คู่มือปฏิบัติงาน

การกำหนดสิทธิ์การใช้งานของผู้ใช้งานระบบสารสนเทศเพื่อการบริหารมหาวิทยาลัย (MIS: Management Information System) และระบบสารสนเทศเพื่อการบริหารทรัพยากรองค์กร (ERP: Enterprise Resource Planning)

นางสาวบังอร เหล่าปิ่นเพชร

นักวิชาการคอมพิวเตอร์

งานระบบสารสนเทศ สำนักคอมพิวเตอร์

มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา

คู่มือปฏิบัติงาน

การกำหนดสิทธิ์การใช้งานของผู้ใช้งานระบบสารสนเทศเพื่อการบริหารมหาวิทยาลัย (MIS: Management Information System) และระบบสารสนเทศเพื่อการบริหารทรัพยากรองค์กร (ERP: Enterprise Resource Planning)

นางสาวบังอร เหล่าปิ่นเพชร

นักวิชาการคอมพิวเตอร์

งานระบบสารสนเทศ สำนักคอมพิวเตอร์

มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา

คำนำ

งานระบบสารสนเทศ เป็นภารกิจหลักส่วนหนึ่งของสำนักคอมพิวเตอร์ มีหน้าที่รับผิดชอบด้านงานระบบสารสนเทศต้องวิเคราะห์ และตรวจสอบเอกสารการขอสิทธิ์ใหม่หรือมีความต้องการเพิ่มเติมจากเดิมที่มีอยู่ด้วยความถูกต้อง แม่นยำ ชัดเจน เพื่อเพิ่มประสิทธิภาพในการปฏิบัติงานการติดต่อสื่อสารและการให้บริการ จึงได้จัดทำคู่มือการปฏิบัติงานการกำหนดสิทธิ์การใช้งานของผู้ใช้งานระบบสารสนเทศเพื่อการบริหารมหาวิทยาลัย (MIS: Management Information System) และระบบสารสนเทศเพื่อการบริหารทรัพยากรองค์กร (ERP: Enterprise Resource Planning) ขึ้น

การจัดทำคู่มือการปฏิบัติงานการกำหนดสิทธิ์การใช้งานของผู้ใช้งานระบบสารสนเทศเพื่อการบริหารมหาวิทยาลัย (MIS: Management Information System) และระบบสารสนเทศเพื่อการบริหารทรัพยากรองค์กร (ERP: Enterprise Resource Planning) ฉบับนี้ ได้นำประสบการณ์จากการทำงานในการปฏิบัติงานด้านระบบสารสนเทศและทำการศึกษาค้นคว้า เรียบเรียง รวบรวม วิเคราะห์ข้อมูลนำแนวคิด ทฤษฎีของผู้ทรงคุณวุฒิมาประยุกต์ใช้ในการจัดทำขึ้นครั้งนี้

ผู้จัดทำหวังเป็นอย่างยิ่งว่า คู่มือการปฏิบัติงานฉบับนี้ จะเป็นประโยชน์แก่บุคลากรที่จะศึกษา เพื่อบูรณาการความรู้ที่ได้รับกับการปฏิบัติงานจริงเป็นแนวทางในการปฏิบัติงานที่ก่อให้เกิดประสิทธิภาพและประสิทธิผลอย่างแท้จริง หากมีข้อบกพร่องประการใด ผู้จัดทำ ต้องขออภัยมา ณ ที่นี้ และจะพัฒนาระบบการดำเนินงานต่างๆ ของงานด้านระบบสารสนเทศ ให้เป็นระบบมากยิ่งขึ้น

บังอร เหล่าปิ่นเพชร

สารบัญ

สารบัญ (ต่อ)

สารบัญตาราง

สารบัญภาพ

สารบัญภาพ (ต่อ)

บทที่ 1
บทนำ

ความเป็นมาและความสำคัญ

ระบบสารสนเทศเพื่อการบริหารมหาวิทยาลัย (MIS: Management Information System) และระบบสารสนเทศเพื่อการบริหารทรัพยากรองค์กร (ERP: Enterprise Resource Planning) เป็นเครื่องมือหนึ่งของการนำเสนอสารสนเทศเพื่อใช้ในด้านการบริหารทรัพยากรมนุษย์ทั้งในเชิงกลยุทธ์ เชิงกลวิธีและเชิงปฏิบัติการ โดยมีการปรับกระบวนการทางธุรกิจให้สอดคล้องกับเทคโนโลยีสารสนเทศที่นำมาใช้ทั้งในด้านการบริหารและการควบคุมด้านต่างๆ เพื่อเพิ่มขีดความสามารถในการปฏิบัติงานตามหน้าที่งานรับผิดชอบของลูกจ้างแต่ละบุคคลภายในองค์การได้อย่างมีประสิทธิภาพ มีผู้เชี่ยวชาญให้ความหมายว่าเป็นระบบที่ใช้สนับสนุนการทำงานภายใต้กิจกรรมต่างๆ ของการบริหารทรัพยากรมนุษย์ อาทิเช่น การนำเสนอข้อมูลของลูกจ้างที่มีความสามารถ การจัดเก็บข้อมูลของลูกจ้างที่มีอยู่ในปัจจุบันและจัดทำแผนเพื่อพัฒนาความสามารถและทักษะของลูกจ้างรายบุคคล เป็นต้น และระบบสารสนเทศเพื่อการบริหารทรัพยากรมนุษย์ยังหมายถึง ระบบที่ถูกออกแบบเพื่อใช้สนับสนุนงานด้านต่างๆ ดังต่อไปนี้ 1) การวางแผนความต้องการด้านทรัพยากรมนุษย์ของธุรกิจ 2) การพัฒนาลูกจ้างให้สามารถทำงานได้อย่างเต็มศักยภาพ 3) การควบคุมนโยบายตลอดจนการวางแผนด้านการบริหารทรัพยากรมนุษย์ของธุรกิจ

มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา ได้ดำเนินการจัดทำโครงการจัดหาและพัฒนาระบบเพื่อการบริหารมหาวิทยาลัย (MIS: Management Information System) และระบบสารสนเทศเพื่อการบริหารทรัพยากรองค์กร (ERP: Enterprise Resource Resource Planning) ตั้งแต่ปี 2552 โดยสำนักคอมพิวเตอร์และคณะกรรมการอำนวยการไอซีที มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยาเป็นผู้รับผิดชอบโครงการ โดยที่มีระบบฐานข้อมูลที่สามารถเก็บข้อมูลไว้ร่วมกันเพื่อป้องกันความซ้ำซ้อนของข้อมูลและเพิ่มประสิทธิภาพการจัดสรรข้อมูลให้ได้ประโยชน์สูงสุด ได้แก่ ระบบบริการการศึกษา ระบบฐานข้อมูลหลัก ระบบตารางสอน ระบบลงทะเบียน ระบบประมวลผล ระบบการเงินนิสิตนักศึกษา ระบบงานบริการ ระบบสำเร็จการศึกษา ระบบรับสมัคร ระบบงานพัฒนานิสิตนักศึกษา ระบบงานศิษย์เก่า ระบบวิเทศสัมพันธ์และภาษา ระบบงานสถิติ ระบบสำหรับผู้ดูแลระบบ MIS ระบบงบประมาณ ระบบบัญชี ระบบจัดซื้อจัดจ้าง ระบบการเงิน ระบบคลังพัสดุ ระบบบริหารงานบุคลากร ระบบแสดงข้อมูลบุคลากรผ่านอินเทอร์เน็ต ระบบต้นทุนต่อหน่วย ระบบข้อมูลสารสนเทศสำหรับงานประกันคุณภาพ ระบบสารบรรณ

อิเล็กทรอนิกส์และระบบสำหรับผู้ดูแลระบบ ERP เป็นต้น โดยได้มีเป้าหมายที่จะพัฒนาระบบสารสนเทศเพื่อบริหารทรัพยากรองค์กรให้สามารถเชื่อมโยงกันเป็นระบบฐานข้อมูลที่เป็นส่วนกลางใช้ในการบริหารงานของมหาวิทยาลัยได้ในการพัฒนาระบบฯ ซึ่งเริ่มดำเนินการจัดซื้อจัดจ้างในปีงบประมาณ 2554 โดยทางมหาวิทยาลัย ได้ทำการจัดจ้าง บริษัท วิชั่นเน็ต จำกัด เป็นผู้พัฒนาระบบ มีการพัฒนาระบบและได้ส่งมอบงานให้กับทางมหาวิทยาลัยเรียบร้อยแล้ว

จากความเป็นมาและความสำคัญ ดังกล่าว จึงเป็นเหตุให้ผู้จัดทำมีความสนใจที่จะจัดทำคู่มือการกำหนดสิทธิ์การใช้งานของผู้ใช้งานระบบสารสนเทศเพื่อการบริหารมหาวิทยาลัย (MIS: Management Information System) และระบบสารสนเทศเพื่อการบริหารทรัพยากรองค์กร (ERP: Enterprise Resource Resource Planning) ของบุคลากรในมหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา

วัตถุประสงค์

1. เพื่อให้ผู้ปฏิบัติงาน สามารถปฏิบัติงานแทนกันได้
2. เพื่อให้การปฏิบัติงานเป็นมาตรฐานเดียวกัน

ประโยชน์ที่คาดว่าจะได้รับ

1. ผู้ปฏิบัติงาน สามารถปฏิบัติงานแทนกันได้
2. การปฏิบัติงานเป็นมาตรฐานเดียวกัน

ขอบเขตคู่มือ

คู่มือการปฏิบัติงานเล่มนี้ ใช้ในการกำหนดหลักการปฏิบัติและขั้นตอนการทำงานของการปฏิบัติงานของบุคลากรสำนักคอมพิวเตอร์ให้กับผู้ใช้งานที่เป็นบุคลากรทั้งหมดของมหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา เป็นประจำทุกวัน

คำจำกัดความเบื้องต้น

ระบบสารสนเทศ หมายถึง ระบบสารสนเทศเพื่อการบริหารมหาวิทยาลัย (MIS: Management Information System) และระบบสารสนเทศเพื่อการบริหารทรัพยากรองค์กร (ERP: Enterprise Resource Resource Planning) ของมหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา

ระบบสารสนเทศเพื่อการบริหารมหาวิทยาลัย (MIS) หมายถึง ระบบบริการการศึกษา ระบบฐานข้อมูลหลัก ระบบตารางสอน ระบบลงทะเบียน ระบบประมวลผล ระบบการเงินนิสิตนักศึกษา ระบบงานบริการ ระบบสำเร็จการศึกษา ระบบรับสมัคร ระบบงานพัฒนานิสิตนักศึกษา ระบบงานศิษย์เก่า ระบบวิเทศสัมพันธ์และภาษา ระบบงานสถิติ ระบบสำหรับผู้ดูแลระบบ MIS

ระบบสารสนเทศเพื่อบริหารทรัพยากรองค์กร (ERP) หมายถึง ระบบงบประมาณ ระบบบัญชี ระบบจัดซื้อจัดจ้าง ระบบการเงิน ระบบคลังพัสดุ ระบบบริหารงานบุคลากร ระบบแสดงข้อมูลบุคลากรผ่านอินเทอร์เน็ต ระบบต้นทุนต่อหน่วย ระบบข้อมูลสารสนเทศสำหรับงานประกันคุณภาพ ระบบสารบรรณอิเล็กทรอนิกส์และระบบสำหรับผู้ดูแลระบบ ERP ของมหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา

ผู้ใช้งาน หมายถึง พนักงานมหาวิทยาลัย พนักงานราชการ ข้าราชการ ลูกจ้างประจำในมหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา

การกำหนดสิทธิ์ หมายถึง การควบคุมการเข้าถึงระบบฯ โดยอนุญาตให้เข้าถึงตามความจำเป็นในการใช้งานระบบสารสนเทศเพื่อการบริหารมหาวิทยาลัย (MIS: Management Information System) และระบบสารสนเทศเพื่อการบริหารทรัพยากรองค์กร (ERP: Enterprise Resource Planning)

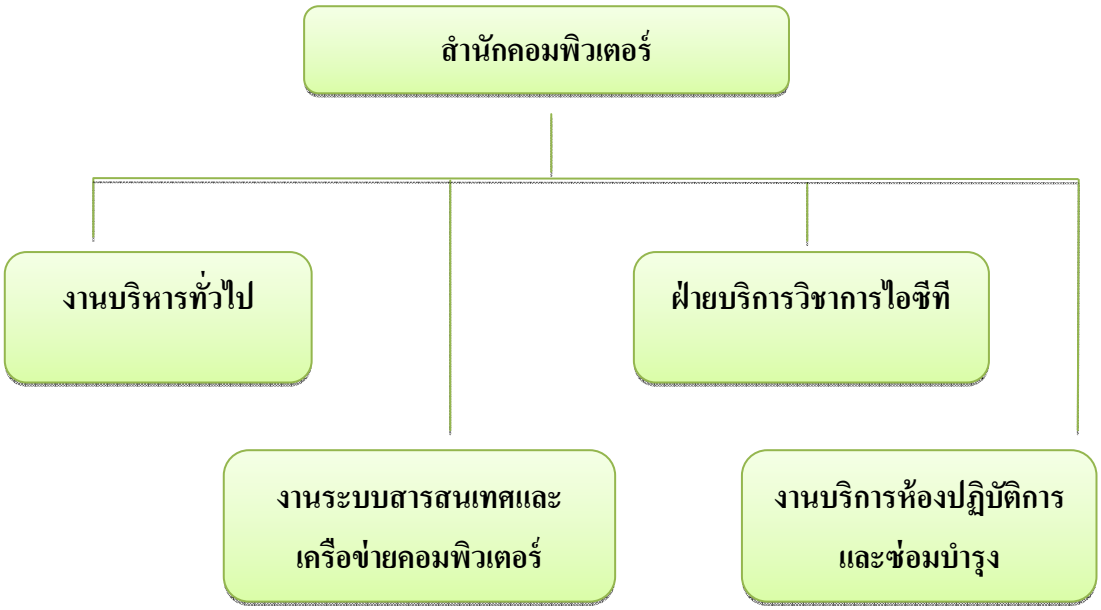
บทที่ 2
โครงสร้างและหน้าที่ความรับผิดชอบ

โครงสร้างหน่วยงานและความรับผิดชอบ

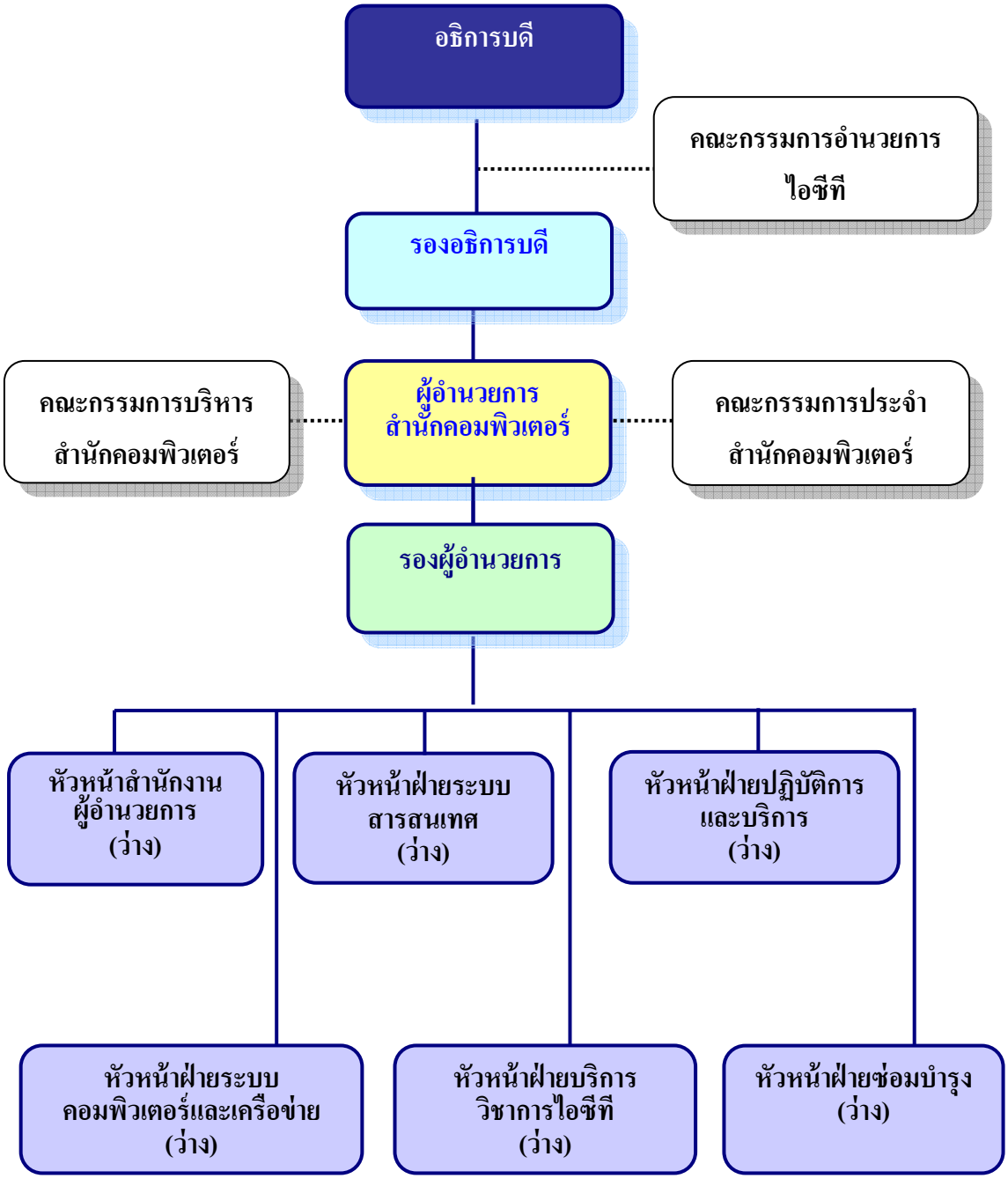
สำนักคอมพิวเตอร์ เป็นหน่วยงานกลางของมหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา โดยมีพันธกิจการพัฒนาและการบริการเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อสนับสนุนภารกิจและการบริหารงานของมหาวิทยาลัย จัดตั้งขึ้นเมื่อปี พ.ศ. 2540 สถาบันราชภัฏบ้านสมเด็จเจ้าพระยาให้มีการจัดตั้ง “ศูนย์คอมพิวเตอร์” ต่อมาในวันที่ 26 กันยายน พ.ศ. 2551 สภามหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา ได้มีมติอนุมัติให้จัดตั้ง “สำนักคอมพิวเตอร์” เป็นหน่วยงานที่มีฐานะเทียบเท่าคณะ โดยมีการแบ่งโครงสร้างการบริหารจัดการองค์กร ดังนี้

1. โครงสร้างการบริหารจัดการองค์กร

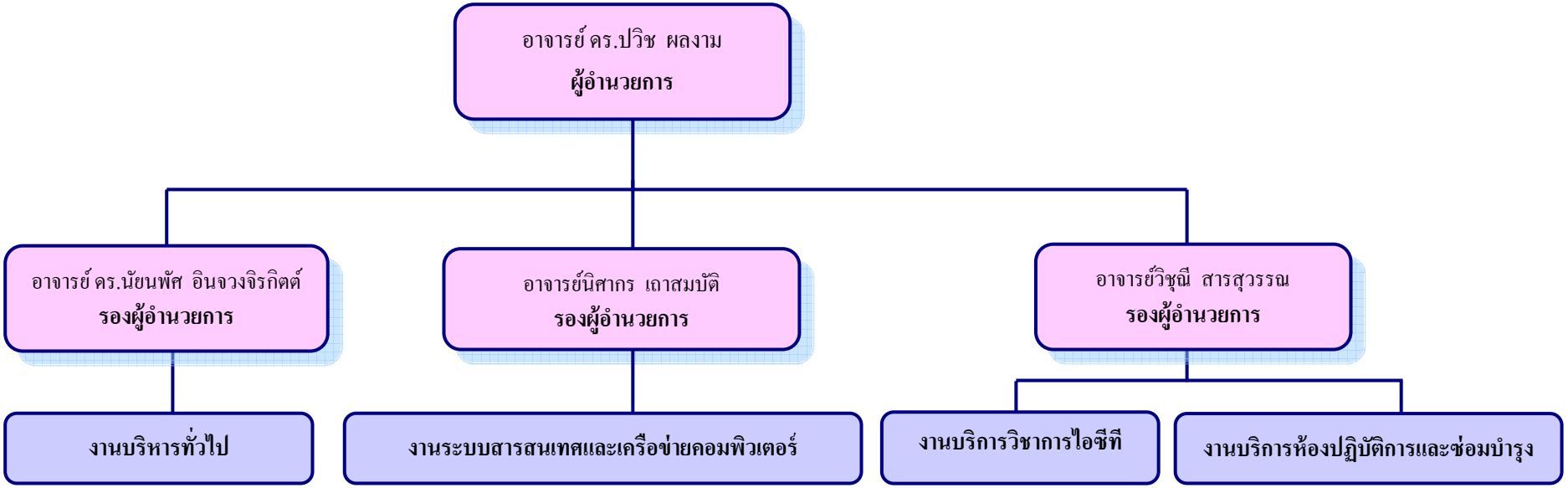
1.1 โครงสร้างของหน่วยงาน (Organization Chart)



1.2 โครงสร้างบริหารหน่วยงาน (Administration Chart)



1.3 โครงสร้างการปฏิบัติงาน (Activity Chart)



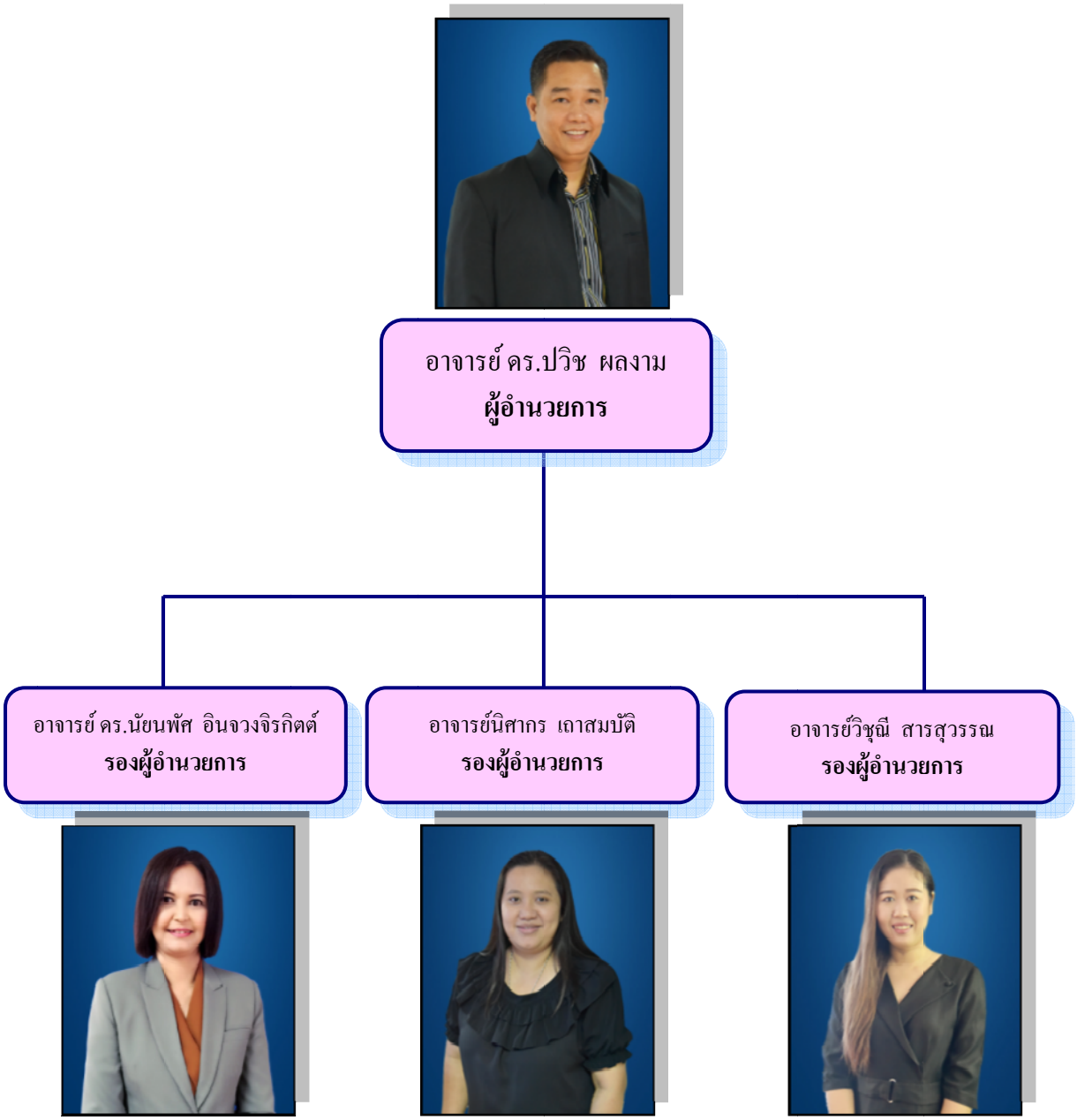
1. นายธรรมศักดิ์ จลาสุภ
   เจ้าหน้าที่บริหารงานทั่วไป ปฏิบัติการ
2. นางสุพิศ รุกขชาติ
   เจ้าหน้าที่บริหารงานทั่วไป ปฏิบัติการ
3. นายจักรพงศ์ จิตรแก้ว
   เจ้าหน้าที่บริหารงานทั่วไป ปฏิบัติการ

1. นายนพฤทธิ จันกลิ่น
   นักวิชาการคอมพิวเตอร์ ปฏิบัติการ
2. น.ส.บังอร เหล่าปิ่นเพชร
   นักวิชาการคอมพิวเตอร์ ปฏิบัติการ
3. นายวีรวุฒิ ฉัตรธนโชติกุล
   นักวิชาการคอมพิวเตอร์ ปฏิบัติการ
4. นายภักดี โตแดง
   นักวิชาการคอมพิวเตอร์ ปฏิบัติการ
5. นายรณกร เรี่ยวแรง
   นักวิชาการคอมพิวเตอร์ ปฏิบัติการ
6. นายวิชชา สุขรัตน์
   นักวิชาการคอมพิวเตอร์ ปฏิบัติการ
7. น.ส.บุรพร ศรีสุวรรณ
   นักวิชาการคอมพิวเตอร์ ปฏิบัติการ

1. นายเดชอาคม คดเกี้ยว
   เจ้าหน้าที่บริหารงานทั่วไป ปฏิบัติการ

1. นายสาธิต ถนอมศักดิ์
   ช่างเครื่อง ปฏิบัติการ
2. นายณัฏฐพล จิรพัฒนากุล
   เจ้าหน้าที่บริหารงานทั่วไป ปฏิบัติการ
3. นายประทีป ขันธวุธ
   เจ้าหน้าที่บริหารงานทั่วไป ปฏิบัติการ
4. นายพงศ์ศักดิ์ บำรุงจิตต์
   ช่างเครื่อง ปฏิบัติการ
5. นายวุฒิพงศ์ โพธิ์เย็น
   ช่างเครื่อง ปฏิบัติการ

1.3.1 โครงสร้างการปฏิบัติงาน (ระดับผู้บริหาร)



1.3.2 โครงสร้างการปฏิบัติงาน (ระดับผู้ปฏิบัติงาน)

งานบริหารทั่วไป

นายธรรมศักดิ์ จลาสุภ
เจ้าหน้าที่บริหารทั่วไป

นางสุพิศ รุกขชาติ
เจ้าหน้าที่บริหารทั่วไป

นายจักรพงศ์ จิตรแก้ว
เจ้าหน้าที่บริหารทั่วไป

งานระบบสารสนเทศและเครือข่ายคอมพิวเตอร์

นายนพฤทธิ จันกลิ่น
นักวิชาการคอมพิวเตอร์

นายภักดี โตแดง
นักวิชาการคอมพิวเตอร์

นางสาวบังอร เหล่าปิ่นเพชร
นักวิชาการคอมพิวเตอร์

นายวีรวุฒิ ฉัตรธนโชติสกุล
นักวิชาการคอมพิวเตอร์

นายรณกร เรี่ยวแรง
นักวิชาการคอมพิวเตอร์

นายวิชชา สุขรัตน์
นักวิชาการคอมพิวเตอร์

นางสาวบุรพร ศรีสุวรรณ
นักวิชาการคอมพิวเตอร์

งานบริการห้องปฏิบัติการและซ่อมบำรุง

นายสาธิต ถนอมศักดิ์
ช่างเครื่องคอมพิวเตอร์

นายณัฏฐพล จิรพัฒนากุล
เจ้าหน้าที่บริหารทั่วไป

นายประทีป ขันธวุธ
เจ้าหน้าที่บริหารทั่วไป

นายพงศ์ศักดิ์ บำรุงจิตต์
เจ้าพนักงานเครื่องคอมพิวเตอร์

นายวุฒิพงศ์ โพธิ์เย็น
ช่างเครื่องคอมพิวเตอร์

งานบริการวิชาการไอซีที

นายเดชอาคม คดเกี้ยว
เจ้าหน้าที่บริหารทั่วไป

2. ภาระหน้าที่ของสำนักคอมพิวเตอร์

สำนักคอมพิวเตอร์ มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา แบ่งส่วนงานภายในสำนัก ออกเป็น 4 ฝ่ายงาน โดยมีการแบ่งงานและกำหนดภาระงานอย่างชัดเจน ดังนี้

2.1 งานบริหารงานทั่วไป

รับผิดชอบงานที่เกี่ยวข้องกับแผนนโยบาย การบริหารและการของสำนักคอมพิวเตอร์ ซึ่งแบ่งออกเป็น 8 งาน ดังนี้

