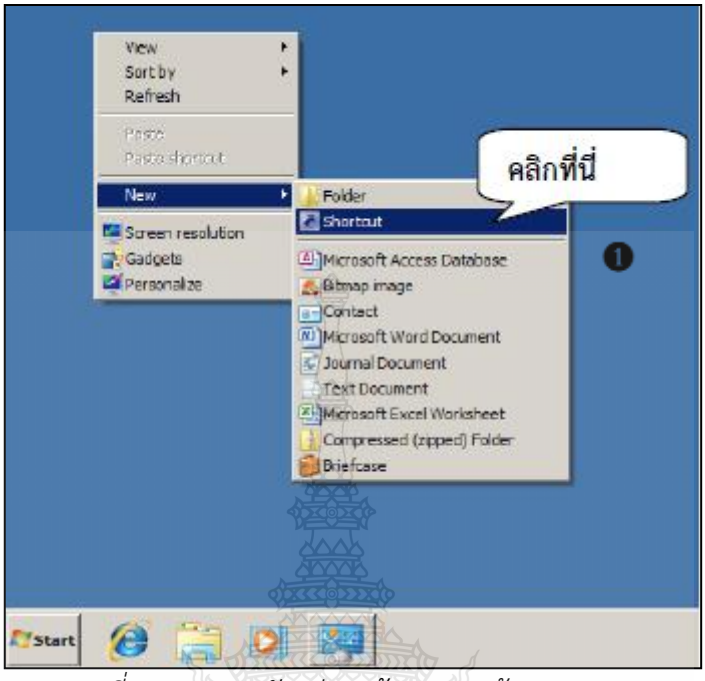
หมายเลข 6 รอจนกระบวนการเสร็จสิ้น



ภาพที่ 4-61 แสดงตัวอย่างหน้าจอการติดตั้งเสร็จสมบูรณ์

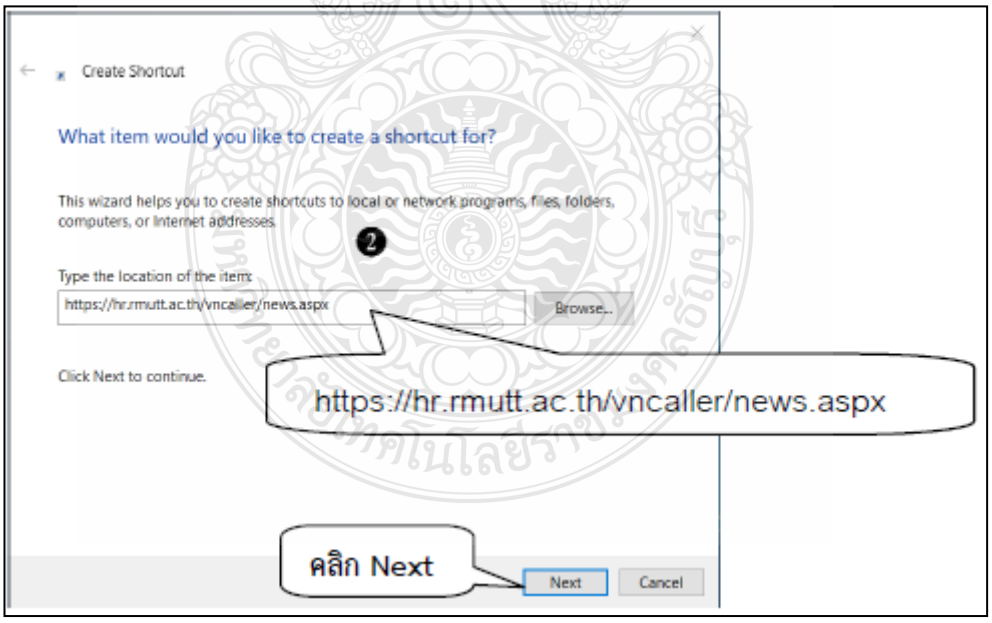
หมายเลข 7 การติดตั้ง VN Backoffice เสร็จสมบูรณ์

การสร้าง ShortCut



ภาพที่ 4-62 แสดงตัวอย่างหน้าจอการสร้าง ShortCut

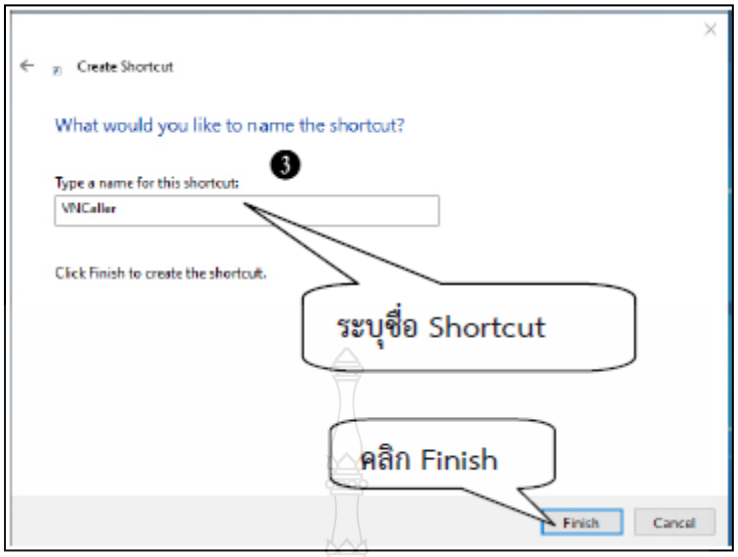
หมายเลข 1 คลิกขวาที่ Desktop > New > Shortcut



ภาพที่ 4-63 แสดงตัวอย่างหน้าจอระบุ Location ของไอคอน

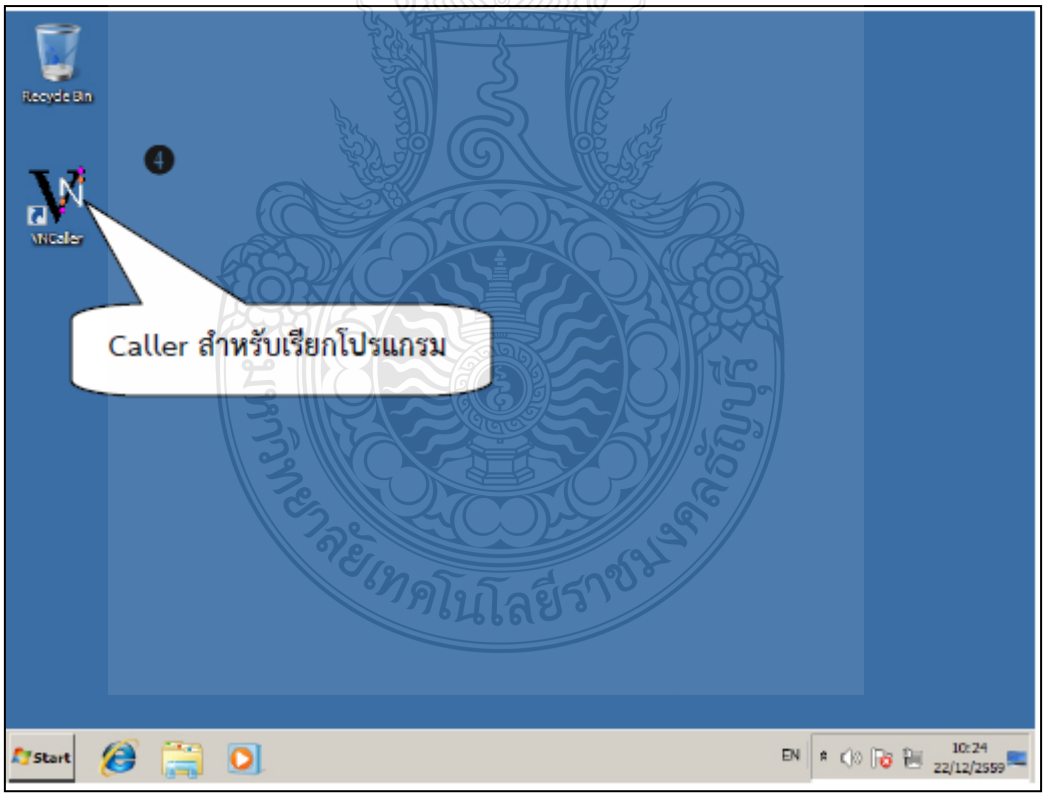
หมายเลข 2 ระบุ Location เป็น https://hr.rmutt.ac.th/vncaller/news.aspx

คลิกปุ่ม Next



ภาพที่ 64 แสดงตัวอย่างหน้าจอระบุชื่อ Shortcut ของไอคอน

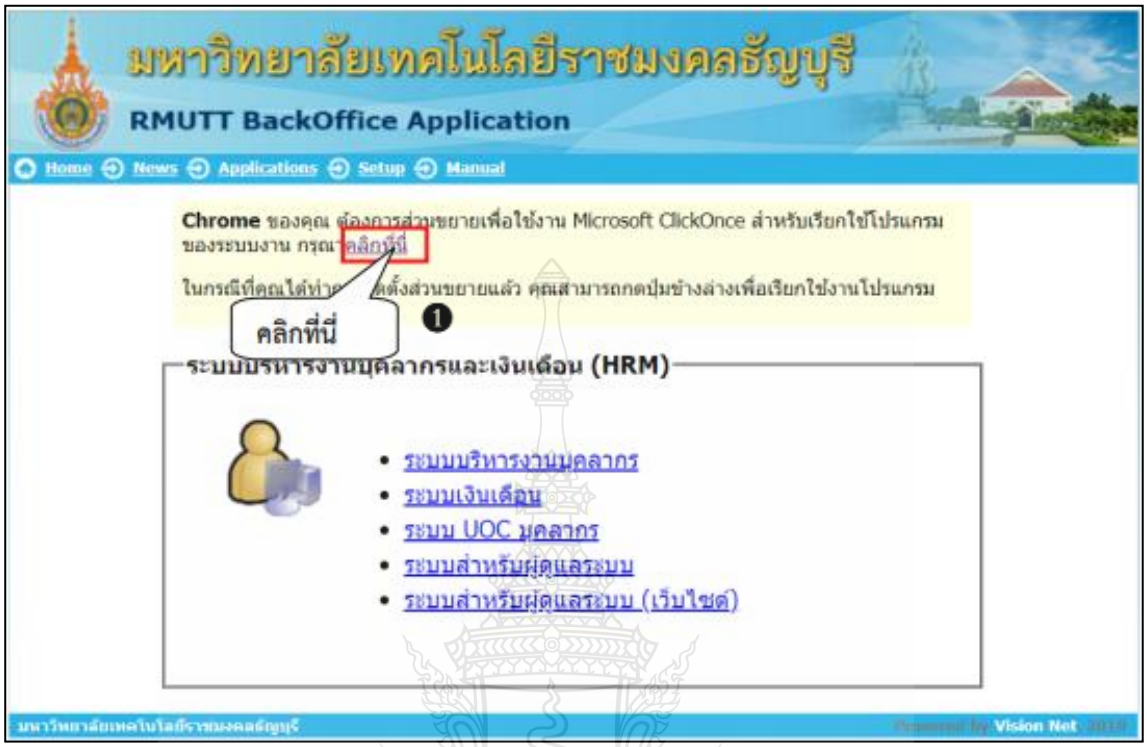
หมายเลข 3 ระบุ Shortcut คลิกปุ่ม Finish



ภาพที่ 4-65 แสดงตัวอย่างหน้าจอไอคอนระบบบริหารงานบุคลากรและเงินเดือน

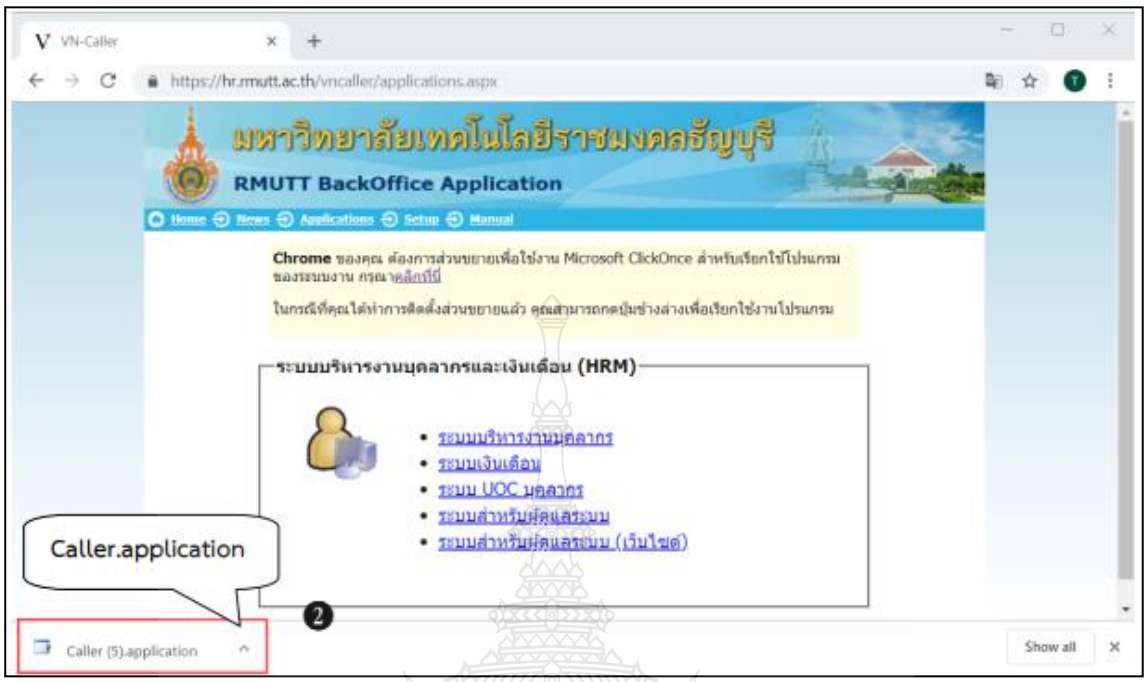
หมายเลข 4 จะปรากฏ caller ที่ desktop ของเครื่องที่ทำการติดตั้ง เป็นอันเสร็จสิ้นการติดตั้งเครื่อง Client

เปิดด้วย Caller ด้วย Chrome



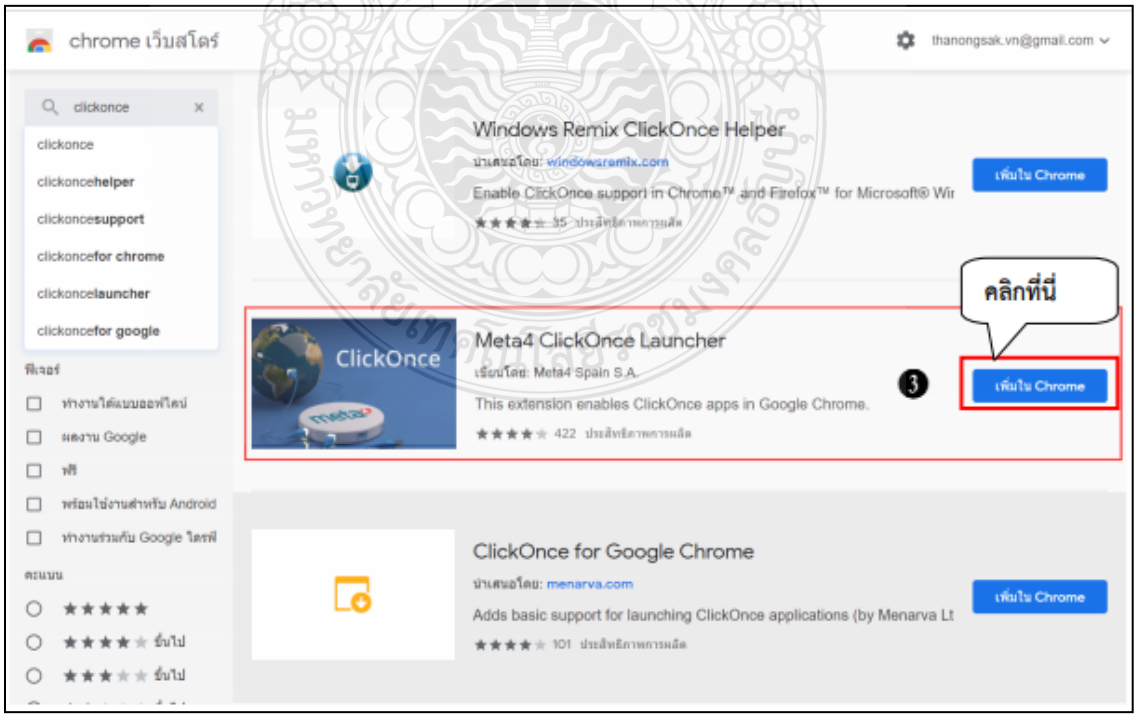
ภาพที่ 4-66 แสดงตัวอย่างหน้าจอการติดตั้งบน Chrome

หมายเลข 1 หากปรากฏกล่องโต้ตอบดังกล่าว แสดงว่าผู้ใช้งานยังไม่ได้ติดตั้ง Microsoft Click Once ผู้ใช้งานจะต้องติดตั้ง Microsoft Click Once โดยให้คลิก “คลิกที่นี่”

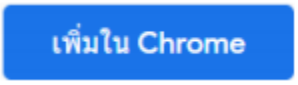


ภาพที่ 4-67 แสดงตัวอย่างหน้าจอแสดงกล่องโต้ตอบกรณียังไม่ได้ติดตั้ง Microsoft Click Once

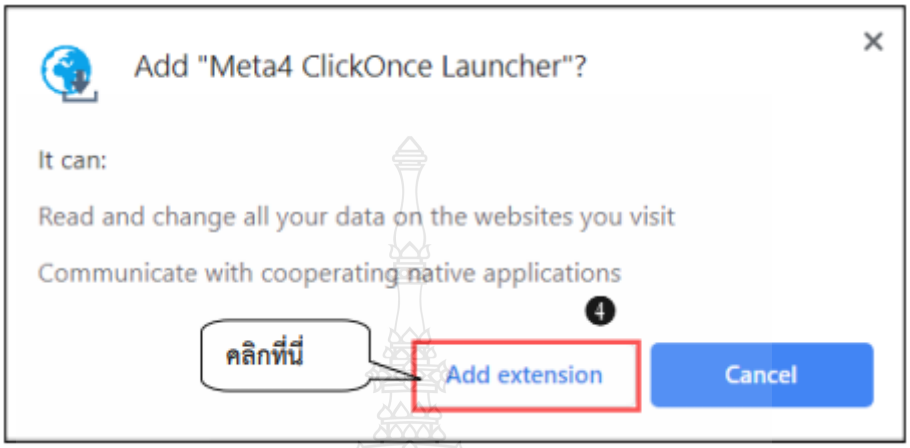
หมายเลข 2 กรณีที่ผู้ใช้งานระบบเปิดด้วย Chrome ระบบจะแสดงข้อความที่แถบ Application และเมื่อคลิกเลือกที่ระบบ จะปรากฏกล่องโต้ตอบสำหรับติดตั้ง Click Once ให้คลิกเปิดเมื่อเสร็จ



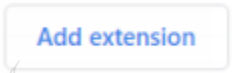
ภาพที่ 4-68 แสดงตัวอย่างหน้าจอแสดงหน้าเว็บสำหรับติดตั้ง Click Once