2.1.1 งานธุรการ

2.1.1.1 ดำเนินงานจัดทำเอกสารเบิกจ่ายสำหรับงานฝึกอบรมและราชการ

2.1.1.2 งานเดินเอกสาร

2.1.1.3 ดำเนินการจัดทำเอกสารขออนุญาตไปราชการ

2.1.1.4 ร่างหนังสือราชการ และนำเสนอผู้บริหารลงนาม

2.1.1.5 ดำเนินการจัดทำคำสั่ง ประกาศ ข้อบังคับและแนวทางปฏิบัติ

2.1.1.6 จัดทำโครงการต่างๆ

2.1.1.7 ลงทะเบียนหนังสือรับ-ส่ง

2.1.2 งานจัดซื้อ/จัดจ้าง

2.1.2.1 จัดทำเอกสารขออนุมัติจัดซื้อ / จัดจ้า

2.1.2.2 งานตรวจรับพัสดุ

2.1.2.3 งานดำเนินขออนุมัติเบิกจ่าย

2.1.3 งานคลังพัสดุ

2.1.3.1 สำรวจพัสดุประจำปี

2.1.3.2 คุมทะเบียนเบิกจ่ายพัสดุ

2.1.3.3 จัดทำรายงานพัสดุคงเหลือ

2.1.3.4 สำรวจความต้องการใช้งานพัสดุ

2.1.3.5 จัดทำรายงานความต้องการใช้งานพัสดุ

2.1.4 งานนโยบายและแผน

2.1.4.1 ดำเนินการประชุม

2.1.4.2 ยกร่างดำเนินการพัฒนางานแผนกกลยุทธ์

2.1.4.3 ดำเนินงานทำประชาพิจารณ์แผนกลยุทธ์

2.1.4.4 จัดทำแผนกลยุทธ์ทางการเงิน

2.1.4.5 จัดทำแผนงาน โครงการ และคำขอตั้ง

2.1.4.6 จัดทำแผนปฏิบัติการประจำปี

2.1.4.7 ตรวจสอบและตัดยอดงบประมาณ

2.1.4.8 จัดทำรายงานผลการใช้จ่ายงบประมาณ

2.1.4.9 ติดตามผลการดำเนินงานตามแผนปฏิบัติการประจำปี

2.1.5 งานประกันคุณภาพ

2.1.5.1 ดำเนินงานแต่งตั้งคณะกรรมการสำหรับงานประกันคุณภาพ

2.1.5.2 รวบรวมเอกสาร หลักฐานที่เกี่ยวข้องกับงานประกันคุณภาพ

2.1.5.3 จัดทำรายงานการประเมินตนเอง (SAR)

2.1.5.4 บันทึกข้อมูลการประกันคุณภาพลงในระบบ CHE QA Online

2.1.6 งานเลขานุการ

2.1.6.1 งานประชุม

2.1.6.2 งานประสานงาน

2.1.7 งาน Call Center

2.1.7.1 ให้คำปรึกษาแนะนำเบื้องต้นเกี่ยวกับการใช้งานระบบสารสนเทศและการสื่อสารของมหาวิทยาลัย

2.1.7.2 รับเรื่องร้องเรียนและแจ้งปัญหาการใช้งาน

2.1.7.3 โอนสายสนทนาจากภายนอก ไปยังผู้รับในหน่วยงาน

2.1.8 ศูนย์ประสานงาน

2.1.8.1 ให้คำปรึกษาแนะนำเบื้องต้นเกี่ยวกับการใช้งานระบบสารสนเทศและการสื่อสารของมหาวิทยาลัย

2.1.8.2 รับเรื่องร้องเรียนและแจ้งปัญหาการใช้งานระบบสารสนเทศและการสื่อสารของมหาวิทยาลัย

2.1.8.3 ตรวจสอบและแก้ปัญหาการใช้งานเบื้องต้น

2.1.8.4 ประสานงานกับฝ่ายที่เกี่ยวข้อง

2.2 งานระบบสารสนเทศและเครือข่ายคอมพิวเตอร์

รับผิดชอบงานระบบสารสนเทศ ประสานงาน วิเคราะห์ ออกแบบ พัฒนาและบำรุงรักษาฐานข้อมูลระบบสารสนเทศเพื่อการบริหารมหาวิทยาลัย (MIS: Management Information System) และระบบสารสนเทศเพื่อการบริหารทรัพยากรองค์กร (ERP: Enterprise Resource Planing) รวมทั้งการให้คำปรึกษาแก่ผู้ใช้ระบบงาน ควบคุมดูแล ประสานงาน บำรุงรักษาบริการระบบคอมพิวเตอร์และเครือข่ายซึ่งแบ่งเป็น 2 งานหลัก ดังนี้

2.2.1 งานระบบสารสนเทศ

2.2.1.1 วางแผนด้านระบบสารสนเทศ

2.2.1.2 ปฏิบัติการด้านระบบสารสนเทศ

2.2.1.3 ประสานงานด้านซอฟต์แวร์และระบบสารสนเทศ

2.2.1.4 บริการด้านระบบสารสนเทศ

2.2.1.5 พัฒนาระบบสารสนเทศเกี่ยวกับระบบจัดการสวัสดิการพนักงานมหาวิทยาลัยงบแผ่นดิน

2.2.1.6 บำรุงรักษาระบบสารสนเทศเกี่ยวกับระบบจัดการสวัสดิการพนักงานมหาวิทยาลัยงบแผ่นดิน

2.2.1.7 พัฒนาระบบสารสนเทศเกี่ยวกับระบบแจ้งปัญหาที่เกี่ยวข้องกับสำนักคอมพิวเตอร์เป็นผู้รับผิดชอบดูแลภายในมหาวิทยาลัย

2.2.1.8 พัฒนาระบบสารสนเทศเกี่ยวกับระบบรายงานการปฏิบัติงานภายในสำนักคอมพิวเตอร์

2.2.1.9 ดำเนินการทดสอบระบบกรอบมาตรฐานคุณวุฒิระดับอุดมศึกษาแห่งชาติ (TQF)

2.2.1.10 พัฒนาระบบสารสนเทศเพื่อให้บริการกับนักศึกษาและบุคลากรในมหาวิทยาลัย

2.2.1.11 พัฒนาระบบสารสนเทศเกี่ยวกับระบบประเมินและติดตามของบุคลากรในมหาวิทยาลัยเกี่ยวข้องกับงานประกันคุณภาพ

2.2.1.12 พัฒนาระบบรักษาความปลอดภัยของระบบสารสนเทศภายในมหาวิทยาลัย

2.2.2 งานระบบเครือข่ายคอมพิวเตอร์

2.2.2.1 วางแผนปฏิบัติการด้านระบบเครือข่าย คอมพิวเตอร์

2.2.2.2 ปฏิบัติการด้านระบบเครือข่ายคอมพิวเตอร์

2.2.2.3 ประสานงานและบริการด้านระบบเครือข่ายคอมพิวเตอร์

2.2.2.4 ดำเนินการวางแผนและดูแลระบบเซิร์ฟเวอร์

2.2.2.5 ดำเนินการควบคุมและดูแลความปลอดภัยของระบบสารสนเทศของมหาวิทยาลัย

2.2.2.6 ดูแลและให้บริการกับหน่วยงานหรือคณะที่ต้องการนำเครื่องเซิร์ฟเวอร์มาฝากไว้กับสำนักคอมพิวเตอร์

2.2.2.7 ดำเนินการจัดหาระบบเพื่ออำนวยความสะดวกในการใช้งานระบบให้แก่บุคคลากรภายในมหาวิทยาลัย

2.3 งานบริการวิชาการไอซีที

รับผิดชอบงานการบริการวิชาการที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งแบ่งเป็น 8 งาน ดังนี้

2.3.1 งานพัฒนาหลักสูตรฝึกอบรม

2.3.2 ประชาสัมพันธ์หลักสูตรฝึกอบรม

2.3.3 รับสมัครผู้เข้ารับการอบรมตามหลักสูตร

2.3.4 ดำเนินการจัดอบรมตามหลักสูตร

2.3.5 ผลิตสื่อสิ่งพิมพ์

2.3.6 ดำเนินการด้านการเงินและบัญชีของหลักสูตรการจัดฝึกอบรม

2.3.7 ประสานงานด้านการจัดฝึกอบรม

2.3.8 งานพัฒนาสื่อ e-learning

2.4 งานบริการห้องปฏิบัติการและซ่อมบำรุง

รับผิดชอบงานปฏิบัติและงานบริการ และซ่อมบำรุงและจัดการบริการเครื่องคอมพิวเตอร์และอุปกรณ์ สนับสนุนการเรียนการสอน การวิจัย การบริการวิชาการ รวมทั้งให้คำปรึกษาด้านคอมพิวเตอร์กับผู้ใช้บริการภายในมหาวิทยาลัย ซึ่งแบ่งเป็น 2 งาน ดังนี้

2.4.1 งานให้บริการห้องปฏิบัติการคอมพิวเตอร์

2.4.1.1 ให้บริการอินเทอร์เน็ตเพื่อการสืบค้นข้อมูล

2.4.1.2 ให้บริการห้องปฏิบัติการเพื่อการเรียนการสอน

2.4.1.3 ให้บริการห้องปฏิบัติการเพื่อการอบรมสัมมนา

2.4.2 งานให้บริการซ่อมบำรุงภายในสำนักคอมพิวเตอร์

2.4.2.1 ซ่องบำรุงเครื่องคอมพิวเตอร์ภายในห้องปฏิบัติการคอมพิวเตอร์

2.4.2.2 บำรุงรักษาเครื่องคอมพิวเตอร์ภายในสำนักงานสำนักคอมพิวเตอร์

2.4.2.3 ให้บริการซ่อมบำรุงแก่หน่วยงานต่างๆ ได้แก่ คณะ ศูนย์ สำนักและสาขาวิชา เป็นต้น

บทบาทหน้าที่ความรับผิดชอบของตำแหน่ง

1. หน้าที่ความรับผิดชอบของตำแหน่งตามมาตรฐานกำหนดตำแหน่ง

ตามมาตรฐานกำหนดตำแหน่งนักวิชาการคอมพิวเตอร์ ระบุบทบาทหน้าที่ความรับผิดชอบของสายงานวิทยาการคอมพิวเตอร์ ดังนี้

1.1 หน้าที่ความรับผิดชอบหลัก

ปฏิบัติงานในฐานะผู้ปฏิบัติงานที่มีประสบการณ์ โดยใช้ความรู้ ความสามารถ ความชำนาญ ทักษะและประสบการณ์สูงในงานด้านวิทยาการคอมพิวเตอร์ ปฏิบัติงานที่ต้องทำการศึกษา ค้นคว้า ทดลอง วิเคราะห์หรือวิจัย เพื่อการปฏิบัติงานหรือพัฒนางานหรือแก้ไขปัญหาในงานที่มีความยุ่งยากและมีขอบเขตกว้างขวางและปฏิบัติงานอื่นตามที่ได้รับมอบหมายหรือปฏิบัติงานในฐานะหัวหน้างาน มีหน้าที่และความรับผิดชอบในการควบคุมการปฏิบัติงานด้านวิทยาการคอมพิวเตอร์ที่มีขอบเขตเนื้อหาของงานหลากหลายและมีขั้นตอนการทำงานที่ยุ่งยากซับซ้อนค่อนข้างมาก โดยต้องกำหนดแนวทางการทำงานที่เหมาะสมกับสถานการณ์ ตลอดจนกำกับตรวจสอบผู้ปฏิบัติงานเพื่อให้งานที่รับผิดชอบสำเร็จตามวัตถุประสงค์และปฏิบัติหน้าที่อื่นตามที่ได้รับมอบหมาย

โดยมีลักษณะงานที่ปฏิบัติในด้านต่างๆ ดังนี้

1.1.1 ด้านการปฏิบัติการ

1.1.1.1 ศึกษา วิเคราะห์ กำหนดคุณลักษณะเฉพาะของเครื่องคอมพิวเตอร์และอุปกรณ์ระบบเครือข่าย ระบบงานประยุกต์และระบบสารสนเทศ การจัดการระบบการทำงานของเครื่องการติดตั้งระบบเครื่อง ทดสอบคุณสมบัติด้านเทคนิคของเครื่องและอุปกรณ์ เพื่อให้ได้อุปกรณ์ เพื่อให้ได้อุปกรณ์คอมพิวเตอร์ที่เป็นมาตรฐานเดียวกันทั้งหน่วยงาน ทันสมัยและตรงตามความต้องการและลักษณะการใช้งานของหน่วยงาน

1.1.1.2 ออกแบบระบบงาน ข้อมูล การประมวลผล การสื่อสาร ระบบเครือข่ายงาน ชุดคำสั่งและฐานข้อมูล ตามความต้องการของหน่วยงาน ติดตั้ง บำรุงรักษา เครื่องคอมพิวเตอร์ระบบอุปกรณ์ต่างๆ ชุดคำสั่งระบบปฏิบัติการ ชุดคำสั่งประยุกต์ เพื่อสนับสนุนการปฏิบัติงานด้านเทคโนโลยีสารสนเทศให้ดำเนินไปได้อย่างราบรื่น สนองต่อความต้องการของผู้รับบริการ

1.1.1.3 ศึกษา ค้นคว้า ทดลอง วิเคราะห์หรือวิจัย ด้านวิทยาการคอมพิวเตอร์ จัดทำเอกสารวิชาการ คู่มือเกี่ยวกับงานในความรับผิดชอบ เผยแพร่ผลงานทางด้านวิทยาการคอมพิวเตอร์ติดตามและพัฒนาเทคโนโลยี เพื่อกำหนดลักษณะและมาตรฐานในการ

ปฏิบัติงานวิทยาการคอมพิวเตอร์ เพื่อหาวิธีการในการแก้ไขปัญหาเกี่ยวกับงานวิทยาการคอมพิวเตอร์ หรือเพื่อพัฒนาแนวทางวิธีการและมาตรฐานการปฏิบัติงานให้มีประสิทธิภาพยิ่งขึ้น

1.1.1.4 ให้บริการวิชาการด้านต่างๆ เช่น ช่วยสอน ฝึกอบรม เผยแพร่ความรู้ความเข้าใจเกี่ยวกับหลักการและวิธีการของงานวิทยาการคอมพิวเตอร์ ให้คำปรึกษาแนะนำตอบปัญหาและชี้แจงเรื่องต่างๆ เกี่ยวกับงานในหน้าที่ เพื่อให้สามารถปฏิบัติงานได้อย่างถูกต้องมีประสิทธิภาพ เข้าร่วมประชุมคณะกรรมการต่างๆ ที่ได้รับแต่งตั้ง เพื่อให้ข้อมูลทางวิชาการประกอบการพิจารณาและตัดสินใจและปฏิบัติหน้าที่อื่นที่เกี่ยวข้อง

1.1.1.5 ในฐานะหัวหน้างาน นอกจากอาจปฏิบัติงานตามข้อ 1.1.1.1-1.1.14 ดังกล่าวข้างต้นแล้วต้องทำหน้าที่กำหนดแผนงาน มอบหมาย ควบคุม ตรวจสอบ ให้คำปรึกษาแนะนำปรับปรุงแก้ไข ติดตาม ประเมินผลและแก้ไขปัญหาข้อขัดข้องในการปฏิบัติงานในหน่วยงานที่รับผิดชอบ เพื่อให้การปฏิบัติงานบรรลุตามเป้าหมายและผลสัมฤทธิ์ที่กำหนด

1.1.2 ด้านการวางแผน

ร่วมกำหนดนโยบายและแผนงานของหน่วยงานที่สังกัด วางแผนหรือร่วมวางแผนการทำงานตามแผนงานหรือโครงการของหน่วยงาน แก้ไขปัญหาในการปฏิบัติงาน เพื่อให้การดำเนินงานบรรลุตามเป้าหมายและผลสัมฤทธิ์ที่กำหนด

1.1.3 ด้านการประสานงาน

1.1.3.1 ประสานการทำงานร่วมกันโดยมีบทบาทในการให้ความเห็นและคำแนะนำเบื้องต้นแก่สมาชิกในทีมงานหรือหน่วยงานอื่น เพื่อให้เกิดความร่วมมือและผลสัมฤทธิ์ตามที่กำหนดไว้

1.1.3.2 ให้ข้อคิดเห็นหรือคำแนะนำเบื้องต้นแก่สมาชิกในทีมงานหรือบุคคลหรือหน่วยงานที่เกี่ยวข้อง เพื่อสร้างความเข้าใจและความร่วมมือในการดำเนินงานตามที่ได้รับมอบหมาย

1.1.4 ด้านการบริการ

1.1.4.1 ให้คำปรึกษา แนะนำ นิเทศ ฝึกอบรม ถ่ายทอดความรู้ทางด้านวิทยาการคอมพิวเตอร์แก่ผู้ใต้บังคับบัญชา นักศึกษา ผู้รับบริการทั้งภายในและภายนอกหน่วยงาน รวมทั้งตอบปัญหาและชี้แจงเรื่องต่างๆ เกี่ยวกับงานในหน้าที่ เพื่อให้ความรู้ความเข้าใจและสามารถดำเนินงานได้อย่างถูกต้อง

1.1.4.2 พัฒนาข้อมูล จัดทำเอกสารวิชาการ สื่อเอกสารเผยแพร่ให้บริการวิชาการด้านวิทยาการคอมพิวเตอร์ที่ซับซ้อน เพื่อก่อให้เกิดการแลกเปลี่ยนเรียนรู้ที่สอดคล้องและสนับสนุนภารกิจของหน่วยงาน

1.2 ชื่อตำแหน่งในสายงานและระดับตำแหน่ง

ตำแหน่งในสายงานนี้มีชื่อและระดับของตำแหน่งดังนี้ คือ

นักวิชาการคอมพิวเตอร์ ระดับเชี่ยวชาญ

นักวิชาการคอมพิวเตอร์ ระดับชำนาญการพิเศษ

นักวิชาการคอมพิวเตอร์ ระดับชำนาญการ

นักวิชาการคอมพิวเตอร์ ระดับปฏิบัติการ

2. หน้าที่ความรับผิดชอบของตำแหน่งตามที่ได้รับมอบหมาย

บทบาทหน้าที่ความรับผิดชอบของ นางสาวบังอร เหล่าปิ่นเพชร ตำแหน่งนักวิชาการคอมพิวเตอร์ ระดับปฏิบัติการ ตามที่ได้รับมอบหมาย มีดังนี้

2.1 วางแผนการปฏิบัติงานด้านระบบสารสนเทศ

2.2 ปฏิบัติการด้านระบบสารสนเทศ

2.2.1 ดำเนินการจัดทำแผนการปฏิบัติงานด้านระบบสารสนเทศ

2.2.2 ดำเนินการจัดหาซอฟแวร์ลิขสิทธิ์

2.2.3 ดำเนินการด้านการจัดหาระบบสารสนเทศ

2.2.4 พัฒนาระบบสารสนเทศ

2.3 บำรุงรักษาระบบสารสนเทศ

2.4 ประสานงานด้านซอฟต์แวร์และระบบสารสนเทศ

2.5 งานบริการด้านระบบสารสนเทศ

2.6 งานประกันคุณภาพทางการศึกษา

2.7 งานอื่นๆ ที่ผู้บังคับบัญชามอบหมาย

(คำสั่งมหาวิยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา ที่ 409/2558 เรื่อง การมอบหมายหน้าที่ความรับผิดชอบของบุคลากรประจำสำนักคอมพิวเตอร์, 2558, น.3)

จากภาระหน้าที่ที่ได้รับมอบหมายดังกล่าวข้างต้น ผู้เขียนได้เลือกเอาการกำหนดสิทธิ์การใช้งานของผู้ใช้งานระบบสารสนเทศเพื่อการบริหารมหาวิทยาลัย (MIS: Management Information System) และระบบสารสนเทศเพื่อการบริหารทรัพยากรองค์กร (ERP: Enterprise Resource Planning) มาเขียนคู่มือการปฏิบัติงาน โดยมี Flow Chart ดังนี้

ขั้นตอนการปฏิบัติงาน : การกำหนดสิทธิ์การใช้งานของผู้ใช้งานระบบสารสนเทศเพื่อการบริหารมหาวิทยาลัย (MIS: Management Information System) และระบบสารสนเทศเพื่อการบริหารทรัพยากรองค์กร (ERP: Enterprise Resource Planning)

ขั้นตอนการดำเนินการกำหนดสิทธิ์การใช้งานของผู้ใช้งานระบบ (MIS-ERP)

ผู้รับผิดชอบ	แผนภูมิสายงาน Flowchart	ขั้นตอน/วิธีดำเนินการ	เอกสารที่เกี่ยวข้อง	ระยะเวลาดำเนินการ
	จุดเริ่มต้น			
หน่วยงานภายในมหาวิทยาลัย	เจ้าของเรื่อง ↓ เจ้าหน้าที่สาขาวิชา/คณะ ประสานงานตรวจสอบเอกสาร	- บันทึกข้อความหรือกรอกแบบฟอร์มขอใช้สิทธิ์ระบบ (MIS-ERP) - ผ่านประธานสาขาวิชา/หัวหน้างาน เซ็นต์เพื่อให้ความเห็นชอบ - คณบดี/ผู้อำนวยการเซ็นต์ - เจ้าหน้าที่สาขาวิชา/คณะ ประสานงานตรวจสอบเอกสารก่อนส่งงานธุรการสำนักคอมพิวเตอร์	บันทึกข้อความหรือแบบฟอร์มขอใช้สิทธิ์ระบบ(MIS-ERP)	ภายใน 15 นาที
งานบริการ	**ไม่ผ่าน** งานธุรการ **ผ่าน**	- ลงทะเบียนรับเอกสาร - ตรวจเช็คเอกสาร **<u>กรณีผ่าน</u>** หมายถึง เอกสารตรวจสอบแล้วพบว่ารายละเอียดถูกต้องไม่พบข้อผิดพลาดหรือข้อแก้ไข	แบบฟอร์มขอใช้สิทธิ์ระบบ (MIS-ERP) ที่มีการตรวจเช็คเอกสารเรียบร้อย	ภายใน 10 นาที

ผู้รับผิดชอบ	แผนภูมิสายงาน Flowchart	ขั้นตอน/วิธีดำเนินการ	เอกสารที่เกี่ยวข้อง	ระยะเวลาดำเนินการ
	A			
		<u>**กรณีไม่ผ่าน**</u> หมายถึง เอกสารตรวจสอบแล้วพบว่าไม่ถูกต้อง พบข้อผิดพลาดหรือพบข้อแก้ไข ก็จะนำเอกสารส่งคืนให้กับหน่วยงานเพื่อแก้ไขเป็นลำดับต่อไป - ส่งให้รองผู้อำนวยการ		
งานบริหาร	รอง ผู้อำนวยการ	- รับเอกสารจากงานธุรการ - ลงนามแบบฟอร์มขอใช้สิทธิ์ระบบ (MIS-ERP) เซ็นต์ มอบหมายงาน	แบบฟอร์มขอใช้สิทธิ์ระบบ (MIS-ERP) ที่ลงนามเรียบร้อย	ภายใน 5 นาที
งานเทคนิค	ผู้ปฏิบัติงาน	- ตรวจสอบความถูกต้อง/ลงนามปฏิบัติงาน - ดำเนินการสร้าง/เพิ่ม/ยกเลิกสิทธิ์การใช้งานระบบ(MIS-ERP) ตามแบบฟอร์มที่ขอมา	แบบฟอร์มขอใช้สิทธิ์ระบบ (MIS-ERP) ที่ดำเนินการสร้างเรียบร้อย	ภายใน 20-30 นาที
งานบริการ	งานธุรการ	งานธุรการลงทะเบียนส่ง บันทึกข้อความตอบกลับแจ้งไปยังสาขาวิชา/คณะ	บันทึกข้อความตอบกลับขอใช้สิทธิ์ระบบ (MIS-ERP) ที่ดำเนินการสร้างให้เรียบร้อยแล้ว	ภายใน 10 นาที
	จบการทำงาน			

บทที่ 3
หลักเกณฑ์และขั้นตอนการปฏิบัติงาน

หลักเกณฑ์วิธีการปฏิบัติงานการกำหนดสิทธิ์การใช้งานของผู้ใช้งานระบบสารสนเทศ

ในการจัดทำคู่มือการกำหนดสิทธิ์การใช้งานของผู้ใช้งานระบบสารสนเทศเพื่อการบริหารมหาวิทยาลัย (MIS: Management Information System) และระบบสารสนเทศเพื่อการบริหารทรัพยากรองค์กร (ERP: Enterprise Resource Resource Planning) ของบุคลากรในมหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา เพื่อการบริหารงานที่เกิดขึ้นนั้นเพื่อรองรับการให้บริการหน่วยงานต่างๆ ลดขั้นตอนการดำเนินงาน สะดวกต่อการตรวจสอบความถูกต้องของข้อมูล มีส่วนช่วยส่งเสริมการเพิ่มประสิทธิภาพในการทำงานและรองรับกระบวนการทำงานของมหาวิทยาลัยได้ดียิ่งขึ้น

1. แนวคิดเกี่ยวกับการกำหนดสิทธิ์การใช้งานของผู้ใช้งานระบบสารสนเทศ

การควบคุมการเข้าถึง (Access Control)

หัวใจสำคัญประการหนึ่งในกระบวนการรักษาความปลอดภัย ก็คือ การควบคุมการเข้าถึง (Access Control) ซึ่งก็คือ นโยบายหรือกลไกในการกำหนดข้อจำกัดในการเข้าไปใช้งานในระบบ การเข้าถึงข้อมูล และสื่อสารต่างๆ ซึ่งโดยปกติแล้ว ถ้า ผู้โจมตีระบบ (Attackers) ไม่สามารถที่จะเข้าถึงแหล่งข้อมูลได้ ก็จะไม่สามารถสร้างความเสียหายให้เกิดขึ้นกับแหล่งข้อมูลนั้นได้ โดยมีความมุ่งหมายหลักในการที่จะป้องกันและหยุดยั้งการโจมตีระบบในรูปแบบต่างๆ โดยเฉพาะอย่างยิ่ง การเจาะข้อมูลระบบ ซึ่งวิธีการป้องกันที่นิยมมากที่สุด คือ ให้มีการล็อกอินเข้าสู่ระบบนั่นเอง

การควบคุมการเข้าถึง (Access Control) แตกต่างจากการเข้ารหัสข้อมูล (Encryption) ตรงที่ กลไกการควบคุมการเข้าถึง เป็นการ ป้องกันการเข้าถึงระบบ ข้อมูลสารสนเทศขององค์กร แต่การเข้ารหัสข้อมูลเป็นการรักษาความลับของข้อมูลนั้นๆ

กระบวนการในการสร้างระบบควบคุมการเข้าถึง มีดังนี้

1. Enumeration of Resources

แจกแจงรายละเอียดที่สำคัญในระบบให้ชัดเจน เช่น ฐานข้อมูลบุคคล ข้อมูลสำคัญทางการค้าที่บรรจุอยู่ใน File Servers จำนวนเครื่อง Consoles ในห้องเซิร์ฟเวอร์ เป็นต้น

2. Sensitivity of Each Resource

เมื่อทราบแล้วว่ามี แหล่งข้อมูล (Resource) กลุ่มไหนบ้างที่ต้องสนใจ ในขั้นนี้ ก็ต้องวิเคราะห์ความสำคัญและความอ่อนไหว (Sensitivity) ของแหล่งข้อมูลนั้น เช่น แหล่งข้อมูลที่อาจจะส่งผลกระทบอย่างมากต่อการประกอบการขององค์กร เช่น หากแหล่งข้อมูลนั้นถูกทำลายไปอาจทำให้องค์กรทั้งองค์กรเสียหายถึงขั้นล้มละลายได้ ก็จะถือว่า แหล่งข้อมูลนั้นมีความสำคัญและมีความเปราะบางมาก คือ มี Sensitivity สูง เป็นต้น

3. การกำหนดว่าใครควรเข้าถึงแหล่งข้อมูลใด

จากนั้นก็จะมา กำหนดว่าใครควรเข้าถึงแหล่งข้อมูลใด โดยปกติมักจะใช้ บทบาทและหน้าที่ (Roles) เป็นตัวกำหนด เช่น บางไฟล์อาจกำหนดให้ User ทุกคนในระบบ สามารถเข้าถึงได้และในบางไฟล์ เช่น System files ต่างๆ อาจกำหนดให้เพียงผู้ที่มีหน้าที่เกี่ยวข้องในการจัดการระบบ จึงจะสามารถเข้าถึงได้ สามารถกำหนดเป็นรายบุคคลก็ได้ แต่นิยมกำหนดตามบทบาทมากกว่า เพราะประหยัดเวลาและง่ายแก่การควบคุมมากกว่าการกำหนดทีละคน เช่น กำหนดเป็นกลุ่ม User ทั่วไป กลุ่ม Admin สมาชิกในกลุ่ม Project เป็นต้น

4. การกำหนดสิทธิ์ในการเข้าถึง (Access Permissions)

หลังจากที่ได้มีการกำหนดขอบเขตของกลุ่มบุคคลต่อแหล่งข้อมูลที่เหมาะสมกับบทบาทและหน้าที่แล้ว ก็ต้องมา กำหนดหน้าที่เฉพาะหรือสิทธิพิเศษในการกระทำต่อข้อมูลนั้นๆ ก็คือ การกำหนดสิทธิในการเข้าถึงข้อมูล (Access Permissions) หรือเรียกกันทั่วไปว่า การอนุญาตให้ใช้งาน (Authorizations) คือการกำหนดในรายละเอียดลงไปอีกว่า เมื่อได้กำหนดกลุ่มตามบทบาท (Role) หรือแต่ละบุคคล (Individual) แล้ว จะให้แต่ละกลุ่มหรือแต่ละบุคคล มีสิทธิในการกระทำกับข้อมูลได้ขนาดไหน เรียกว่า ข้อกำหนดในการเข้าถึงข้อมูล (Access Control Policy) ยกตัวอย่างเช่น user ที่ login เข้ามา อาจได้รับสิทธิ์ในการเข้าถึงได้เพียงเฉพาะที่เกี่ยวข้องและสามารถทำได้เพียงแค่การอ่านข้อมูล แต่ไม่มีสิทธิ์แก้ไข ในขณะที่ Admin มีสิทธิ์ที่จะเข้าถึงได้ทุกไฟล์และกระทำกับข้อมูลได้ทุกอย่าง

ปกติแล้ว สิทธิ์ในการเข้าถึง (Access Permissions) จะถูกกำหนดจากความเป็นไปได้ในการจัดการข้อมูล (Possibilities) เช่น ในระบบ UNIX สามารถกำหนดสิทธิ์ได้ตามลักษณะของความเป็นไปได้ 3 ประการ คือ สิทธิในการอ่านอย่างเดียว (Read-Only) สิทธิในการเขียนหรือเปลี่ยนแปลงข้อมูล (Write- โดยการ Create, Change, Delete) และสิทธิในการประมวลผล (Execute) เป็นต้น ซึ่ง User หรือกลุ่มผู้ใช้ อาจได้รับสิทธิที่ไม่เหมือนกัน คืออาจกระทำได้ทั้งหมดหรือได้รับ 2 สิทธิ หรือทั้งหมดก็ได้

5. การจัดสร้างและระบบควบคุมการเข้าถึง

เป็นขั้นตอนสุดท้ายของระบบควบคุมการเข้าถึง ซึ่งก็คือการตัดสินใจว่าจะ กำหนดขอบเขตในการป้องกันการเข้าถึงให้แก่แต่ละแหล่งข้อมูล (Resources) อย่างไร เช่น สำหรับเครื่องแม่ข่าย (Server) ที่มีความสำคัญหรือมีความเปราะบาง (Sensitive) สูง อาจกำหนดให้มีเพียงคนกลุ่มน้อยที่มีความจำเป็นเท่านั้น ที่จะสามารถเข้าถึงได้ โดยการกำหนดขั้นตอนต่างๆ ให้มีมากและยากแก่การเข้าถึงข้อมูล หรือกำหนดให้การติดต่อกับเครื่องแม่ข่าย ต้องผ่านระบบ firewalls เป็นต้น ซึ่งหลังจากที่ได้มีการตัดสินใจเรียบร้อยแล้ว ก็ต้องนำไปประกาศไว้ในข้อกำหนดป้องกันการเข้าถึง (Access Protection Policy)