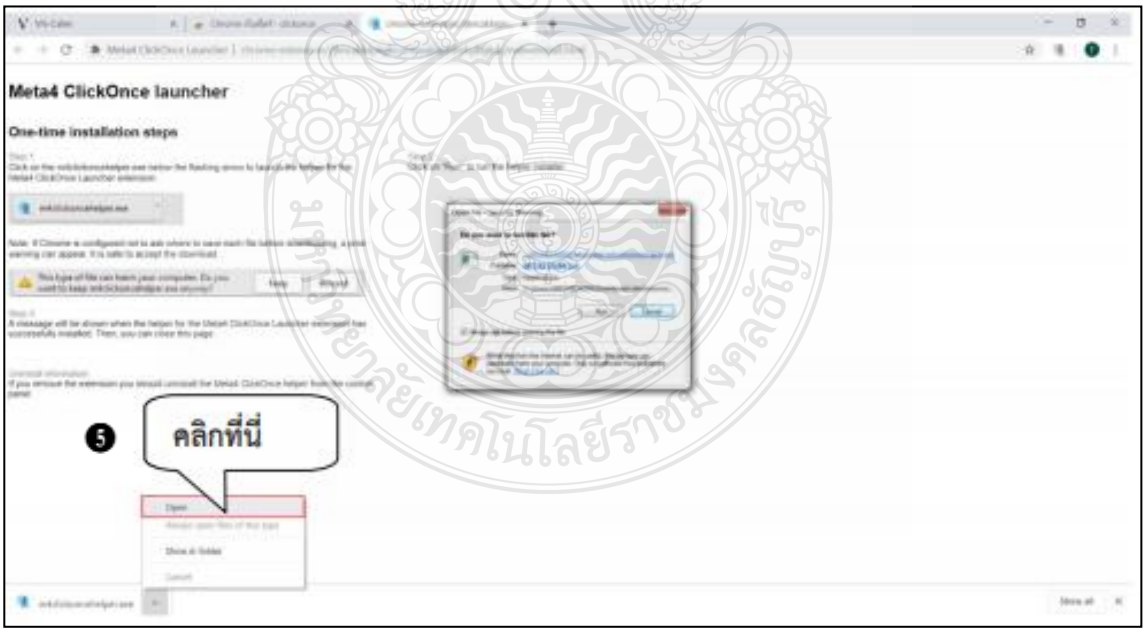
หมายเลข 3 คลิกปุ่ม 

ในช่องของ Meta4 ClickOnce Launcher



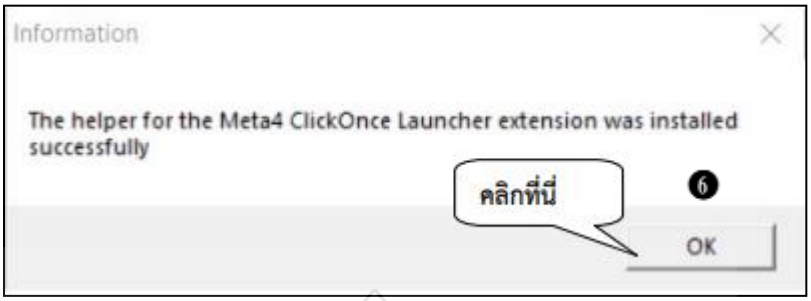
ภาพที่ 4-69 แสดงตัวอย่างหน้าจอแสดงปุ่มโต้ตอบ

หมายเลข 4 จากนั้นจะแสดงปุ่มโต้ตอบ ให้คลิก 



ภาพที่ 70 แสดงตัวอย่างหน้าจอการติดตั้ง Click Once

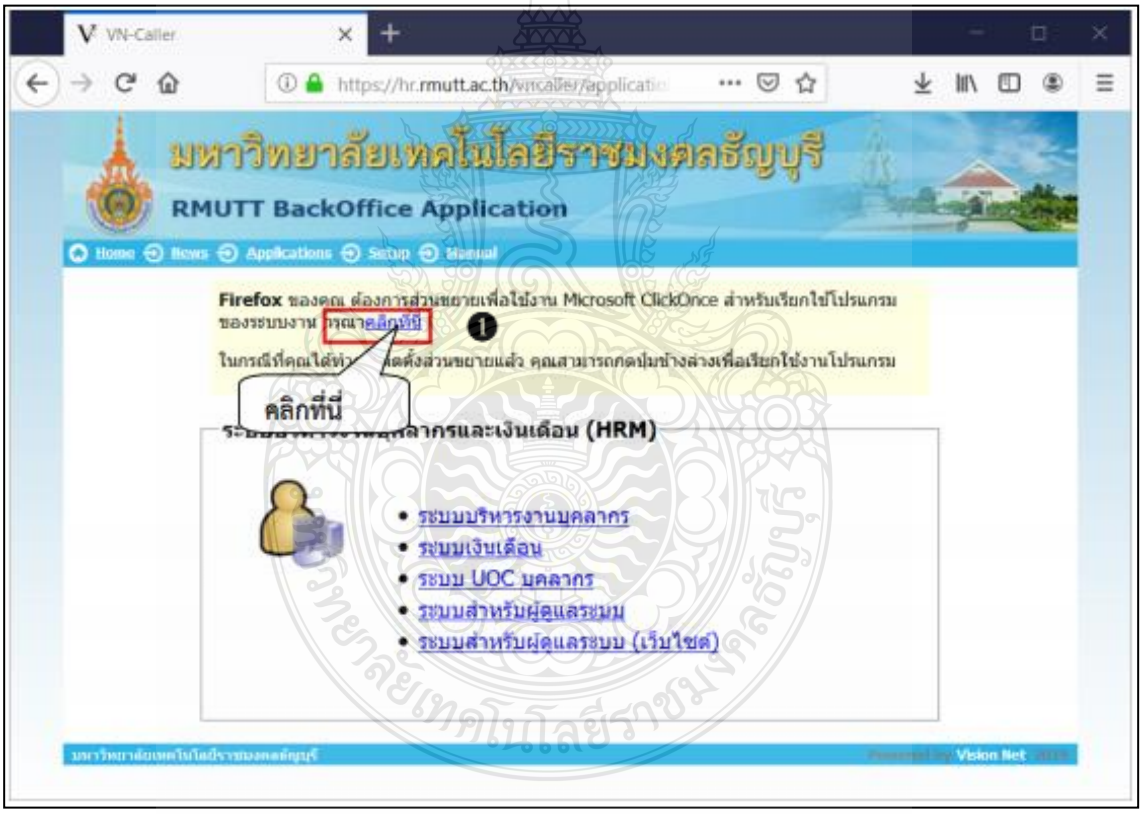
หมายเลข 5 เมื่อคลิกจะแสดงหน้าจอไฟล์ดาวน์โหลดให้คลิกที่ Open



ภาพที่ 4-71 แสดงตัวอย่างหน้าจอติดตั้งเสร็จสมบูรณ์

หมายเลข 6 เมื่อติดตั้งสำเร็จจะแสดงหน้าจอ Information ให้คลิกปุ่ม OK เพื่อเสร็จสิ้น

เปิด Caller ด้วย Firefox

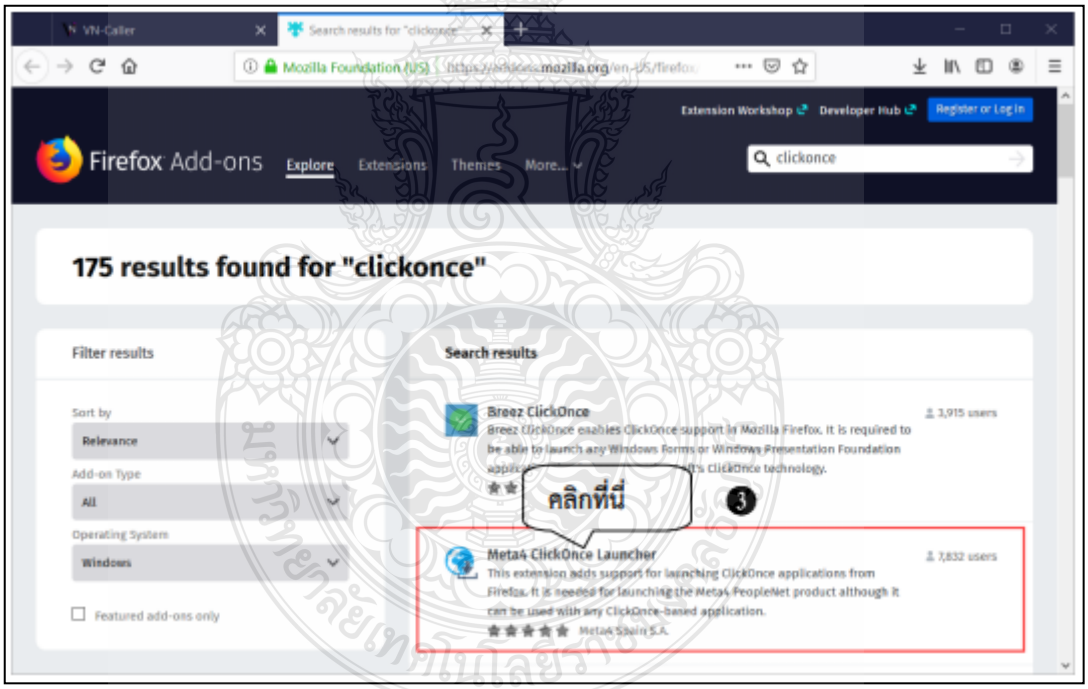


ภาพที่ 4-72 แสดงตัวอย่างหน้าจอการติดตั้งบน Firefox

หมายเลข 1 กรณีที่ผู้ใช้งานเปิดด้วย Firefox จะแสดงข้อความที่แถบ Application และเมื่อคลิกเลือกที่ระบบ จะปรากฏกล่องโต้ตอบสำหรับติดตั้ง ผู้ใช้งานจะต้องติดตั้ง Microsoft Click Once โดยให้คลิก “คลิกที่นี่”

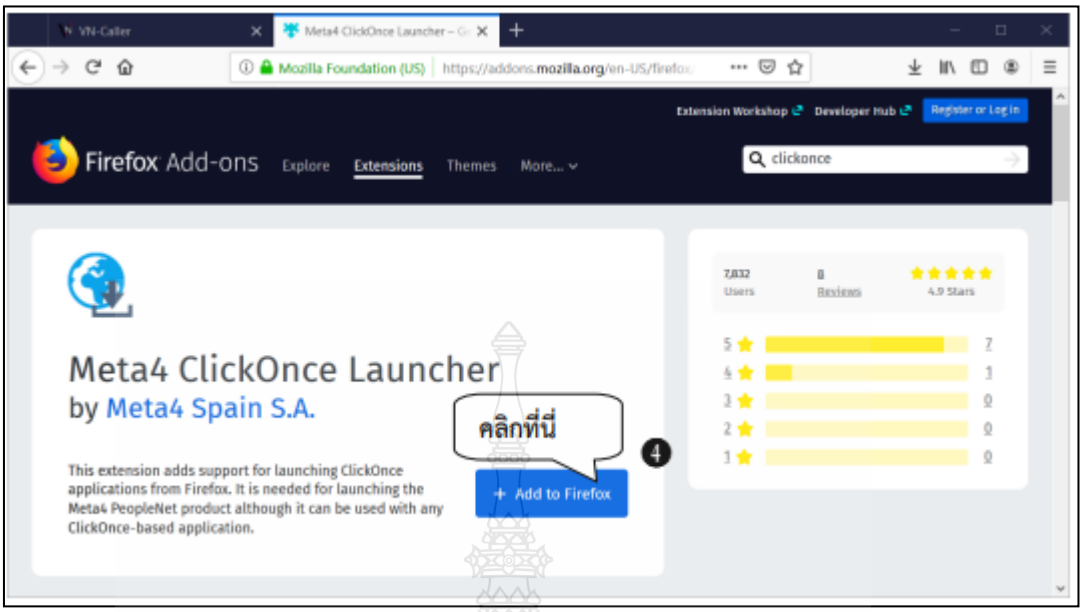
ภาพที่ 4-73 แสดงตัวอย่างหน้าจอแสดงกล่องโต้ตอบกรณียังไม่ได้ติดตั้ง Microsoft Click Once

หมายเลข 2 หากปรากฏกล่องโต้ตอบดังกล่าว แสดงว่าผู้ใช้งานยังไม่ได้ติดตั้ง Microsoft Click Once ให้คลิกปุ่ม “บันทึกไฟล์”



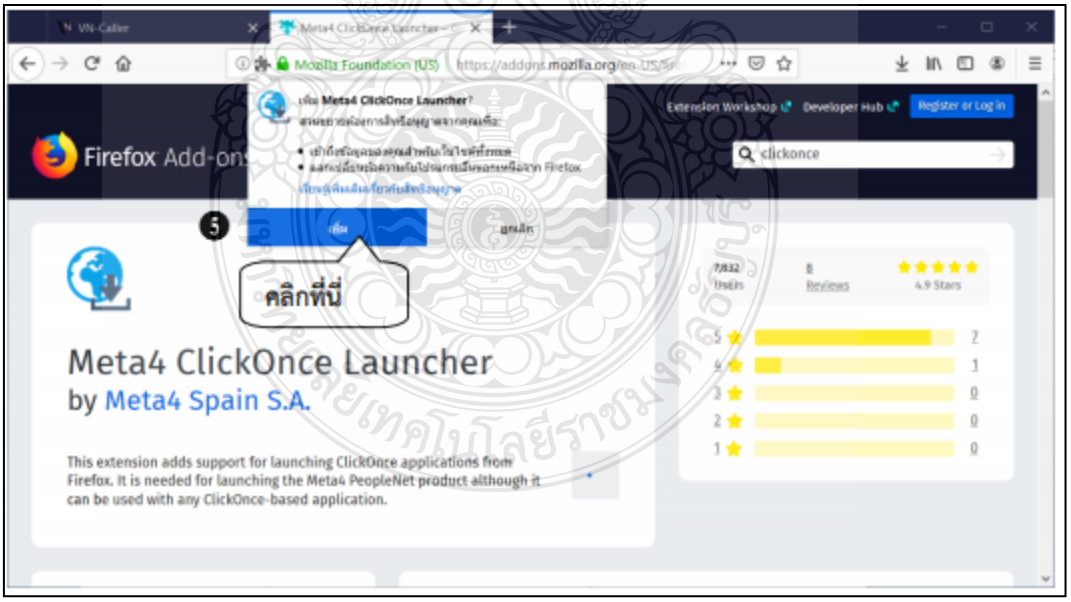
ภาพที่ 4-74 แสดงตัวอย่างหน้าจอแสดงหน้าเว็บสำหรับติดตั้ง Click Once

หมายเลข 3 ผู้ใช้งานจะต้องติดตั้ง Microsoft Click Once จะแสดงหน้าเว็บสำหรับติดตั้ง โดยคลิก “Meta4 ClickOnce Lancher”



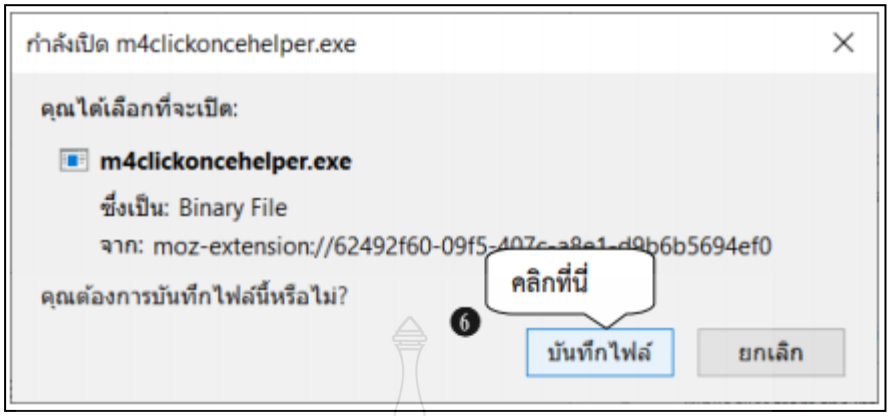
ภาพที่ 4-75 แสดงตัวอย่างหน้าจอการ Add Firefox ลงใน FxClickOnce

หมายเลข 4 คลิกปุ่ม  ในช่องของ FxClickOnce



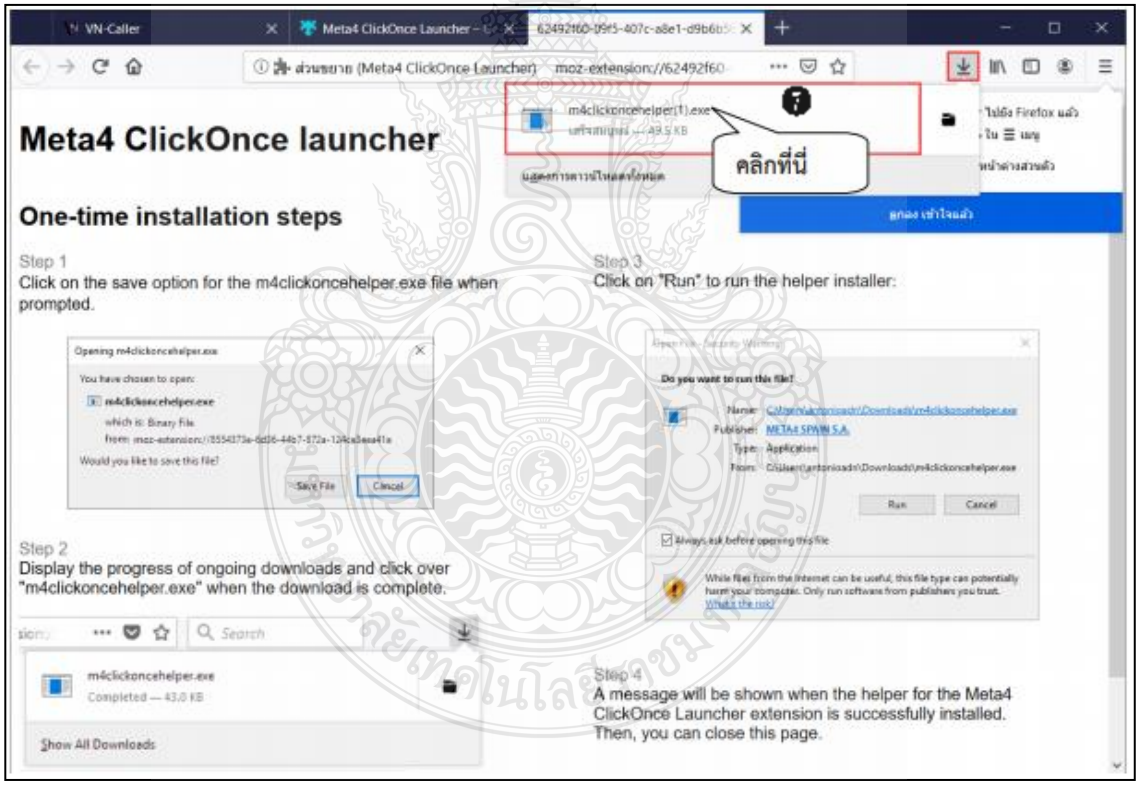
ภาพที่ 4-76 แสดงตัวอย่างหน้าจอแสดงปุ่มโต้ตอบ

หมายเลข 5 จะปรากฏกล่องโต้ตอบ ให้คลิกปุ่ม 



ภาพที่ 4-77 แสดงตัวอย่างหน้าจอยืนยันการบันทึกไฟล์ FxClickOnce

หมายเลข 6 จากนั้นคลิกปุ่ม  อีกครั้ง



ภาพที่ 4-78 แสดงตัวอย่างหน้าจอการเปิดไฟล์ FxClickOnce

หมายเลข 7 จากนั้นคลิก  และดับเบิ้ลคลิกที่ m4clickoncehelper.exe

ภาพที่ 4-79 แสดงตัวอย่างหน้าจอติดตั้งเสร็จสมบูรณ์

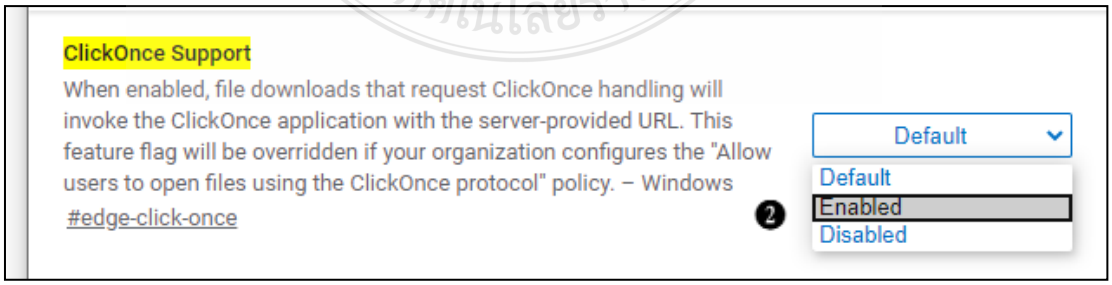
หมายเลข 8 หลังจากนั้นติดตั้ง Clickonce เรียบร้อยแล้ว ระบบแสดงข้อความ Information ให้คลิกปุ่ม OK เพื่อเสร็จสิ้น และผู้ใช้งานจะสามารถเรียกใช้งานระบบได้ปกติ

ปัญหาการเรียกใช้งานโปรแกรมบน Microsoft Edge (Chromium)

เพื่อแก้ปัญหา Microsoft Edge (Chormium) ไม่อนุญาตให้ทำการเรียกใช้งานโปรแกรมด้วยการเชื่อมต่อแบบ ClickOnce ดังนี้

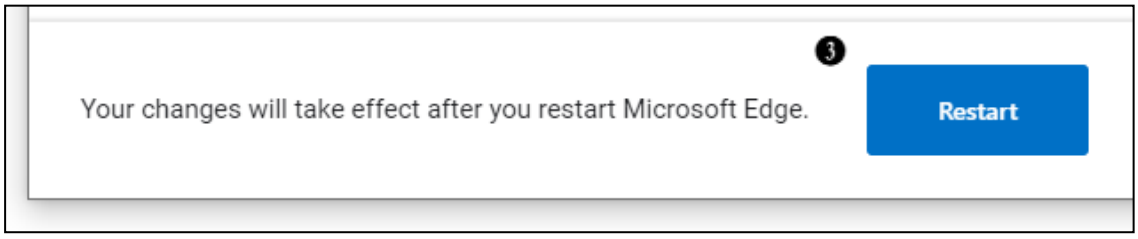
ภาพที่ 4-80 แสดงตัวอย่างหน้าจอการวางข้อความในช่อง URL เพื่อไปยังที่อยู่ของ Microsoft Edge

หมายเลข 1 พิมพ์ข้อความในช่องข้างล่างไปยังช่องที่อยู่ของ Microsoft Edge จากนั้น กดปุ่ม Enter ที่แป้นพิมพ์



ภาพที่ 4-81 แสดงตัวอย่างหน้าจอการอนุญาตการติดตั้ง ClickOnce Support

หมายเลข 2 เลื่อนไปยังหัวข้อ ClickOnce Support และทำการเลือกตัวเลือก Enabled ทางด้านขวา



ภาพที่ 4-82 แสดงตัวอย่างหน้าจอเริ่มต้นทำงานเว็บบราวเซอร์ใหม่

หมายเลข 3 เริ่มต้นทำงานเว็บบราวเซอร์ใหม่ โดยการกดปุ่ม Restart ที่อยู่ท้ายหน้า

การเข้าใช้งานระบบบริหารงานบุคลากรและเงินเดือน

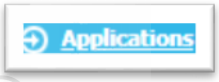
ภาพที่ 4-83 แสดงตัวอย่างหน้าจอไอคอนระบบบริหารงานบุคลากรและเงินเดือน

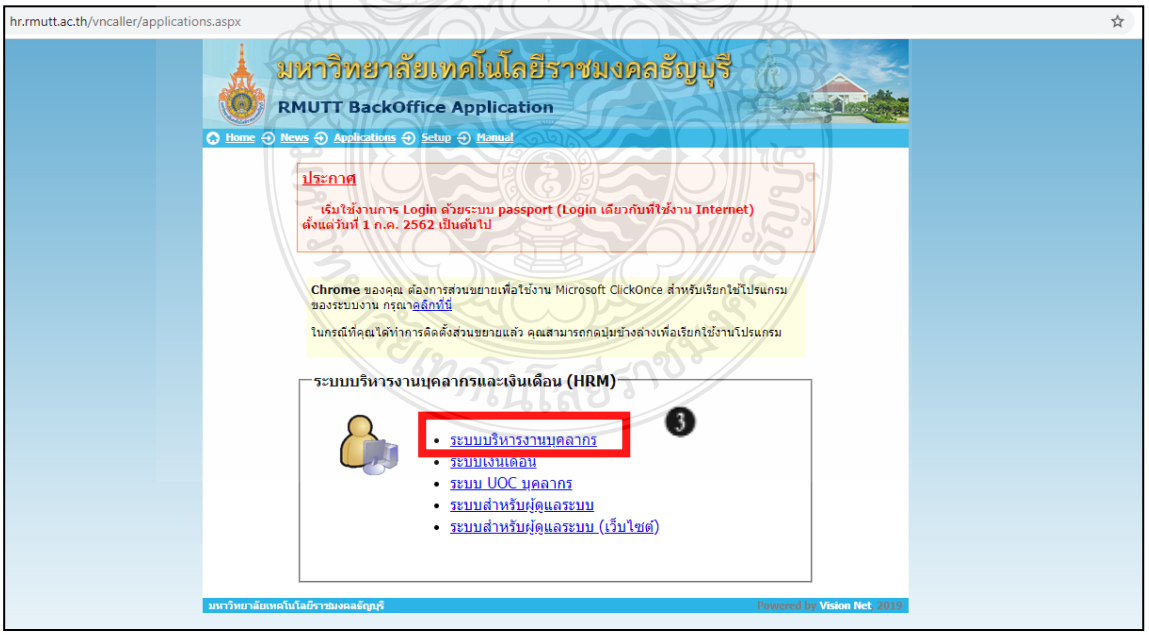
หมายเลข 1 สามารถเข้าใช้งานโดยการ Double Click ไอคอน 

เพื่อเป็นการเรียกโปรแกรม

ภาพที่ 4-84 แสดงตัวอย่างหน้าจอการเรียกใช้งานระบบ

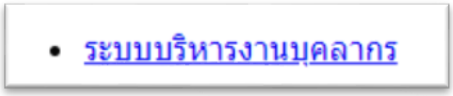
หมายเลข 2 จะปรากฏหน้าเว็บให้ทำการคลิกแถบ



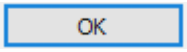


ภาพที่ 4-85 แสดงตัวอย่างหน้าจอการใช้งานระบบบริหารงานบุคลากร

หมายเลข 3 คลิก

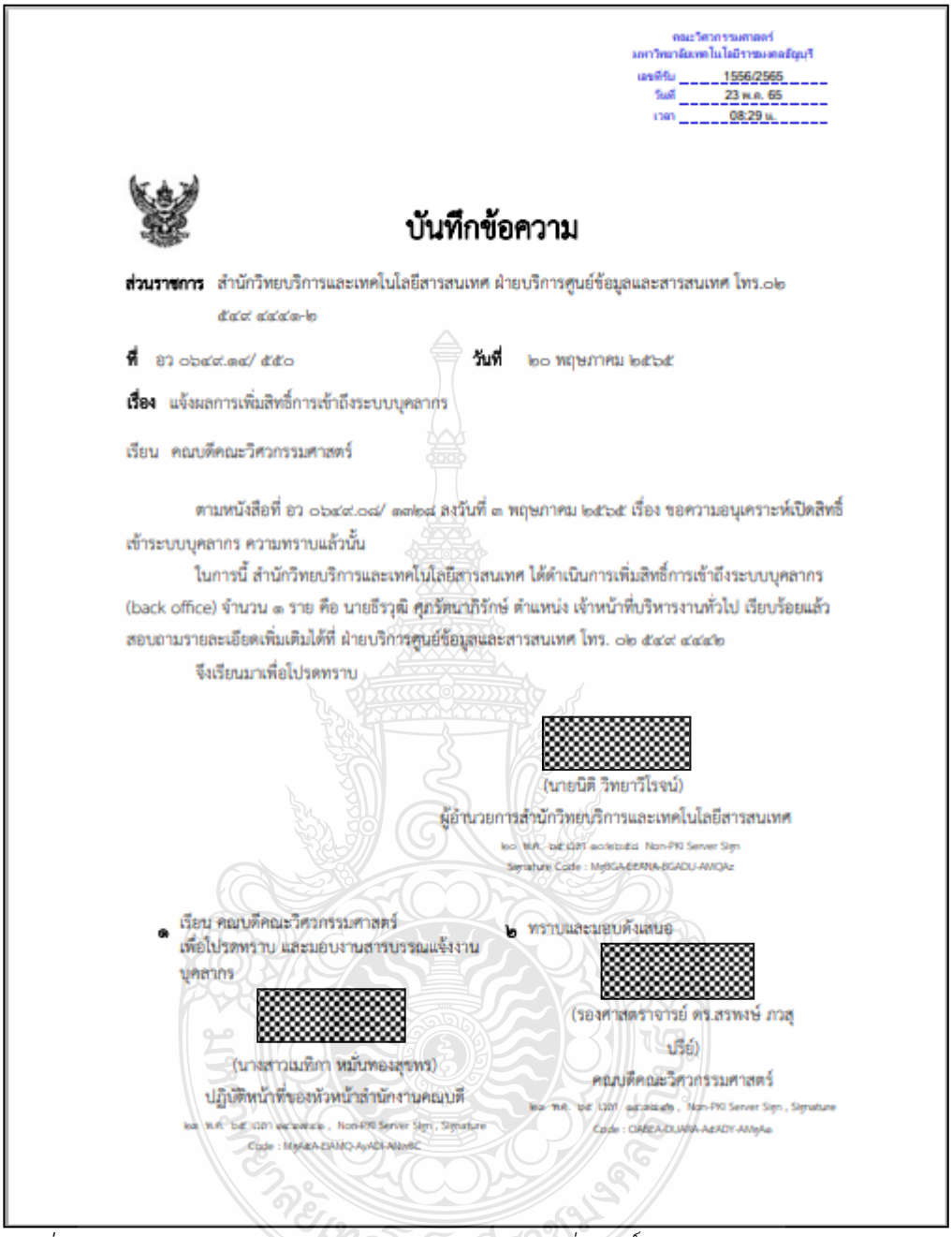


ภาพที่ 4-86 แสดงตัวอย่างหน้าจอการ Logon

หมายเลข 4 ระบุ Username และ Password (Username และ Password เป็นตัวเดียวกับที่ใช้งานอินเตอร์เน็ตของมหาวิทยาลัยฯ) จากนั้นคลิกปุ่ม 

เพื่อเข้าใช้งาน

ขั้นตอนที่ 7 ผู้บริหารจัดการระบบแจ้งผลการดำเนินการกับทางต้นเรื่อง โดยส่งรายละเอียดไปทาง e-mail พร้อมแนบคู่มือการใช้งานระบบ แนะนำการเข้าใช้งานเบื้องต้น และทำหนังสือตอบกลับเรื่องแจ้งผลการเพิ่มสิทธิ์การเข้าใช้งานระบบ ดังตัวอย่างภาพที่ 4-87



คณะวิศวกรรมศาสตร์
มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี
เลขที่รับ 1556/2565
วันที่ 23 พ.ค. 65
เวลา 08:29 น.

บันทึกข้อความ

ส่วนราชการ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ฝ่ายบริการศูนย์ข้อมูลและสารสนเทศ โทร.๐๒ ๕๔๙ ๔๔๔๓-๒

ที่ อว ๐๖๔๙.๑๔/ ๕๕๐ **วันที่** ๒๐ พฤษภาคม ๒๕๖๕

เรื่อง แจ้งผลการเพิ่มสิทธิ์การเข้าถึงระบบบุคลากร

เรียน คณบดีคณะวิศวกรรมศาสตร์

ตามหนังสือที่ อว ๐๖๔๙.๐๔/ ๑๓๒๔ ลงวันที่ ๓ พฤษภาคม ๒๕๖๕ เรื่อง ขอความอนุเคราะห์เปิดสิทธิ์เข้าระบบบุคลากร ความทราบแล้วนั้น

ในการนี้ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ได้ดำเนินการเพิ่มสิทธิ์การเข้าถึงระบบบุคลากร (back office) จำนวน ๑ ราย คือ นายธีรวุฒิ ศุภรัตนาภิรักษ์ ตำแหน่ง เจ้าหน้าที่บริหารงานทั่วไป เรียบร้อยแล้ว สอบถามรายละเอียดเพิ่มเติมได้ที่ ฝ่ายบริการศูนย์ข้อมูลและสารสนเทศ โทร. ๐๒ ๕๔๙ ๔๔๔๒

จึงเรียนมาเพื่อโปรดทราบ

(นายนิติ วิทยาวิโรจน์)
ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ

๑ เรียน คณบดีคณะวิศวกรรมศาสตร์
เพื่อโปรดทราบ และมอบงานสารบรรณแจ้งงานบุคลากร

(นางสาวเมทิกา หมั่นทองสุขทร)
ปฏิบัติหน้าที่ของหัวหน้าสำนักงานคณบดี

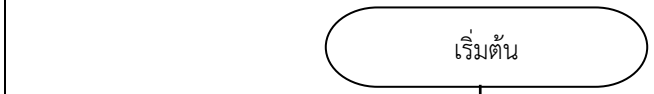
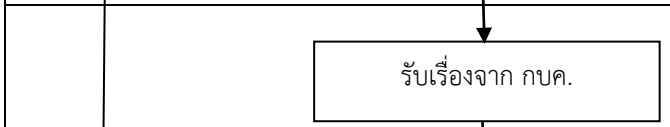
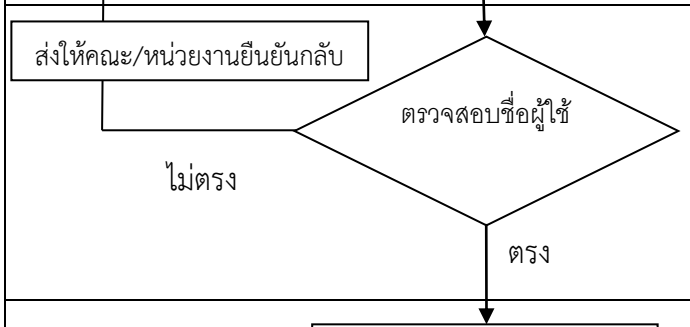
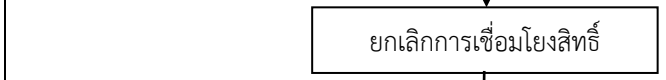
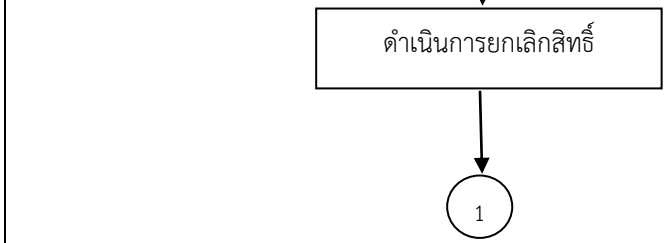
๒ ทราบและมอบดังเสนอ

(รองศาสตราจารย์ ดร.สรพงษ์ ภวสุปรีย์)
คณบดีคณะวิศวกรรมศาสตร์

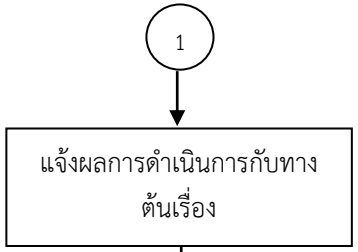
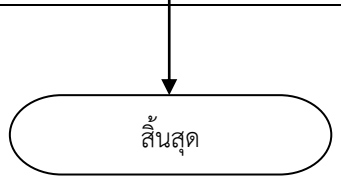
ภาพที่ 4-87 แสดงตัวอย่างหนังสือตอบกลับแจ้งผลการเพิ่มสิทธิ์ไปยังหน่วยงาน/คณะต้นสังกัด

ตารางที่ 4.1.4 การยกเลิกสิทธิ์ของระบบบริหารงานบุคลากรและเงินเดือน สามารถแสดงได้ ดังตารางที่ 4.4

4.4 การยกเลิกสิทธิ์ของระบบบริหารงานบุคลากรและเงินเดือน

ผังกระบวนการ	รายละเอียดงาน	ผู้รับผิดชอบ	เอกสารที่เกี่ยวข้อง	ระยะเวลา
	-	-	-	-
	**ขั้นตอนที่** 1 ผู้ขอใช้บริการแจ้งขอยกเลิกสิทธิ์โดยหน่วยงาน/คณะ ทำหนังสือผ่านผู้บังคับบัญชาส่งถึงผู้อำนวยการกองบริหารงานบุคคล	หน่วยงาน/คณะ	บันทึกข้อความจากหน่วยงาน/คณะต้นสังกัด	ไม่แน่นอนตามกระบวนการ
	**ขั้นตอนที่ 2** รับเรื่องจากกองบริหารงานบุคคล เพื่อให้ผู้บริหารจัดการระบบดำเนินการ	ผู้บริหารจัดการระบบ	บันทึกข้อความจากหน่วยงาน/คณะต้นสังกัด	2-3 วัน
	**ขั้นตอที่ 3** ผู้บริหารจัดการระบบตรวจสอบชื่อบัญชีผู้ใช้ กรณีชื่อผู้ใช้งานในระบบตรงกับตามที่หน่วยงาน/คณะส่งมา ให้ดำเนินการยกเลิกสิทธิ์ในขั้นตอนที่ 4 กรณีชื่อผู้ใช้งานในระบบไม่ตรงให้ดำเนินการส่งให้คณะ/หน่วยงานยืนยันกลับไปที่ขั้นตอนที่ 1	ผู้บริหารจัดการระบบ	ระบบบริหารงานบุคลากรและเงินเดือน	1 นาที
	**ขั้นตอนที่ 4** ผู้บริหารจัดการระบบยกเลิกการเชื่อมโยงสิทธิ์การเข้าใช้งานกับ Account Wifi Rmutt	ผู้บริหารจัดการระบบ	ระบบบริหารงานบุคลากรและเงินเดือน	5 นาที
	**ขั้นตอนที่ 5** ผู้บริหารจัดการระบบดำเนินการยกเลิกสิทธิ์การเข้าถึงเมนูระบบบริหารงานบุคลากรและเงินเดือน	ผู้บริหารจัดการระบบ	ระบบบริหารงานบุคลากรและเงินเดือน	5 นาที