มาตรฐานของระบบควบคุมและป้องกันการเข้าถึง (Policy-Based Access Control and Protection)

การที่องค์กรกำหนดให้มีมาตรการควบคุมและป้องกันการเข้าถึงแหล่งข้อมูลที่สำคัญ มีคุณประโยชน์มากมาย คือ

1. แหล่งข้อมูลต่างๆ ขององค์กร ได้รับการป้องกันตามมาตรฐาน

อย่างน้อยองค์กรนั้นๆ ก็ได้มีการสละเวลา ที่จะคำนึงถึงการจัดตั้งระบบรักษาความปลอดภัยให้กับแหล่งข้อมูลต่างๆ และจะจัดการอย่างไรกับแหล่งข้อมูลอันสำคัญเหล่านั้น นั่นก็คือได้ให้ความสำคัญและใส่ใจในการบริหารข้อมูลขององค์กร

2. มีแนวทางในการเลือกและกำหนดระดับการป้องกันข้อมูล

เมื่อได้มีการตั้ง Server ขึ้นมาใช้สำหรับองค์กร ก็จะมีการกำหนดไฟล์วอลล์และกระบวนการในการป้องกันต่างๆ ก็จะได้มีแนวทางในการดำเนินการในเรื่องระบบรักษาความปลอดภัยข้อมูล ตามบทบาทและหน้าที่ ตลอดจนสภาพแวดล้อมในการระวังป้องกันแหล่งข้อมูลที่สำคัญเหล่านั้น

3. การตรวจสอบและทดสอบแผนรักษาความปลอดภัยข้อมูลขององค์กรอย่างสม่ำเสมอ

องค์กรใดมีมาตรฐานการรักษาความปลอดภัยข้อมูลที่ดี ย่อมเป็นการประกันว่าระบบนั้นมีความมั่นคงเพียงพอ ที่จะป้องกันข้อมูลได้อย่างมีประสิทธิภาพและพร้อมที่จะรับการตรวจสอบและทดสอบระบบได้ โดยที่จะไม่ทำให้เกิดความเสียหายต่อข้อมูลที่มีอยู่

การรักษาความปลอดภัยข้อมูล

การรักษาความปลอดภัยข้อมูล ประกอบด้วย 3 องค์ประกอบหลัก คือ

1. ความลับของข้อมูล (Confidentiality) หมายถึง การอนุญาตให้เฉพาะผู้ที่ได้รับอนุญาตเข้าถึงข้อมูลได้ ซึ่งก็จะต้องมีกลไกในการรักษาความลับ คือ

1.1 การเข้ารหัสข้อมูล (Cryptography หรือ Encryption) ซึ่งเป็นการจัดข้อมูลให้อยู่ในรูปแบบที่ไม่สามารถอ่านหรือเข้าใจได้ ไม่รู้วิธีการและคีย์ในการเข้าและถอดรหัส

1.2 การควบคุมการเข้าถึง (Access Control) เพื่อพิสูจน์ทราบตัวตนของผู้ที่เข้ามาใช้งานระบบ เป็นการปกป้องความลับของข้อมูลที่จัดเก็บไว้ในระบบ

2. ความคงสภาพของข้อมูล (Integrity)

หมายถึง ความเชื่อถือได้ของข้อมูลหรือแหล่งที่มา ซึ่งการรักษาความคงสภาพของข้อมูลนั้น หมายถึงการป้องกันไม่ให้ข้อมูลถูกเปลี่ยนแปลงจากสภาพเดิม โดยจะประกอบด้วย 2 ส่วน คือ ความถูกต้องของเนื้อหาข้อมูลและความถูกต้องของแหล่งที่มา

กลไกในการรักษาความคงสภาพของข้อมูลก็จะประกอบด้วย 2 ส่วน คือ

2.1 การป้องกัน (Prevention) เพื่อรักษาความคงสภาพของข้อมูล โดยการป้องกันความพยายามที่จะเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต

2.2 การตรวจสอบ (Detection) เพื่อตรวจสอบว่าข้อมูลยังคงมีความเชื่อถือได้อยู่หรือไม่

3. ความพร้อมใช้งานของข้อมูล

หมายถึง ความสามารถในการใช้ข้อมูลหรือทรัพยากรเมื่อต้องการ เป็นส่วนหนึ่งของความมั่นคงของระบบ (Reliability) โดยความพยายามที่จะทำลายความพร้อมใช้งาน เรียกว่า การโจมตีแบบปฏิเสธการให้บริการ (Denial of Service-DoS)

นอกจากคุณสมบัติทั้ง 3 ด้านที่กล่าวมาแล้ว ยังมีแนวความคิดเกี่ยวกับการรักษาความปลอดภัยข้อมูลอื่นๆ อีก เช่น ความเป็นส่วนบุคคล (Privacy) การระบุตัวตน (Identification) การพิสูจน์ทราบตัวตน (Authentication) การอนุญาตใช้งาน (Authorization) การตรวจสอบได้ (Accountability) เป็นต้น

การควบคุมการเข้าถึงด้วยรหัสผ่าน (Password-Based Access Control)

1. Reusable Passwords

ในการที่จะ Login เข้าไปในเครื่องแม่ข่าย ตามปกติก็จะมีการให้กรอก User Name หรือ Account แล้วตามด้วยรหัสผ่าน (Password) ซึ่ง user สามารถใช้ผ่านเข้าออกในระบบได้ช่วงระยะเวลาหนึ่ง

ในการพยายามที่จะเจาะเข้าสู่ระบบ ผู้โจมตีระบบ อาจล่วงรู้ถึงชื่อ Account (ในการ Identify) แต่ไม่ล่วงรู้ Password ซึ่งผู้โจมตีก็จะพยายามคาดเดา Password และพยายามอีกหลายครั้งในการเจาะระบบผ่าน Account นั้น แต่ไม่สามารถผ่านได้ เมื่อกระทำการแบบเดียวกันในหลายๆ ครั้ง Account นั้น ก็จะถูกระงับการให้บริการ และนำไปเก็บไว้ใน Locked-Out Account ชั่วคราว

ซึ่งอาจทำให้ User ที่เป็นเจ้าของจริง ไม่สามารถเข้าสู่ระบบได้ ก่อให้เกิดสภาวะที่เรียกว่า ปฏิเสธการให้บริการ (Denial-of-service-DoS) ในกรณีเช่นนี้ ก็ต้องมีการเปิดบริการให้แก่ User ที่แท้จริงอีกครั้ง เมื่อครบห้วงระยะเวลาที่กำหนด หรือเมื่อได้รับการแจ้งจาก User ตัวจริง การที่อนุญาตให้ Account ตลอดจน Password ดังกล่าวกลับมาใช้ได้อีกครั้ง เรียกว่า การอนุญาตให้นำรหัสผ่านกลับมาใช้อีกครั้งหนึ่งหรือ Reusable Passwords นั่นเอง ถือเป็นการแก้ปัญหาในการผ่านเข้าสู่ระบบให้กับ User วิธีหนึ่ง แต่...

การอนุญาตให้นำรหัสผ่านเดิมกลับมาใช้ใหม่ได้อีก มีข้อเสียคือ ทำให้ผู้โจมตี มีโอกาสมากขึ้นในการที่จะคาดเดารหัสผ่าน เพื่อเจาะเข้าสู่ระบบได้

อย่างไรก็ตาม เป็นการยากที่จะพยายามสุ่มเดารหัสผ่านไปเรื่อยๆ ซึ่งหลังจากความพยายามหลายๆ ครั้ง ส่วนใหญ่จะจบลงด้วยการเลิกความพยายาม แต่ก็มีความพยายามในรูปแบบอื่น เช่น การ Install โปรแกรมในการตรวจจับการกรอกรหัสผ่าน จากแฟ้มข้อมูลรหัสผ่าน (Password file) แล้วนำไปถอดรหัสต่อไปในภายหลัง

เพราะโดยปกติแล้ว ตัวรหัสผ่านเอง จะไม่เก็บอยู่ในรูปของ Plain Text ธรรมดา แต่จะถูกเข้ารหัส (Encryption) ด้วยอัลกอริธึมบางอย่าง แล้วนำไปเก็บไว้ที่ไฟล์หนึ่ง เรียกว่า Password File เช่น ลีนุกซ์และยูนิกซ์ จะมีการเข้ารหัสผ่านโดยใช้ฟังก์ชัน crypt ( ) ที่ใช้อันกอลิธึมชื่อ DES แล้วนำไปเก็บไว้ที่ไฟล์ /etc/passwd ซึ่งก็ต้องมีกระบวนการในการแปลงรหัสผ่านออกมาอีก จะยังไม่กล่าวถึงตอนนี้ รายละเอียดจะมีในคาบต่อๆ ไป

สำหรับ WindowsNT จะมีรูปแบบคล้ายๆ กัน โดยรหัสผ่านจะถูกเก็บไว้ในไฟล์ SAM (Security Access Manager) โดยรหัสผ่าน จะถูกเข้ารหัสโดยใช้อัลกอริธึม MD4 ออกมาเป็นค่าแฮช ที่มีความยาว 128 บิต (16 ไบต์) เช่น คำนวณรหัสผ่านออกมาเป็นรูปแบบเลขฐาน 16 เป็น 123a4bd42f123a123b3c3a3de27844af เป็นต้น

2. Hacking Root

Account ที่บรรดาแฮ็กเกอร์ปรารถนาที่สุด ย่อมเป็น Account ที่สามารถเข้าถึงได้ทุกไฟล์ ทุกไดเรคทอรี และกระทำการได้ทุกอย่างกับไฟล์บนระบบนั้น เรียกว่า Super Account

ในระบบ UNIX สิ่งที่เป็น Super Account คือ Root Account ซึ่งอนุญาตให้ผู้ที่ได้รับสิทธิ สามารถเข้าสู่ Root ได้ ทำให้มีความเป็นไปได้ในการเจาะระบบเข้าสู่ Root เรียกว่า การ Hacking Root

สำหรับระบบ Windows ส่วนที่เป็น Super Account คือ Administrator

สำหรับระบบ Novell NetWare ส่วนที่เป็น Super Account คือ Supervisor

ซึ่งโดยปกติ น้อยครั้งที่จะเกิดการแฮ็กที่ Root เพราะมีขั้นตอนที่ค่อนข้างลำบาก และโดยปกติแล้ว Password สำหรับ Root Account จะเป็น Password ที่ยากแก่การคาดเดาเป็นอย่างมาก การแฮ็กรหัสผ่านที่เกิดขึ้นส่วนใหญ่จึงจะเป็นการแฮ็กที่ User Account ทั่วๆ ไป แต่นั่นก็มิได้หมายความว่า การแฮ็กที่ User Account จะไม่ก่อให้เกิดความเสียหากมาก เพราะแท้ที่จริง ยังมีกระบวนการในการที่จะแฮ็กเข้าสู่ User Account ที่มีสิทธิในการเข้าถึงอันจำกัด แล้วทำการเปลี่ยนแปลง โดยการยกระดับ Account นั้น ให้มีสิทธิในการเข้าถึง Root และสามารถกระทำการได้เช่นเดียวกับ Root Account (หรือเปลี่ยนตัวเองกลายเป็น Root Account)

3. การแกะรหัสบนเครื่องแม่ข่าย (Server Password Cracking)

สำหรับ Admin ของระบบ มิใช่มีหน้าที่เพียงเข้าไปตรวจสอบเครื่องแม่ข่ายว่าเรียบร้อยดีหรือไม่เท่านั้น ยังจะต้อง Login ไปในระบบ (ด้วย Super Account ดังที่ได้เรียนไปแล้ว) เพื่อทำการตรวจสอบการทำงานของระบบด้วย ว่าปกติดีหรือไม่ อย่างไร มีสิ่งแปลกปลอมหรือไม่ หรือจะพัฒนาระบบรักษาความปลอดภัยอย่างไร และอาจต้องมีการตรวจสอบความพยายามในการแกะรหัส (Password Cracking) จากผู้โจมตีระบบด้วย

ผู้โจมตีระบบ อาจใช้โปรแกรมช่วยในการแกะรหัส เรียกว่า การแกะรหัสการเข้าถึงทางกายภาพ (Physical Access Password Cracking) ซึ่งเป็นโปรแกรมทดสอบระบบ ที่ต้อง execute บนเครื่องที่จะทำการทดสอบ (จึงต้องการ Physical Access) สำหรับระบบปฏิบัติการเครื่องแม่ข่ายที่เป็นระบบ Windows โปรแกรมที่ช่วยในการแกะรหัสยอดนิยมคือ L0phtcrack (L-Zero-phtcrack) ซึ่งผู้โจมตีระบบนิยมใช้เพื่อแกะรหัสและในขณะเดียวกัน ผู้ดูแลระบบ ก็นิยมใช้ในการทดสอบความแข็งแรงของระบบต่อการแกะรหัสเช่นกัน

3.1 L0phtcrack

เป็นโปรแกรมที่ใช้สำหรับการทดสอบและซ่อมแซมระบบ ปัจจุบันเรียกอีกชื่อหนึ่งว่า LC5 แรกเริ่มผลิตโดยกลุ่ม Mudge จากบริษัท L0pht Heavy Industries มีขีดความสามารถในการทดสอบความแข็งแรงของระบบรักษาความปลอดภัยที่ใช้ password ในการ authenticate โดยใช้วิธีการโจมตีระบบแบบ dictionary brute-force และการผสมผสานหลายๆ แบบ (hybrid attack) ต่อมา บริษัท L0pht Heavy Industries ได้ควบรวมกิจการกับบริษัท @stake ทำให้โปรแกรมนี้กลายเป็นสมบัติของบริษัท @stake ซึ่งบริษัท Symantec ก็ได้ซื้อโปรแกรมนี้ต่อมาจาก @stake อีกทีในปี 2004 แต่เนื่องจากเป็นโปรแกรมที่มีราคาสูง และมี Availability ต่ำ ประกอบกับถูกจำกัดสิทธิในการจำหน่ายจากรัฐบาลสหรัฐฯ ทำให้ บริษัท Symantec ประกาศที่จะเลิกพัฒนาและจำหน่ายโปรแกรมนี้ตั้งแต่ปี 2006 เป็นต้นไป

3.2 Brute-force Password Guessing

เป็นความพยายามแกะรหัสผ่านที่ผ่านกระบวนการเข้ารหัส (Cryptographic Scheme) ไว้ โดยพยายามเดา password จาก Character ที่อาจเป็นไปได้ เริ่มตั้งแต่ตัวแรก ไปสองตัว สามตัว ไปเรื่อยๆ ซึ่งจะขึ้นอยู่กับการกำหนดขอบเขต และความเป็นไปได้ (Possibility) จากผู้ที่พยายามแกะรหัส แต่ต้องคำนึงไว้ว่า ยิ่งกำหนดขอบเขตความเป็นไปได้มาก ก็ยิ่งต้องใช้ระยะเวลามากในการแกะรหัส เช่น อาจกำหนดให้มีขอบเขตการเดารหัสที่ ตัวอักษรภาษาอังกฤษ 26 ตัว กับตัวเลข 0-9 หรือกำหนดขอบเขตให้เป็นตัวอักขระที่มีขนคีย์บอร์ดทั้งหมด เป็นต้น จากนั้นจะนำขอบเขตที่กำหนดได้มาทำการ Combination รูปแบบต่างๆ ซึ่งจะทำให้เกิดรหัสผ่านที่อาจเป็นไปได้ (Possibility) ขึ้นมา ตามสูตร จำนวนขอบเขตยกกำลัง N โดยให้ N แทนความยาวของจำนวนอักขระของ password เช่น ถ้ากำหนดให้ขอบเขตของรหัส เป็นตัวอักษรภาษาอังกฤษเท่านั้น โดยไม่สนใจว่าตัวเล็กตัวใหญ่ และไม่ให้เป็นตัวเลข และให้เป็นรหัสจำนวน 8 อักขระ ก็จะได้ รหัสผ่าน ที่อาจเป็นไปได้ขึ้นมาจำนวน 26^N รหัส เป็นต้น

3.3 ความยาวอักขระของรหัสผ่าน (Password Length)

Password ที่ปลอดภัย ต้องเป็น Password ที่ยาว เพราะจะเกี่ยวข้องกับจำนวนความเป็นไปได้ ที่นักแกะรหัส ต้องพยายามค้นหา ลองเปรียบเทียบความเป็นไปได้ของรหัสผ่าน ที่นักแกะรหัส ต้องคำนวณออกมาต่อความยาวของอักขระที่เพิ่มขึ้น ตามตาราง

3.4 การโจมตีแบบสุ่มคำพื้นฐาน (Dictionary Attacks)

คือ การนำคำธรรมดาทั่วไป มารวมกันเป็นฐานข้อมูลในการแกะ Password ที่นิยมใช้รูปแบบคำธรรมดา ซึ่งจะใช้เวลาไม่นานเลยในการแกะรหัสผ่านเหล่านี้ จากการสำรวจในประเทศสหรัฐอเมริกาและกลุ่มประเทศในทวีปยุโรปพบว่า

25% ของพนักงานในองค์กรส่วนใหญ่ ใช้คำธรรมดาทั่วไปเป็น Password เช่น ชื่อผลไม้ ชื่อดารา ชื่อนักกีฬา เช่น Banana, Madonna เป็นต้น หรือแม้แต่นำคำพื้นฐานมาต่อกัน เช่น Iloveyou เป็นต้น

50% เป็นชื่อของบุคคลในครอบครัว เพื่อนสนิท ชื่อสัตว์เลี้ยง

30% เป็นชื่อดารา นักกีฬาหรือบุคคลที่ชื่นชอบ

มีเพียงประมาณ 10% เท่านั้น ที่ใช้ password เป็นคำที่ซับซ้อนและยากแก่การแกะ

3.5 การโจมตีแบบผสมคำ (Hybrid Attacks)

การพยายามแกะรหัส โดยนำคำธรรมดามาผสมกับสัญลักษณ์หรือตัวเลข เช่น การเติมตัวเลขท้ายคำแล้วกำหนดเป็น Password เป็นต้น

4. Password Policies

4.1 การตั้งรหัสผ่านที่ดี (Good Passwords)

เป็นเรื่องสำคัญที่องค์กรควรจะต้องมีนโยบาย ในการส่งเสริมให้พนักงานของตนตั้งรหัสผ่าน (Password) ที่ยากแก่การแกะรหัส ข้อแนะนำในการตั้งรหัสผ่านที่ดี เช่น

- มีความยาวอย่างน้อย 6 ตัวอักษร
- มีการเปลี่ยนแปลงตัวอักษรในบางแห่ง ซึ่งไม่ควรเป็นตัวแรก เช่นจะใช้คำว่า Superman อาจเปลี่ยนเป็น Supemman เป็นต้น
- ควรมีตัวเลข (0-9) อย่างน้อย 1 ตัว และไม่ควรเป็นตัวสุดท้าย
- ถ้าเป็นไปได้ ควรใส่อักขระพิเศษที่ไม่ใช่ ตัวอักษรและตัวเลข ทั่วไป เช่น #, @ เป็นต้น

นอกจากนี้ผู้ดูแลระบบรักษาความปลอดภัยข้อมูลขององค์กร ก็ควรจะต้องมีการดำเนินการในเรื่องต่างๆ อันเกี่ยวเนื่องกับการตั้งรหัสผ่านเข้าสู่ระบบ เช่น

1. การอบรมเรื่องการใช้รหัสผ่านแก่ผู้ใช้ในองค์กร
2. ใช้คอมพิวเตอร์สร้างรหัสผ่านตามมาตรฐาน FIPS PUB 181
3. การใช้การตรวจสอบรหัสผ่านแบบ Reactive เพื่อค้นหารหัสผ่านที่ง่ายต่อการคาดเดา หากพบระบบจะยกเลิกรหัสผ่านนั้น แล้วแจ้งให้ผู้ใช้ทราบ เพื่อแก้ไขรหัสผ่านของตนใหม่
4. ใช้การตรวจสอบรหัสผ่านแบบ Proactive เพื่อให้เกิดสมดุลระหว่างการยอมรับของผู้ใช้ควบคู่กับความแข็งแกร่งของรหัสผ่าน โดยผู้ใช้จะได้รับอนุญาตให้เลือกรหัสผ่านที่ต้องการแล้วระบบจะตรวจสอบเพื่อยอมรับหรือปฏิเสธรหัสผ่านนั้น

สรุปคำแนะนำในการตั้งรหัสผ่าน

1. มีจำนวนอักษรหรือสัญลักษณ์ไม่น้อยกว่า 6-8 ตัว
2. ควรประกอบด้วย ตัวหนังสือ ตัวเลขและสัญลักษณ์
3. ช่วงตำแหน่งที่ 2-6 ควรมีสัญลักษณ์อย่างน้อย 1 ตัว
4. ควรมีความแตกต่างอย่างมากจากรหัสผ่านที่เคยใช้
5. ไม่ควรใช้ชื่อผู้ใช้หรือคนใกล้ชิด
6. ไม่ใช้คำที่เป็นที่รู้จักกันโดยทั่วไป เช่น ศัพท์ในพจนานุกรม

4.2 การทดสอบและการบังคับให้กระทำตามนโยบายการตั้งรหัสผ่าน

Admin ที่ดี จะต้อง ทดสอบระบบที่ตนเองดูแลอย่างสม่ำเสมอ เช่น อาจ run โปรแกรม l0phtcrack เพื่อทดสอบการละเมิดนโยบาย (เช่น สามารถแกะรหัสที่เป็นคำธรรมดา

หรือไม่เป็นไปตามนโยบาย) ซึ่งก็อาจมีการตักเตือน หรือหักเงินเดือน หรือไล่ออก เป็นต้น (แล้วแต่นโยบายขององค์กร) หรือในอีกทางหนึ่ง ก็คือ การตั้งข้อจำกัดในการตั้ง password เลยตั้งแต่แรก หากไม่เป็นไปตามนโยบายที่กำหนด ก็จะไม่ Submit รหัสผ่านนั้นตั้งแต่แรก เป็นต้น ซึ่งถือเป็นการลดจุดอ่อน (Vulnerable) ของระบบด้วยเช่นกัน

4.3 นโยบายการกำหนดห้วงเวลาให้กับรหัสผ่าน (Password Duration Policies)

สำหรับแหล่งข้อมูลที่สำคัญๆ ควรกำหนดให้มีการเปลี่ยน Password เป็นระยะๆ เช่น ทุก 3 เดือน เป็นต้น ทั้งนี้ เพื่อให้เกิดความลำบากต่อผู้ที่ไม่ประสงค์ดีและกำลังพยายามแกะรหัสของบุคคลที่สามารถเข้าถึงข้อมูลนั้นได้

4.4 นโยบายการแชร์รหัสผ่าน (Shared Password Policies)

สิ่งที่ถือว่าเป็นอันตรายอย่างมากประการหนึ่งคือ การที่มี User หลายคนใช้ Account และรหัสผ่านเดียวกันในการแชร์ข้อมูลในกลุ่มของตน ซึ่งการกระทำดังกล่าว มีข้อเสียอย่างยิ่ง 2 ประการ คือ

4.4.1 การแชร์รหัสผ่านระหว่างหลายบุคคล ทำให้ไม่สามารถพิสูจน์ได้ชัดเจนว่า ใครเป็นผู้ใช้รหัสผ่านนั้นเข้าสู่ระบบ โดยเฉพาะหากมีกรณีที่ก่อให้เกิดความเสียหายต่อระบบ จะเป็นการยากในการระบุผู้กระทำผิด

4.4.2 ไม่ค่อยมีการเปลี่ยนแปลงรหัสผ่านตามระยะเวลาที่กำหนด ทั้งนี้ เพราะการเปลี่ยนแปลงรหัสผ่านที่แชร์กันอยู่ ต้องแจ้งให้ทุกคนทราบ ทำให้เกิดความลำบากและสร้างความรำคาญ จึงมักไม่ยอมเปลี่ยนแปลง ซึ่งก็ทำให้เกิดเป็นข้อบกพร่องตามนโยบายการป้องกันการเข้าถึงของระบบได้

วิธีที่ดีกว่าการแชร์รหัสผ่าน คือการกำหนดสิทธิในการเข้าถึง (Assigning Access Rights) ที่เท่าเทียมให้กับคนในกลุ่ม (Groups) เดียวกัน ทำให้ทุกคนในกลุ่มสามารถเข้าถึงฐานข้อมูลที่ต้องการใช้ร่วมกัน และได้รับสิทธิเท่าเทียมกันในการกระทำใดๆ กับฐานข้อมูลนั้น โดยที่ต่างคนต่างก็ Login เข้าสู่ระบบ ด้วย Identification และ Authentication ของตนเอง แต่ก็เป็นที่น่าเสียดายที่ในบาง Application ไม่ได้สนับสนุนการปฏิบัติดังกล่าว แต่บังคับให้ต้องใช้วิธีการแชร์รหัสผ่านเท่านั้น เช่น โปรแกรม Microsoft Exchange เวอร์ชันเก่าๆ เป็นต้น

4.5 การระงับการใช้รหัสผ่านที่หมดอายุแล้ว (Disabling Invalid Passwords)

ควรมีการตรวจสอบอย่างสม่ำเสมอ ว่า Account ใดที่หมดอายุแล้ว ก็ควรระงับการใช้งานในทันที จากข้อมูลขององค์กรด้านข้อมูลต่างๆ ในระดับนานาชาติ พบว่าในองค์กรขนาดใหญ่ที่มีการใช้ระบบรักษาความปลอดภัยแบบรหัสผ่าน ในการเข้าถึงฐานข้อมูลขององค์กร มีถึง 30-60% ที่หมดอายุแล้ว เช่น เป็น Account ของพนักงาน ที่ออกจากองค์กรไปแล้ว (ลาออก/ไล่ออก/

เปลี่ยนงาน ฯลฯ) หรือเป็น Account ชั่วคราว ที่ได้เปิดบริการให้กับบริษัทคู่ค้าหรือองค์กรที่ติดต่อประสานงานกันช่วงระยะเวลาหนึ่ง แต่ในปัจจุบันสภาวะการติดต่อระหว่างกันได้จบลงแล้ว

4.6 การจัดการกับรหัสผ่านที่สูญหาย

การสูญเสียรหัสผ่าน มีได้หลายแบบ เช่น อาจจดไว้แล้วทำหาย หรือ อาจจะลืม เป็นต้น จากสถิติพบว่า อัตราการเกิดการสูญหายรหัสผ่าน เป็นเหตุการณ์ที่เกิดขึ้นถึง 1 ใน 3 ของจำนวนคำร้องเรียนหรือคำขอรับความช่วยเหลือจากส่วนงานที่มีหน้าที่ให้ความช่วยเหลือ (Help Desk) ซึ่งการแก้ปัญหาจากเหตุการณ์นี้ นับว่าเป็นการกระทำที่ค่อนข้างอันตราย ซึ่งในการแก้ปัญหาการเกิดรหัสผ่านสูญหาย ปกติแล้ว Help Desk จะไม่มีสิทธิในการเข้าไปตรวจสอบดูว่ารหัสผ่านที่ถูกต้องคืออะไร จึงไม่สามารถบอกรหัสเดิมแก่พนักงานผู้นั้นได้ แต่จะได้รับสิทธิในการสร้างรหัสผ่านใหม่ สำหรับ Account นั้น ซึ่งการกระทำเช่นนี้ เรียกว่า การตั้งค่ารหัสผ่านใหม่ (password reset)

4.6.1 การโจมตีแบบวิศวสังคม (Social Engineering Attacks)

อันตรายอันอาจเกิดขึ้นได้ จากการโจมตีที่เรียกว่า การโจมตีแบบวิศวสังคม (Social Engineering Attacks) คือ การปลอมตัวเป็นเจ้าของ Account เป้าหมาย ติดต่อไปยัง Help Desk เพื่อแจ้งการสูญหายของรหัสผ่าน เพื่อขอตั้งค่ารหัสผ่านใหม่ โดยมักจะอ้างความจำเป็นรีบด่วนและมีความสำคัญสูง เพื่อกดดันและล่อลวงเจ้าหน้าที่ Help Desk ให้รีบทำการ Reset Password ให้ ซึ่งหากเจ้าหน้าที่ขาดประสบการณ์ หรือเกิดความลนลานและกระทำตาม ก็จะทำให้ผู้โจมตีสามารถกำหนดรหัสผ่านใหม่ในการเข้าสู่ระบบได้ และทำให้เจ้าของ Account ตัวจริงถูก Locked out หรือไม่สามารถเข้าสู่ระบบได้ (จนกว่าจะได้รับการแก้ไข)

4.6.2 การใช้เครื่องตอบรับอัตโนมัติ (Answering Machines)

วิธีหนึ่งในการป้องกันการโจมตีแบบวิศวสังคม (แม้จะไม่ใช่วิธีการที่ดีนัก แต่ก็ยังดีกว่าการโทรศัพท์ไปบอกรหัสผ่านให้ Help Desk ผ่านทางระบบโทรศัพท์) คือ การคิดรหัสผ่านใหม่ที่ต้องการ แล้วฝากเป็นข้อความทิ้งไว้ใน Voice Mailbox ของหน่วยงาน โดยให้เจ้าหน้าที่ Help Desk ติดต่อเข้ามายัง Voice Mailbox ของเจ้าของ Account เพื่อรับฟังรหัสผ่านใหม่ที่ต้องการเปลี่ยน ถือว่าเป็นการพิสูจน์ตัวตน Authenticate ในระดับหนึ่ง ว่า บุคคลนั้น เป็นผู้แจ้งขอเปลี่ยนแปลงรหัสผ่านจริง (หากมีรหัสผ่านใหม่ ใน Voice Mailbox ของผู้แจ้ง) แต่ต้องพิจารณาว่าทุกคนที่ติดต่อเข้ามาใน Voice Mailbox นั้น ก็จะได้ยินและรับทราบรหัสผ่านนั้นด้วย เพราะฉะนั้นควรจะต้องมีขั้นตอนในการจำกัดการเข้าสู่ Voice Mailbox อีกขั้นตอนหนึ่ง เช่น อาจจะบังคับให้ต้องมีการพิสูจน์คลื่นเสียง หรือ Voice Print Identification เพื่อพิสูจน์ตัวตน ก่อนที่จะได้รับทราบรหัสผ่านใหม่ที่ทิ้งไว้ใน Voice Mailbox เป็นต้น เรียกว่าเป็นการพิสูจน์ตัวตนแบบที่ใช้คุณสมบัติ

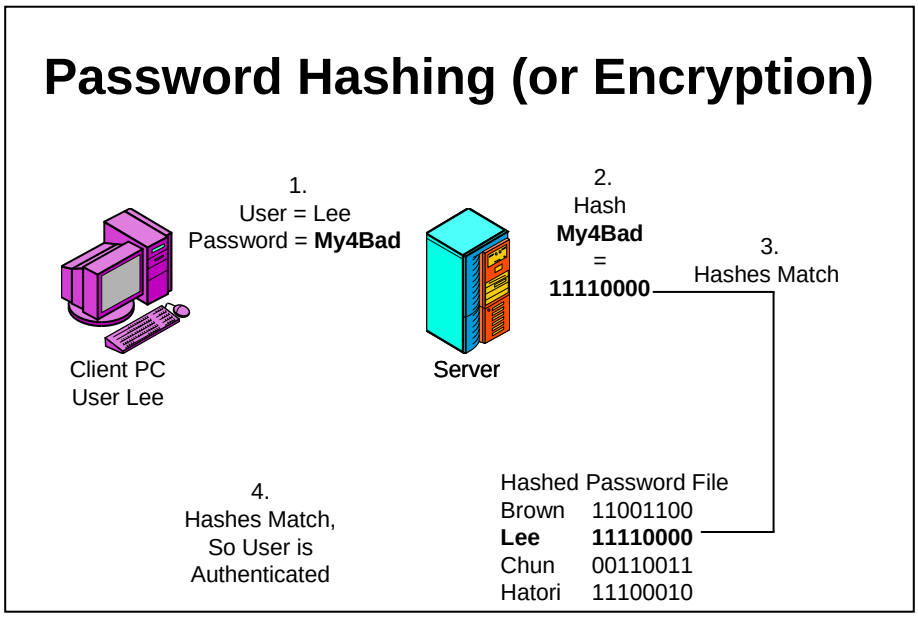
ทางชีวภาพ (Biometrics) ซึ่งนับว่าเป็นระบบพิสูจน์ตัวตนที่แข็งแกร่งที่สุด แต่มีข้อเสียที่อาจทำให้เกิดการปฏิเสธการเข้าถึงหลายครั้ง เพราะข้อแตกต่างแม้เพียงเล็กน้อยก็จะทำให้ไม่สามารถเข้าสู่ระบบได้ (โดยเฉพาะในเรื่องของคลื่นเสียง)

4.6.3 การใช้ระบบตั้งค่ารหัสผ่านใหม่อัตโนมัติ (Automating Password Resets)

โดยการเตรียมคำถามไว้ล่วงหน้า สำหรับผู้ที่ต้องการขอเข้าไปแก้รหัสผ่านใหม่ เช่น “คุณเกิดที่ไหน” เป็นต้น โดยเจ้าของ Account นั้น ต้อง Login เข้าสู่ระบบร้องขอรหัสผ่านใหม่ แล้วกรอกชื่อ Account เพื่อเป็นการ Identify ตนเองในเบื้องตน จากนั้นระบบจะถามคำถามที่เตรียมไว้ หากสามารถตอบได้ถูก ก็จะได้รับสิทธิให้เข้าไปแก้ไขรหัสผ่าน สิ่งสำคัญที่ควรระวังคือ หากผู้ที่ต้องการแฮ็ครหัสผ่าน มีความสนิทสนมหรือรู้ข้อมูลส่วนตัวของเจ้าของ Account เป็นอย่างดี ก็อาจสามารถตอบคำถามเหล่านี้ได้เช่นกัน

4.7 การเข้ารหัสไฟล์ที่เก็บรหัสผ่าน (Password Files)

เป็นวิธีการหนึ่งในความพยายามที่จะป้องกันการแฮ็ครหัสผ่าน ซึ่งระบบปฏิบัติการคอมพิวเตอร์สมัยใหม่จะทำการเข้ารหัส (Encrypt) ไฟล์ที่เก็บรหัสผ่าน (Password Files) โดยใช้กระบวนการมาตรฐานในการเข้ารหัสข้อมูล เรียกว่า DES – Data Encryption Standard (จะมีเรียนในบทที่ 7) โดยใช้ ค่า 7 บิตต่ำสุด ของตัวอักษร 8 ตัวแรกของรหัสผ่านของผู้ใช้ เป็นคีย์ในการเข้ารหัส ซึ่งเมื่อผ่านกระบวนการแล้ว จะได้ผลลัพธ์ออกมาเป็นคีย์ขนาด 56 บิต นำไปเก็บไว้เป็น Encrypted String เพื่อทำการเปรียบเทียบกับการ Login ของเจ้าของ Account ในครั้งต่อๆ ไป



ภาพที่ 3.1 Password Hashing (or Encryption)

จากกระบวนการในการเข้ารหัส Password File ที่ได้กล่าวไปแล้ว หากผู้โจมตีต้องการแกะรหัสผ่าน จะต้องหาทางพยายามโจรกรรม Encrypted Password Files เสียก่อน จากนั้นจึงทำการคาดเดาถึง Password จำนวนมากมายที่อาจเป็นไปได้ แล้วทำการเข้ารหัส เพื่อเปรียบเทียบคีย์ที่ได้ กับคีย์ที่ได้จาก Encrypted Password Files แล้วทำการคาดเดาความสัมพันธ์ต่อไป ซึ่งหากมีเวลาเพียงพอ ก็อาจจะสามารถคาดเดารหัสผ่านที่ถูกต้องออกมาได้

4.8 ระบบ password บน Windows

4.8.1 LAN Manager Password

ระบบปฏิบัติการเครือข่าย (Network Operating System – NOS) สำหรับติดตั้งบนเครื่องแม่ข่าย ระบบแรกของ Microsoft คือ LAN Manager ซึ่งค่อนข้างอ่อนแอในเรื่องระบบรักษาความปลอดภัย โดยการจำกัดจำนวนอักขระของ password ไว้เพียง 7 อักขระ แม้ว่าจะสามารถกำหนดเพิ่มได้มากสุดที่ 14 อักขระ แต่ในความเป็นจริงแล้ว จะถูกแบ่งออกเป็น 2 ส่วน (Strings) เช่น ตั้ง password ว่า Headquarters ก็จะถูกแบ่งเป็น 2 Strings คือ “Headqua” กับ “rters” ซึ่งหากเดาสตริงแรกถูก ก็ง่ายที่จะทำการเดาสตริงที่ 2 จึงถือว่าเป็นระบบที่ไม่ปลอดภัยเท่าที่ควร

4.8.2 Windows NT Password

ระบบปฏิบัติการเครือข่ายลำดับต่อมาของ Microsoft คือ Windows NT Server จึงได้มีการออกแบบระบบรหัสผ่านใหม่ เรียกว่า Windows NT LAN Manager – NTLM ซึ่งมี 2 version หลักการคร่าวๆ คือ จะใช้รูปแบบการพิสูจน์ตัวตนในลักษณะของการโต้ตอบกับเครื่องแม่ข่าย แบ่งเป็น 3 ประเภท (Type) เริ่มต้นที่เครื่องลูกข่ายส่ง Type 1 Message ไปว่าต้องการเข้าสู่ระบบ ที่ประกอบได้ด้วย Flag of Feature ต่างๆ เช่น Key Size, Request for Mutual Authentication, Etc. จากนั้น เครื่องแม่ข่ายก็จะส่ง Type 2 Message มา โดยมีกลุ่มของข้อมูลต่างๆ ที่ต้องการ พร้อมกับส่ง Data ในการพิสูจน์ตัวตน ขนาด 8 Bytes มาด้วย (เรียกว่า Challenge) สุดท้าย เครื่องลูกข่ายก็จะนำเอา Tpye2 Message ที่ได้รับมาทำการประมวลผล โดยใช้อัลกอริธึมของ NTLM โดยการประยุกต์ MD4/5 hashing algorithms และ การเข้ารหัสข้อมูลแบบ DES มาคำนวณ เป็น Type3 Message เรียกว่า Response ส่งกลับคืนไปยังเครื่องแม่ข่าย เพื่อยืนยันตัวตนเข้าสู่ระบบ ซึ่งระบบ NTLM นี้มีความปลอดภัยเพิ่มมากขึ้นมาก เพราะ Sensitive ต่อตัวอักษร เล็ก-ใหญ่ แล้ว ยังสามารถเลือกบังคับให้มีการตั้งรหัสผ่านที่ยากแก่การแกะด้วย ระบบถึงจะยอมรับรหัสผ่านนั้น แม้จะไม่ใช่ค่าที่กำหนดไว้เป็นมาตรฐาน (Default) ก็ตาม

4.9 Shoulder Surfing

การแอบดูรหัส ในระหว่างที่เข้าของ Account กำลังกรอกรหัส ด้วยวิธีการต่างๆ เช่น อาจชวนคุยเพื่อให้เสียสมาธิหรือไม่สังเกต เป็นต้น อาจเห็นเป็นบางตัวอักขระและสามารถนำไปคาดเดาต่อ อาจสังเกตไปถึงจังหวะในการพิมพ์รหัสผ่าน หรือฟังจำนวนที่กด ฯลฯ

4.10 Keystroke Capture Software

เป็นอีกวิธีหนึ่งในการดักจับการกรอกรหัสผ่านจาก user โดยการติดตั้งโปรแกรมสำหรับดักจับการกรอกรหัส ไว้บนเครื่องคอมพิวเตอร์เป้าหมาย ซึ่งปกติมักกระทำกับเครื่องแม่ข่าย เรียกโปรแกรมจำพวกนี้ว่า Keystroke Capture Software ซึ่งโปรแกรมพวกนี้ นอกจากจะดักจับรหัสผ่านแล้ว ยังสามารถดักจับกุญแจรหัสที่ใช้ในกระบวนการเข้ารหัส (Encryption) ได้อีกด้วย ซึ่งนับได้ว่าเป็นวิธีที่อาจต้องเป็นนักแกะรหัสมืออาชีพสักหน่อย มีหลายลักษณะ ยกตัวอย่าง เช่น

4.10.1 Protected RAM Buffer

เมื่อ user กรอกรหัสผ่านเสร็จ รหัสผ่าน นั้น จะถูกนำไปเก็บไว้ใน RAM Buffer เพื่อทำการประมวลผล วิธีการก็คือ การใช้โปรแกรมหรือวิธีการต่างๆ เพื่อลักลอบเข้าไปใน RAM Buffer เพื่อดูรหัสผ่าน ซึ่งสามารถกระทำได้ใน Windows 98, ME, XP (home) เนื่องจากไม่มีระบบป้องกันนี้ แต่สำหรับระบบปฏิบัติการ UNIX และ Microsoft Windows Server XP (Pro), 2000 การกระทำดังกล่าว จะทำได้ยาก เพราะมีแต่ตัว OS เองเท่านั้น ที่จะเข้าไปใน RAM Buffer นี้ได้

4.10.2 Trojan horse

สำหรับวิธีการแกะรหัสบนเครื่องลูกข่าย วิธีหนึ่งที่นิยมคือ การใช้โปรแกรมสอดแนมที่เรียกว่า Trojan Horse Password Capture Program ซึ่งก็มีหลายลักษณะ หลายวิธี แต่หลักการโดยรวม คือการลักลอบนำโปรแกรมสอดแนมเพื่อแกะรหัสนี้ ไปใส่หรือปลูก (Plant) ไว้บนเครื่องลูกข่าย แล้วมีการหลอกลวง User ให้กรอกรหัสผ่านด้วยวิธีการต่างๆ เช่น อาจทำให้เกิดหน้าต่างข้อความ (Pop-Up) ระบุให้กรอก Username และ Password เพื่อตรวจสอบต่างๆ โดยที่ทำหน้าต่างนั้นให้เหมือนกับเป็นส่วนหนึ่งของระบบปฏิบัติการเครือข่ายนั้น เป็นต้น

4.11 ระบบรหัสบนระบบปฏิบัติการวินโดวส์ บนเครื่องลูกข่าย (Windows Client PC Software)

ถ้าผู้โจมตีระบบสามารถเข้ามาใช้งานเครื่องคอมพิวเตอร์ในสำนักงาน ก็อาจจะทำการ Login ไปสู่เครื่องแม่ข่าย ด้วยสิทธิในการเข้าถึงระดับ User เพื่อกระทำการใดๆ ต่อไปได้ ซึ่งก็จำเป็นที่ผู้ดูแลระบบ จะต้องมีการเตรียมการป้องกันในกรณีดังกล่าวไว้ด้วย ดังต่อไปนี้

4.11.1 Login Password

ในระบบปฏิบัติการวินโดวส์ 95, 98, ME, XP (Home Edition) เมื่อเปิดเครื่องแล้ว จะมีการสอบถามรหัสผ่าน (Login Password) เพื่อเข้าสู่ระบบ อย่างไรก็ตาม ทุกคนสามารถละเลยขั้นตอนนี้ได้ โดยการกดปุ่มยกเลิก (Escape) ก็จะสามารถเข้าสู่ระบบได้ เพราะการใส่รหัสผ่านในขั้นตอนนี้ เป็นการกำหนดคุณลักษณะการแชร์ไฟล์และการสั่งพิมพ์ ไม่ได้เป็นการพิสูจน์ตัวตนในระบบรักษาความปลอดภัยข้อมูลแต่อย่างใด ซึ่งระบบปฏิบัติการ Windows ที่มีการพิสูจน์ตัวตนตามระบบรักษาความปลอดภัย อย่างน้อย จะต้องเป็นระดับมืออาชีพ (Professional Edition) หรือเป็นระบบปฏิบัติการสำหรับเครื่องแม่ข่าย (Windows Server) เช่น Windows 2000 Professional และ Windows XP Professional เป็นต้น

4.11.2 BIOS Password

ในเครื่องคอมพิวเตอร์ทุกเครื่อง เมื่อมีการเปิดเครื่องและทำการบู๊ตขึ้นมา ก่อนที่จะไปสู่ขั้นตอนของการเข้าสู่ระบบปฏิบัติการวินโดวส์ จะมีการตรวจสอบรหัสผ่านเข้าสู่ระบบ BIOS (Basic Input/Output System) ซึ่งถือว่าเป็นกระบวนการในการเข้าถึง (Access Control) ระดับหนึ่ง แต่ตามปกติแล้ว กระบวนการในการกำหนดรหัสผ่านบน BIOS ในแต่ละเครื่องจะแตกต่างกันไป โดยที่ User แต่ละคน มีส่วนกำหนดขึ้นมาเอง

อย่างไรก็ดี หากผู้โจมตีระบบมีเวลาและมีโอกาสเหมาะ (เช่น ไม่มีคนอื่นอยู่) ก็สามารถที่จะเปิดเครื่องคอมพิวเตอร์ แล้วทำการถอดแบตเตอรี่ ที่ทำหน้าที่หล่อเลี้ยงพลังงานให้กับหน่วยความจำ BIOS ออกได้ จะทำให้ค่าการติดตั้งทั้งหมดถูกลบออกไปจากหน่วยความจำ BIOS กลับไปอยู่ในสภาพเดิมเหมือนกับที่ผลิตออกมาจากโรงงานใหม่ๆ ซึ่งก็หมายรวมถึง รหัสผ่านเข้าสู่ BIOS ด้วยเช่นกัน

4.11.3 Screensaver with Passwords

แม้ว่า BIOS Password จะเป็นการป้องกันระบบในระดับหนึ่งซึ่งดำเนินไปตั้งแต่เริ่มบู๊ตเครื่อง แต่ถ้าผู้ใช้งานมีธุระจำเป็นที่จะต้องไปติดต่องานยังสถานที่ต่างๆ และต้องผละจากเครื่องคอมพิวเตอร์เครื่องนั้นไปในช่วงระยะเวลาหนึ่ง โดยที่ไม่ได้ปิดเครื่องไว้ ก็อาจเกิดเป็นช่องว่างให้ผู้โจมตีกระทำการใดๆ กับเครื่องได้ ในกรณีเช่นนี้ การตั้งค่ารหัสผ่านบนหน้าจอ Screensaver หรือเรียกว่า (Screensaver Password) จะถูกนำมาใช้เพื่อปกป้องระบบ เมื่อต้องการจะเข้าระบบอีกครั้ง ก็ต้องมีการกรอกรหัสผ่าน จึงควรตั้งให้มีการแสดงผลของ Screensaver ให้เร็วที่สุด เพื่อให้ช่วงเวลาที่ผู้โจมตีจะเข้าสู่ระบบโดยไม่ผ่านการ Authentication จาก Screensaver มีน้อยที่สุด ทั้งนี้ จะต้องระวังปัญหาเรื่องการทำรหัสผ่านของ Screensaver สูญหายด้วย

ภาพที่ 3.2 รูปสามเหลี่ยมระบบรักษาความปลอดภัยข้อมูล

รูปสามเหลี่ยมประกอบความเข้าใจในระบบรักษาความปลอดภัยข้อมูล ดังนี้

1. การพิสูจน์ตัวตน (Authentication - Who is who?)

คือ ขั้นตอนการยืนยันความถูกต้องของหลักฐาน (Identity) ที่แสดงว่าเป็นบุคคลที่กล่าวอ้างจริง ในทางปฏิบัติจะแบ่งออกเป็น 2 ขั้นตอน คือ

- การระบุตัวตน (Identification) คือ ขั้นตอนที่ผู้ใช้แสดงหลักฐานว่าตนเองคือใคร เช่น Username

- การพิสูจน์ตัวตน (Authentication) คือ ขั้นตอนที่ตรวจสอบหลักฐานเพื่อแสดงว่าเป็นบุคคลที่กล่าวอ้างจริง เช่น Password

2. การกำหนดสิทธิ์ (Authorization - Who can access it?)

คือ ขั้นตอนในการอนุญาตให้แต่ละบุคคลสามารถเข้าถึงข้อมูลหรือระบบใดได้บ้าง ก่อนอื่นต้องทราบก่อนว่าบุคคลที่กล่าวอ้างนั้นคือใครตามขั้นตอนการพิสูจน์ตัวตนและต้องให้แน่ใจด้วยว่าการพิสูจน์ตัวตนนั้นถูกต้อง

3. การเข้ารหัส (Encryption - Who can see it?)

คือ การเก็บข้อมูลด้วยวิธีการพิเศษเพื่อป้องกันข้อมูลไว้ให้ผู้ที่มีสิทธิเท่านั้น (ปกป้องข้อมูลจากบุคคลอื่นที่ไม่ได้รับอนุญาต)

4. การรักษาความสมบูรณ์ (Integrity - Who can change it?)

คือ การรับรองว่าข้อมูลจะไม่ถูกเปลี่ยนแปลงหรือทำลายไปจากต้นฉบับ (Source) ไม่ว่าจะเป็นไปโดยบังเอิญหรือโดยเจตนาก็ตาม

5. การตรวจสอบ (Audit - Who done it?)

คือ การตรวจสอบหลักฐานทางอิเล็กทรอนิกส์ ซึ่งสามารถใช้ในการติดตามการดำเนินการเพื่อตรวจสอบความถูกต้องของการใช้งาน เช่นการตรวจสอบบัญชีชื่อผู้ใช้ โดยผู้ตรวจบัญชี ซึ่งการตรวจสอบความถูกต้องของการดำเนินการเพื่อให้แน่ใจว่าหลักฐานทางอิเล็กทรอนิกส์นั้นได้ถูกสร้างและสั่งให้ทำงานโดยบุคคลที่ได้รับอนุญาต และในการเชื่อมต่อเหตุการณ์เข้ากับบุคคลจะต้องทำการตรวจสอบหลักฐานของบุคคลนั้นด้วย ซึ่งถือเป็นหลักการพื้นฐานของขั้นตอนการทำงานของการพิสูจน์ตัวตนด้วย

สรุปว่า การกำหนดสิทธิ์การใช้งานระบบสารสนเทศในการการควบคุมการเข้าถึง (Access Control) เป็นหมวดที่กำหนดขึ้นเพื่อให้เกิดความมั่นคงปลอดภัยของสารสนเทศ องค์กรจำเป็นต้องมีการกำหนดนโยบายการเข้าถึงระบบ การบริหารการจัดการเข้าถึงของผู้ใช้และการควบคุมการเข้าถึงเครือข่าย โดยองค์กรสามารถกำหนดมาตรฐานได้ดังต่อไปนี้

1. การควบคุมการเข้าถึงระบบ องค์กรต้องมีนโยบายควบคุมการเข้าถึงระบบเครือข่ายและระบบสารสนเทศอย่างเป็นลายลักษณ์อักษร และทบทวนตามระยะเวลาที่กำหนดไว้ โดยพิจารณาให้สอดคล้องกับภารกิจของมหาวิทยาลัยและความมั่นคงปลอดภัยในการเข้าถึงทรัพย์สินสารสนเทศ

2. การจัดการการเข้าถึงของผู้ใช้ องค์กรต้องมีการกำหนดมาตรการและแนวปฏิบัติอย่างเป็นระบบเพื่อใช้ในการกำหนดรหัสบัญชีผู้ใช้สำหรับนิสิตและบุคลากร การจัดการสิทธิในการเข้าใช้ระบบสารสนเทศ การจัดการรหัสผ่าน รวมถึงการทบทวนสิทธิการเข้าถึงของผู้ใช้

3. หน้าที่ความรับผิดชอบของผู้ใช้งาน เพื่อป้องกันการเข้าถึงโดยมิได้รับอนุญาต ผู้ใช้งานต้องให้ความร่วมมือในการปฏิบัติตามมาตรการด้านการรักษาความปลอดภัยในการเข้าถึงอย่างเคร่งครัด เช่น ไม่กำหนดรหัสผ่านแบบที่ไม่ปลอดภัย ไม่เปิดเผยรหัสผ่านให้ผู้อื่นล่วงรู้ เป็นต้น

4. การควบคุมการเข้าถึงเครือข่าย การเข้าถึงเครือข่ายจากภายในองค์กรหรือการเชื่อมต่อจากภายนอกต้องมีมาตรการควบคุมที่ชัดเจน ต้องผ่านการพิสูจน์ตัวตนและตรวจสอบสิทธิตามขั้นตอนอย่างมีประสิทธิภาพ โดยระบบต้องยอมให้เฉพาะผู้ใช้งานที่ได้รับอนุญาตผ่านเข้าสู่เครือข่ายและใช้บริการได้ตามสิทธิที่กำหนดให้เท่านั้น

5. การควบคุมการใช้งานระบบปฏิบัติการ การเข้าถึงระบบปฏิบัติการต้องกำหนดกระบวนการในการเข้าถึงระบบให้มีความมั่นคงปลอดภัย โดยต้องผ่านการพิสูจน์ตัวตนและตรวจสอบสิทธิและมีการควบคุมการใช้โปรแกรมยูทิลิตี้สำหรับระบบเพื่อป้องกันการเข้าถึงโดยมิได้รับอนุญาต

6. การควบคุมการใช้งานระบบสารสนเทศ การเข้าถึงระบบสารสนเทศต้องมีการควบคุมการใช้งานสารสนเทศ ซึ่งได้แก่ มีการกำหนดสิทธิในการใช้งานระบบสารสนเทศ อาทิ เขียน อ่าน ลบ ได้ มีการกำหนดกลุ่มของผู้ใช้ตามความจำเป็นในการปฏิบัติงานได้ มีการแยกการติดตั้งระบบสารสนเทศที่มีความสำคัญหรือมีความเสี่ยงสูงไว้ในบริเวณเครือข่ายที่ปลอดภัย

2. แนวคิดหลักของความมั่นคงปลอดภัยของสารสนเทศ

วรัญญา ปิ่นทอง (2557) ได้กล่าวถึง กลุ่มอุตสาหกรรมความมั่นคงปลอดภัยของคอมพิวเตอร์ ซึ่งได้กำหนดแนวคิดหลักของความมั่นคงปลอดภัยของคอมพิวเตอร์ขึ้นประกอบด้วยดังต่อไปนี้

1. ความลับ Confidentiality

1.1 เป็นการรับประกันว่าผู้มีสิทธิ์และได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงข้อมูลได้

1.2 องค์กรต้องมีมาตรการป้องกันการเข้าถึงสารสนเทศที่เป็นความลับ เช่น การจัดประเภทของสารสนเทศ การรักษาความปลอดภัยในกับแหล่งจัดเก็บข้อมูล กำหนดนโยบายรักษาความมั่นคงปลอดภัยและนำไปใช้ให้การศึกษาแก่ทีมงานความมั่นคงปลอดภัยและผู้ใช้

1.3 ภัยคุกคามที่เพิ่มมากขึ้นในปัจจุบัน มีสาเหตุมาจากความก้าวหน้าทางเทคโนโลยี ประกอบกับความต้องการความสะดวกสบายในการสั่งซื้อสินค้าของลูกค้า โดยการยอมให้สารสนเทศส่วนบุคคลแก่ website เพื่อสิทธิ์สนการทำธุรกรรมต่างๆ โดยลืมไปว่าเว็บไซต์เป็นแหล่งข้อมูลที่สามารถขโมยสารสนเทศไปได้ไม่ยากนัก

2. ความสมบูรณ์ Integrity

2.1 ความสมบูรณ์ คือ ความครบถ้วน ถูกต้อง และไม่มีสิ่งแปลกปลอม สารสนเทศที่มีความสมบูรณ์จึงเป็นสารสนเทศที่นำไปใช้ประโยชน์ได้อย่างถูกต้องครบถ้วน

2.2 สารสนเทศจะขาดความสมบูรณ์ ก็ต่อเมื่อสารสนเทศนั้นถูกนำไปเปลี่ยนแปลงปลอมปนด้วยสารสนเทศอื่น ถูกทำให้เสียหาย ถูกทำลายหรือถูกกระทำในรูปแบบอื่นๆ เพื่อขัดขวางการพิสูจน์การเป็นสารสนเทศจริง

3. ความพร้อมใช้ Availability

3.1 ความพร้อมใช้ หมายถึง สารสนเทศจะถูกเข้าถึงหรือเรียกใช้งานได้อย่างราบรื่นโดยผู้ใช้หรือระบบอื่นที่ได้รับอนุญาตเท่านั้น

3.2 หากเป็นผู้ใช้หรือระบบที่ไม่ได้รับอนุญาต การเข้าถึงหรือเรียกใช้งานจะถูกขัดขวางและล้มเหลวในที่สุด

4. ความถูกต้องแม่นยำ Accuracy

4.1 ความถูกต้องแม่นยำ หมายถึง สารสนเทศต้องไม่มีความผิดพลาดและต้องมีค่าตรงกับความคาดหวังของผู้ใช้เสมอ

4.2 เมื่อใดก็ตามที่สารสนเทศมีค่าผิดเพี้ยนไปจากความคาดหวังของผู้ใช้ ไม่ว่าจะเกิดจากการแก้ไขด้วยความตั้งใจหรือไม่ก็ตาม เมื่อนั้นจะถือว่าสารสนเทศ “ไม่มีความถูกต้องแม่นยำ”

5. เป็นของแท้ Authenticity

สารสนเทศที่เป็นของแท้ คือ สารสนเทศที่ถูกจัดทำขึ้นจากแหล่งที่ถูกต้อง ไม่ถูกทำซ้ำโดยแหล่งอื่นที่ไม่ได้รับอนุญาตหรือแหล่งที่ไม่คุ้นเคยและไม่เคยทราบมาก่อน

6. ความเป็นส่วนตัว Privacy

6.1 ความเป็นส่วนตัว คือ สารสนเทศที่ถูกรวบรวม เรียกใช้และจัดเก็บโดยองค์กรจะต้องถูกใช้ในวัตถุประสงค์ที่ผู้เป็นเข้าของสารสนเทศรับทราบ ณ ขณะที่มีการรวบรวมสารสนเทศนั้น

6.2 มิฉะนั้นจะถือว่าเป็นการละเมิดสิทธิส่วนบุคคลด้านสารสนเทศ

สรุปว่า การใช้งานคอมพิวเตอร์และการเข้าถึงข้อมูลบนเครือข่าย มีความเสี่ยงต่อการถูกบุกรุก โจมตี รวมถึงการล้วงเอาข้อมูลโดยไม่ได้รับอนุญาตด้วยรูปแบบและวิธีการแตกต่างกันไป บางวิธีอาจมีผลเสียหายต่อระบบเพียงเล็กน้อย แต่บางวิธีการนำมาซึ่งความเสียหายอย่างร้ายแรง จนบางครั้งระบบคอมพิวเตอร์ไม่สามารถทำงานได้ต่อไปส่งผลถึงความเสียหายทางธุรกิจต่างๆ ได้ การเตรียมการรักษาความปลอดภัยจากการใช้งานจึงเป็นวิธีการดีที่สุดที่จะไม่ให้เกิดเหตุการณ์เหล่านี้ได้

2. องค์ประกอบของระบบสารสนเทศ

ระบบสารสนเทศ ซึ่งเป็นระบบสนับสนุนการบริหารงาน การจัดการและการปฏิบัติงานของบุคลากร ไม่ว่าจะเป็นระดับบุคคล ระดับกลุ่มหรือระดับองค์กร ไม่ใช่มีเพียงเครื่องคอมพิวเตอร์เท่านั้น แต่ยังมีองค์ประกอบอื่นๆ ที่เกี่ยวข้องกับความสำเร็จของระบบอีก รวม 5 องค์ประกอบ ซึ่งจะขาดองค์ประกอบใดไม่ได้ คือ

2.1 ฮาร์ดแวร์ เป็นองค์ประกอบสำคัญของระบบสารสนเทศ หมายถึง เครื่องคอมพิวเตอร์ อุปกรณ์ต่อพ่วง รวมทั้งอุปกรณ์สื่อสารสำหรับเชื่อมโยงคอมพิวเตอร์เข้าเป็นเครือข่าย เช่น เครื่องพิมพ์อุปกรณ์กระจายสัญญาณ

2.2 ซอฟต์แวร์หรือโปรแกรมคอมพิวเตอร์ เป็นองค์ประกอบที่สำคัญประการที่สอง ซึ่งก็คือลำดับขั้นตอนของคำสั่งที่จะสั่งงานให้ฮาร์ดแวร์ทำงาน เพื่อประมวลผลข้อมูลให้ได้ผลลัพธ์ตาม