4.4 การยกเลิกสิทธิ์ของระบบบริหารงานบุคลากรและเงินเดือน (ต่อ)

ผังกระบวนการ	รายละเอียดงาน	ผู้รับผิดชอบ	เอกสารที่เกี่ยวข้อง	ระยะเวลา
	**ขั้นตอนที่ 6** ผู้บริหารจัดการระบบแจ้งผลการดำเนินการกับทางต้นเรื่อง และทำหนังสือตอบกลับเรื่องแจ้งผลการยกเลิกสิทธิ์การเข้าใช้งานระบบ	ผู้บริหารจัดการระบบ	บันทึกข้อความ	15 นาที
				

รายละเอียดของกระบวนการและขั้นตอนการปฏิบัติงาน

ขั้นตอนที่ 1 หน่วยงาน/คณะต้นสังกัดแจ้งขอยกเลิกสิทธิ์โดยทำบันทึกข้อความส่งในระบบสารบรรณอิเล็กทรอนิกส์ (e-office) ผ่านผู้บังคับบัญชาส่งถึงผู้อำนวยการกองบริหารงานบุคคล ดังตัวอย่างภาพที่ 4-88

กองบริหารงานบุคคล
มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี
รับที่ 2530
วันที่ - 5 ส.ค. 2563
เวลา 11.39

บันทึกข้อความ

ส่วนราชการ คณะพยาบาลศาสตร มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี โทร. 0 2549 3119

ที่ อว 0649.35/ 614 **วันที่** 5 สิงหาคม 2563

สำนักวิทยบริการฯ
มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี
รับที่ 11 ส.ค. 2563

เรื่อง ขอความอนุเคราะห์ยกเลิกสิทธิเข้าระบบบุคลากร

เรียน ผู้อำนวยการกองบริหารงานบุคคล

ด้วยคณะพยาบาลศาสตร์ มีความประสงค์ขอยกเลิกสิทธิการเข้าระบบบุคลากร ราย นางภาวินี ทุ้งเฟื่อง ตำแหน่ง เจ้าหน้าที่บริหารงานทั่วไป เนื่องจากบุคลากรรายดังกล่าวไม่ได้ปฏิบัติหน้าที่ด้านงานบุคลากร และย้ายไปปฏิบัติหน้าที่ด้านงานประกันคุณภาพและงานวิจัย

จึงเรียนมาเพื่อโปรดพิจารณาดำเนินการในส่วนที่เกี่ยวข้องต่อไปด้วย จักขอบคุณยิ่ง

[redacted]

(รองศาสตราจารย์ ดร.ชูสุข พึ่งคานนท์)
คณบดีคณะพยาบาลศาสตร์

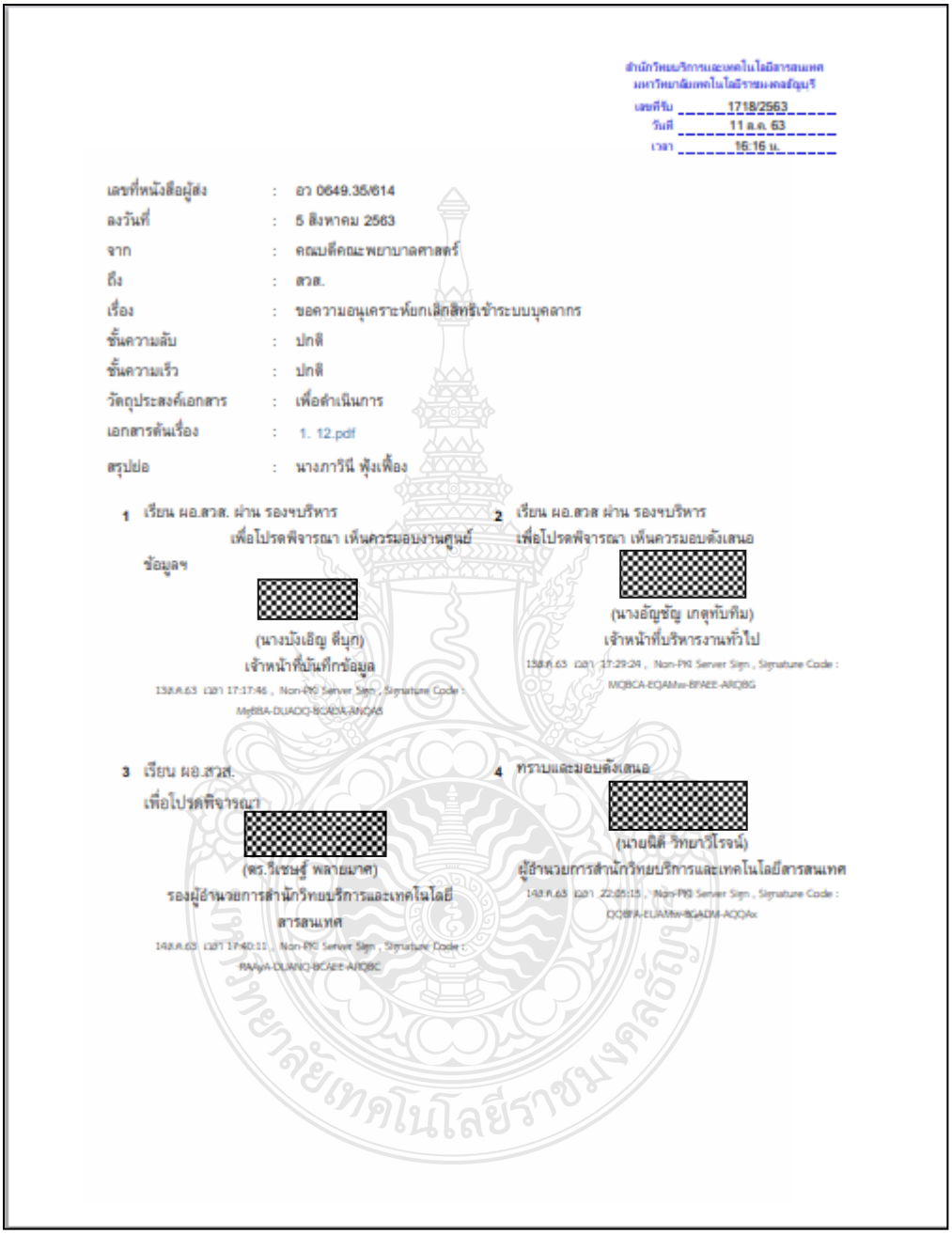
เรียน ผอ.กบค
เพื่อโปรดพิจารณาดำเนินการ ตามเสนอ คณะพยาบาลศาสตร์แจ้ง

[redacted]

[redacted]

ภาพที่ 4-88 แสดงตัวอย่างบันทึกข้อความหน่วยงาน/คณะต้นสังกัดแจ้งขอยกเลิกสิทธิ์

ขั้นตอนที่ 2 รับเรื่องจากกองบริหารงานบุคคล โดยผู้บังคับบัญชาพิจารณามอบหมายงานเพื่อให้ผู้บริหารจัดการระบบดำเนินการยกเลิกสิทธิ์การเข้าใช้งาน ดังตัวอย่างภาพที่ 4-89



สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี
เลขที่รับ 1718/2563
วันที่ 11 ส.ค. 63
เวลา 16:16 น.

เลขที่หนังสือผู้ส่ง	:	อว 0649.35/614
ลงวันที่	:	5 สิงหาคม 2563
จาก	:	คณบดีคณะพยาบาลศาสตร์
ถึง	:	สวส.
เรื่อง	:	ขอความอนุเคราะห์ยกเลิกสิทธิ์เข้าระบบบุคลากร
ชั้นความลับ	:	ปกติ
ชั้นความเร็ว	:	ปกติ
วัตถุประสงค์เอกสาร	:	เพื่อดำเนินการ
เอกสารต้นเรื่อง	:	1. 12.pdf
สรุปย่อ	:	นางภาวินี พุ่งเพื่อง

1 เรียน ผอ.สวส. ผ่าน รองฯบริหาร
เพื่อโปรดพิจารณา เห็นควรมอบงานศูนย์ข้อมูลฯ

(นางบังเอิญ ดีบุก)
เจ้าหน้าที่บันทึกข้อมูล
13/8/63 เวลา 17:17:46 , Non-PKI Server Sign , Signature Code : MyBBA-DUAOQ-BGADA-AIQAB

2 เรียน ผอ.สวส ผ่าน รองฯบริหาร
เพื่อโปรดพิจารณา เห็นควรมอบดังเสนอ

(นางอัญชัญ เกตุทับทิม)
เจ้าหน้าที่บริหารงานทั่วไป
13/8/63 เวลา 17:29:24 , Non-PKI Server Sign , Signature Code : MQBCA-EQAMw-BFAEE-ARQBG

3 เรียน ผอ.สวส.
เพื่อโปรดพิจารณา

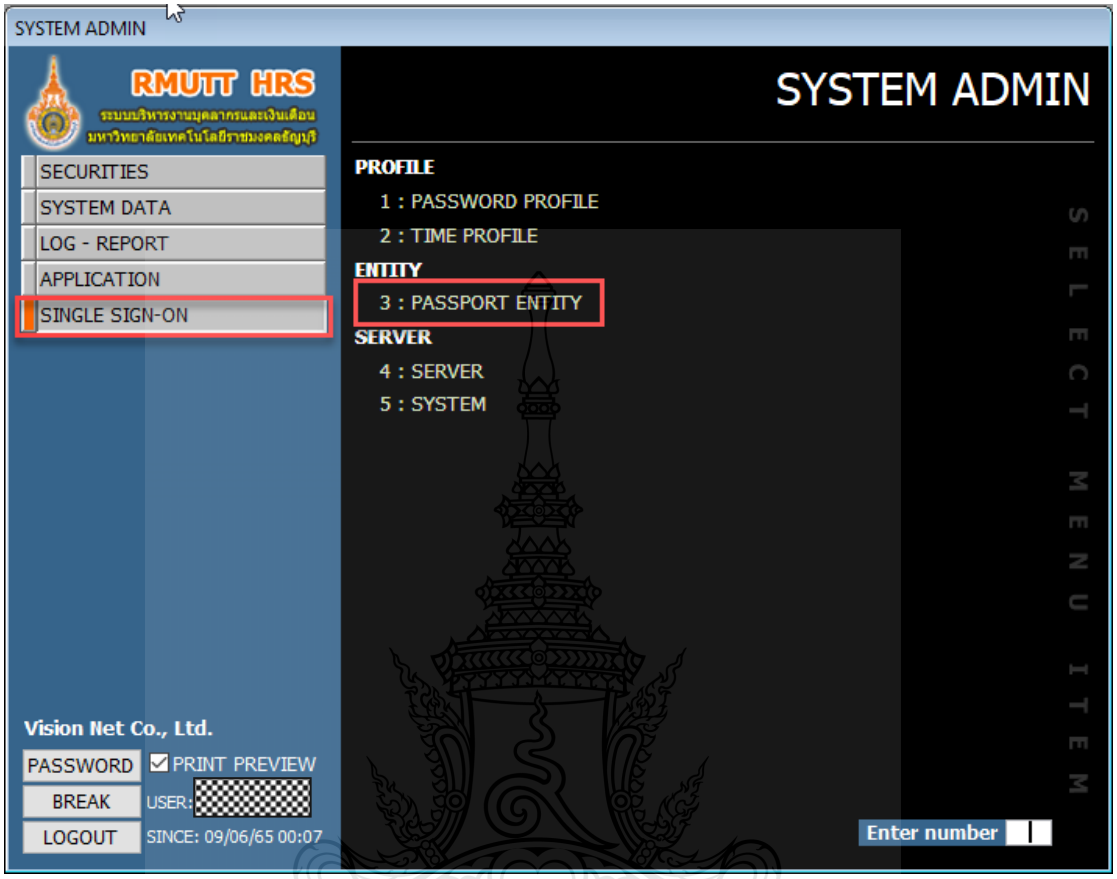
(ดร.วีเชษฐ์ พลายมาศ)
รองผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ
14/8/63 เวลา 17:40:11 , Non-PKI Server Sign , Signature Code : RAAyA-DUAKQ-BCAEE-AIQBC

4 ทราบและมอบดังเสนอ

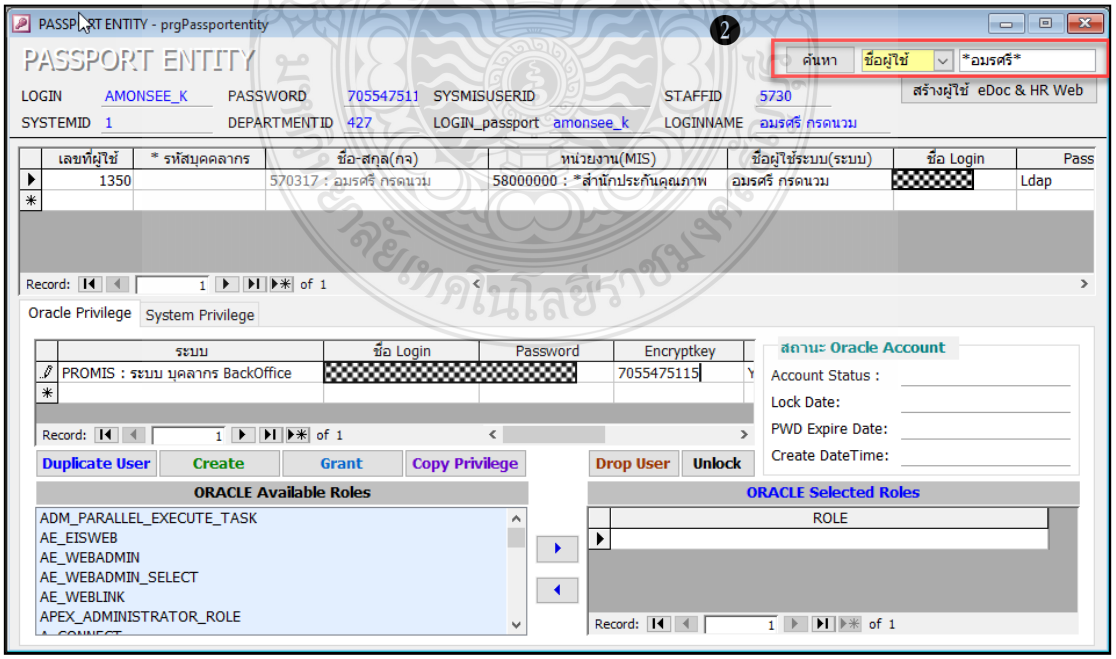
(นายนิติ วิทยาวิโรจน์)
ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ
14/8/63 เวลา 22:05:15 , Non-PKI Server Sign , Signature Code : OQBFA-ELAMw-BGADM-AQQAx

ภาพที่ 4-89 ตัวอย่างหนังสือรับภายใน (กระดาษ) ที่รับเรื่องมาจากกองบริหารงานบุคคล

ขั้นตอนที่ 3 ผู้บริหารจัดการระบบตรวจสอบชื่อบัญชีผู้ใช้ สามารถดำเนินการได้ ดังต่อไปนี้



ภาพที่ 4-90 แสดงตัวอย่างหน้าจอ SINGLE SIGN-ON



ภาพที่ 4-91 แสดงตัวอย่างหน้าจอค้นหาและตรวจสอบชื่อผู้ใช้งาน

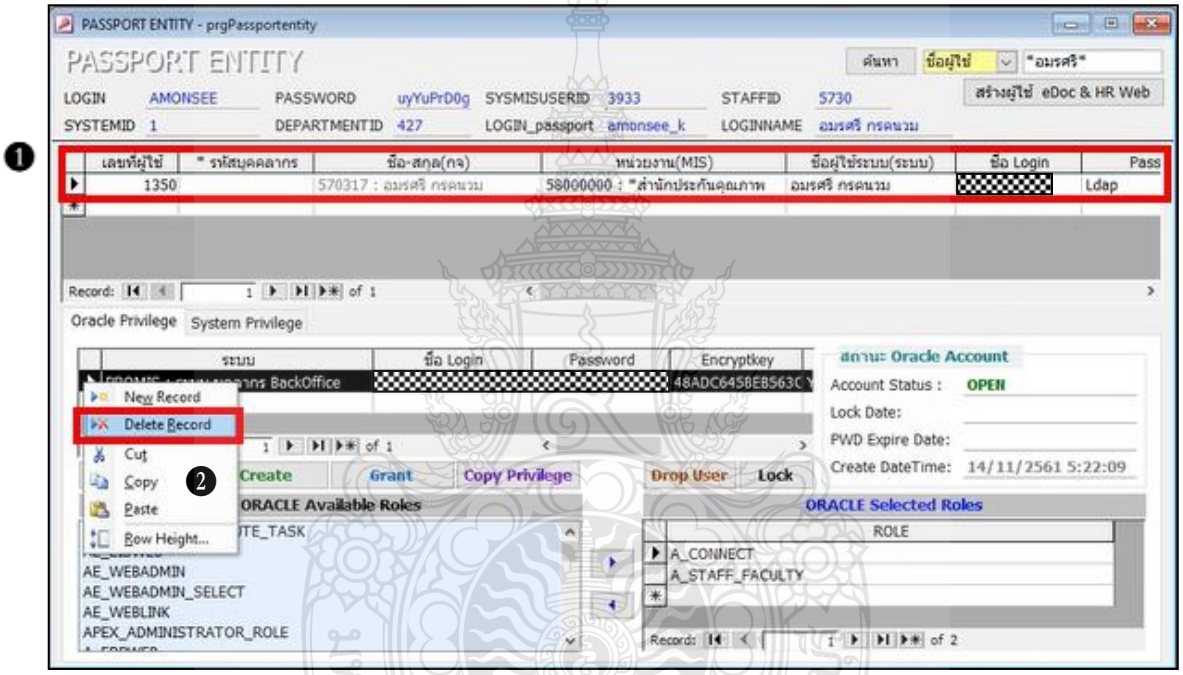
หมายเลข 1 เรียกเมนู ระบบสำหรับผู้ดูแลระบบ >> SINGLE SIGN-ON>> PASSPORT ENTITY

หมายเลข 2 ค้นหาและตรวจสอบชื่อผู้ใช้งานอยู่สังกัดหน่วยงานไหน และตรวจสอบชื่อผู้ใช้งาน (User) แถบ Oracle Privilege

กรณีชื่อผู้ใช้งานในระบบตรงตามที่หน่วยงาน/คณะส่งมา ผู้บริหารจัดการระบบจะดำเนินการยกเลิกสิทธิ์ในขั้นตอนที่ 4

กรณีชื่อผู้ใช้งานในระบบไม่ตรงให้ดำเนินการส่งให้คณะ/หน่วยงานยืนยันกลับไปที่ขั้นตอนที่ 1