ความต้องการของการใช้งาน ในปัจจุบันมีซอฟต์แวร์ระบบปฏิบัติงาน ซอฟต์แวร์ควบคุมระบบงาน ซอฟต์แวร์สำเร็จและซอฟต์แวร์ประยุกต์สำหรับงานต่างๆ ลักษณะการใช้งานของซอฟต์แวร์ก่อนหน้านี้ผู้ใช้จะต้องติดต่อใช้งานโดยใช้ข้อความเป็นหลัก แต่ในปัจจุบันซอฟต์แวร์มีลักษณะการใช้งานที่ง่ายขึ้น โดยมีรูปแบบการติดต่อที่สื่อความหมายให้เข้าใจง่าย เช่น มีส่วนต่อประสานกราฟฟิกส์กับผู้ใช้ที่เรียกว่า จียูไอ (Graphical User Interface: GUI) ส่วนซอฟต์แวร์สำเร็จที่มีใช้ในท้องตลาดทำให้การใช้งานคอมพิวเตอร์ในระดับบุคคลเป็นไปอย่างกว้างขวางและเริ่มมีลักษณะส่งเสริมการทำงานของกลุ่มมากขึ้น ส่วนงานในระดับองค์กรส่วนใหญ่มักจะมีการพัฒนาระบบตามความต้องการโดยการว่าจ้างหรือโดยนักคอมพิวเตอร์ขององค์กร เป็นต้น ซอฟต์แวร์สามารถแบ่งได้ดังนี้

2.1.1 ซอฟต์แวร์ระบบ หมายถึง โปรแกรมทุกโปรแกรมที่ทำหน้าที่ติดต่อกับส่วนประกอบต่างๆ ของฮาร์ดแวร์คอมพิวเตอร์และอำนวยเครื่องมือสำหรับทำงานพื้นฐานต่างๆ ที่เกี่ยวข้องกับฮาร์ดแวร์

2.1.2 ซอฟต์แวร์ประยุกต์ จะเป็นโปรแกรมที่ทำให้คอมพิวเตอร์สามารถทำงานต่างๆ ตามที่ผู้ใช้ต้องการ ไม่ว่างานด้านการจัดทำเอกสาร การทำบัญชี การจัดเก็บข้อมูลข่าวสาร ตลอดจนงานทุกๆ ด้านตามแต่ผู้ใช้ต้องการจนสามารถกล่าวได้ว่าซอฟต์แวร์ประยุกต์ก็คือซอฟต์แวร์ที่ทำให้เกิดการใช้งานคอมพิวเตอร์กันอย่างกว้างขวางและทำให้คอมพิวเตอร์เป็นปัจจัยที่ไม่สามารถขาดได้ในยุคสารสนเทศนี้ในองค์กรขนาดใหญ่หรืองานที่มีความต้องการเฉพาะด้าน การจัดหาซอฟต์แวร์มาใช้งานจะใช้วิธีพัฒนาซอฟต์แวร์ขึ้นมาเองหรือว่าจ้างบริษัทซอฟต์แวร์เพื่อทำซอฟต์แวร์เฉพาะงานขึ้นมาใช้เอง ซอฟต์แวร์ประเภทนี้จะเรียกว่าซอฟต์แวร์เฉพาะงาน(Tailor Made Software) มีข้อดีคือมีความเหมาะสมกับงานและสามารถแก้ไขตามความต้องการได้ข้อเสียคือค่าใช้จ่ายสูงและใช้เวลาสำหรับการพัฒนา ปัจจุบันนี้จึงมีโปรแกรมคอมพิวเตอร์ที่เขียนขึ้นมาเพื่อใช้สำหรับงานทั่วๆ ไป วางจำหน่ายเป็นชุดสำเร็จรูปเรียกว่าซอฟต์แวร์สำเร็จรูป (Software Package)

2.3 ข้อมูล เป็นองค์ประกอบที่สำคัญอีกประการหนึ่งของระบบสารสนเทศ อาจจะเป็นตัวชี้ความสำเร็จหรือความล้มเหลวของระบบได้ เนื่องจากจะต้องมีการเก็บข้อมูลจากแหล่งกำเนิด ข้อมูลจะต้องมีความถูกต้อง มีการกลั่นกรองและตรวจสอบแล้วเท่านั้นจึงจะมีประโยชน์ ข้อมูลจำเป็นจะต้องมีมาตรฐาน โดยเฉพาะอย่างยิ่งเมื่อใช้งานในระดับกลุ่มหรือระดับองค์กร ข้อมูลต้องมีโครงสร้างในการจัดเก็บที่เป็นระบบระเบียบเพื่อการสืบค้นที่รวดเร็วมีประสิทธิภาพ

2.4 บุคลากร ในระดับผู้บริหาร ผู้ดูแลระบบ ผู้พัฒนาระบบ นักวิเคราะห์ระบบนักเขียนโปรแกรม และผู้ใช้บริการ เป็นองค์ประกอบสำคัญในความสำเร็จของระบบสารสนเทศบุคลากรมีความรู้ความสามารถทางคอมพิวเตอร์มากเท่าใด โอกาสที่จะใช้งานระบบสารสนเทศและระบบ

คอมพิวเตอร์ได้เต็มศักยภาพและคุ้มค่ายิ่งมากขึ้นเท่านั้น โดยเฉพาะระบบสารสนเทศในระดับบุคคล ซึ่งเครื่องคอมพิวเตอร์มีขีดความสามารถมากขึ้น ทำให้ผู้ใช้มีโอกาสพัฒนาความสามารถของตนเอง และพัฒนาระบบงานได้เองตามความต้องการ สำหรับระบบสารสนเทศในระดับกลุ่มและองค์กรที่มีความซับซ้อนมาก อาจจะต้องใช้บุคลากรในสาขาคอมพิวเตอร์ โดยตรงมาพัฒนาและดูแลระบบงาน

2.5 ขั้นตอนการปฏิบัติงาน ขั้นตอนการปฏิบัติงานที่ชัดเจนของผู้ใช้หรือของบุคลากรที่เกี่ยงข้องก็เป็นเรื่องสำคัญอีกประการหนึ่ง เมื่อได้พัฒนาระบบงานแล้วจำเป็นต้องปฏิบัติงานตามลำดับขั้นตอนในขณะที่ใช้งานก็จำเป็นต้องคำนึงถึงลำดับขั้นตอน การปฏิบัติของคนและความสัมพันธ์กับเครื่อง ทั้งในกรณีปกติและกรณีฉุกเฉิน เช่น ขั้นตอนการบันทึกข้อมูล ขั้นตอนการประมวลผล ขั้นตอนการปฏิบัติเมื่อเครื่องมือชำรุดหรือข้อมูลสูญหาย และขั้นตอนการทำสำเนาข้อมูลสำรองเพื่อความปลอดภัย เป็นต้น สิ่งเล่านี้ต้องมีการซักซ้อม มีการเตรียมการและการทำเอกสารคู่มือการใช้งานให้ชัดเจน

สรุปว่า องค์กรต่างๆ จะต้องมีการลงทุนจำนวนมากในการจัดหาระบบสารสนเทศที่มีประสิทธิภาพเพื่อนำมาช่วยงานทั้งด้านการบริหารและการจัดการงานทั่วไปขององค์กร โดยเน้นที่คุณภาพของระบบสารสนเทศและความคุ้มค่าในการลงทุน การใช้ระบบสารสนเทศจะเริ่มจากการนำข้อมูลป้อนเข้าสู่เครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์จะทำการประมวลข้อมูลเหล่านั้น แล้วจึงส่งผลลัพธ์ออกมาให้กับผู้ใช้ ผู้ใช้ระบบสารสนเทศจะนำสารสนเทศนั้นไปใช้ประกอบการตัดสินใจในการทำกิจกรรมใดกิจกรรมหนึ่ง หากผลลัพธ์ที่ได้จากการประมวลผลไม่ถูกต้องหรือไม่สมบูรณ์ ก็ต้องย้อนมาพิจารณาเริ่มต้นที่ขั้นตอนการป้อนข้อมูลใหม่อีกครั้งว่า ข้อมูลเข้าและขั้นตอนอื่นๆ มีความถูกต้อง สมบรูณ์หรือไม่ นั้นต่อไป

3. บทบาทของระบบสารสนเทศในองค์กร

การบริหารงานเพื่อให้เกิดประสิทธิภาพและประสิทธิผลตามเป้าหมายที่กำหนดไว้นั้น ผู้บริหารจำเป็นต้องอาศัยการบริหารที่เป็นระบบและเหมาะสมกับสภาพแวดล้อมขององค์การ ผู้บริหารจะต้องใช้ทรัพยากรที่มีอย่างจำกัดให้เกิดประโยชน์สูงสุด ดังนั้น ข้อมูลและสารสนเทศนับเป็นปัจจัยสำคัญยิ่งต่อการวางแผนปฏิบัติงาน และการควบคุมเพื่อให้เกิดความสำเร็จตามวัตถุประสงค์

องค์การและสิ่งแวดล้อมตามความหมายทางเทคนิค หมายถึง โครงสร้างทางสังคมอย่างเป็นทางการที่มีความมั่นคง โดยรับเอาทรัพยากรจากสิ่งแวดล้อมมาผ่านกระบวนการเพื่อสร้างหรือผลิตผลลัพธ์เน้นองค์ประกอบขององค์การ 3 ส่วน คือ

1. ปัจจัยหลักด้านการผลิต
2. กระบวนการผลิต
3. ผลผลิต

ระบบสารสนเทศสามารถถูกนำมาเป็นเครื่องมือในการเปลี่ยนแปลงกระบวนการดำเนินงานขององค์การ บางระบบอาจเปลี่ยนแปลงความสมดุลทางสิทธิ ภาระหน้าที่และความรับผิดชอบที่เคยมีในขณะเดียวกันองค์การเองก็มีผลกระทบต่อการออกแบบระบบสารสนเทศและเป็นผลกระทบต่อระบบสารสนเทศต่อองค์การ คือ

1. ลดระดับขั้นตอนของการจัดการ
2. มีความคล่องตัวในการดำเนินงาน
3. ลดขั้นตอนการดำเนินงาน
4. เปลี่ยนแปลงกระบวนการจัดการ
5. กำหนดขอบเขตการดำเนินงานใหม่ระบบสารสนเทศที่จะเชื่อมต่อผ่านเครือข่ายช่วยให้สามารถแลกเปลี่ยนข้อมูลระหว่างองค์การได้และมีการสร้างความสัมพันธ์ระหว่างองค์การและคู่ค้า ซึ่งเป็นการกำหนดขอบเขตการดำเนินงานใหม่

สรุปว่า เทคโนโลยีอินเทอร์เน็ตได้กลายมาเป็นเทคโนโลยีพื้นฐานที่ถูกนำมาสร้างเป็นโครงสร้างของระบบสารสนเทศภายในองค์การ ระบบอินเทอร์เน็ตได้รับความนิยมอย่างรวดเร็วและส่งเสริมการพาณิชย์อิเล็กทรอนิกส์เพื่อใช้ในการสร้างช่องทางการตลาด การขายและให้การสนับสนุนลูกค้าองค์การเสมือนจริง เป็นรูปแบบขององค์การแบบใหม่ ซึ่งเป็นเครือข่ายขององค์การที่เชื่อมโยงกันด้วยเทคโนโลยีสารสนเทศเพื่อแลกเปลี่ยนทักษะ ลดต้นทุน สร้างและกระจายสินค้าและบริการลักษณะขององค์การเสมือนจริงประกอบด้วย มีขอบเขตขององค์การไม่ชัดเจน ใช้เทคโนโลยีสื่อสารโทรคมนาคม มีความเป็นเลิศ มีความไว้วางใจและมีโอกาสทางตลาดระดับของผู้ใช้ระบบสารสนเทศโดยทั่วไปจำแนกออกเป็นผู้ปฏิบัติงาน ผู้บริหารระดับปฏิบัติการ ผู้บริหารระดับกลางผู้บริหารระดับสูง

4. ประเภทของระบบสารสนเทศ

สุชาดา กีระนันทน์ (2542) ได้กล่าวว่า ระบบสารสนเทศสามารถแบ่งออกได้ ดังนี้

4.1 ระบบสารสนเทศจำแนกตามประเภทของธุรกิจโดยส่วนใหญ่จะเป็นระบบของสารสนเทศขนาดใหญ่ที่ประกอบด้วยระบบสารสนเทศที่จำแนกตามหน้าที่ย่อยๆ หลายระบบ ตัวอย่างเช่น ระบบสารสนเทศงานบริหารโรงแรม ประกอบด้วยระบบสารสนเทศย่อย ได้แก่ ระบบสำรองห้องพัก ระบบบัญชี ระบบจัดการห้องพักและระบบบริหารงานบุคคล

4.2 ระบบสารสนเทศจำแนกตามหน้าที่ของงาน ซึ่งในแต่ละส่วนระบบจะสามารถประกอบด้วยระบบสารสนเทศย่อยๆ ที่เป็นกิจกรรมของงานหลัก เช่น ระบบสารสนเทศจัดการทรัพยากรมนุษย์ ประกอบด้วยระบบย่อย ได้แก่ ระบบจัดการข้อมูลพนักงาน ระบบการสรรหาและคัดเลือก ระบบฝึกอบรม ระบบประเมินผลและระบบสวัสดิการ

4.4 ระบบสารสนเทศจำแนกตามลักษณะการดำเนินงาน ผู้บริหารในองค์การระดับที่แตกต่างกัน มีความต้องการในการใช้ระบบสารสนเทศที่แตกต่างกัน ดังนั้นระบบสารสนเทศจึงได้ถูกออกแบบให้มีความสอดคล้องกับลักษณะงานและระดับของผู้ใช้งานเพื่อให้สอดคล้องกับการนำสารสนเทศไปใช้ประกอบการบริหารและตัดสินใจ โดยทั่วไประบบสารสนเทศที่อิงคอมพิวเตอร์แบ่งออกเป็น 6 ประเภท คือ

4.4.1 ระบบสารสนเทศประมวลผลธุรกรรม (Transaction Processing Systems: TPS) เป็นระบบที่มีการประมวลผลที่รวดเร็ว ลดค่าใช้จ่ายและทำหน้าที่รวบรวม บันทึกข้อมูลในแฟ้มข้อมูลหรือฐานข้อมูลและประมวลผลข้อมูลที่เกิดจากการทำธุรกรรมและการปฏิบัติงานประจำขององค์การเพื่อนำไปจัดทำระบบสารสนเทศที่เกี่ยวข้องกับข้อมูลนั้นๆ การประมวลผลข้อมูลของ TPS แบ่งเป็น 2 ประเภท คือ การประมวลผลแบบกลุ่มและการประมวลผลแบบทันที

4.4.2 ระบบสารสนเทศเพื่อการจัดการ (Management Information Systems: MIS) จัดทำรายงานในรูปแบบที่แตกต่างกัน สามารถจำแนกได้เป็น 4 ประเภท คือ รายงานที่จัดทำตามระยะเวลาที่กำหนด รายงานสรุป รายงานที่จัดทำตามเงื่อนไขเฉพาะและรายงานที่จัดทำตามต้องการ

4.4.3 ระบบสนับสนุนการตัดสินใจ (Decision Support Systems: DSS) เป็นระบบสารสนเทศที่นำข้อมูลจากฐานข้อมูลต่างๆ มาใช้ในการตัดสินใจ โดยปกติแล้ว TPS และ MIS จะจัดทำรายงานสำหรับควบคุมและกำกับดูแลการปฏิบัติงานทั่วๆไป เพื่อให้องค์การดำเนินงานได้อย่างถูกต้อง

4.4.4 ระบบสารสนเทศสำหรับผู้บริหารระดับสูง (Executive Information Systems: EIS หรือ Executive Support Systems: ESS) เป็นระบบสารสนเทศที่ช่วยสนับสนุนการวิเคราะห์ปัญหา ศึกษาแนวโน้มและการวางแผนกลยุทธ์ ผู้บริหารสามารถเข้าถึงสารสนเทศโดยกำหนดมุมมองได้ในรูปแบบต่างๆ จึงเป็นระบบที่มีความยืดหยุ่นและคล่องตัวสูง

4.5 ปัญญาประดิษฐ์ (Artificial Intelligence: AI) และระบบผู้เชี่ยวชาญ (Expert Systems: ES) เป็นความพยายามที่จะพัฒนาระบบคอมพิวเตอร์ให้สามารถปฏิบัติงานเหมือนกับมนุษย์หรือเลียนแบบการทำงานของมนุษย์ AI มีหลายสาขา เช่น การประมวลผลภาษาธรรมชาติ ศาสตร์ด้านหุ่นยนต์ ระบบการมองเห็น ระบบการเรียนรู้ เครือข่ายเส้นประสาทและระบบผู้เชี่ยวชาญ

4.6 ระบบสารสนเทศสำนักงาน (Office Information Systems: OIS) หรือระบบสำนักงานอัตโนมัติ (Office Automation Systems: OAS) เป็นระบบสารสนเทศที่นำเทคโนโลยีมาประยุกต์ใช้เพื่อช่วยเพิ่มประสิทธิภาพในการทำงานของผู้ปฏิบัติงานและผู้บริหาร ซึ่ง OIS สามารถนำมาช่วยงานในหลายๆ กิจกรรม เช่น การจัดทำเอกสาร รายงาน จดหมายธุรกิจ การส่งข้อความ การบันทึกตารางนัดหมายและการค้นหาข้อมูลจากเว็บเพจ

สรุปว่า ปัจจุบันจะเห็นความสัมพันธ์ระหว่างองค์กรกับระบบสารสนเทศและเทคโนโลยีสารสนเทศชัดเจนมากขึ้นและเนื่องจากการบริหารงานในองค์กรมีหลายระดับ กิจกรรมขององค์กรแต่ละประเภทอาจจะแตกต่างกัน ดังนั้นระบบสารสนเทศของแต่ละองค์กรอาจแบ่งประเภทแตกต่างกันออกไป ขึ้นอยู่กับการพิจารณาจำแนกระบบสารสนเทศตามการสนับสนุนระดับการทำงานในองค์กรนั้นๆ ออกไปได้

5. การวางแผนระบบสารสนเทศในองค์การ

การสร้างระบบสารสนเทศใหม่เป็นสิ่งสำคัญอย่างหนึ่งของกระบวนการวางแผนองค์การ โดยจะต้องมีการพัฒนาแผนระบบสารสนเทศให้สนับสนุนกับแผนรวมขององค์การทั้งหมด ซึ่งองค์กรควรจะมีแผนกลยุทธ์ขององค์กรก่อนเพื่อใช้เป็นแนวทางในการกำหนดแผนกลยุทธ์ด้านระบบสารสนเทศให้รองรับกับแผนกลยุทธ์ขององค์การ จากนั้นจึงกำหนดแผนปฏิบัติการและโครงสร้างด้านสารสนเทศเพื่อนำมาใช้ในองค์การต่อไปโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ (IT) ความหมายครอบคลุมทั้งทางด้านเทคนิคและทางด้านการบริหารในด้านเทคนิคหมายความรวมถึง ฮาร์ดแวร์ซอฟต์แวร์ เครือข่ายและฐานข้อมูล ส่วนด้านการจัดการ คือการดำเนินงานของหน่วยงานที่รับผิดชอบด้านคอมพิวเตอร์ เช่น ศูนย์คอมพิวเตอร์ บทบาทหน้าที่ของผู้บริหารที่เกี่ยวข้อง การตัดสินใจเกี่ยวกับระบบสารสนเทศ เป็นต้น

5.1 แผนกลยุทธ์ด้านระบบสารสนเทศ

เป็นการกำหนดวัตถุประสงค์ระยะยาวเกี่ยวกับโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ และการริเริ่มในการนำระบบสารสนเทศมาใช้ในการดำเนินงานให้บรรลุวัตถุประสงค์ขององค์การแผนกลยุทธ์ด้านระบบสารสนเทศ มีลักษณะ 3 ประการคือ

- แผนกลยุทธ์ด้านระบบสารสนเทศจะต้องมีสัมพันธ์กับแผนกลยุทธ์ของหน่วยงานนั้นๆ

- แผนกลยุทธ์ด้านระบบสารสนเทศควรที่จะมีการกำหนดโครงสร้างด้านเทคโนโลยี (IT Architecture) ซึ่งต้องทำให้ฐานข้อมูล แอพพลิเคชั่นและผู้ใช้มีการเชื่อมโยงเป็นระบบเดียวกัน

- มีการจัดสรรทรัพยากรด้านการพัฒนาระบบสารสนเทศ ให้สำเร็จตามเวลาและทำตามหน้าที่ที่กำหนดไว้

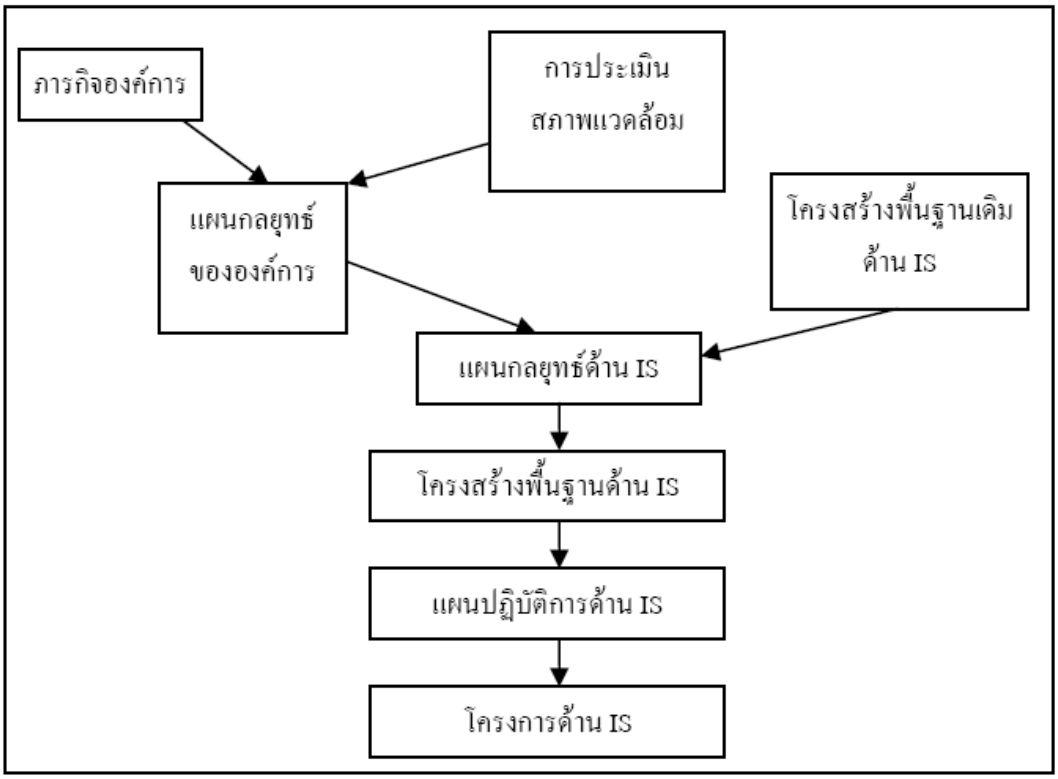
5.2 แผนปฏิบัติการด้านระบบสารสนเทศ

แผนปฏิบัติการด้านระบบสารสนเทศประกอบด้วย พันธกิจของระบบสารสนเทศ สิ่งแวดล้อมของระบบสารสนเทศ เป็นการกล่าวถึงความจำเป็นด้านข่าวสารของหน่วยงานต่างๆ วัตถุประสงค์ของระบบสารสนเทศและข้อจำกัดของระบบสารสนเทศ ทั้งข้อจำกัดทางด้านเทคโนโลยีด้านการงานและด้านบุคลากร ความจำเป็นของระบบในระยะยาวแผนระยะสั้น

5.3 กระบวนการวางแผนระบบสารสนเทศ

วิสัยทัศน์และแผนกลยุทธ์ขององค์กร วิสัยทัศน์ องค์กรกำลังมุ่งไปในทิศทางใด แผนกลยุทธ์ องค์กรจะเดินไปตามทิศทางที่กำหนดไว้อย่างไรระบบสารสนเทศจะสนับสนุนวิสัยทัศน์และกลยุทธ์ขององค์กรอย่างไร ระบบสารสนเทศจะมีบทบาทในการสนับสนุนวิสัยทัศน์ขององค์กรอย่างไร ระบบสารสนเทศเดิมเป็นอย่างไร แผนระบบสารสนเทศในปัจจุบันเป็นอย่างไร แผนระบบสารสนเทศในอนาคตจะพัฒนาในลักษณะอย่างไร

สรุปว่า ระบบสารสนเทศในปัจจุบัน ได้สนับสนุนองค์การมากน้อยเพียงไร มีความเหมาะสมหรือไม่ มีจุดอ่อนจุดแข็ง ควรจะปรับปรุงระบบปัจจุบันอย่างไร มีข้อเสนอแนะ หลักการและเหตุผล ความสามารถของระบบใหม่ฮาร์ดแวร์ซอฟต์แวร์ข้อมูลและการสื่อสารข้อมูลอย่างไรนั้น พร้อมทั้งกลยุทธ์ทางการบริหารแผนการจัดหา ช่วงเวลาดำเนินการ การจัดโครงสร้างองค์การใหม่การปรับปรุงระบบงานภายในองค์การ การควบคุม ฝึกอบรมกลยุทธ์ด้านบุคลากรและแผนปฏิบัติการ ปัญหาที่คาดว่าจะเกิดขึ้นมา รายงานความก้าวหน้าของระบบสารสนเทศด้านงบประมาณที่ต้องการใช้ รวมถึงค่าใช้จ่ายทั้งหมดที่จะเกิดขึ้นในโครงการนั้นๆ พอจะสรุปกระบวนการวางแผนระบบสารสนเทศได้ดังแผนภาพนี้



ภาพที่ 3.3 กระบวนการวางแผนระบบสารสนเทศ

ข้อควรระวังในการปฏิบัติงาน

ความปลอดภัยของข้อมูล

สิ่งหนึ่งที่สำคัญสำหรับงานข้อมูลสารสนเทศ คือ การกำหนดสิทธิผู้ใช้งานที่จะสามารถเพิ่ม ลบ แก้ไขข้อมูลและออกรายงานแสดงผลข้อมูลที่จัดเก็บในส่วนของสิทธิที่ตนได้รับ โดยระบบสามารถจำแนกกลุ่มผู้ใช้งานออกได้เป็นหลายๆ ระดับเพื่อการกำหนดสิทธิการใช้งานและการรักษาความปลอดภัยในการนำเสนอข้อมูลออกทางจอภาพหรือรายงาน โดยผู้ดูแลระบบสามารถที่จะควบคุมการทำงานโปรแกรมต่างๆ ให้เกิดประสิทธิภาพสูงสุด เช่น การให้บริการผ่าน Web สำหรับนักศึกษาหรืออาจารย์ สามารถรองรับมาตรฐาน SSL ได้ โดยการรักษาความปลอดภัยข้อมูลของระบบได้ดังต่อไปนี้

1. การตรวจสอบรหัสผ่าน

การตรวจสอบรหัสผ่าน มีไว้เพื่อตรวจสอบเจ้าหน้าที่ ที่ต้องการเข้ามาใช้งานระบบ โดยระบบจะตรวจสอบสิทธิ์ต่างๆ ในการใช้งานข้อมูลตามกลุ่มผู้ใช้งาน เช่น สิทธิ์ในการใช้งานระบบงานสิทธิ์ในการบันทึกข้อมูลเพิ่ม ลบ แก้ไขหรือแสดงรายงานและสิทธิ์การเข้าใช้งานระบบเป็นต้น นอกจากนี้ระบบจะป้องกันมิให้ผู้ใช้งานที่ไม่ทราบรหัสผ่านเข้ามาใช้งานระบบได้ คือ มีการ

ตัดสิทธิ์การเข้าระบบถ้าบันทึกผิดเกินกำหนดที่ตั้งค่าไว้ หากผู้ใช้งานลืมรหัส Admin ต้อง Reset รหัสผ่านให้ใหม่เท่านั้นและระบบสามารถกำหนดนโยบายบังคับให้ผู้ใช้สามารถเปลี่ยนรหัสผ่านหรือกำหนดช่วงเวลาในการเปลี่ยนรหัสผ่านหรือกำหนดช่วงระยะเวลาการเข้าใช้งานในระบบได้อย่างสมบูรณ์

2. อนุมัติการใช้งานเครื่องที่ถูกล็อคสิทธิ์

สำหรับผู้ใช้งานที่ไม่ทราบรหัสผ่านเข้ามาใช้งานระบบหรือจำรหัสผ่านไม่ได้และได้ใส่รหัสผ่านผิดเกินกำหนด ระบบจะมีการตัดสิทธิ์การเข้าระบบ ซึ่งผู้ใช้งานสำหรับกลุ่มที่มีสิทธิ์ในการปลดล็อค เช่น เจ้าหน้าที่ดูแลระบบ (Administrator) จะเป็นผู้ที่อนุมัติการใช้งานให้กับบุคคลที่ถูกตัดสิทธิ์เหล่านั้นได้

3. ตรวจสอบการทำงาน

ในส่วนของฐานข้อมูลจะมีการเก็บข้อมูลการเพิ่ม ลบ ต่างๆ จากผู้ใช้งานในส่วนที่เกี่ยวข้องกับข้อมูลที่สำคัญไว้ในฐานข้อมูล เช่น เงินเดือน การเปลี่ยนแปลงประวัติ โดยชื่อตาราง (Table) จะตามท้ายด้วย xxxxLog การกำหนดการตรวจสอบเป็นการกำหนดระยะเวลาในการเก็บ Log การทำงานและการเข้าใช้งานโปรแกรมของแต่ละ User ระบบงานได้ออกแบบระบบงานให้มีความสัมพันธ์ในการใช้งานระหว่างหน่วยงานต่างๆ ซึ่งผู้ดูแลระบบจำเป็นต้องเข้าใจถึงโครงสร้างออกแบบการทำงานเพื่อให้ใช้งานระบบได้อย่างมีประสิทธิภาพสูงสุด สามารถที่จะวางแผนเริ่มต้นระบบและกำหนดสิทธิ์การใช้งานให้กับกลุ่มบุคคลต่างๆ ได้อย่างมีประสิทธิภาพ

4. สิทธิ์การใช้งาน (Authorization System)

เมนูโปรแกรม–เมนูโปรแกรม เป็นส่วนกำหนดรหัสและชื่อให้แต่ละโปรแกรมในระบบ ซึ่งจะเป็นส่วนที่สามารถกำหนดสิทธิ์การใช้งานข้อมูลได้ เช่น สามารถให้สิทธิ์การเพิ่ม ลบ แก้ไขรายการเมนูภายในระบบ

กลุ่มผู้ใช้งาน–การกำหนดกลุ่มผู้ใช้งาน มีวัตถุประสงค์ในการแบ่งกลุ่มของผู้ใช้งานเพื่อให้สิทธิ์ในการใช้งานระบบงาน เช่น การเพิ่มข้อมูล ลบ แก้ไข สอบถามหรือพิมพ์รายงานเป็นต้น

ผู้ใช้งาน–ผู้ใช้งานในระบบ สามารถจำแนกประเภทบุคลากร กำหนดรหัสผ่าน กำหนดกลุ่มผู้ใช้งานและบันทึกสิทธิ์การทำงานในระดับข้อมูลหน่วยงาน

สิทธิ์การใช้งานระบบ–สิทธิ์การใช้งานโปรแกรม เป็นการกำหนดสิทธิ์ให้กลุ่มผู้ใช้งานสามารถมองเห็นหรือเรียกใช้งานโปรแกรมต่างๆ ในระบบและสามารถกำหนดว่าในแต่ละโปรแกรมนั้น จะสามารถบันทึก เพิ่ม ลบ แก้ไขหรือพิมพ์รายงานข้อมูลได้

แนวคิดและงานวิจัยที่เกี่ยวข้อง

ชนาธิป ใจดีและประวิทย์ บุญมี (2551) ได้ทำการศึกษาวิจัย เรื่อง ระบบจัดการสารสนเทศ พบว่า เพื่อให้การทำงานบางส่วนในองค์กรมีการดำเนินงานอย่างสะดวก รวดเร็ว มีประสิทธิภาพ จึงได้มีแนวคิดที่จะจัดทำระบบเพื่ออำนวยความสะดวกให้กับบุคลากรในองค์กรในส่วนของการทำเรื่องการลา การบันทึกเวลาการทำงาน การจองห้องประชุม เป็นต้น โดยระบบจะกำหนดสิทธิ์การใช้งานตามผู้ใช้แต่ละคนผู้ใช้งานระบบจะมีสิทธิ์ในการเข้าใช้งานระบบที่แตกต่างกัน ขึ้นอยู่ที่การกำหนดสิทธิ์ให้แต่ละบุคคล ซึ่งในระบบจัดการสารสนเทศนี้จะมีผู้ใช้อยู่ 3 ส่วน ได้แก่ พนักงาน เจ้าหน้าที่ส่วนกลางและผู้ดูแลระบบ

พนักงานจะมีการกำหนดสิทธิ์ให้สามารถเข้าใช้งานระบบเพื่อทำเรื่องการลา ตรวจสอบสถานการณ์ลาบันทึกเวลาทำงาน จองห้องประชุมและแก้ไขข้อมูลส่วนตัว ในระบบได้เท่านั้น ส่วนเจ้าหน้าที่จะสามารถจัดการเวลาทำงาน อนุมัติการลา อนุมัติการจองห้องประชุมได้และผู้ดูแลระบบจะสามารถเข้าใช้งานระบบในส่วนของจัดการสมาชิกของระบบ

โสภิษฐ์ อ่อนแก้ว (2554) ได้ทำการศึกษาวิจัย เรื่อง ออกแบบและพัฒนาระบบสารสนเทศเพื่อการจัดการความรู้สำหรับ องค์การภาครัฐ ด้วยปัจจุบันเทคโนโลยีมีบทบาทสำคัญต่อการจัดการความรู้ ซึ่งจะเป็นตัวขับเคลื่อนหลักขององค์การ เพื่อให้องค์การประสบความสำเร็จ ภาครัฐได้ให้ความสำคัญกับการจัดการความรู้เพื่อให้เกิดการพัฒนาความรู้ ความสามารถและการเรียนรู้ร่วมกันของบุคลากร ในพระราชกฤษฎีกาว่าด้วยหลักเกณฑ์และวิธีการบริหารกิจการ บ้านเมืองที่ดี พ.ศ. 2546 ได้กำหนดไว้ในมาตรา 11 ให้มีการส่งเสริมการใช้เทคโนโลยีสารสนเทศสนับสนุนการจัดการความรู้ เพื่อให้เกิดการเรียนรู้แลกเปลี่ยนข้อมูลระหว่างกันได้อย่างมีเอกภาพและเกิดประสิทธิผลต่อการปฏิบัติงาน งานวิจัยนี้จึงมีวัตถุประสงค์เพื่อออกแบบและพัฒนาระบบสารสนเทศเพื่อการจัดการความรู้สำหรับองค์การภาครัฐ โดยเลือกใช้วิจัยและพัฒนา ซึ่งมีขั้นตอนการดำเนินการวิจัย ดังนี้ 1) ศึกษาสถานภาพและความต้องระบบสารสนเทศเพื่อการจัดการความรู้สำหรับองค์การภาครัฐด้วยวิธีการสังเคราะห์ข้อมูลจากเอกสาร งานวิจัยที่เกี่ยวข้องและการสัมภาษณ์ผู้บริหาร จำนวน 10 คน ได้เลือกใช้วิธีการสุ่มตัวอย่างแบบเจาะจง (Purposive Sampling) จากกลุ่มประชากรในองค์การภาครัฐจำนวน 10 แห่ง เพื่อให้ได้เป็นองค์ความรู้ใหม่ 2) นำองค์ความรู้ใหม่ที่ได้จากแนวคิดของ ผู้วิจัยมาทำการออกแบบระบบสารสนเทศเพื่อการจัดการความรู้สำหรับองค์การภาครัฐและให้ผู้เชี่ยวชาญด้านเทคโนโลยีสารสนเทศและการสื่อสาร จำนวน 5 คน ด้านการจัดการความรู้ จำนวน 5 คน และด้านการวิจัย จำนวน 5 คน รวมเป็น 15 คน ซึ่งได้มาจากการสุ่มตัวอย่างแบบเจาะจง (Purposive Sampling) ทำการตรวจสอบร่างรูปแบบ ระบบสารสนเทศเพื่อการจัดการความรู้สำหรับองค์การภาครัฐ ด้วยวิธีการสนทนากลุ่ม (Focus Group Discussion) และผู้วิจัยได้ทำการปรับปรุง

รูปแบบตามข้อเสนอแนะของผู้เชี่ยวชาญที่เป็นฉันทามติ เพื่อให้ได้รูปแบบที่สมบูรณ์ และเหมาะสม 3) นำผลที่ได้มาพัฒนาระบบสารสนเทศเพื่อการจัดการความรู้สำหรับองค์การภาครัฐ ตามแนวทางทฤษฎีวงจรการพัฒนาระบบ (System Development Life Cycle: SDLC) และประเมินประสิทธิภาพระบบ โดยใช้โปรแกรมคอมพิวเตอร์ SPSS มาวิเคราะห์หาค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานจากแบบประเมินประสิทธิภาพและทดสอบสมมติฐาน

ผลการวิจัยพบว่า 1) ผลการศึกษาสถานภาพและความต้องการระบบสารสนเทศเพื่อการจัดการความรู้สำหรับองค์การภาครัฐ คือ บุคลากรในองค์การภาครัฐต้องการจัดเก็บข้อมูลองค์ความรู้ของผู้บริหารไว้ในระบบสารสนเทศ เพื่อป้องกันการสูญหายไปจากองค์การเมื่อผู้นั้นลาออกเกษียณหรือตายไปกับต้องการเชื่อมโยงบูรณาการข้อมูลความรู้ระหว่าง หน่วยงานภาครัฐเพื่อให้เกิดการแลกเปลี่ยนเรียนรู้ร่วมกันและเพื่อเป็นการพัฒนาบุคลากรให้มีประสิทธิภาพ 2) ผลการออกแบบระบบสารสนเทศเพื่อการจัดการความรู้สำหรับองค์การภาครัฐในรูปแบบใหม่ตามแนวคิดของผู้วิจัยที่ได้จากการสังเคราะห์เนื้อหาได้รูปแบบระบบสารสนเทศเพื่อการจัดการความรู้สำหรับองค์การภาครัฐและนำรูปแบบระบบมาพัฒนาระบบสารสนเทศเพื่อการจัดการความรู้สำหรับองค์การภาครัฐพร้อมทดสอบการใช้งาน จึงได้ระบบสารสนเทศเพื่อการจัดการความรู้สำหรับองค์การภาครัฐ 3) ประเมินประสิทธิภาพการท างานของระบบจากกลุ่มตัวอย่างที่ 2 คือ กลุ่มเทคนิคมีความคิดเห็นว่าระบบ มีประสิทธิภาพสูงเฉลี่ยที่ 3.9168 และจากกลุ่มตัวอย่างที่ 3 คือ กลุ่มผู้ใช้งานมีความคิดเห็นว่าระบบมีประสิทธิภาพสูง เฉลี่ยที่ 3.5147 เมื่อเปรียบเทียบกับเกณฑ์ระดับคะแนนที่กำหนดไว้ อยู่ในช่วงระดับคะแนนระหว่าง 3.50-4.49 ระบบมีประสิทธิภาพสูงและผลการทดสอบสมมติฐานยอมรับสมมติฐาน เพราะความคิดเห็นของกลุ่มเทคนิคและกลุ่ม ผู้ใช้งานมีความคิดเห็นว่าระบบสารสนเทศเพื่อการจัดการความรู้สำหรับองค์การภาครัฐมีประสิทธิภาพในระดับสูง

ข้อเสนอแนะ 1) เพื่อให้ระบบมีความสมบูรณ์มากขึ้นองค์การภาครัฐต้องสรรหาและนำเข้าองค์ความรู้ที่เหมาะสมกับ องค์การไว้ในระบบเพื่อได้เกิดการแลกเปลี่ยนเรียนรู้ร่วมกันระหว่างองค์การและหากจะนำไปประยุกต์ใช้ให้เหมาะสมกับองค์การจำเป็นต้องศึกษาความต้องการเพิ่มเติมแล้วนำไปพัฒนาต่อยอดเพื่อให้สอดคล้องกับความต้องการขององค์การได้อย่างมีประสิทธิภาพ 2) ผู้วิจัยจะศึกษาเพิ่มเติมเกี่ยวกับความพึงพอใจของผู้ใช้งานระบบสารสนเทศเพื่อการจัดการความรู้สำหรับองค์การภาครัฐจากผู้เข้าใช้บริการด้วยแบบสอบถามผ่านทางอินเตอร์เน็ต

สุมิตรา นวลมีศร (2555) ได้ทำการศึกษาวิจัย เรื่อง การพัฒนาระบบสารสนเทศเพื่อการพยากรณ์ผู้เข้าศึกษาโดยผ่านเครือข่ายอินเทอร์เน็ตการรับสมัครผู้เข้าศึกษาในระดับปริญญาตรีในสถาบันอุดมศึกษาบันเป็นสิ่งที่สำคัญเป็นอย่างมากเนื่องจากจะส่งผลโดยตรงต่อการจัดการศึกษาและการวางแผนงบประมาณเพื่อการบริหารสถาบันการศึกษา งานวิจัยนี้จึงพัฒนาระบบสารสนเทศเพื่อการพยากรณ์ผู้เข้าศึกษาโดยผ่านเครือข่ายอินเทอร์เน็ตเพื่อช่วยในการพยากรณ์ผู้เข้าศึกษาได้อย่างถูกต้องและแม่นยำการดำเนินการวิจัยผู้วิจัยสร้างและทดสอบการตัวแบบการพยากรณ์ผู้เข้าศึกษา โดยใช้กฎ การจำแนกเทคนิคต้นไม้ตัดสินใจด้วยวิธีการตรวจสอบไขว้ จำนวน 3 ตัวแบบ วิธีการแบ่งข้อมูล แบบสุ่มด้วยการแบ่งร้อยละ จำนวน 3 ตัวแบบและวิธีการแบ่งข้อมูลสร้างตัวแบบและทดสอบออก จากการนับ จำนวน 1 ตัวแบบรวมทั้งสิ้น 7 ตัวแบบการพยากรณ์ ผลจากการศึกษาพบว่า วิธีการแบ่งข้อมูลสร้างตัวแบบและทดสอบออกจากกันได้ค่าประสิทธิภาพต่างๆ สูงกว่าตัวแบบอื่นๆ โดยมีค่าความถูกต้องเท่ากับ 94% ค่าความแม่นยา เท่ากับ 94.30% ค่าความระลึกเท่ากับ 94% และค่าความถ่วงดุลเท่ากับ 93.70% แสดงว่าตัวแบบที่สร้างด้วยวิธีการแบ่งข้อมูลสร้างตัวแบบและทดสอบออก จากกันมีความถูกต้องและแม่นยำในการพยากรณ์ผู้เข้าศึกษา ผู้วิจัยได้นำกฎการจำแนกเทคนิคต้นไม้ตัดสินใจที่ได้มาพัฒนาเป็นระบบสารสนเทศเพื่อการพยากรณ์ผู้เข้าศึกษาโดยผ่านเครือข่ายอินเทอร์เน็ตโดยทำการประเมินประสิทธิภาพของระบบด้วยค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐาน จากกลุ่มตัวอย่าง 2 กลุ่ม คือ ผู้เชี่ยวชาญจำนวน 4คน และบุคลากรจำนวน 40 คน ผลการประเมินประสิทธิภาพของระบบมีค่าเฉลี่ยจากผู้เชี่ยวชาญ เท่ากับ 4.17 และผลการทดสอบค่าเฉลี่ยจากบุคลากรเท่ากับ 4.34 กล่าวได้ว่า ระบบสารสนเทศเพื่อการพยากรณ์ผู้เข้าศึกษาโดยผ่านเครือข่ายอินเทอร์เน็ตมีประสิทธิภาพอยู่ในเกณฑ์ดีและสามารถนำไปประยุกต์ เพื่อใช้ในการพยากรณ์ผู้เข้าศึกษาได้อย่างมีประสิทธิภาพ

ศิโรรัตน์ ไกรสุริยวงศ์ (2551) ได้ทำการศึกษาวิจัย เรื่อง ความต้องการพัฒนาระบบสารสนเทศเพื่อการบริหารจัดการของครูโรงเรียนเอกชนสังกัดสำนักบริหารงานคณะกรรมการส่งเสริมการศึกษาเอกชน จังหวัดปทุมธานี การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อศึกษาความต้องการพัฒนาระบบสารสนเทศเพื่อการบริหารจัดการของครูโรงเรียนเอกชน สังกัดสำนักบริหารงานคณะกรรมการส่งเสริมการศึกษาเอกชน จังหวัดปทุมธานี และเพื่อเปรียบเทียบความต้องการพัฒนาระบบสารสนเทศเพื่อการบริหารจัดการของครูโรงเรียนเอกชน สังกัดสำนักบริหารงานคณะกรรมการส่งเสริมการศึกษาเอกชน จังหวัดปทุมธานี จำแนกตาม ระดับคุณวุฒิ ประสบการณ์ทำงานและประเภทของโรงเรียนเอกชนที่ครูปฏิบัติงาน ประชากรที่ใช้ในการวิจัยครั้งนี้เป็นครูโรงเรียนเอกชน สังกัดสำนักบริหารงานคณะกรรมการส่งเสริมการศึกษาเอกชน จังหวัดปทุมธานี จำนวน 1,981 คน สุ่มตัวอย่างแบบหลายขั้นตอนได้กลุ่มตัวอย่าง จำนวน 330 คน เครื่องมือที่ใช้ใน

การวิจัยเป็นแบบสอบถาม ลักษณะเป็นแบบมาตราส่วนประมาณค่า 5 ระดับ ที่ผู้วิจัยสร้างขึ้น การเก็บรวบรวมข้อมูลผู้วิจัยไปติดต่อขอรับแบบสอบถามคืนด้วยตนเอง ได้รับแบบสอบถามคืน 330 ชุด คิดเป็นร้อยละ 100 วิเคราะห์ข้อมูลโดยใช้สถิติเชิงพรรณนา (Descriptive Statistics) สถิติที่ใช้คือ ค่าร้อยละ ค่าเฉลี่ย (Mean) ส่วนเบี่ยงเบนมาตรฐาน (Standard Deviation) ส่วนการวิเคราะห์ข้อมูลโดยใช้สถิติเชิงอนุมาน (Inferential Statistics) เพื่อทดสอบสมมุติฐาน (Hypothesis Testing) โดยการวิเคราะห์ความแปรปรวนแบบทางเดียว (One-Way ANOVA)

ผลการวิจัยพบว่า

1. ความต้องการพัฒนาระบบสารสนเทศเพื่อการบริหารจัดการของครูโรงเรียนเอกชน สังกัดสำนักบริหารงานคณะกรรมการส่งเสริมการศึกษาเอกชน จังหวัดปทุมธานี โดยภาพรวมอยู่ในระดับมาก เมื่อพิจารณาเป็นรายด้าน มีค่าเฉลี่ยอยู่ในระดับมากทุกด้าน โดยเรียงลำดับจากมากไปหาน้อย ได้แก่ ด้านการเก็บรวบรวมข้อมูล ด้านการตรวจสอบข้อมูล ด้านการจัดเก็บและการบริการข้อมูล ด้านการนำข้อมูลไปใช้ ด้านการวิเคราะห์ข้อมูล และด้านการประมวลผลข้อมูล

2. การเปรียบเทียบ ความต้องการพัฒนาระบบสารสนเทศเพื่อการบริหารจัดการของครูโรงเรียนเอกชน สังกัดสำนักบริหารงานคณะกรรมการส่งเสริมการศึกษาเอกชน จังหวัดปทุมธานี จำแนกตาม ระดับคุณวุฒิ ประสบการณ์ทำงาน และประเภทของโรงเรียนเอกชนที่ครูปฏิบัติงานในภาพรวมไม่แตกต่างกัน แต่เมื่อพิจารณารายด้านจำแนกตามระดับคุณวุฒิ พบว่าครูโรงเรียนเอกชนที่มีคุณวุฒิสูงกว่าปริญญาตรีมีความต้องการพัฒนาด้านการตรวจสอบข้อมูล ด้านการประมวลผลข้อมูลและด้านการนำข้อมูลไปใช้สูงกว่าครูโรงเรียนเอกชนที่มีคุณวุฒิต่ำกว่าปริญญาตรีอย่างมีนัยสำคัญทางสถิติที่ระดับ .05 เมื่อจำแนกตามประสบการณ์ทำงาน พบว่า ครูโรงเรียนเอกชนที่มีประสบการณ์ทำงานระหว่าง 10-11 ปี มีความต้องการพัฒนาด้านการตรวจสอบข้อมูล ด้านการประมวลผลข้อมูลและด้านการนำข้อมูลไปใช้สูงกว่าครูที่มีประสบการณ์ทำงานระหว่าง 5-10 ปี อย่างมีนัยสำคัญทางสถิติที่ระดับ .05 และเมื่อจำแนกตามประเภทของโรงเรียนเอกชนที่ครูปฏิบัติงาน พบว่า ครูที่ปฏิบัติงานอยู่ในโรงเรียนที่เปิดสอนระดับก่อนประถมศึกษา ถึงมัธยมศึกษามีความต้องการพัฒนาด้านการประมวลผลข้อมูลสูงกว่าครูที่ปฏิบัติงานอยู่ในโรงเรียนเอกชนที่เปิดสอนระดับก่อนประถมศึกษา อย่างมีนัยสำคัญทางสถิติที่ระดับ .05

บทที่ 4
เทคนิคการปฏิบัติงาน

ในการปฏิบัติงานตามคู่มือการกำหนดสิทธิ์การใช้งานของผู้ใช้งานระบบสารสนเทศเพื่อการบริหารมหาวิทยาลัย (MIS: Management Information System) และระบบสารสนเทศเพื่อการบริหารทรัพยากรองค์กร (ERP: Enterprise Resource Resource Planning) ของบุคลากรในมหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา ผู้ปฏิบัติงานด้านระบบสารสนเทศต้องวิเคราะห์ และตรวจสอบเอกสารการขอสิทธิ์ใหม่หรือมีความต้องการเพิ่มเติมจากเดิมที่มีอยู่ด้วยความถูกต้อง แม่นยำ ชัดเจน จึงจำเป็นต้องมีวิธีหรือเทคนิคการกำหนดสิทธิ์การใช้งานระบบให้กับผู้รับบริการได้อย่างถูกต้องโดยมีขั้นตอนและเทคนิคในการปฏิบัติ ดังนี้

กิจกรรม/แผนการปฏิบัติงาน

ตารางที่ 4.1 กิจกรรม/แผนการปฏิบัติงานการกำหนดสิทธิ์การใช้งานของผู้ใช้งานระบบสารสนเทศ

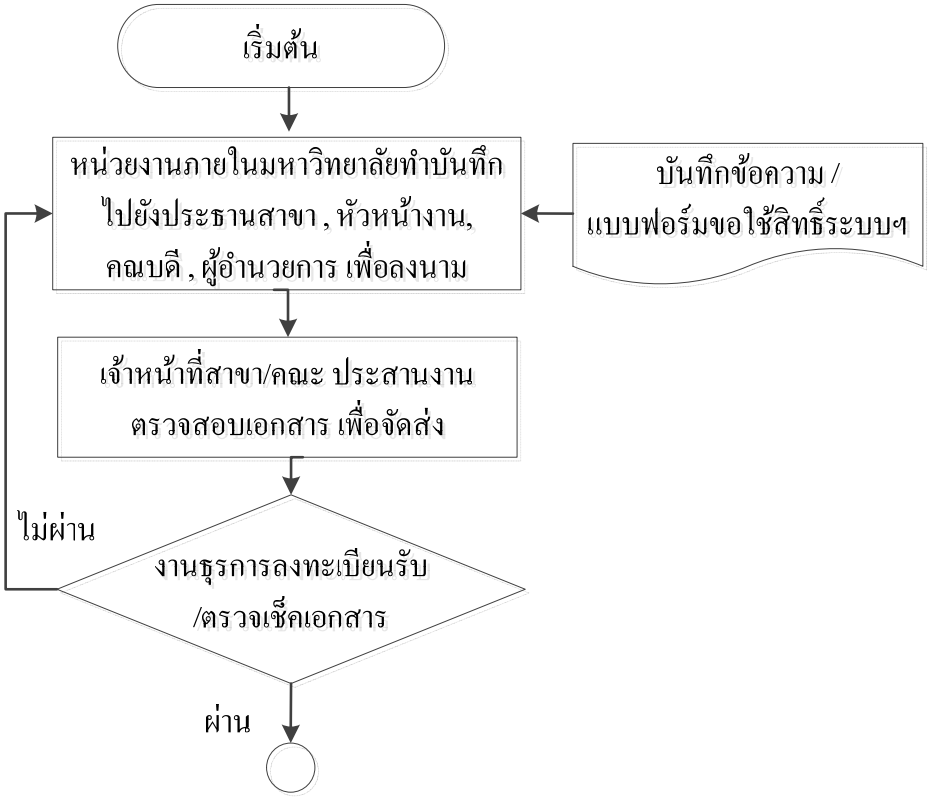
กิจกรรม	เวลาดำเนินการ												หมายเหตุ
	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	
1. บันทึกข้อความหรือกรอกแบบฟอร์มขอใช้สิทธิ์ระบบ (MIS-ERP) - ผ่านประธานสาขาวิชา/หัวหน้างาน เซ็นต์เพื่อให้ความเห็นชอบ - คณบดี/ผู้อำนวยการเซ็นต์ - เจ้าหน้าที่สาขาวิชา/คณะ ประสานงานตรวจสอบเอกสารก่อนส่งเอกสารมายังสำนักคอมพิวเตอร์	←											→	
2. ตรวจสอบความถูกต้อง/ลงนามปฏิบัติงานของบันทึกข้อความ/แบบฟอร์มขอใช้สิทธิ์ระบบ (MIS-ERP)	←											→	

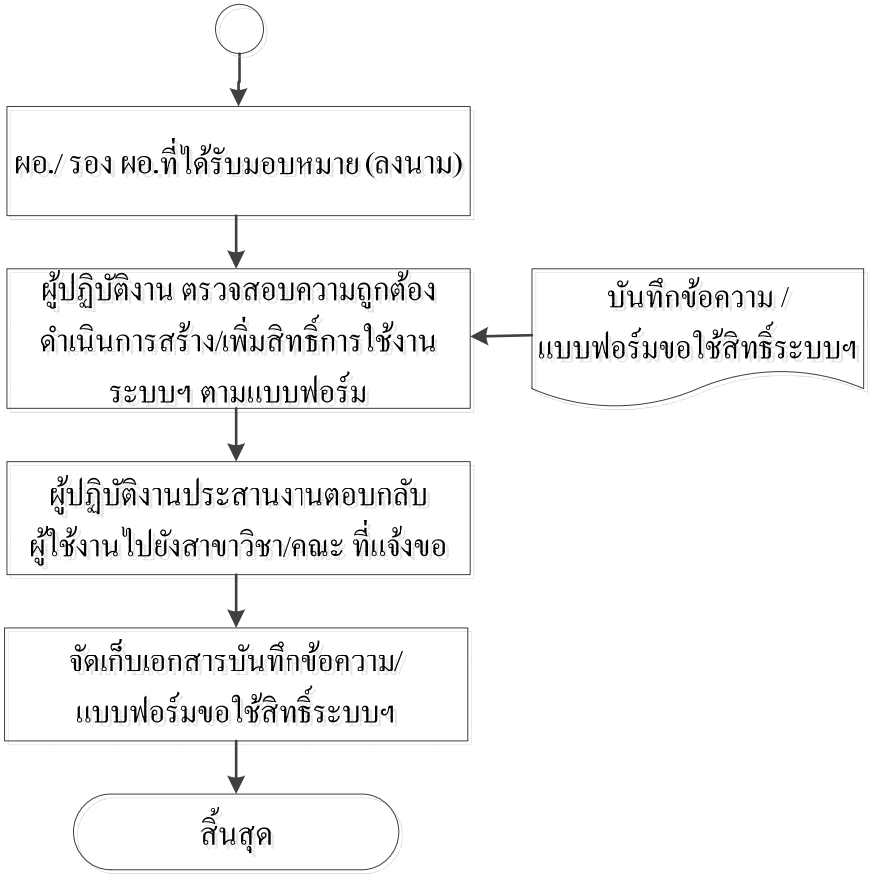
ตารางที่ 4.1 (ต่อ)

กิจกรรม	เวลาดำเนินการ												หมายเหตุ
	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	
3. ดำเนินการสร้าง/เพิ่ม/ยกเลิกสิทธิ์การใช้งานระบบ (MIS-ERP) ตามบันทึกข้อความ/แบบฟอร์มที่ขอมา	←											→	
4. จัดทำบันทึกข้อความตอบกลับ/ โทรกลับเพื่อแจ้งข้อมูลขอใช้สิทธิ์ระบบ (MIS-ERP) ที่ดำเนินการสร้างให้เรียบร้อยแล้ว	←											→	

หลักเกณฑ์การปฏิบัติงานการกำหนดสิทธิ์การใช้งานของผู้ใช้งานระบบสารสนเทศ

จากภาระหน้าที่ที่ได้รับมอบหมาย ผู้เขียนได้เลือกเอางานด้านระบบสารสนเทศ (งานด้านประสานงานและกำหนดสิทธิ์การเข้าใช้งานระบบสารสนเทศ) มาเขียนเป็นคู่มือปฏิบัติงาน โดยมีกระบวนการปฏิบัติงาน ดังภาพที่ 1





ภาพที่ 4.1 ผังแสดงกระบวนการปฏิบัติงานการกำหนดสิทธิ์การใช้งาน ของผู้ใช้งานระบบ (MIS-ERP)

จากผังกระบวนการปฏิบัติงาน ดังกล่าวข้างต้น สามารถนำมาเขียนสรุปกระบวนการที่ผู้รับผิดชอบงานด้านระบบสารสนเทศ จะต้องดำเนินการในการกำหนดสิทธิ์การใช้งานของผู้ใช้งานระบบสารสนเทศให้กับผู้รับบริการ ดังนี้

1. หน่วยงานภายในทำบันทึกไปยังประธานสาขา, หัวหน้างาน, คณบดี, ผู้อำนวยการ เพื่อลงนาม

1.1 บันทึกข้อความ เพื่อขอใช้สิทธิ์ใหม่ เพิ่มเติม หรือยกเลิกการใช้งานระบบสารสนเทศ ที่มีความถูกต้อง และไม่ถูกต้อง

1.1.1 ระบุวันที่ / เดือน / ปี ที่ขอใช้งาน

1.1.2 พิมพ์ชื่อเรื่อง

1.1.3 เรียน ผู้อำนวยการสำนักคอมพิวเตอร์

1.1.4 พิมพ์รายละเอียดเกี่ยวกับเรื่องที่จะขอใช้สิทธิ์ใหม่ เพิ่มเติมหรือยกเลิกการใช้งานระบบสารสนเทศ ซึ่งประกอบด้วย

- ชื่อของสังกัดหน่วยงาน
- รายละเอียดเหตุผลความรับผิดชอบในหน้าที่ที่ต้องใช้งานระบบดังกล่าว
- ระบุชื่อระบบสารสนเทศที่ต้องการใช้งานใหม่/เพิ่มเติม
- ระบุชื่อระบบสารสนเทศที่ทำการยกเลิก/ชื่อผู้ใช้ที่ยกเลิก
- ชื่อ-นามสกุล ภาษาไทยและภาษาอังกฤษ
- รหัสประชาชน ตำแหน่ง
- เบอร์โทรศัพท์ติดต่อกลับของผู้รับผิดชอบ/ผู้ใช้งาน

1.1.5 เสนอประธานสาขา, หัวหน้างาน, คณบดี, ผู้อำนวยการ/สถาบัน /ศูนย์ / สำนัก เพื่อลงนามหนังสือต่อไป

1.1.6 เจ้าหน้าที่ของหน่วยงานภายในดังกล่าว ลงเลขหนังสือออก ที่ ศธ ...../.....

1.1.7 เจ้าหน้าที่ของหน่วยงานภายในดังกล่าว ส่งบันทึกข้อความขอใช้สิทธิ์ใหม่ เพิ่มเติมหรือยกเลิกการใช้งานระบบสารสนเทศ มายังสำนักคอมพิวเตอร์

บันทึกข้อความ

1.1.4

1.1.1

คณะวิทยาศาสตร์และเทคโนโลยี
เลขที่ 141
วันที่ ๑๑ ม.ค. ๒๕๖๑
เวลา 13.00 น.