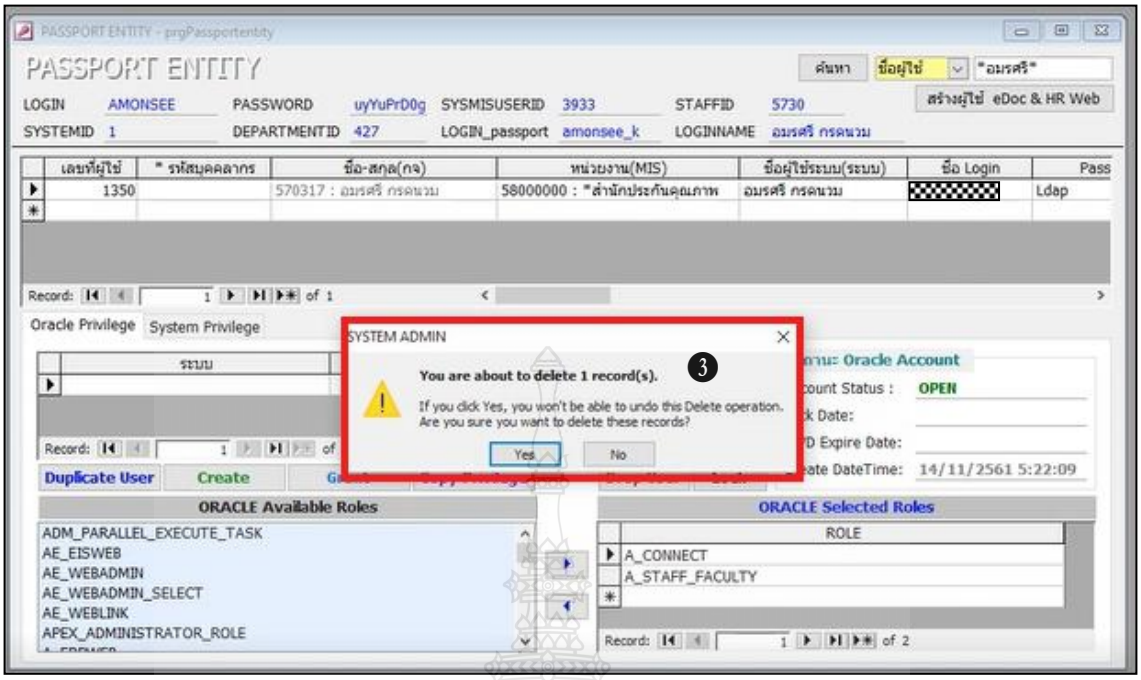
ขั้นตอนที่ 4 ผู้บริหารจัดการระบบยกเลิกการเชื่อมโยงสิทธิ์การเข้าใช้งานกับ Account Wifi Rmutt สามารถดำเนินการได้ ดังต่อไปนี้



ภาพที่ 4-92 แสดงตัวอย่างหน้าจอยกเลิกการเชื่อมโยงสิทธิ์การเข้าใช้งานกับ Account Wifi

หมายเลข 1 เมื่อกดปุ่มค้นแล้วจะปรากฏชื่อผู้ใช้งานที่ต้องการยกเลิกสิทธิ์

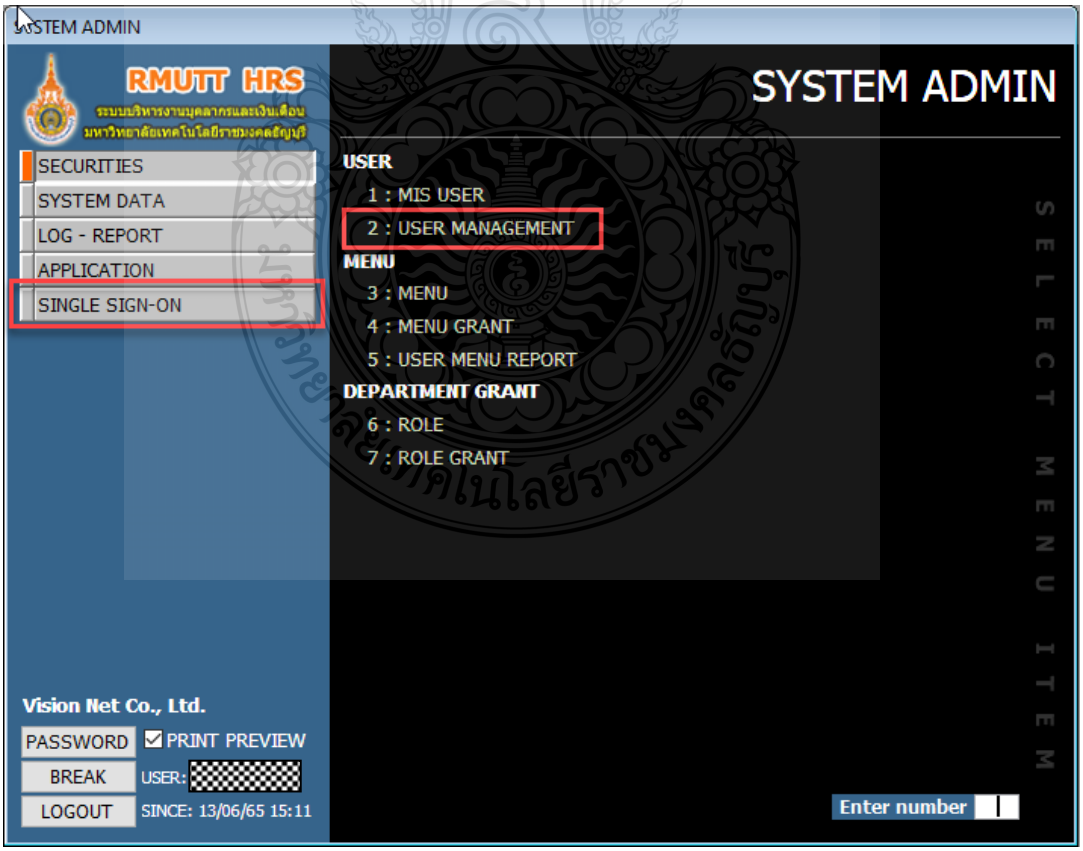
หมายเลข 2 คอลัมน์ระบบให้ทำการยกเลิกสิทธิ์ โดยการคลิกแถบ  PROMIS: ระบบบุคลากร และคลิกขวาเลือก Delete Record



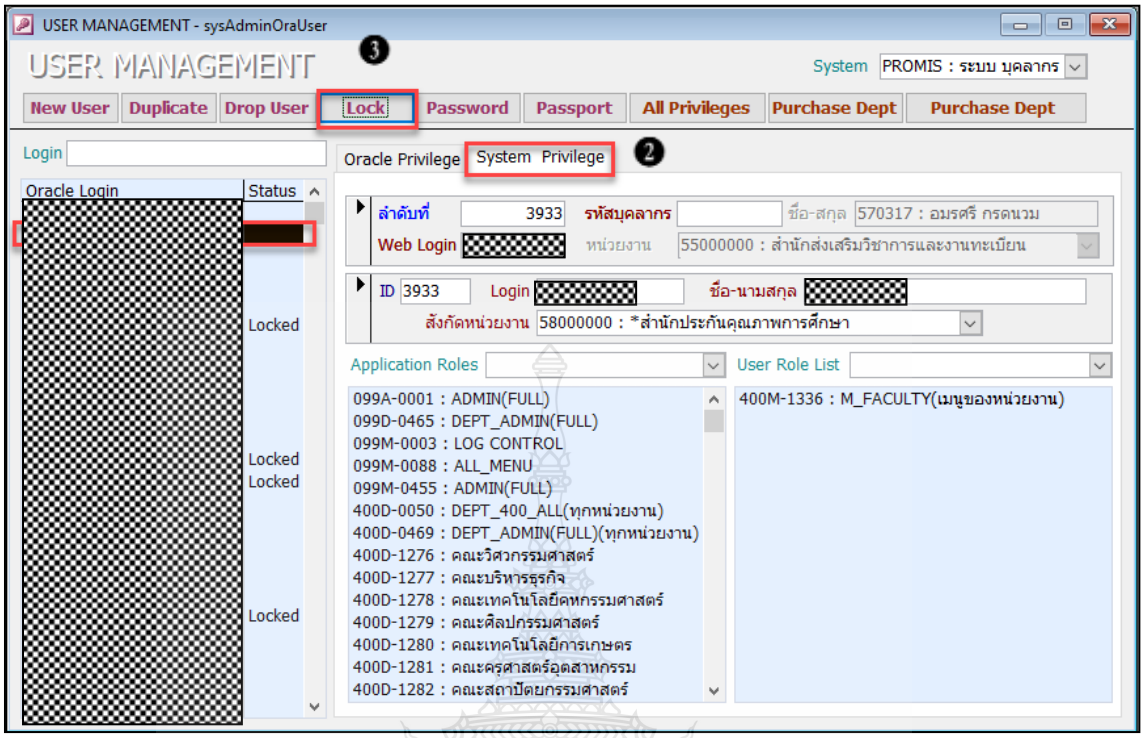
ภาพที่ 4-93 แสดงตัวอย่างหน้าจอยืนยันยกเลิกการเชื่อมโยงสิทธิ์การเข้าใช้งานกับ Account Wifi

หมายเลข 3 กดปุ่ม Yes ระบบจะทำการ Delete Record ที่เลือก

ผู้บริหารจัดการระบบดำเนินการยกเลิกการเชื่อมต่อ Single Sign-On ดังนี้



ภาพที่ 4-94 แสดงตัวอย่างหน้าจอ SINGLE SIGN-ON

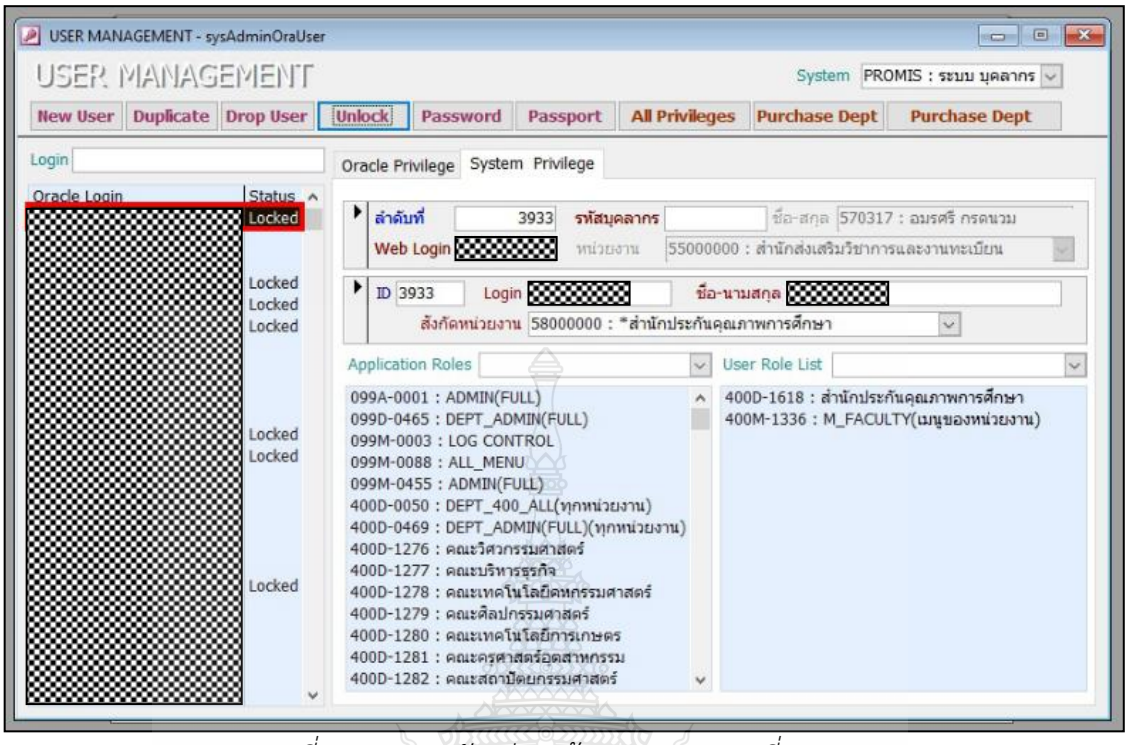


ภาพที่ 4-95 แสดงตัวอย่างหน้าจอการ LOCK User

หมายเลข 1 เรียกเมนู ระบบสำหรับผู้ดูแลระบบ >> SECURITIES >> USER MANAGEMENT

หมายเลข 2 คลิกเลือก User ตรวจสอบในแถบ System Privilege ชื่อ-นามสกุล และชื่อผู้ใช้งาน (User) ที่ต้องการยกเลิกสิทธิ์

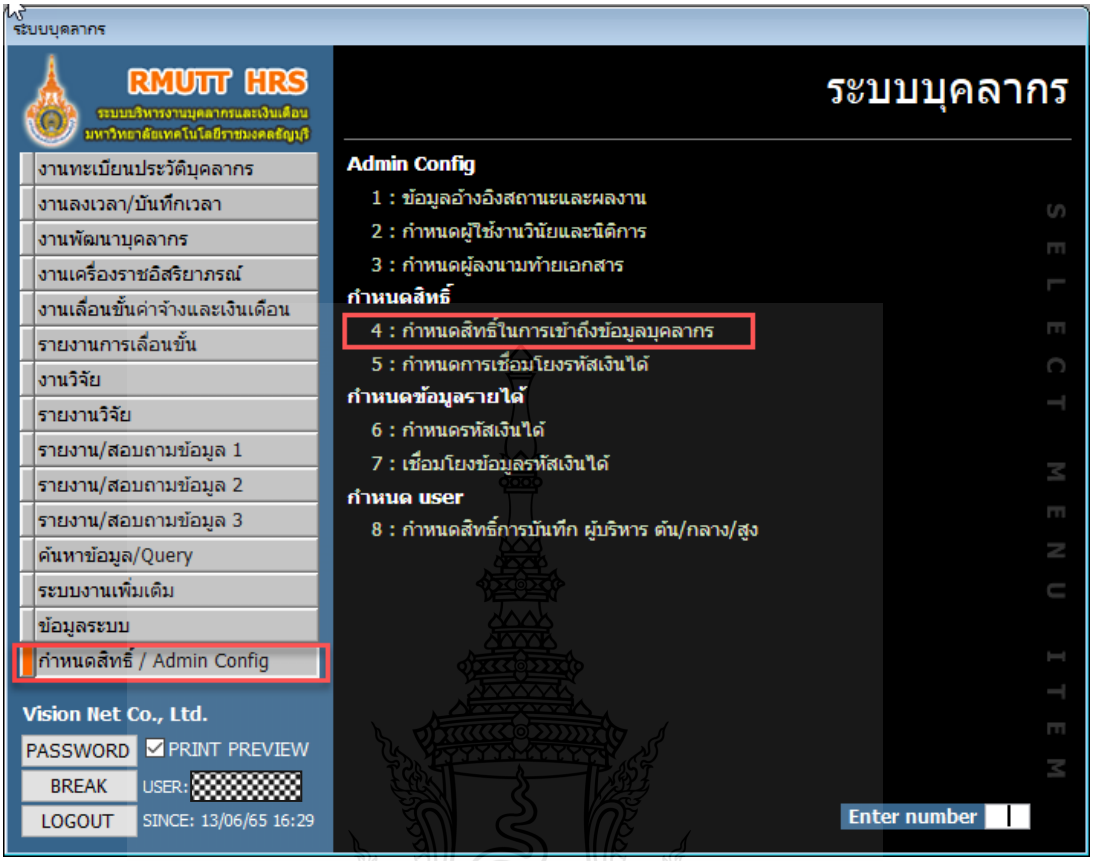
หมายเลข 3 กดปุ่ม LOCK



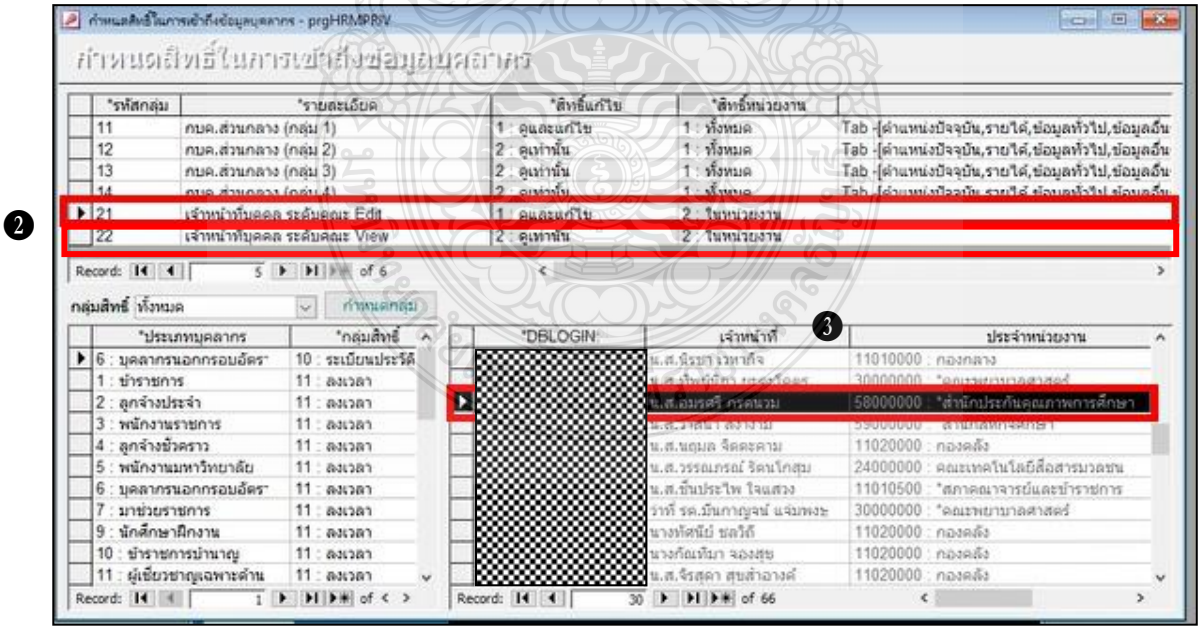
ภาพที่ 4-96 แสดงตัวอย่างหน้าจอแสดง User ที่ถูก LOCK

หมายเลข 4 ในช่อง Oracle LOG IN Status: Locked แสดงว่า ชื่อผู้ใช้งานนี้ได้ทำการ Locked ในส่วนของระบบบริหารงานบุคลากรแล้ว

ขั้นตอนที่ 5 ผู้บริหารจัดการระบบดำเนินการยกเลิกสิทธิ์การเข้าถึงเมนูระบบบริหารงานบุคลากรและเงินเดือน สามารถดำเนินการได้ ดังต่อไปนี้