ส่วนราชการ คณะวิทยาศาสตร์และเทคโนโลยี โทร. ๓๐๐๐ – ๓๐๐๓

ที่ ศธ ๐๕๖๔.๐๘/ **122** 1.1.6 **วันที่** ๑๑ มกราคม ๒๕๖๑

เรื่อง ขอยกเลิกสิทธิ์และขอเปิดสิทธิ์ในการใช้งานระบบ ERP และ MIS 1.1.2

เรียน ผู้อำนวยการสำนักคอมพิวเตอร์ 1.1.3

ด้วยคณะวิทยาศาสตร์และเทคโนโลยีมีการเปลี่ยนประธานสาขาวิชาคณิตศาสตร์และสถิติประยุกต์ใหม่ ตามคำสั่งมหาวิทยาลัยฯ ที่ ๑๙๘๒/๒๕๕๙ ลงวันที่ ๒๓ มิถุนายน ๒๕๕๙ จากเดิมอาจารย์อังคณา จรรยาอดิศัย เป็นอาจารย์ ดร.ธนภัทร เตชาภิรมณ์

ในการนี้จึงใคร่ขอความอนุเคราะห์จากหน่วยงานท่านดังนี้ 1.1.4

๑. ยกเลิกสิทธิ์ของประธานสาขาวิชาเดิม ในการใช้งานระบบ e-Document ในกล่องเอกสารของสาขาวิชาเท่านั้น แต่กล่องเอกสารรายบุคคลยังคงไว้ และยกเลิกสิทธิ์ของประธานสาขาวิชาท่านเดิมในการใช้ระบบ ERP และ MIS (ระบบ ERP ได้แก่ งบประมาณ จัดซื้อ/จัดจ้าง คลังพัสดุ และการเงิน ระบบ MIS ได้แก่ ตารางสอน เป็นต้น)

๒. เปิดสิทธิ์เบื้องต้นที่พึงมีให้ประธานสาขาวิชาใหม่ ในการใช้งานระบบ e-Document ในกล่องเอกสารของสาขาวิชาเท่านั้น และเปิดสิทธิ์เบื้องต้นที่พึงมีให้ประธานสาขาวิชาใหม่ในการใช้ระบบ ERP และ MIS (ระบบ ERP ได้แก่ งบประมาณ จัดซื้อ/จัดจ้าง คลังพัสดุ และการเงิน ระบบ MIS ได้แก่ ตารางสอน เป็นต้น)

จึงเรียนมาเพื่อโปรดพิจารณาให้ความอนุเคราะห์ และขอขอบคุณมา ณ โอกาสนี้

(รองศาสตราจารย์ ดร.สาธิต โกวิทวที) 1.1.5
คณบดีคณะวิทยาศาสตร์และเทคโนโลยี

ขอข้อมูลหรือรายละเอียดต่าง ๆ ได้ที่
ผู้ประสานงาน หัวหน้าสำนักงานคณบดี (คุณศศิภา) 1.1.4

ภาพที่ 4.2 แสดงตัวอย่างการทำบันทึกข้อความจากหน่วยงานต่างๆ ที่ถูกต้อง

1.1.4 ไม่มีเบอร์โทรศัพท์ที่สามารถติดต่อกลับได้

บันทึกข้อความ

ส่วนราชการ คณะวิทยาศาสตร์และเทคโนโลยี

ที่ ศว ๐๕๖๔.๐๘/ว๖๕๘ **วันที่** ๑๒ มิถุนายน ๒๕๖๐

เรื่อง ขอความอนุเคราะห์เปิดสิทธิ์ใช้งานระบบ e-document

สำนักคอมพิวเตอร์ รับที่ 999 16/6/60 เวลา

คณะวิทยาศาสตร์และเทคโนโลยี เลขที่ 1008 รับที่ ๑๓ มิ.ย. ๒๕๖๐

เรียน ผู้อำนวยการสำนักคอมพิวเตอร์

ด้วยคณะวิทยาศาสตร์และเทคโนโลยี มีการเปลี่ยนแปลงผู้ใช้งานในระบบ e-document ในส่วนของสำนักงานคณะวิทยาศาสตร์ฯ เนื่องจากมีบุคลากรที่จะทำงานในส่วนของสำนักงานคณะวิทยาศาสตร์ฯ เพิ่มขึ้น จำนวน ๒ ท่าน คือ นางสาวศิริกาญ แซ่อึ้อ และ นางสาวจรรยา อัมภรัตน์

ในการนี้ จึงใคร่ขอความอนุเคราะห์เปิดสิทธิ์ในการใช้งานสารบรรณ (e-document) ดังนี้

๑. เปิดกล่องสำนักงานคณะวิทยาศาสตร์ฯ (หนังสือภายใน , หนังสือภายนอก , ส่งเรื่องภายใน ฯลฯ)

๒. สามารถนำข้อมูลในระบบแยกลงตามกลุ่มภาระงานที่กำหนดไว้ได้

๓. ยกเลิกสิทธิ์การใช้งานระบบ e-document ของ นางสาวเสาวนีย์ เหลื่อมศรี เนื่องจากได้ลาออกจากคณะวิทยาศาสตร์และเทคโนโลยี แล้ว

จึงเรียนมาเพื่อโปรดพิจารณาให้ความอนุเคราะห์ และขอขอบคุณมา ณ โอกาสนี้

(นางเพลินตา บุญถาวร)
เจ้าหน้าที่บริหารงานทั่วไป

เรียน ผู้อำนวยการสำนักคอมพิวเตอร์
☐ เพื่อโปรดทราบ
☑ เพื่อโปรดพิจารณา
☑ เห็นควร ...

(รองศาสตราจารย์ ดร.สาธิต โกวิทวที)
คณบดีคณะวิทยาศาสตร์และเทคโนโลยี

ภาพที่ 4.3 แสดงตัวอย่างการทำบันทึกข้อความจากหน่วยงานต่างๆ ที่ไม่ถูกต้อง

2. กรอกแบบฟอร์มขอใช้สิทธิ์ระบบ (MIS-ERP)

2.1 ช่องทางการดาวน์โหลดแบบฟอร์มขอใช้สิทธิ์ระบบสารสนเทศ

2.1.1 ทางเว็บไซต์สำนักคอมพิวเตอร์ http://cc.bsru.ac.th

- หัวข้อ ดาวน์โหลด
- ชื่อแบบฟอร์มต่างๆ

ภาพที่ 4.4 หน้าเว็บไซต์สำนักคอมพิวเตอร์ http://cc.bsru.ac.th

2.1.2 ทางเว็บไซต์มหาวิทยาลัย www.bsru.ac.th

- หัวข้อ ดาวน์โหลด
- ชื่อแบบฟอร์มต่างๆ

ภาพที่ 4.5 หน้าเว็บไซต์มหาวิทยาลัย www.bsru.ac.th

2.2 วิธีการกรอกแบบฟอร์มขอใช้สิทธิ์ระบบสารสนเทศต่างๆ (ถูกต้องและไม่ถูกต้อง)

2.2.1 เลือกดาวน์โหลดตามประเภทแบบฟอร์มที่จะขอสิทธิ์ใช้งานระบบต่างๆ

แบบฟอร์มขอใช้สิทธิ์ระบบ ERP

- สำหรับสถานีบริการสารสนเทศ
- สำหรับสาขาวิชา / กอง / งาน
- สำหรับคณะ / สำนัก / สถาบัน
- สำหรับเข้าดู Slip เงินเดือนผ่าน Website

แบบฟอร์มขอใช้สิทธิ์ระบบ [แบ่งตามประเภท]

- ระบบสารบรรณอิเล็กทรอนิกส์ / ระบบแสดงข้อมูลบุคลากร / ระบบบริการการศึกษา (สำหรับบุคลากรเดิม)
- สำหรับอาจารย์ประจำ (ที่บรรจุใหม่)
- สำหรับบุคลากรสายสนับสนุน (ที่บรรจุใหม่)

2.2.2 ชื่อระบบสารสนเทศ

2.2.3 ชื่อหน่วยงาน..... สาขาวิชา.....

2.2.4 เบอร์โทรติดต่อกลับ.....

2.2.5 ลงวันที่.....เดือน.....ปี.....

2.2.6 ชื่อ-นามสกุล (ไทย)

2.2.7 ชื่อ-นามสกุล (อังกฤษ)

2.2.8 รหัสประชาชน สำหรับอาจารย์ประจำ (ที่บรรจุใหม่)

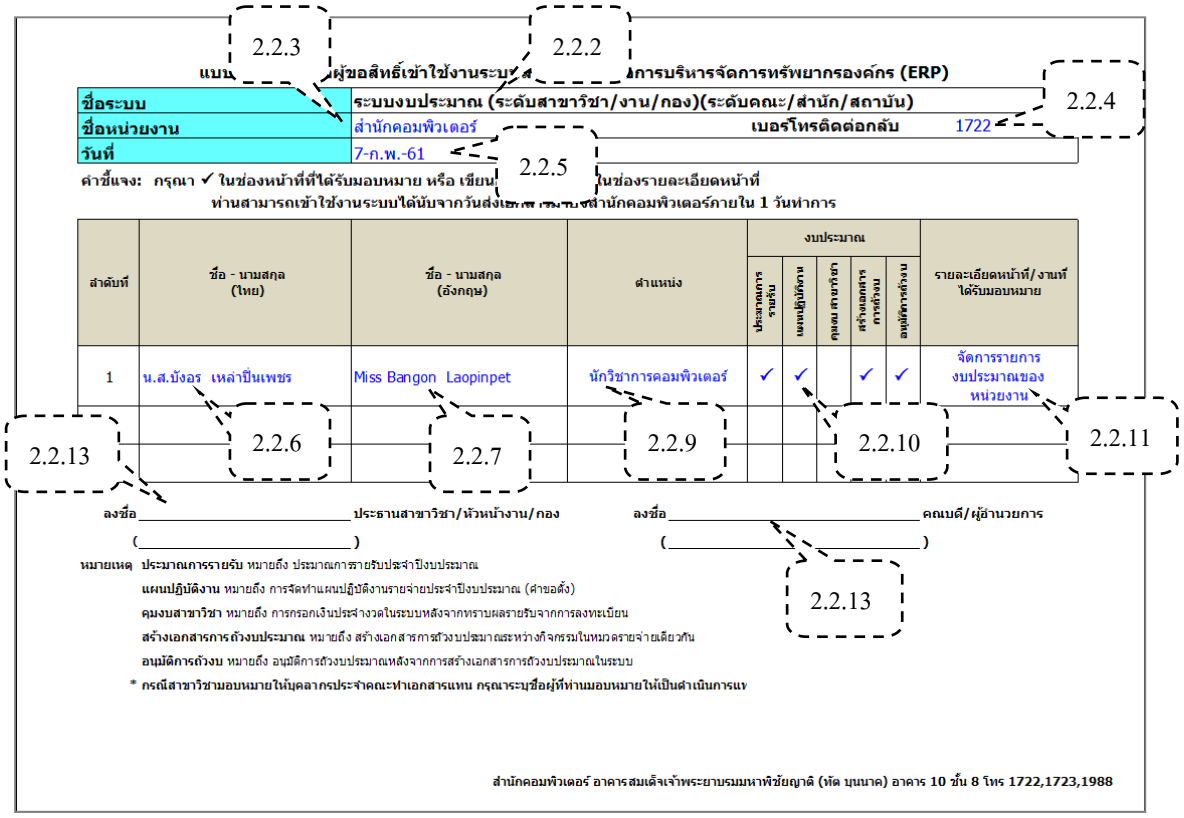
2.2.9 ใส่ตำแหน่งปัจจุบัน

2.2.10 ใส่เครื่องหมาย ✓ ช่องข้อมูลระบบที่ต้องการ

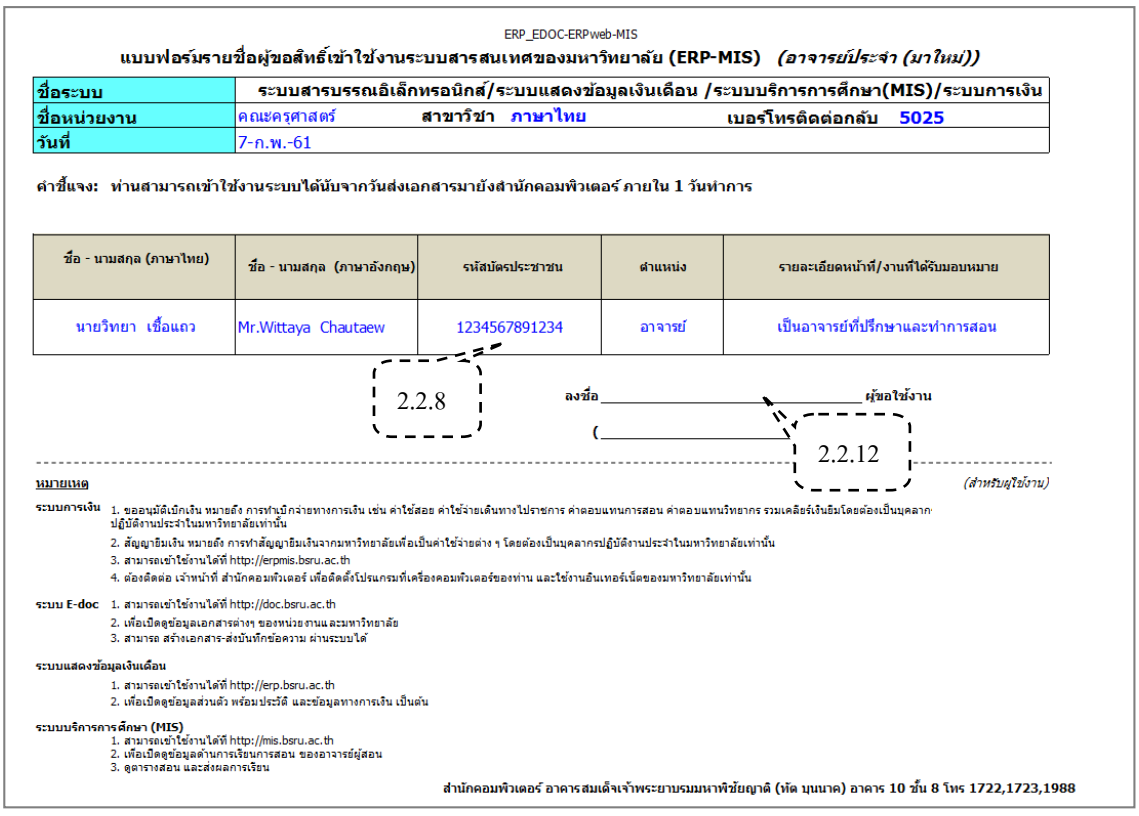
2.2.11 รายละเอียดหน้าที่/งานที่ได้รับมอบหมาย

2.2.12 ลงนาม ผู้ขอใช้งานระบบ

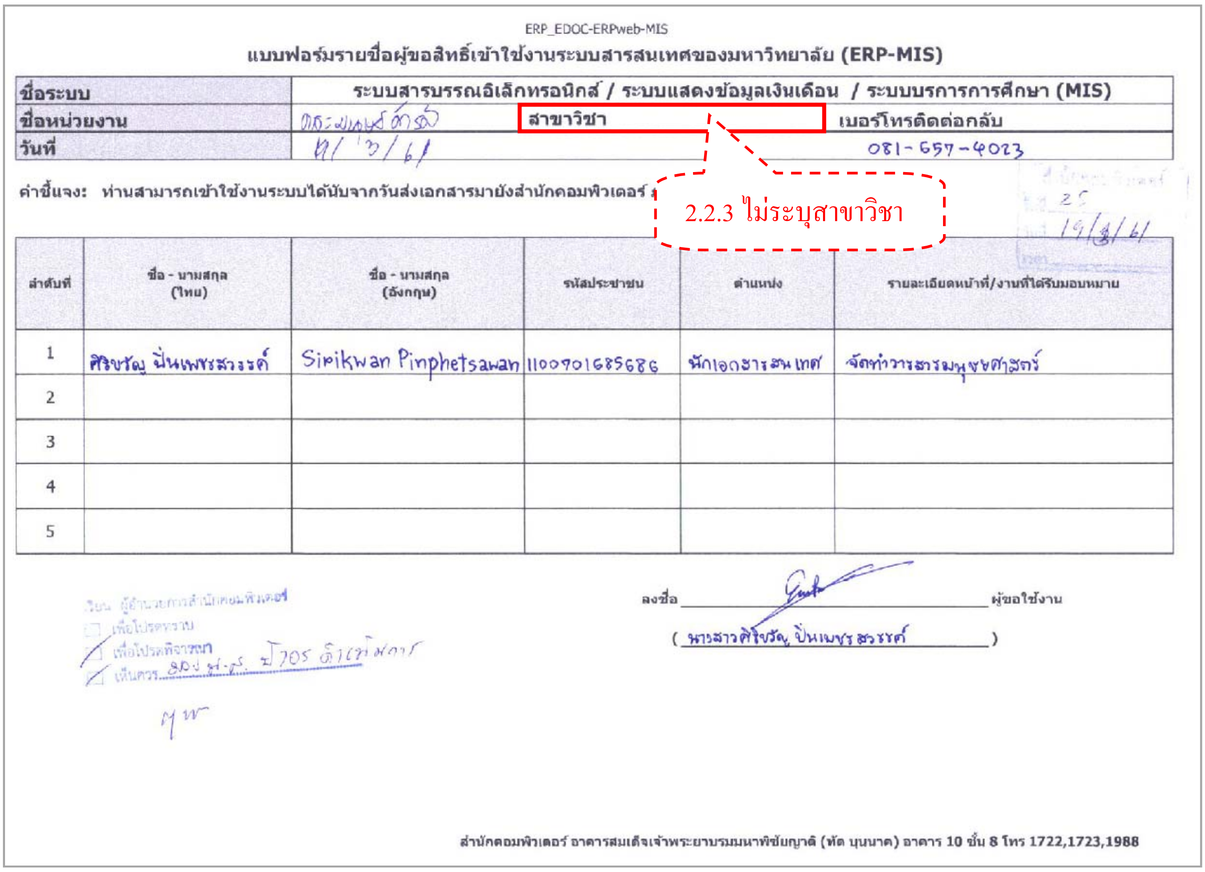
2.2.13 ลงนามโดยผู้บังคับบัญชาของหน่วยงาน เช่น ประธานสาขา, หัวหน้างาน, คณบดี, ผู้อำนวยการ/สถาบัน /ศูนย์ /สำนัก



ภาพที่ 4.6 แสดงตัวอย่างการกรอกแบบฟอร์มขอใช้สิทธิ์ระบบ ERP (ถูกต้อง)



ภาพที่ 4.7 แสดงตัวอย่างการกรอกแบบฟอร์มขอใช้สิทธิ์ระบบสำหรับอาจารย์ประจำ (ที่บรรจุใหม่)


ERP_EDOC-ERPweb-MIS

แบบฟอร์มรายชื่อผู้ขอสิทธิ์เข้าใช้งานระบบสารสนเทศของมหาวิทยาลัย (ERP-MIS)

ชื่อระบบ	ระบบสารบรรณอิเล็กทรอนิกส์ / ระบบแสดงข้อมูลเงินเดือน / ระบบบริการการศึกษา (MIS)		
ชื่อหน่วยงาน	คณะมนุษยศาสตร์	สาขาวิชา	เบอร์โทรติดต่อกลับ
วันที่	8/3/61		081-657-4023

คำชี้แจง: ท่านสามารถเข้าใช้งานระบบได้นับจากวันส่งเอกสารมายังสำนักคอมพิวเตอร์

ลำดับที่	ชื่อ - นามสกุล (ไทย)	ชื่อ - นามสกุล (อังกฤษ)	รหัสประชาชน	ตำแหน่ง	รายละเอียดหน้าที่/งานที่ได้รับมอบหมาย
1	ศิริขวัญ ปิ่นเพชรสวรรค์	Sirikwan Pinphetsawan	1100701685686	นักเอกสารสนเทศ	จัดทำวารสารมนุษยศาสตร์
2					
3					
4					
5					

ลงชื่อ ______________ ผู้ขอใช้งาน

(นางสาวศิริขวัญ ปิ่นเพชรสวรรค์)

สำนักคอมพิวเตอร์ อาคารสมเด็จเจ้าพระยาบรมมหาพิชัยญาติ (ทัต บุนนาค) อาคาร 10 ชั้น 8 โทร 1722,1723,1988

ภาพที่ 4.8 แสดงการกรอกแบบฟอร์มขอใช้งานระบบสารสนเทศ (ERP-MIS) (ที่ไม่ถูกต้อง)

3. งานธุรการลงทะเบียนรับ/ตรวจเช็คเอกสาร (บันทึกข้อความ/แบบฟอร์ม)

3.1 กรณีผ่าน หมายถึง เอกสารตรวจสอบแล้วพบว่ารายละเอียดถูกต้อง ไม่พบข้อผิดพลาดหรือข้อแก้ไข

3.2 กรณีไม่ผ่าน หมายถึง เอกสารตรวจสอบแล้วพบว่าไม่ถูกต้อง พบข้อผิดพลาดหรือพบข้อแก้ไข ก็จะนำเอกสารส่งคืนให้กับหน่วยงาน เพื่อแก้ไขเป็นลำดับต่อไป

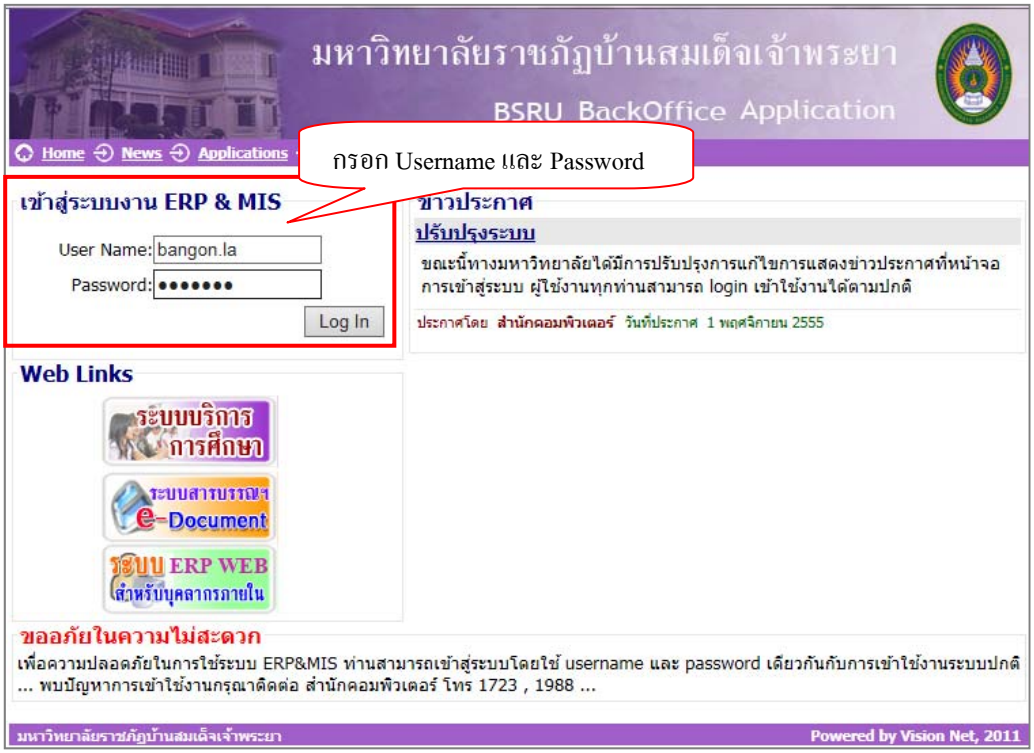
4. นำเสนอ ผู้อำนวยการ/รองผู้อำนวยการ สำนักคอมพิวเตอร์ ที่ได้รับมอบหมายเพื่อเกษียนหนังสือต่อไป

5. ผู้ปฏิบัติงานตรวจสอบความถูกต้อง ดำเนินการสร้างเพิ่มสิทธิ์การใช้งานระบบสารสนเทศ ตามบันทึกข้อความหรือแบบฟอร์มการขอสิทธิ์การใช้งานระบบ

5.1 ตรวจสอบเอกสารบันทึกข้อความ/แบบฟอร์มการขอสิทธิ์การใช้งานระบบ

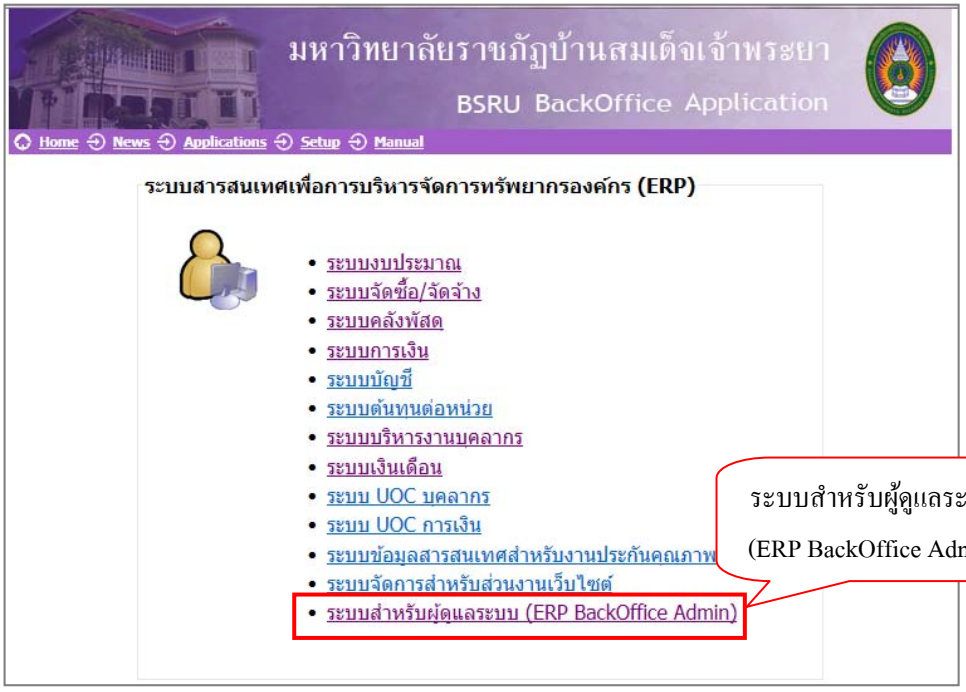
5.2 เข้าระบบสำหรับผู้ปฏิบัติงาน ระบบสารสนเทศเพื่อการบริหารทรัพยากรองค์กร (ERP: Enterprise Resource Resource Planning)

5.2.1 เข้าเว็บไซต์ http://erpmis.bsru.ac.th กรอก Username และ Password



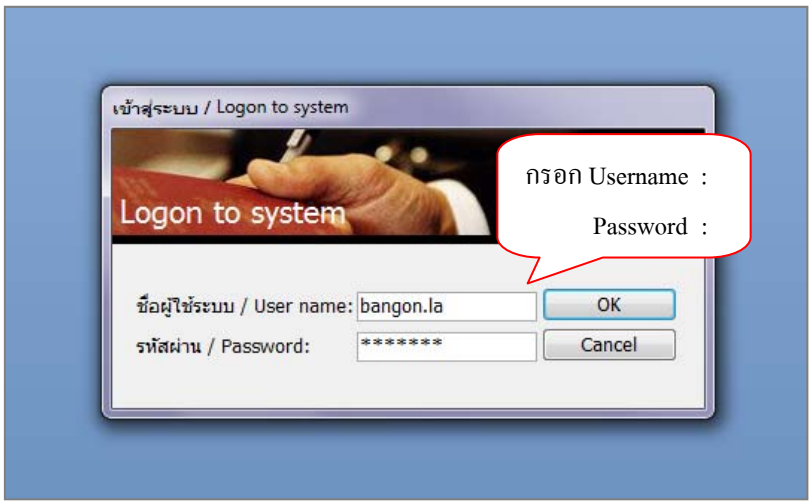
ภาพที่ 4.9 หน้าจอ เว็บไซต์ http://erpmis.bsru.ac.th

5.2.1 คลิกเลือก ระบบสำหรับผู้ดูแลระบบ (ERP BackOffice Admin)



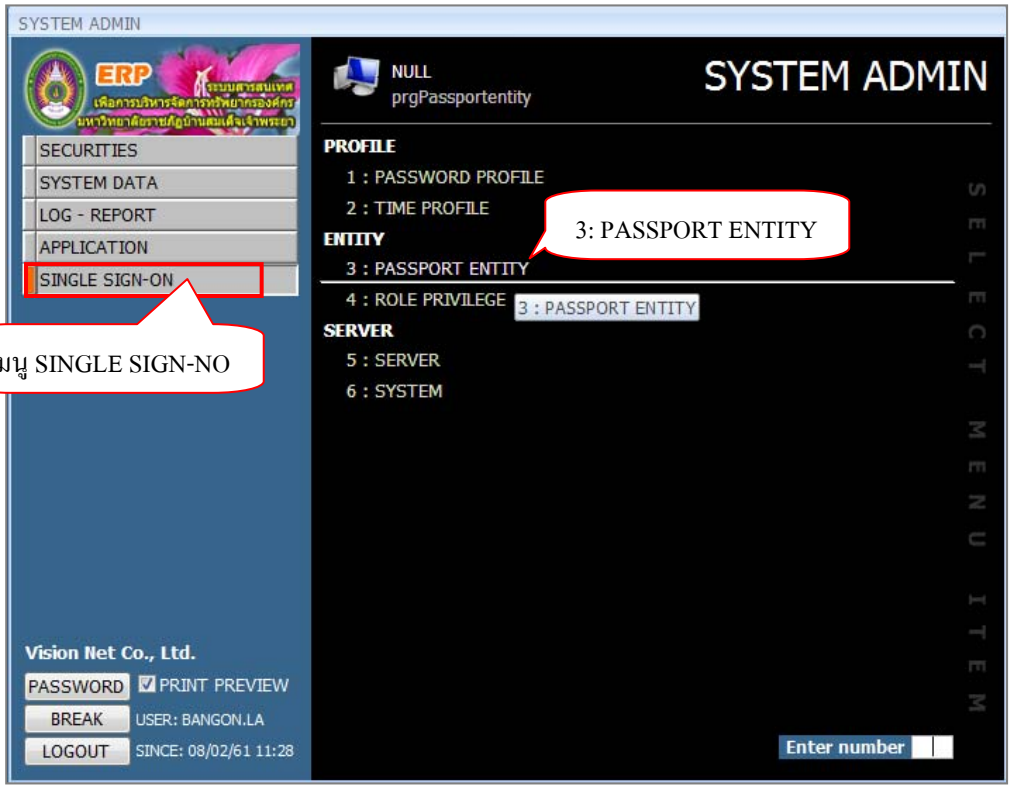
ภาพที่ 4.10 หน้าจอแสดงระบบสารสนเทศเพื่อการบริหารจัดการทรัพยากรองค์กร (ERP)

5.2.2 ระบบจะปรากฏหน้าจออีกรูปแบบหนึ่ง เพื่อให้กรอก Username และ Password เพื่อเข้าสู่ระบบสำหรับผู้ดูแลระบบ