ภาพที่ 4-97 แสดงตัวอย่างหน้าจอกำหนดสิทธิ์ / Admin Config

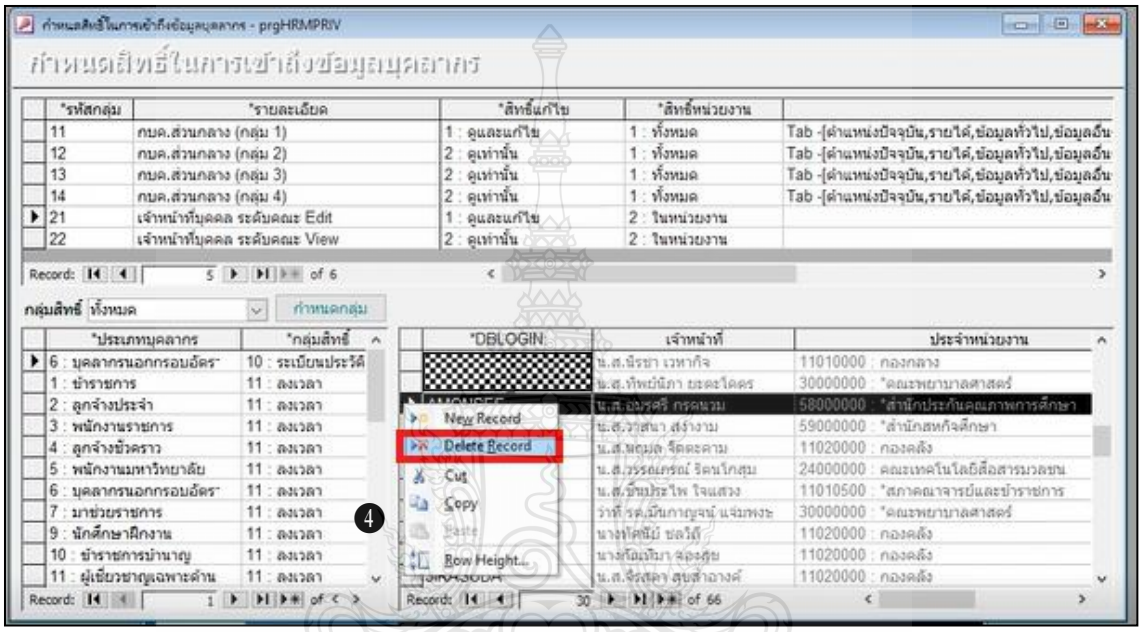


ภาพที่ 4-98 แสดงตัวอย่างหน้าจอตรวจสอบสิทธิ์การเข้าถึงแต่ละประเภทกลุ่มสิทธิ์

หมายเลข 1 เรียกเมนู >> ระบบบริหารงานบุคลากร >> กำหนดสิทธ์ / Admin Config >> กำหนดสิทธิ์ในการเข้าถึงข้อมูลบุคลากร

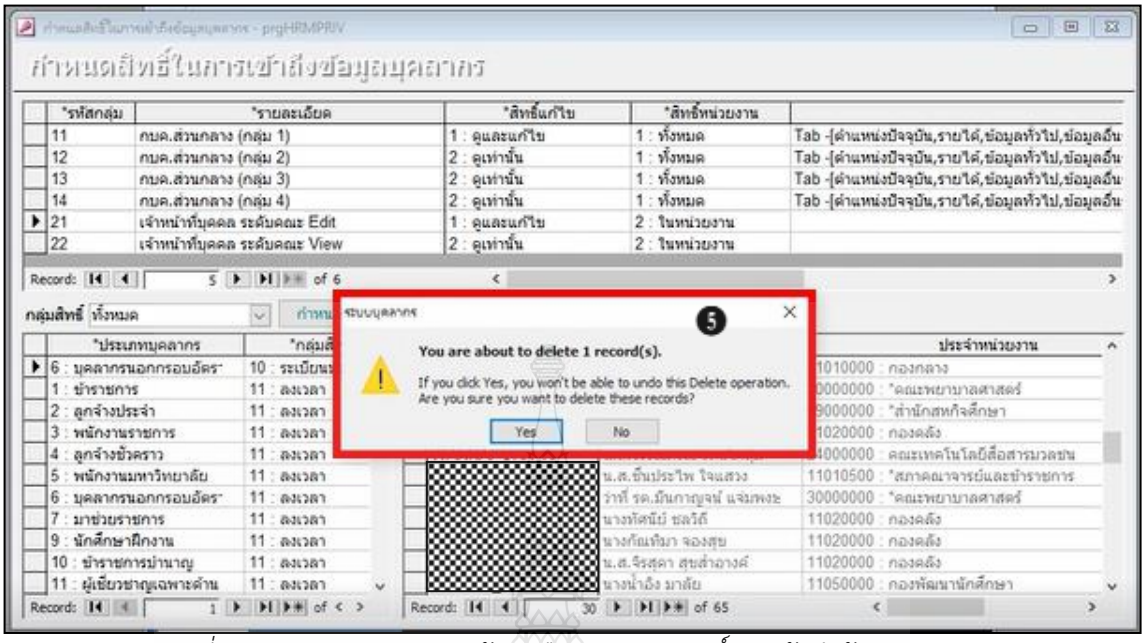
หมายเลข 2 คลิก ▶ แถว *รหัสกลุ่ม 21 เจ้าหน้าที่บุคลากร ระดับคณะ Edit และ *รหัสกลุ่ม 22 เจ้าหน้าที่บุคคล ระดับคณะ View

หมายเลข 3 คลิก ▶ แถวชื่อผู้ใช้งาน (User) ในช่อง *DBLOGIN



ภาพที่ 4-99 แสดงตัวอย่างหน้าจอยกเลิกสิทธิ์การเข้าถึงข้อมูลบุคลากร

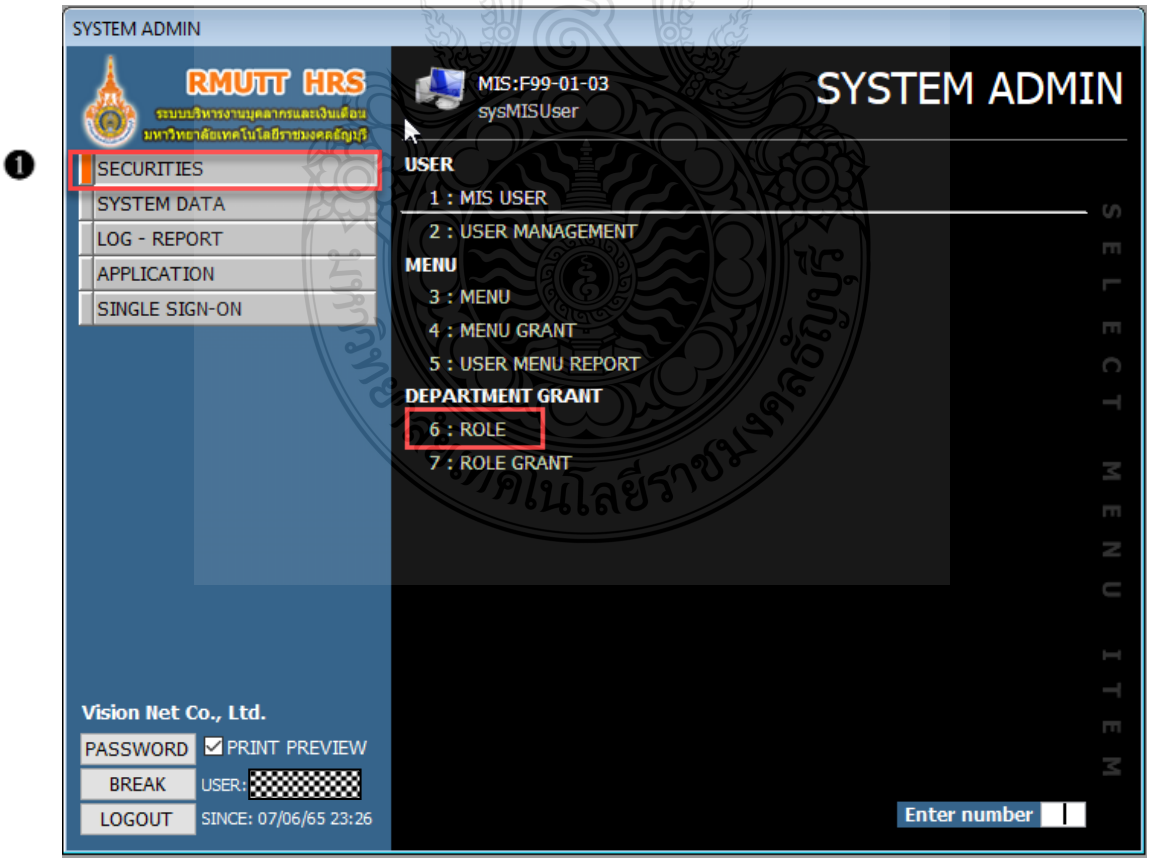
หมายเลข 4 คลิกขวาเลือก Delete Record ชื่อผู้ใช้งานที่ต้องการยกเลิกสิทธิ์



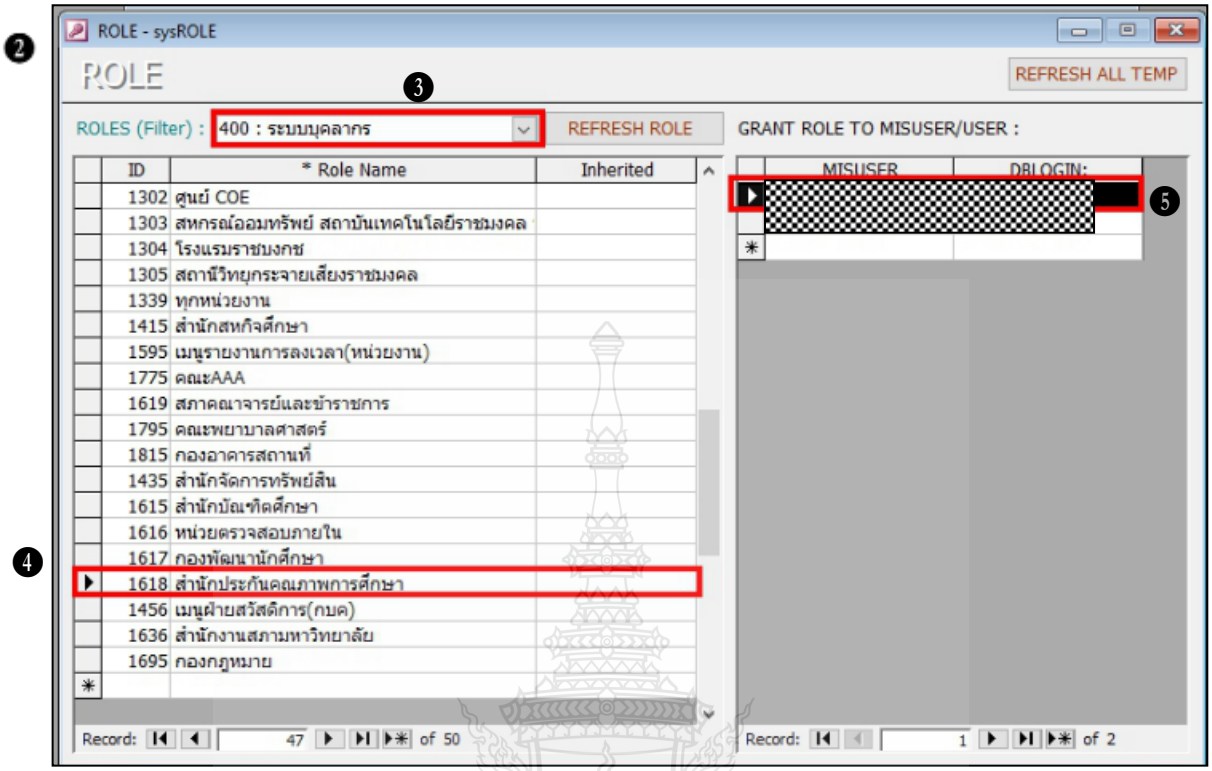
ภาพที่ 4-100 แสดงตัวอย่างหน้าจอยืนยันยกเลิกสิทธิ์การเข้าถึงข้อมูลบุคลากร

หมายเลข 5 ระบบจะแสดงป๊อปอัพในการลบ Record ให้กดปุ่ม Yes เพื่อยืนยันการลบ

การลบ ROLE



ภาพที่ 4-101 แสดงตัวอย่างหน้าจอ ROLE



ภาพที่ 4-102 แสดงตัวอย่างหน้าจอแสดง USER ทั้งหมดที่ได้สิทธิ์ ในแต่ละ Role

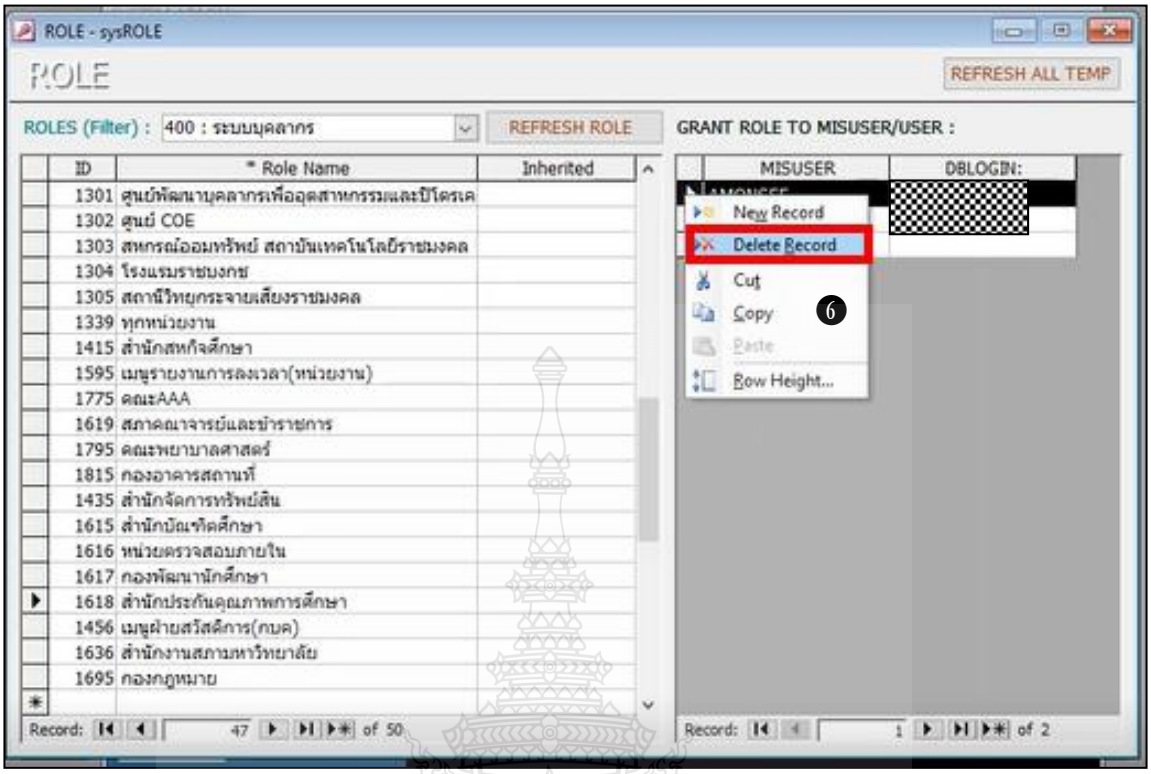
หมายเลข 1 เรียกเมนู ระบบสำหรับผู้ดูแลระบบ >> SECURITIES >> ROLE

หมายเลข 2 แสดง USER ทั้งหมดที่ได้สิทธิ์ ในแต่ละ Role สิทธิ์ในการเข้าถึงวิทยาเขต, หน่วยงาน, งบประมาณ,เล่มบัญชี

หมายเลข 3 เลือกระบบที่ต้องการลบ Role

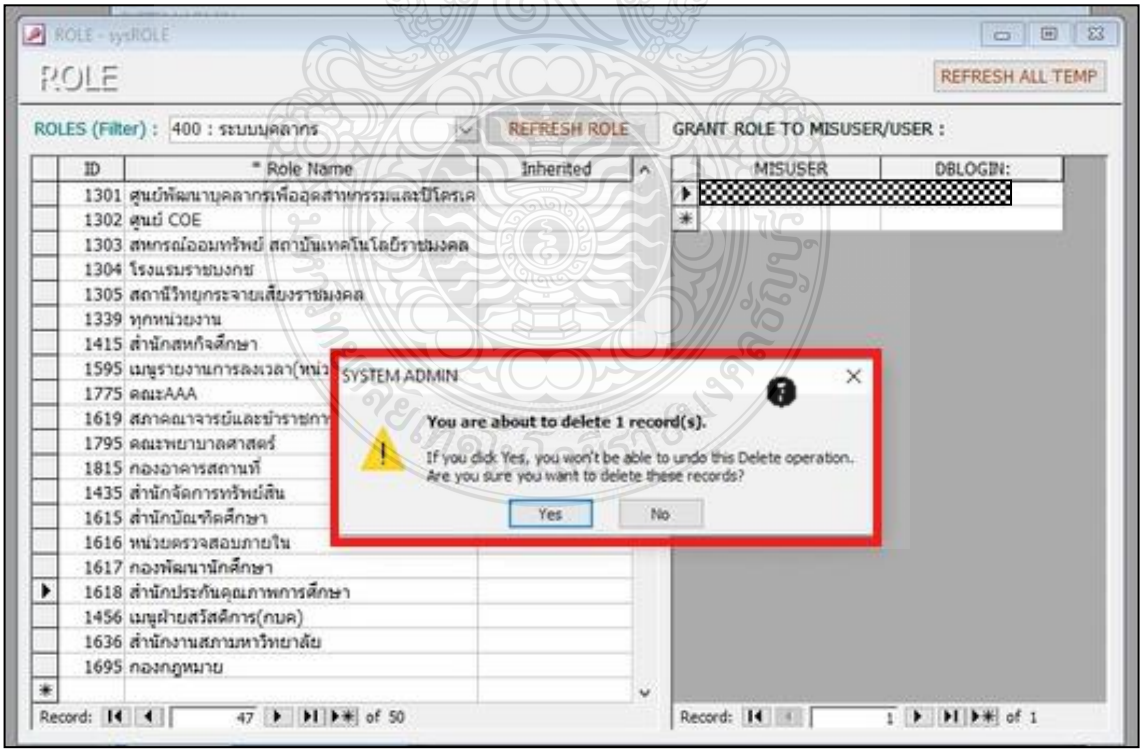
หมายเลข 4 คลิก ▶ แถวชื่อหน่วยงานที่ต้องการลบ

หมายเลข 5 ทางด้านขวามือจะปรากฏคอลัมน์ MISUSER และ DBLOGIN: คลิก ▶ ชื่อผู้ใช้งาน (User)



ภาพที่ 4-103 แสดงตัวอย่างหน้าจอยกเลิกสิทธิ์การเข้าถึงข้อมูลบุคลากรภายในหน่วยงาน

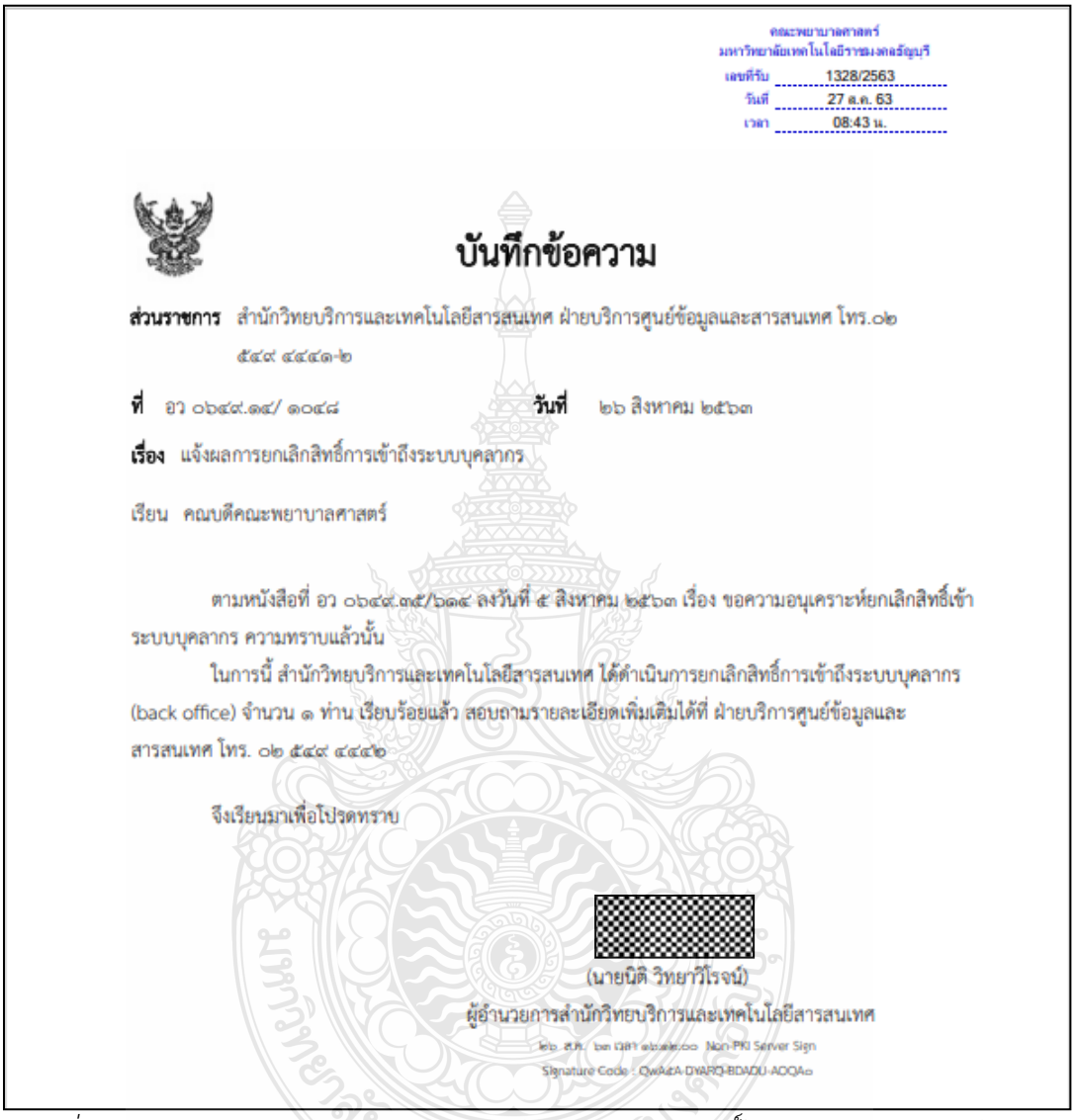
หมายเลข 6 คลิกขวาเลือก Delete Record



ภาพที่ 4-104 แสดงตัวอย่างหน้าจอยืนยันยกเลิกสิทธิ์การเข้าถึงข้อมูลบุคลากรภายในหน่วยงาน

หมายเลข 7 ระบบจะแสดงป๊อปอัพในการลบ Record ให้กดปุ่ม Yes เพื่อยืนยันการลบ

ขั้นตอนที่ 6 ผู้บริหารจัดการระบบแจ้งผลการดำเนินการกับทางต้นเรื่อง และทำหนังสือตอบกลับเรื่องแจ้งผลการยกเลิกสิทธิ์การเข้าใช้งานระบบ ดังตัวอย่างภาพที่ 4-105



คณะพยาบาลศาสตร์
มหาวิทยาลัยเทคโนโลยีราชมงคลอีสาน
เลขที่รับ 1328/2563
วันที่ 27 ส.ค. 63
เวลา 08:43 น.

บันทึกข้อความ

ส่วนราชการ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ฝ่ายบริการศูนย์ข้อมูลและสารสนเทศ โทร.๐๒ ๕๔๙ ๔๔๔๑-๒

ที่ อว ๐๖๔๙.๑๔/ ๑๐๔๘ **วันที่** ๒๖ สิงหาคม ๒๕๖๓

เรื่อง แจ้งผลการยกเลิกสิทธิ์การเข้าถึงระบบบุคลากร

เรียน คณบดีคณะพยาบาลศาสตร์

ตามหนังสือที่ อว ๐๖๔๙.๑๔/๖๑๔ ลงวันที่ ๕ สิงหาคม ๒๕๖๓ เรื่อง ขอความอนุเคราะห์ยกเลิกสิทธิ์เข้าระบบบุคลากร ความทราบแล้วนั้น

ในการนี้ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ได้ดำเนินการยกเลิกสิทธิ์การเข้าถึงระบบบุคลากร (back office) จำนวน ๑ ท่าน เรียบร้อยแล้ว สอบถามรายละเอียดเพิ่มเติมได้ที่ ฝ่ายบริการศูนย์ข้อมูลและสารสนเทศ โทร. ๐๒ ๕๔๙ ๔๔๔๒

จึงเรียนมาเพื่อโปรดทราบ

(นายนิติ วิทยาวิโรจน์)
ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ

Non-PKI Server Sign
Signature Code : QwA4zA-DWARQ-BDADU-ADQAo

ภาพที่ 4-105 แสดงตัวอย่างหนังสือตอบกลับแจ้งผลการยกเลิกสิทธิ์ไปยังหน่วยงาน/คณะต้นสังกัด

กล่าวโดยสรุป ภาพรวมในบทที่ 4 ผู้เขียนได้ถึงเขียนกระบวนการและขั้นตอนการปฏิบัติงาน ซึ่งประกอบด้วยแผนผังการปฏิบัติงาน (Work Flow) รายละเอียดของกระบวนการและขั้นตอนการปฏิบัติงาน ซึ่งเป็นลำดับการทำงาน เพื่อให้ผู้ปฏิบัติงานเห็นภาพและขั้นตอนการทำงานเพื่อลดข้อผิดพลาดและเพิ่มความรวดเร็วในการปฏิบัติงาน เป็นการถ่ายทอดความรู้และประสบการณ์ของผู้เขียนให้ผู้ปฏิบัติงานแทนในการจัดการระบบบริหารงานบุคลากรและเงินเดือน เป็นคู่มือและเป็นเครื่องนำทางในการปฏิบัติงานจากเริ่มและสิ้นสุดเพื่อให้งานเสร็จสิ้นตามกระบวนการได้อย่างถูกต้อง ส่วนปัญหาและอุปสรรค แนวทางการแก้ไข และแนวการพัฒนางานจะกล่าวถึงในบทที่ 5

บทที่ 5

ปัญหาอุปสรรคและแนวทางการแก้ไขปัญหา

การจัดการระบบบริหารงานบุคลากรและเงินเดือน มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี เป็นการจัดการการเข้าใช้งานให้กับกองบริหารงานบุคคล และเจ้าหน้าที่บุคคลากรคณะ/หน่วยงานของทั้งมหาวิทยาลัยฯ

จากประสบการณ์การปฏิบัติงาน ผู้เขียนได้พบปัญหาในกระบวนการปฏิบัติงานต่าง ๆ ในบทที่ 5 นี้จึงได้รวบรวมปัญหา อุปสรรคและแนวทางการแก้ไขปัญหา เป็นการเสนอแนวทางเพื่อแก้ไขปัญหาและอุปสรรคที่มีผลกระทบต่อการปฏิบัติงาน เพื่อให้เกิดการเรียนรู้และนำไปปรับปรุงแก้ไขในการปฏิบัติงานให้เกิดผลสำเร็จและมีประสิทธิภาพ ซึ่งจะอธิบายดังต่อไปนี้

5.1 ปัญหาอุปสรรคและแนวทางในการแก้ปัญหา

ปัญหาและอุปสรรค	แนวทางการแก้ไขปัญหา
5.1.1 การทวนสอบสิทธิ์ของผู้ใช้งาน 1) การเปลี่ยนแปลงโยกย้าย ทางหน่วยงาน/คณะไม่มีการแจ้งสถานะมายังผู้บริหารจัดการระบบ ชื่อผู้ใช้งาน (User) จึงไม่เป็นปัจจุบัน	1.1 ผู้บริหารจัดการระบบ ทำการปรับปรุงบัญชีผู้ใช้งานเพื่อเป็นการทวนสอบสิทธิ์ประจำปี อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงโครงสร้างภายใน โดยการจัดส่งรายชื่อและรายงานใช้ LOG IN เข้าระบบให้กับผู้บังคับบัญชา และให้ทางหน่วยงาน/คณะ ยืนยันชื่อผู้ใช้งาน (User) กลับ เพื่อให้ผู้บริหารจัดการระบบทำการทวนสอบสิทธิ์ผู้ใช้งานได้ 1.2 ผู้บริหารจัดการระบบทำหนังสือแจ้งเวียนไปยังคณะ/หน่วยงาน กรณีที่มีการเปลี่ยนสถานะ หรือเปลี่ยนแปลงตำแหน่งงานให้ทางคณะ/หน่วยงานทำหนังสือแจ้งกลับมายังสำนักวิทยบริการและเทคโนโลยีสารสนเทศ โดยผ่านผู้อำนวยการกองบริหารงานบุคคล
5.1.2 การกำหนดสิทธิ์ของระบบบุคลากรและเงินเดือน 1) เมื่อมีการรับบุคลากรใหม่ โดยทางคณะ/หน่วยงานส่งหนังสือคำสั่งบรรจุแต่งตั้งไปยังกองบริหารงานบุคคล แต่อยู่ในระหว่างขั้นตอนการบันทึกทะเบียน	1.1 ผู้บริหารจัดการระบบ ประสานงานแจ้งทางคณะหน่วยงานกรณียังไม่ได้ส่งข้อมูลประวัติและคำสั่งบรรจุแต่งตั้งบุคลากรให้กับกองบริหารงานบุคคล หากเจ้าหน้าที่บุคคลมีความต้องการใช้งานระบบเพื่อใช้ในการปฏิบัติงานด้านบุคลากรแบบ

ปัญหาและอุปสรรค	แนวทางการแก้ไขปัญหา
ประวัติบุคลากร ทำให้ไม่มีข้อมูลบุคลากรบรรจุใหม่ในระบบ ผู้บริหารจัดการระบบจึงไม่สามารถกำหนดสิทธิ์ให้กับเจ้าหน้าที่บุคลากรคณะ/หน่วยงานได้	เร่งด่วน ให้นำเอกสารคำสั่งบรรจุแต่งตั้งบุคลากรให้ทางคณะ/หน่วยงานเซ็นรับรอง แล้วให้ทางกองบริหารงานบุคคลยืนยันการเพิ่มสิทธิ์เพื่อแจ้งกลับมาทางผู้บริหารจัดการระบบ จากนั้นผู้บริหารจัดการระบบจะดำเนินการกำหนดสิทธิ์ให้กับบุคลากรใหม่ 1.2 ผู้บริหารจัดการระบบ ประสานงานแจ้งทางคณะ/หน่วยงาน กรณีอยู่ในขั้นตอนการบันทึกทะเบียนประวัติบุคลากรใหม่ และต้องการเพิ่มสิทธิ์การเข้าใช้งานให้ทำหนังสือแจ้งขอเพิ่มสิทธิ์โดยผ่านผู้อำนวยการกองบริหารงานบุคคล โดยให้ทางกองบริหารงานบุคคลยืนยันการเพิ่มสิทธิ์เพื่อแจ้งกลับมา จากนั้นผู้บริหารจัดการระบบจะดำเนินการกำหนดสิทธิ์ให้กับบุคลากรใหม่
2) การแจ้งขอสิทธิ์เข้าใช้งานระบบตำแหน่งงานของผู้ปฏิบัติงานที่ได้รับมอบหมายงานบุคลากร ไม่ตรงตามภาระงาน	2.1 ผู้บริหารจัดการระบบประสานงานแจ้งทางคณะ/หน่วยงานทำหนังสือแจ้งขอเพิ่มสิทธิ์การเข้าใช้งานระบบพร้อมแนบคำสั่งแต่งตั้งบุคลากรให้ปฏิบัติหน้าที่ เพื่อให้กองบริหารงานบุคคลดำเนินการการพิจารณากลั่นกรอง และผู้บริหารจัดการระบบจะดำเนินการกำหนดสิทธิ์การเข้าใช้งานระบบ
3) การปฏิบัติงานภายใน ผู้บังคับบัญชามีการมอบหมายงานบุคลากรให้ช่วยงานโดยทางคณะ/หน่วยงานไม่มีการแจ้งขอเพิ่มสิทธิ์การเข้าใช้งานระบบ ซึ่งเจ้าหน้าที่บุคลากรมีการมอบ Username/Password ให้ผู้ที่ได้รับมอบหมายงานเข้าใช้งาน อาจเกิดข้อผิดพลาดหรือข้อมูลเสียหายได้	3.1 ผู้บริหารจัดการระบบประสานงานแจ้งบุคลากรคณะ/หน่วยงาน ให้ทำเรื่องขอการเพิ่มสิทธิ์การเข้าใช้งานให้กับผู้ที่ได้รับมอบหมายผ่านกองบริหารงานบุคคล และทางกองบริหารงานบุคคลพิจารณากลั่นกรองว่าจะให้สิทธิ์การเข้าใช้งานหรือไม่ และสำนักวิทยบริการและเทคโนโลยีสารสนเทศกำหนดนโยบายการควบคุมการเข้าถึงข้อมูลและสารสนเทศของมหาลัย (Information Access control) ในส่วนหน้าที่ความรับผิดชอบของผู้ใช้งาน

ปัญหาและอุปสรรค	แนวทางการแก้ไขปัญหา
5.1.3 การยกเลิกสิทธิ์ของระบบบริหารงานบุคลากรและเงินเดือน 1) เจ้าหน้าที่บุคลากรลาออก ทางหน่วยงาน/คณะไม่มีการแจ้งข้อมูลมายังผู้บริหารจัดการระบบ จึงไม่ได้ดำเนินการยกเลิกสิทธิ์การเข้าใช้งานระบบ ทำให้เกิดข้อมูลขยะภายใน	1.1 ผู้บริหารจัดการระบบประสานงานแจ้งบุคลากรคณะ/หน่วยงาน ทำหนังสือแจ้งยกเลิกสิทธิ์การเข้าใช้งานผ่านผู้อำนวยการกองบริหารงานบุคคล และทางผู้บริหารจัดการระบบทำหนังสือตอบกลับ โดยแจ้งรายละเอียดชื่อผู้ใช้งานปัจจุบันที่สามารถเข้าใช้งานระบบได้ หากมีการแก้ไขเปลี่ยนแปลงให้ทางคณะ/หน่วยงานทำหนังสือแจ้งกลับมายังสำนักวิทยบริการและเทคโนโลยีสารสนเทศ 1.2 ผู้บริหารจัดการระบบ ทำการปรับปรุงบัญชีผู้ใช้งานเพื่อเป็นการทวนสอบสิทธิ์ประจำปี อย่างน้อยปีละ 1 ครั้ง 1.3 สำนักวิทยบริการและเทคโนโลยีสารสนเทศกำหนดนโยบายการบริหารจัดการการเข้าถึงผู้ใช้งาน (User Access Management) เพื่อกำหนดระยะเวลาการจัดเก็บข้อมูลบุคลากรสถานะลาออก
5.1.4 การใช้งานระบบ 1) เมื่อมีการรับบุคลากรใหม่หรือเปลี่ยนแปลงเจ้าหน้าที่บุคลากรคณะ/หน่วยงาน ไม่มีการสอนงาน ผู้บริหารจัดการระบบต้องใช้วิธีการส่งคู่มือและแนะนำวิธีการใช้งาน ซึ่งเจ้าหน้าที่ที่มาปฏิบัติงานเป็นบุคลากรใหม่ ยังไม่เคยใช้และยังไม่เกิดความคุ้นชินระบบจึงเกิดความเข้าใจยากต่อการใช้งาน	1.1 จัดโครงการอบรมและเป็นวิทยากรให้ความรู้ความเข้าใจในการใช้งานระบบบริหารงานบุคคลากรและเงินเดือน อย่างน้อยปีละ 1 ครั้ง และเปิดโอกาสให้บุคลากรแต่ละหน่วยงานได้ชี้แจงความต้องการรูปแบบของปัญหาที่พบเจอขณะใช้โปรแกรม เพื่อรวบรวมข้อปัญหาในการจัดประชุมกลุ่มย่อย การประชุมเชิงปฏิบัติการ (Workshop) ช่วยแก้ไขปัญหาที่เกิดขึ้นให้กับผู้ใช้โปรแกรม และพัฒนาทักษะให้ผู้ใช้โปรแกรมมีความคล่องตัวมากขึ้น อีกทั้งต้องบ่งบอกถึงประโยชน์ที่ได้รับเมื่อนำโปรแกรมไปใช้งานอย่างเต็มศักยภาพ 1.2 ผู้บริหารจัดการระบบจัดทำคู่มือการใช้งานเป็นคลิปวีดีโอและเผยแพร่บนเว็บไซต์ของสำนักฯ และสื่อออนไลน์ของมหาวิทยาลัยฯ เพื่อให้เจ้าหน้าที่บุคลากรคณะ/หน่วยงานเข้าถึงและสามารถเรียนรู้ได้ด้วยตนเอง

5.2 ข้อเสนอแนะ

5.2.1 จัดทำคู่มือการจัดการระบบบริหารงานบุคลากรและเงินเดือน เป็นคลิปวีดีโอแบบสั้นโดยแบ่งเป็นหัวข้อ และนำไปเผยแพร่บนเว็บไซต์ฝ่ายบริการศูนย์ข้อมูลและสารสนเทศ (Information Center)

5.2.2 รวบรวมปัญหา อุปสรรค ข้อคำถามในการใช้งาน และจัดทำคำถามที่พบบ่อย FAQ (Frequently Asked Question) คือรายการคำถามและคำตอบ ซึ่งคาดว่าเป็นข้อคำถามที่ผู้ใช้งานมักถามเสมอ เป็นการตอบปัญหาและใส่วิธีการแก้ไขปัญหา โดยแปะไว้ที่เว็บไซต์ของสำนักฯ และระบบบริหารงานบุคลากรและเงินเดือน เพื่อให้เจ้าหน้าที่บุคลากรคณะ/หน่วยงานสามารถแก้ไขปัญหาได้ด้วยตนเอง

5.2.3 ปรับปรุงระบบให้สามารถรองรับการใช้งานผ่าน Web บนสมาร์ทโฟนและแท็บเล็ต เพื่อการเข้าถึงการใช้งานได้ง่าย สะดวกรวดเร็วและมีประสิทธิภาพมากยิ่งขึ้น

บรรณานุกรม

กรมสุขภาพจิต. (2562). **มาตรฐานทางจรรยาบรรณและจรรณยาบรรณทางวิชาชีพบุคลากร**, สืบค้นเมื่อ 15 พฤษภาคม 2564. จาก http://www.oic.go.th/FILEWEB/CABINFOCENTER50/DRAWER060/GENERAL/DATA0000/00000195.PDF

ไกรทพนธ์ เติมวิทย์ขจร ,ศิริชัย นามบุรี,นิมานูนี หะยีวาเงาะ. (2559). **การพัฒนาระบบสารสนเทศสำหรับการจัดการ(Information System Development)**, สืบค้นเมื่อ 29 เมษายน 2564. จาก https://journal.oas.psu.ac.th/index.php/asj/article/viewFile/1163/1075

นางรัตนาภรณ์ ศรีหาพล.นายรอปี มิง แมะเราะ. (2556).**ความพึงพอใจต่อการใช้บริการและระบบสารสนเทศเพื่อการบริหาร มหาวิทยาลัยราชภัฏยะลา,** สืบค้นเมื่อ 15 พฤษภาคม 2564.

นิติ วิทยาวิโรจน์. (2558). **วิสัยทัศน์ กลยุทธ์ การบริหารจัดการและแผนพัฒนา พ.ศ. 2558 – 2561 สำนักวิทยบริการและเทคโนโลยีสารสนเทศ**, สืบค้นเมื่อ 5 พฤษภาคม 2564. จาก https://www.arit.rmutt.ac.th/download/20150923-Arit-Planning.pdf

พีระพล รัตนาไพบูลย์. (2560) .**การบริหารความมั่นคงสารสนเทศ**, สืบค้นเมื่อ 12 กรกฎาคม 2564. จาก https://sites.google.com/site/peempeerapon/kar-brihar-khwam-mankhng-sarsnthes/bth-thi-7

เพจ Facebook ชื่อ Bc0411 การจัดการความมั่นคงของระบบสารสนเทศ. (2562). **การพิสูจน์ตัวตน (Authentication)**, สืบค้นเมื่อ 12 มิถุนายน 2564.

มหาวิทยาลัยสงขลานครินทร์. (๒๕๕๘). **นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยสงขลานครินทร์**, สืบค้นเมื่อ 5 พฤษภาคม 2564. จาก https://www.cc.psu.ac.th/phocadownload/itplan/2-24062558.pdf

มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี. (2552). **ข้อบังคับมหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี ว่าด้วยจรรยาบรรณของข้าราชการและบุคลากรของมหาวิทยาลัย พ.ศ. 2552**, สืบค้นเมื่อ 15 พฤษภาคม 2564. จาก https://www.ped.rmutt.ac.th/?wpfb_dl=64

มัทธนา ก้อนสันทัด. (2562). **คู่มือรับแจ้งปัญหาระบบฐานข้อมูล ฝ่ายบริการศูนย์ข้อมูลกลาง (Information Center)**. สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี, สืบค้นเมื่อ 12 มิถุนายน 2564.

ราชกิจจานุเบกษา. (2562). **พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562**, สืบค้นเมื่อ 5 พฤษภาคม 2564. จาก http://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/T_0052.PDF

เว็บไซต์ บริษัท วิชั่นเน็ต จำกัด. (2553). **HR & Payroll**, สืบค้นเมื่อ 12 กรกฎาคม 2564. จาก https://vn.co.th/v2/?p=68

เว็บไซต์ บริษัท แมงโก้ คอนซัลแตนท์ จำกัด. (2551) .**ความสำคัญของการกำหนดสิทธิ์การเข้าถึงข้อมูลของพนักงาน**, สืบค้นเมื่อ 12 กรกฎาคม 2564. จาก https://www.mangoconsultant.com/th/news-knowledge/knowledge/317

สมาคมธนาคารไทย. (2562). **การพิสูจน์และการยืนยันตัวตน**, สืบค้นเมื่อ 29 กรกฎาคม 2564. จาก https://www.tba.or.th/wp-content/uploads/2020/02/TBCERTTR19-006.1.pdf

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน). (2563). **แนวทางการจัดทำกระบวนการและการดำเนินงานทางดิจิทัลเรื่องการใช้ดิจิทัลไอดีสำหรับบริการภาครัฐ–การพิสูจน์และยืนยันตัวตนทางดิจิทัล**, สืบค้นเมื่อ 29 กรกฎาคม 2564.

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ. (2562). **รายงานประเมินตนเองประจำปีการศึกษา 2562** การบริหารงานตามแผนยุทธศาสตร์ 4 ปี และแผนปฏิบัติราชการประจำปี, สืบค้นเมื่อ 5 พฤษภาคม 2564. จาก https://www.arit.rmutt.ac.th/download/Self_Assessment/sar62/20200427_SAR25622_2.pdf

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ. (2566). มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี. **โครงสร้างสำนักวิทยบริการและเทคโนโลยีสารสนเทศ**, สืบค้นเมื่อ 21 กันยายน 2566. จาก https://www.arit.rmutt.ac.th/ceo-arit/

สำนักบริหารหนี้สาธารณะ. (2558). **แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำนักงานบริหารหนี้สาธารณะ กระทรวงการคลัง ปีงบประมาณ พ.ศ. 2558**, สืบค้นเมื่อ 5 พฤษภาคม 2564. จาก http://www1.pdmo.go.th/internal-audit/upload/regulation/file_161012124942.pdf

ภาคผนวก

ภาคผนวก ก

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ภาคผนวก ข

(ร่าง) แต่งตั้งคณะกรรมการเตรียมการเพื่อดำเนินการให้สอดคล้องกับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี

ร่าง

คำสั่งมหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี

ที่ /๒๕๖๖

เรื่อง แต่งตั้งคณะกรรมการเตรียมการเพื่อดำเนินการให้สอดคล้อง

กับกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี

เพื่อให้การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ในการบริหารราชการและการดำเนินงานของมหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรีเป็นไปด้วยความเรียบร้อย มีประสิทธิภาพ

อาศัยอำนาจตามความในมาตรา ๒๔ และมาตรา ๒๗ แห่งพระราชบัญญัติมหาวิทยาลัยเทคโนโลยีราชมงคล พ.ศ. ๒๕๔๘ จึงมีคำสั่ง ดังต่อไปนี้

ข้อ ๑ ให้มีคณะกรรมการอำนวยการ ประกอบด้วย

(๑) อธิการบดีมหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี	ประธานกรรมการ
(๒) รองอธิการบดี (ผู้ช่วยศาสตราจารย์อภิชาติ ไก่ฟ้า)	รองประธานกรรมการ
(๓) รองอธิการบดี (นายวิรัช โหตระไวศยะ)	รองประธานกรรมการ
(๔) รองอธิการบดี (ผู้ช่วยศาสตราจารย์พงศ์พิชญ์ ต่วนภูษา)	รองประธานกรรมการ
(๕) รองอธิการบดี (รองศาสตราจารย์กฤษณ์ชนม์ ภูมิกิตติพิชญ์)	รองประธานกรรมการ
(๖) รองอธิการบดี (ผู้ช่วยศาสตราจารย์เมธา ศิริกูล)	รองประธานกรรมการ
(๗) รองอธิการบดี (ผู้ช่วยศาสตราจารย์อิทธิพล โพธิพันธุ์)	รองประธานกรรมการ
(๘) รองอธิการบดี (รองศาสตราจารย์สุมนมาลย์ เนียมหลาง)	รองประธานกรรมการ
(๙) รองอธิการบดี (นายเรืองศักดิ์ ภูธรธราช)	รองประธานกรรมการ
(๑๐) ผู้ช่วยอธิการบดี (ผู้ช่วยศาสตราจารย์ปณิตา สงวนทรัพย์)	รองประธานกรรมการ
(๑๑) ผู้ช่วยอธิการบดี (นายนิติ วิทยาวิโรจน์)	รองประธานกรรมการ
(๑๒) คณบดีคณะวิศวกรรมศาสตร์	กรรมการ
(๑๓) คณบดีคณะบริหารธุรกิจ	กรรมการ
(๑๔) คณบดีคณะครุศาสตร์อุตสาหกรรม	กรรมการ
(๑๕) คณบดีคณะเทคโนโลยีการเกษตร	กรรมการ
(๑๖) คณบดีคณะวิทยาศาสตร์และเทคโนโลยี	กรรมการ
(๑๗) คณบดีคณะเทคโนโลยีสื่อสารมวลชน	กรรมการ

(๑๘) คณบดีคณะศิลปะศาสตร์ กรรมการ

(๑๙) คณบดีคณะเทคโนโลยีคหกรรมศาสตร์ กรรมการ

(๒๐) คณบดีคณะศิลปกรรมศาสตร์ กรรมการ

(๒๑) คณบดีคณะสถาปัตยกรรมศาสตร์ กรรมการ

(๒๒) คณบดีคณะพยาบาลศาสตร์ กรรมการ

(๒๓) คณบดีคณะการแพทย์บูรณาการ กรรมการ

(๒๔) ผู้อำนวยการสำนักส่งเสริมวิชาการและงานทะเบียน กรรมการ

(๒๕) ผู้อำนวยการกองพัฒนานักศึกษา กรรมการ

(๒๖) ผู้อำนวยการสำนักบัณฑิตศึกษา กรรมการ

(๒๗) ผู้อำนวยการกองนโยบายและแผน กรรมการ

(๒๘) ผู้อำนวยการกองกลาง กรรมการ

(๒๙) ผู้อำนวยการกองอาคารสถานที่ กรรมการ

(๓๐) ผู้อำนวยการกองคลัง กรรมการ

(๓๑) ผู้อำนวยการกองประชาสัมพันธ์ กรรมการ

(๓๒) ผู้อำนวยการสถานีวิทยุกระจายเสียงราชมงคล กรรมการ

(๓๓) ผู้อำนวยการกองยุทธศาสตร์ต่างประเทศ กรรมการ

(๓๔) ผู้อำนวยการสำนักประกันคุณภาพการศึกษา กรรมการ

(๓๕) ผู้อำนวยการสำนักจัดการทรัพย์สิน กรรมการ

(๓๖) ผู้อำนวยการสำนักสหกิจศึกษา กรรมการ

(๓๗) ผู้อำนวยการสถาบันวิจัยและพัฒนา กรรมการ

(๓๘) ผู้อำนวยการสำนักบัณฑิตศึกษา กรรมการ

(๓๙) หัวหน้าสำนักงานสภามหาวิทยาลัย กรรมการ

(๔๐) ประธานสภาคณาจารย์และข้าราชการ กรรมการ

(๔๑) ผู้อำนวยการโรงเรียนสาธิตนวัตกรรม กรรมการ

(๔๒) ผู้จัดการหน่วยบ่มเพาะวิสาหกิจ กรรมการ

(๔๓) ผู้จัดการหอพักนักศึกษา กรรมการ

(๔๔) ผู้อำนวยการสถาบันจิงซื่อ กรรมการ

(๔๕) ผู้อำนวยการสำนักความร่วมมืออุตสาหกรรม กรรมการ

(๔๖) ผู้อำนวยการสำนักงานบริการวิชาการ กรรมการ

(๔๗) หัวหน้าหน่วยตรวจสอบภายใน มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี กรรมการ

(๔๘) ผู้อำนวยการกองกฎหมาย กรรมการและเลขานุการ

(๔๙) ผู้อำนวยการกองบริหารงานบุคคล กรรมการและผู้ช่วยเลขานุการ

(๕๐) ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ กรรมการและผู้ช่วยเลขานุการ

ให้คณะกรรมการอำนวยการ มีหน้าที่และอำนาจ ดังนี้

(๑) ให้ข้อเสนอแนะ กำหนดนโยบาย มาตรการและกลไกขับเคลื่อน กำกับติดตามและสนับสนุน เพื่อดำเนินการทั่วทั้งมหาวิทยาลัยให้สอดคล้องกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ รวมถึงกฎหมายอื่นที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

(๒) กำหนดหลักเกณฑ์การแต่งตั้งผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO: Data Protection Officer) และบุคลากรอื่นใดเพื่อให้เป็นไปตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒

ข้อ ๒ ให้มีคณะกรรมการระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ ประกอบด้วยบุคคล ดังต่อไปนี้

(๑) ผู้ช่วยศาสตราจารย์อำนวย เรืองวารี	ประธานกรรมการ
(๒) ผู้ช่วยศาสตราจารย์บุญธิดา เอื้อพิพัฒนากูล	กรรมการ
(๓) ผู้ช่วยศาสตราจารย์บุณฑริกา ทองดอนพุ่ม	กรรมการ
(๔) ผู้ช่วยศาสตราจารย์จตุรพิธ เกราะแก้ว	กรรมการ
(๕) ผู้ช่วยศาสตราจารย์ศิระเชษฐ์ โพธิ์หิรัญ	กรรมการ
(๖) ผู้ช่วยศาสตราจารย์ปองพล นิลพฤกษ์	กรรมการและเลขานุการ
(๗) นางสาวปาริชาติ ศริยานนท์พินิจ	กรรมการและผู้ช่วยเลขานุการ
(๘) นางพรสุภา บุญทศ	กรรมการและผู้ช่วยเลขานุการ

ให้คณะกรรมการระบบบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ มีหน้าที่และอำนาจ ดังนี้

(๑) จัดทำนโยบายคุ้มครองข้อมูลส่วนบุคคลของมหาวิทยาลัย ให้เป็นไปตามกฎหมาย

(๒) บริหารจัดการระบบความมั่นคงปลอดภัย เพื่อสนับสนุนนโยบายคุ้มครองข้อมูลส่วนบุคคลของมหาวิทยาลัย

(๓) ติดตาม ประเมินผล เผยแพร่ และรายงานผลการบริการจัดการความมั่นคงปลอดภัยตามนโยบายการคุ้มครองข้อมูลส่วนบุคคลของมหาวิทยาลัย

ทั้งนี้ ตั้งแต่บัดนี้ เป็นต้นไป

สั่ง ณ วันที่ ตุลาคม พ.ศ. ๒๕๖๖

(รองศาสตราจารย์สมหมาย ผิวสอาด)
อธิการบดีมหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี

ภาคผนวก ค

หนังสือแจ้งเวียนประกาศใช้งานระบบ RMUTT Single Sign On

เรื่อง ขอแจ้งปรับเปลี่ยนรูปแบบการเข้าใช้งาน (LOGIN) ของระบบบริหารงานบุคลากร(Backoffice)

บันทึกข้อความ

ส่วนราชการ ฝ่ายบริการศูนย์ข้อมูลและสารสนเทศ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ โทร. ๐๒ ๕๔๙ ๔๔๔๑-๒

ที่ อว ๐๖๔๙.๑๔/ ๑๙๕ **วันที่** ๒๖ มิถุนายน ๒๕๖๒

เรื่อง ขอแจ้งปรับเปลี่ยนรูปแบบการเข้าใช้งาน (Login) ของระบบบุคลากร (Back office)

เรียน หัวหน้าหน่วยงานมหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี

ตามที่สำนักวิทยบริการและเทคโนโลยีสานสนเทศ ได้รับมอบหมายให้ดูแลและประสานงานการพัฒนาระบบบริหารงานบุคคล เพื่อให้ผู้ใช้งานสามารถปฏิบัติงานได้สะดวกและมีประสิทธิภาพมากยิ่งขึ้น ทางสำนักฯ ได้ทำการปรับเปลี่ยนรูปแบบการเข้าใช้งาน (Login) ของระบบ Back office เป็นแบบเข้าใช้ผ่าน User wifi ของผู้ใช้งานได้นั้น

ในการนี้ ได้มีการปรับเปลี่ยนรูปแบบการเรียกใช้งานโปรแกรมเป็นการเรียกใช้งานผ่าน Web Browser โดยผู้ใช้งานสามารถติดตั้งโปรแกรมใหม่และเข้าใช้ได้ด้วยตนเองที่เว็บไซต์ https://hr.rmutt.ac.th/vncaller พร้อมกันนี้ได้แนบเอกสารคู่มือการติดตั้งและการใช้งานดังเอกสารแนบท้าย ทั้งนี้ผู้ใช้งานสามารถเข้าใช้งานโปรแกรมรูปแบบใหม่ได้ตั้งแต่วันที่ ๑ กรกฎาคม ๒๕๖๒ เป็นต้นไป หากพบปัญหาในการติดตั้งหรือใช้งานสามารถแจ้งมาได้ที่ https://helpdesk.rmutt.ac.th ระบบแจ้งซ่อมออนไลน์ หมายเลขโทรศัพท์ ๐๒ ๕๔๙ ๔๔๔๑-๒

จึงเรียนมาเพื่อโปรดทราบ

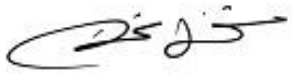
(นายนิติ วิทยาวิโรจน์)
ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ

๒๖ มิ.ย. ๖๒ เวลา ๑๔:๒๒:๕๖ Non-PKI Server Sign
Signature Code : MQAyA-DgAQg-A๕AEU-ANQA๒

๑ เรียน ผู้อำนวยการสำนักสหกิจศึกษา เพื่อโปรดทราบและแจ้งบุคลากรในสำนักฯ ทราบ

นางสาววาสนา สง่างาม
เจ้าหน้าที่บริหารงานทั่วไป
๒๖ มิ.ย. ๖๒ เวลา ๑๖:๑๗:๓๒ , Non-PKI Server Sign , Signature
Code : OAA๑A-EEAOA-AzAEI-AQwBG

๒ ทราบและมอบดังเสนอ



(นายกิตติวัณณ์ นิ่มเกิดผล)
ผู้อำนวยการสำนักสหกิจศึกษา
๒๖ มิ.ย. ๖๒ เวลา ๑๖:๒๓:๓๔ , Non-PKI Server Sign , Signature
Code : NgBGA-DcAQg-BBAEU-AQwAz

๓ ทราบ

นางสาวปวริศา สุขภาคี
เจ้าหน้าที่บริหารงานทั่วไป
๒๗ มิ.ย. ๖๒ เวลา ๑๓:๐๙:๔๓ , Non-PKI Server Sign , Signature
Code : QgBEA-DYARA-BEADY-AQgBF

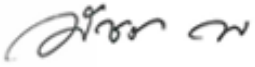
๔ ทราบ

นางสาววัชรี อุตตะมะ
นักวิชาการศึกษา
๒๗ มิ.ย. ๖๒ เวลา ๑๔:๑๗:๒๑ , Non-PKI Server Sign , Signature
Code : MQAxA-DgARQ-AxADM-AMAA๑

๕ ทราบ

นางสาวนันท์นภัส ชัยประเสริฐ
นักวิชาการศึกษา ระบบสารสนเทศ
๒๘ มิ.ย. ๖๒ เวลา ๐๙:๓๑:๕๓ , Non-PKI Server Sign , Signature
Code : RQA๑A-DEAQw-AyAEE-AQgAx

๖ ทราบ



(นางสาวพัชรา ขำสา)
นักวิชาการศึกษา
๑๐ ส.ค. ๖๒ เวลา ๒๐:๕๒:๑๖ , Non-PKI Server Sign , Signature
Code : RAA๕A-EIAQg-AzAEQ-AMABE

ภาคผนวก ง

รายงานการประเมินตนเอง (Salf Assessment Report : SAR)

ของมหาวิทยาลัย

รายงานการประเมินตนเอง (Salf Assessment Report : SAR)

ประวัติผู้เขียน

ชื่อ-นามสกุล นางพรสุภา บุญทศ

ตำแหน่ง เจ้าหน้าที่บริหารงานทั่วไป ระดับปฏิบัติการ

การศึกษา พ.ศ. 2555 ปริญญาตรี การจัดการ-การจัดการทรัพยากรมนุษย์

สถานที่ทำงาน ฝ่ายบริการศูนย์ข้อมูลและสารสนเทศ (Information Center) สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี

โทรศัพท์ 02-549-4442

Email Address pornsupa_o@rmutt.ac.th

ประวัติการทำงาน

พ.ศ. 2556 – 2556 เจ้าพนักงานธุรการ (ลูกจ้างชั่วคราว)
สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี

พ.ศ. 2556 - 2557 นักวิชาการคอมพิวเตอร์ (ลูกจ้างชั่วคราว)
สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี

พ.ศ. 2557 - ปัจจุบัน เจ้าหน้าที่บริหารงานทั่วไป (พนักงานมหาวิทยาลัย)
สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี

การจัดการระบบบริหารงานบุคลากรและเงินเดือน