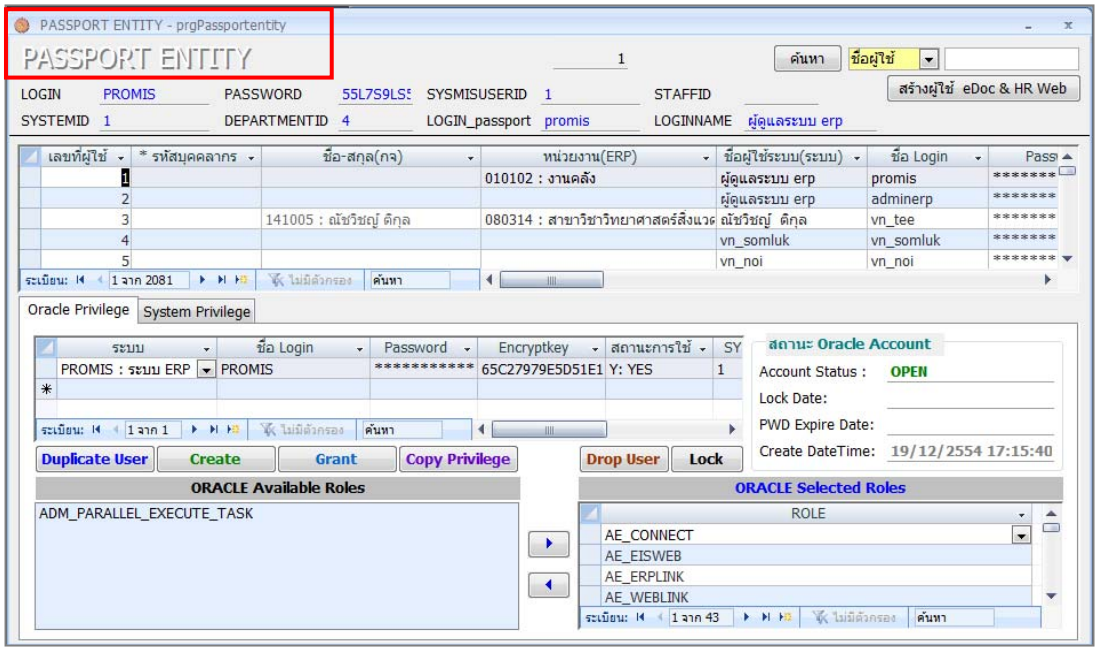
ภาพที่ 4.11 หน้าจอ Login (ERP)

5.2.3 คลิกเลือกที่ เมนู SINGLE SIGN-NO หัวข้อ ENTITY ข้อ 3 : PASSPORT ENTITY



ภาพที่ 4.12 หน้าจอ SYSTEM ADMIN (ERP)

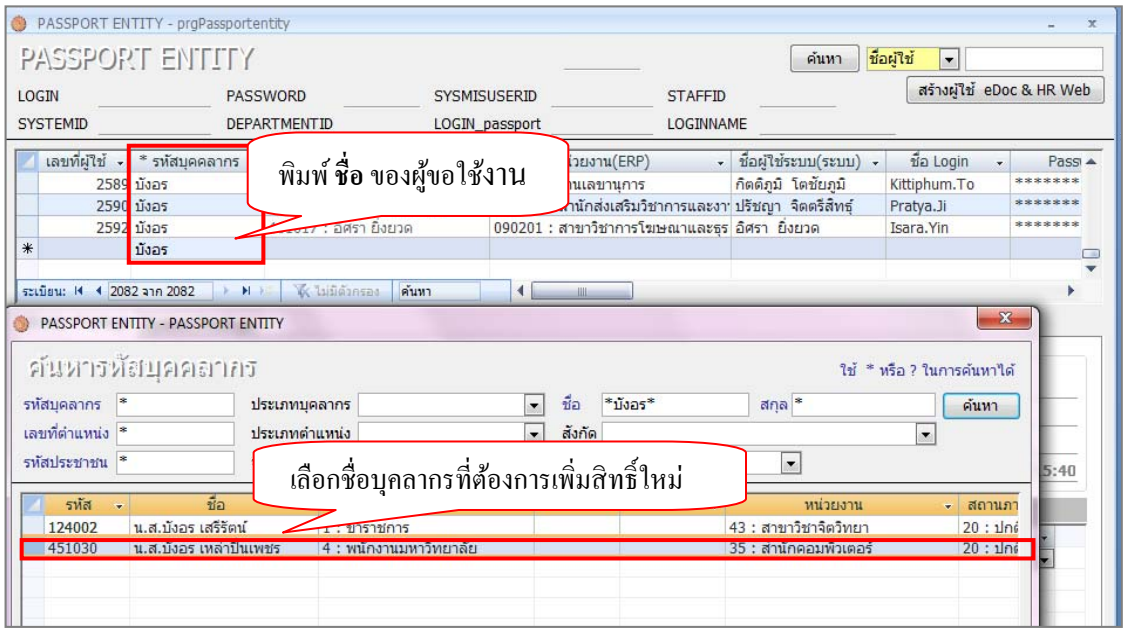
5.2.4 คลิกเลือกที่ ข้อ 3 : PASSPORT ENTITY



ภาพที่ 4.13 หน้าจอ PASSPORT ENTITY (ERP)

5.2.5 วิธีการเพิ่มสิทธิ์ใหม่ของผู้ใช้งาน โดยจะเพิ่มสิทธิ์พื้นฐานของบุคลากรที่ได้

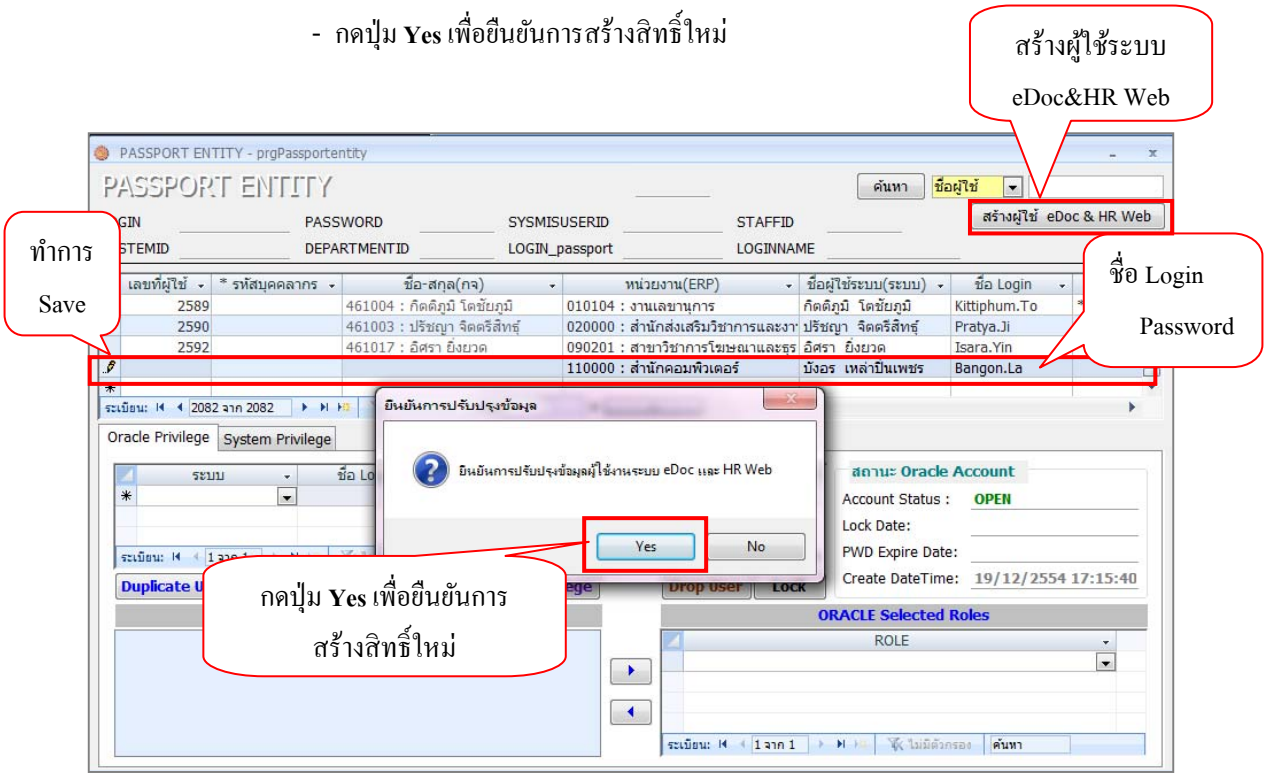
- พิมพ์ **ชื่อ** ของผู้ขอใช้งาน ที่ช่องรหัสบุคลากร
- ในหน้าจอ **ค้นหาบุคลากร** ให้คลิกเลือกชื่อของบุคลากรที่ต้องการเพิ่มสิทธิ์ให้ใหม่



ภาพที่ 4.14 หน้าจอแสดงการพิมพ์ชื่อ เพื่อค้นหาบุคลากร (ERP)

5.2.6 การสร้างสิทธิ์ผู้ใช้งาน โดยจะมีสิทธิ์ใช้งานระบบสารสนเทศพื้นฐาน ดังนี้ ระบบสารบรรณอิเล็กทรอนิกส์ (eDoc) และระบบบุคลากรผ่านเว็บไซต์ (HR Web)

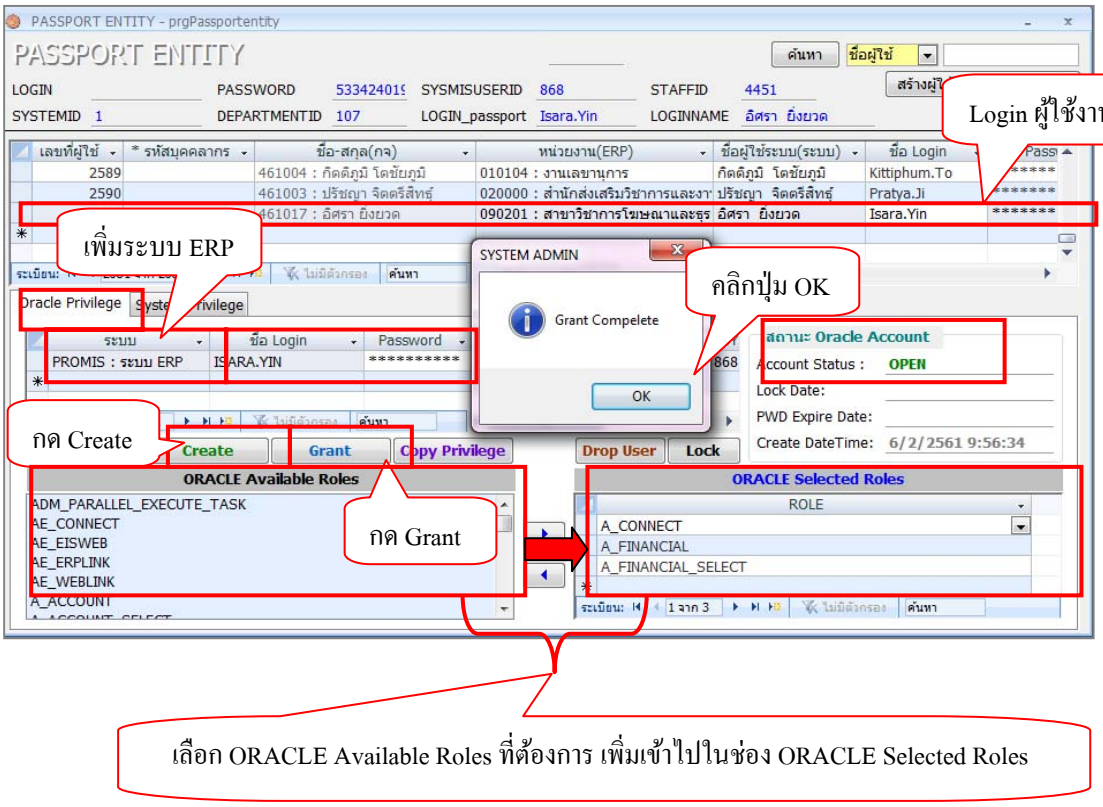
- ได้ ชื่อ Login และ Password
- ทำการ Save สัญลักษณ์รูปดินสอ ที่ปรากฏหน้าระเบียน
- กดปุ่ม **สร้างผู้ใช้ eDoc&HR Web** เพื่อสร้างสิทธิ์ใหม่ระบบ eDoc และ HR Web
- กดปุ่ม **Yes** เพื่อยืนยันการสร้างสิทธิ์ใหม่



ภาพที่ 4.15 หน้าจอ แสดงการสร้างสิทธิ์ผู้ใช้งาน (ERP)

5.2.7 วิธีการเพิ่มสิทธิ์เพิ่มเติมของผู้ใช้งาน โดยจะเพิ่มสิทธิ์ระบบต่างๆ ที่ขอมา เลือกแท็ป Oracle Privilege เพื่อใช้ระบบ ERP

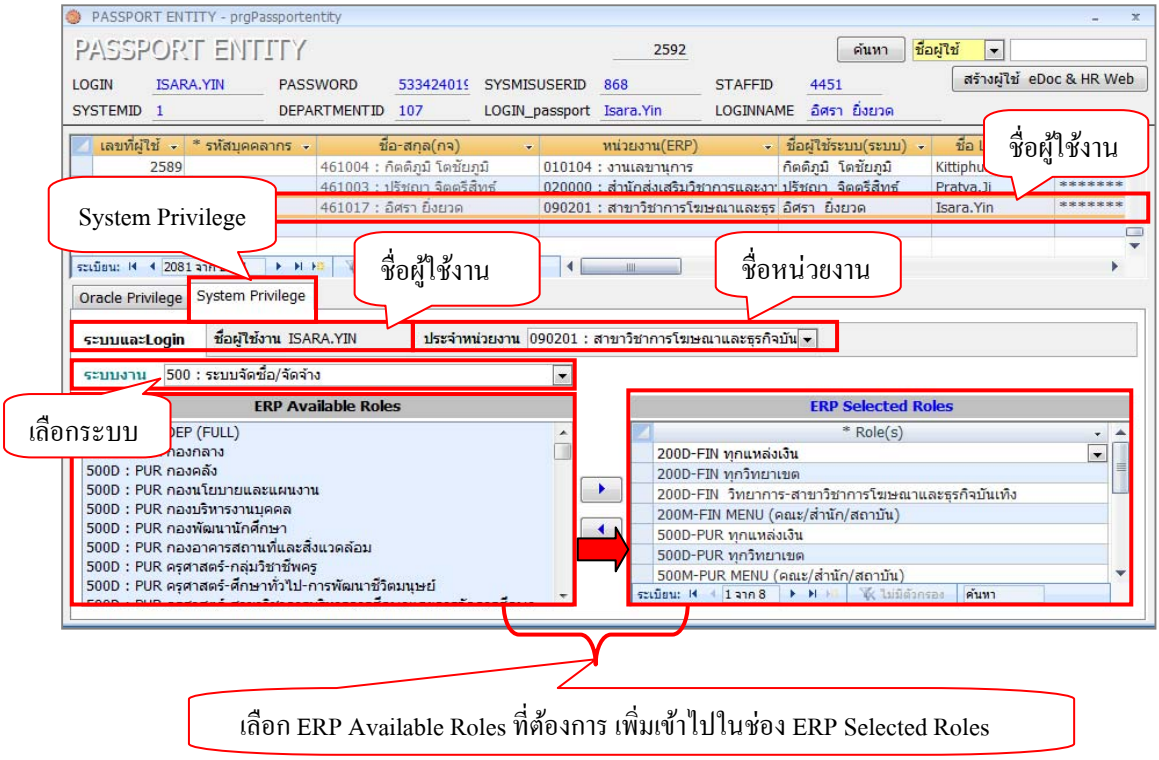
- ใส่ชื่อ Login ของผู้ใช้งานใหม่ และสร้าง Password แบบอัตโนมัติ
- กดปุ่ม Create เพื่อเพิ่มสถานะ Oracle Account : OPEN
- ช่อง ORACLE Available Roles เลือก Roles ที่ต้องการ เพิ่มเข้าไปในช่อง ORACLE Selected Roles เช่น ระบบการเงิน คือ A_FINANCIAL และ A_FINANCIAL_SELECT, ระบบจัดซื้อจัดจ้าง คือ A_PURCHASE และ A_PURCHASE_SELECT, ระบบคลังพัสดุ คือ A_STOCK และ A_STOCK_SELECT เป็นต้น
- กดปุ่ม Grant เพื่อยืนยันสิทธิ์ Grant Complete



ภาพที่ 4.16 หน้าจอ แสดงการเพิ่มสิทธิ์แท็ป Oracle Privilege เพื่อใช้ระบบ ERP

เลือกแท็ป System Privilege เพื่อใช้ระบบ ERP

- เลือกชื่อผู้ใช้งานที่จะเพิ่มสิทธิ์
- ตรวจสอบชื่อผู้ใช้งาน Login Name เช่น ISARA.YIN และประจำหน่วยงาน ให้เลือกหน่วยงาน เช่น 090201 : สาขาวิชาการโฆษณาและธุรกิจบันเทิง
- คลิกที่ **ระบบงาน** ทำการเลือกระบบที่ต้องการเพิ่ม อาทิ เช่น ระบบการเงิน ระบบจัดซื้อจัดจ้าง และระบบคลังพัสดุ
- ช่อง ERP Available Roles เลือก Roles ที่ต้องการ เพิ่มเข้าไปในช่อง ERP Selected Roles เช่น ระบบการเงิน ระบบจัดซื้อจัดจ้าง และระบบคลังพัสดุ (แสดงในตารางที่ 1)



ภาพที่ 4.17 หน้าจอ แสดงการเพิ่มสิทธิ์แท็ป System Privilege เพื่อใช้ระบบ ERP

ตารางที่ 4.2 แสดงข้อมูลการเพิ่มสิทธิ์ระบบ ERP

ระบบจัดซื้อจัดจ้าง	
ORACLE Selected Roles	**ERP Selected Roles**
A_CONNECT	500D-PUR ทุกแหล่งเงิน
A_PURCHASE	500D-PUR ทุกวิทยาเขต
A_PURCHASE_SELECT	500D-PUR หน่วยงาน/สังกัด เช่น สาขาวิชา…
	500P-SP-PUP หน่วยงาน/สังกัด เช่น สาขาวิชา…
	500M-PUR MENU (คณะ)
	**** 500M-PUR MENU (พัสดุ)***
	**** 500D-PUR ทุกหน่วยงาน***
	**** 500P-SP PUR ALL***

ตารางที่ 4.2 (ต่อ)

ระบบคลังพัสดุ	
ORACLE Selected Roles	**ERP Selected Roles**
A_CONNECT	800D-STK ทุกแหล่งเงิน
A_STOCK	800D-STK ทุกวิทยาเขต
A_STOCK_SELECT	800D-STK หน่วยงาน/สังกัด เช่น สาขาวิชา…
	800M-STK MENU (คณะ/สำนัก/สถาบัน)
	**** 800M-STK MENU (งานพัสดุ)***
	**** 800D-STK ทุกหน่วยงาน***
ระบบงบประมาณ	
ORACLE Selected Roles	**ERP Selected Roles**
A_CONNECT	300D-BUD ทุกแหล่งเงิน
A_BUDGET	300D-BUD ทุกวิทยาเขต
A_BUDGET_EST (ประมาณการรายรับ)	300D-BUD หน่วยงาน / สังกัด เช่น สาขาวิชา…
A_BUDGET_SELECT	300M-BUD MENU (คณะ)
	**** 300M-BUD MENU (กองแผน)***
	**** 300D-BUD ทุกหน่วยงาน***
ระบบการเงิน	
ORACLE Selected Roles	**ERP Selected Roles**
A_CONNECT	200D-FIN ทุกแหล่งเงิน
A_FINANCIAL	200D-FIN ทุกวิทยาเขต
A_FINANCIAL_SELECT	200D-FIN หน่วยงาน / สังกัด เช่น สาขาวิชา…
	200M-FIN MENU (คณะ)
	**** 200M-FIN MENU (กองคลัง)***
	**** 200D-FIN ทุกหน่วยงาน***

ตารางที่ 4.2 (ต่อ)

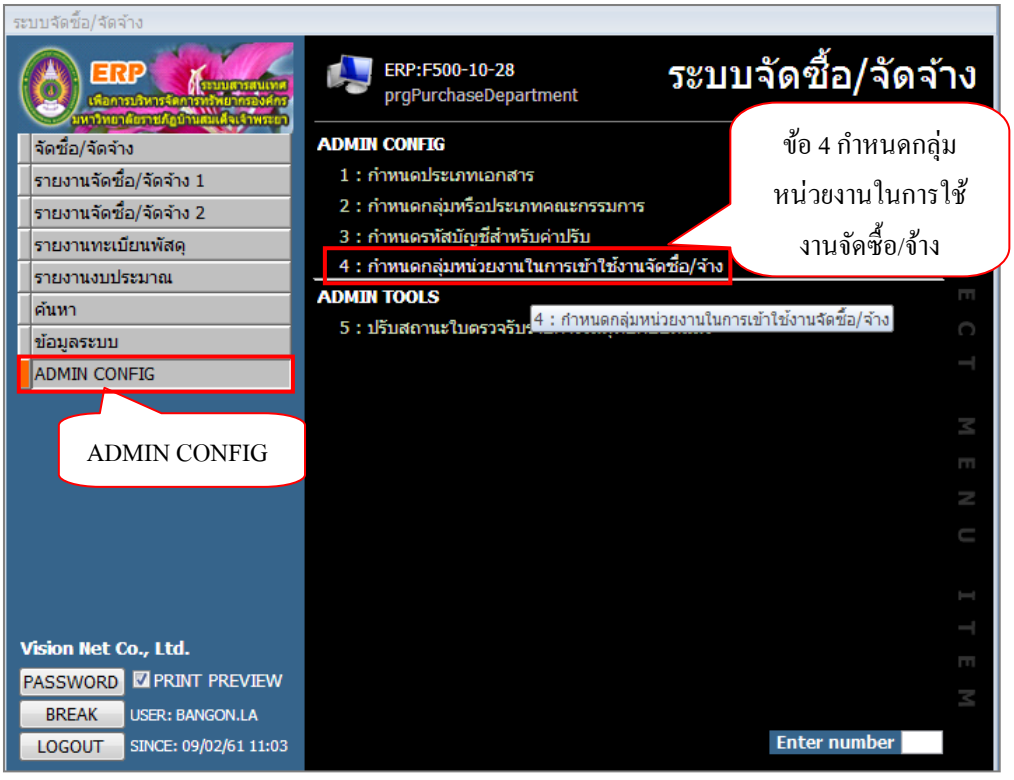
ระบบงานบุคลากร	
ORACLE Selected Roles	**ERP Selected Roles**
A_CONNECT	400D-HRM DEP (FULL)
A_STAFF	400D-HRM DEP Menu (FULL)
A_STAFF_SELECT	400D-HRM DEP Menu (กจ) (FULL)
	400D-HRM_DEP_คณะ....
	400D-HRM_DEP_อบรม
ระบบงานบัญชี	
ORACLE Selected Roles	**ERP Selected Roles**
A_CONNECT	100D-ACC DEP (FULL)
A_ACCOUNT	100D-ACC DEP (CENTER)
A_ACCOUNT_SELECT	100M-ACC MENU (เจ้าหน้าที่การเงิน)
	100M-ACC MENU (เปิด/ปิดบัญชี)
	100M-ACC MENU (CENTER)
	100M-ACC MENU (ALL MENU)
	100M-ACC MENU (ดูเฉพาะรายงานเท่านั้น)
	100M-ACC MENU (ดูเฉพาะหน้าจอเท่านั้น)
ระบบเงินเดือน	
ORACLE Selected Roles	**ERP Selected Roles**
A_CONNECT	600D-PAR DEP (FULL)
A_PAYROLL	600M-PAR Menu (Full)
A_PAYROLL_SELECT	600M-PAR Menu (กองแผน)
	600M-PAR Menu งานเงินเดือน
	600M-PAR Menu (ดูเฉพาะรายงานเท่านั้น)

ตารางที่ 4.2 (ต่อ)

ระบบต้นทุนต่อหน่วย	
ORACLE Selected Roles	**ERP Selected Roles**
A_CONNECT	700D-COS DEP (FULL)
A_COST	700M-COS MENU (FULL)
A_COST_SELECT	700M-COS MENU REPORT
	700M-COS MENU (ดูเฉพาะรายงานเท่านั้น)
	700M-COS MENU (ดูเฉพาะหน้าจอเท่านั้น)
	700M-COS MENU ข้อมูลระบบเท่านั้น

5.2.8 ส่วนที่ต้องมีการเพิ่มสิทธิ์ ระบบจัดซื้อจัดจ้าง ให้กับผู้ใช้งาน เข้าสู่ ระบบจัดซื้อจัดจ้าง

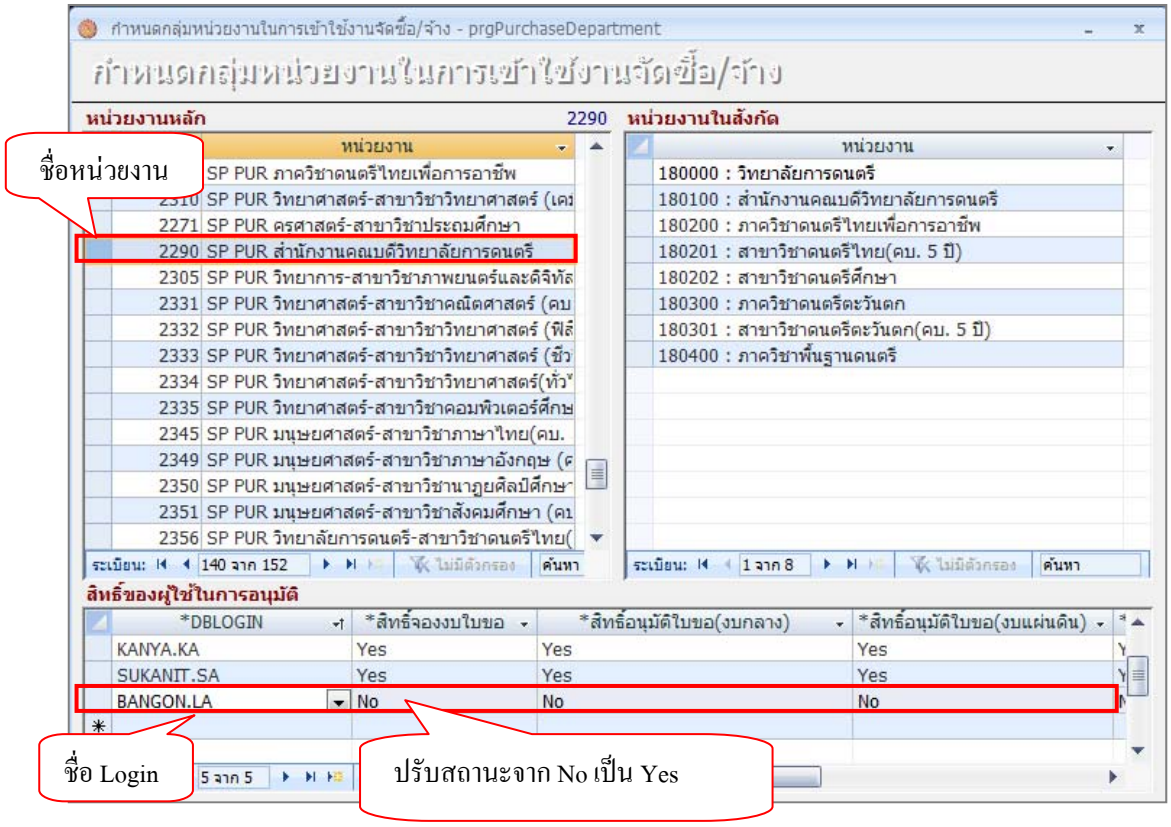
- เลือก เมนู ADMIN CONFIG
- เลือก ข้อ 4 กำหนดกลุ่มหน่วยงานในการใช้งานจัดซื้อ/จ้าง



ภาพที่ 4.18 หน้าจอ แสดงการเข้าสู่ระบบจัดซื้อจัดจ้าง

การดำเนินการเพิ่มชื่อผู้ใช้งานให้มองเห็นข้อมูลหน่วยงานของตนเองได้

- เลือก ชื่อหน่วยงาน
- พิมพ์ชื่อ Login ของผู้ใช้งาน เช่น BANGON.LA
- ปรับสถานะจาก No เป็น Yes เช่น สิทธิ์จองงบใบขอ, สิทธิ์อนุมัติใบขอ (งบกลาง), สิทธิ์อนุมัติใบขอ (งบแผ่นดิน) เป็นต้น

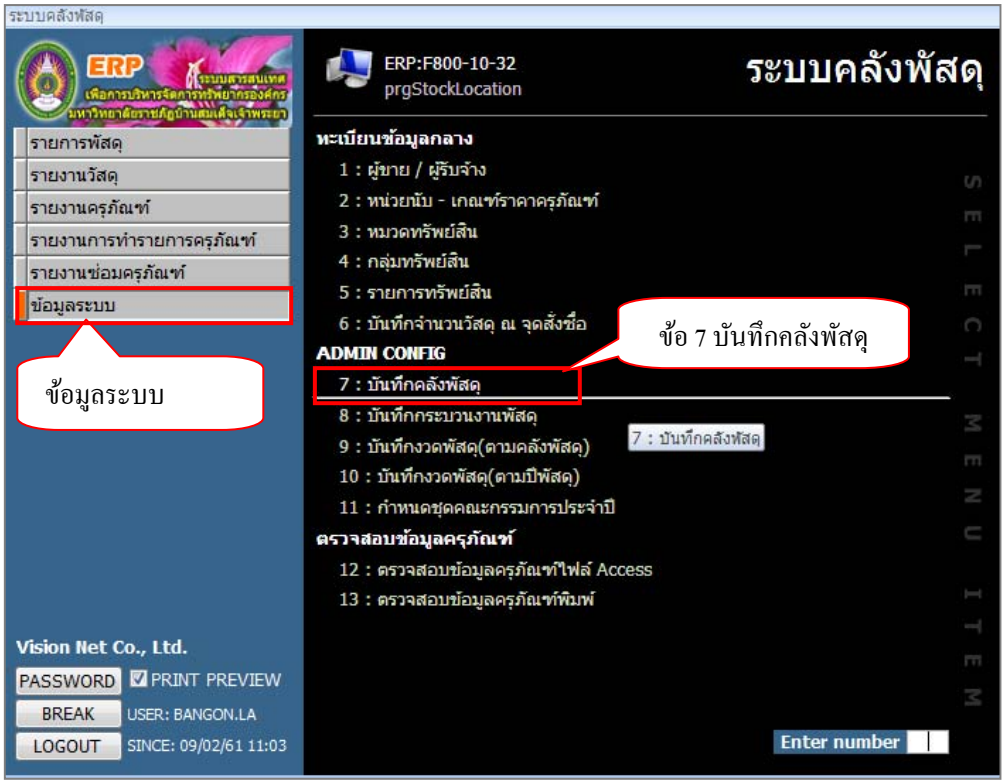


ภาพที่ 4.19 หน้าจอแสดงการเพิ่มชื่อผู้ใช้งานให้มองเห็นข้อมูลหน่วยงานของตนเองได้

5.2.9 ส่วนที่ต้องมีการเพิ่มสิทธิ์ ระบบคลังพัสดุ ให้กับผู้ใช้งาน

เข้าสู่ ระบบคลังพัสดุ

- เลือก เมนู ข้อมูลระบบ
- เลือก ADMIN CONFIG ข้อ 7 บันทึกคลังพัสดุ

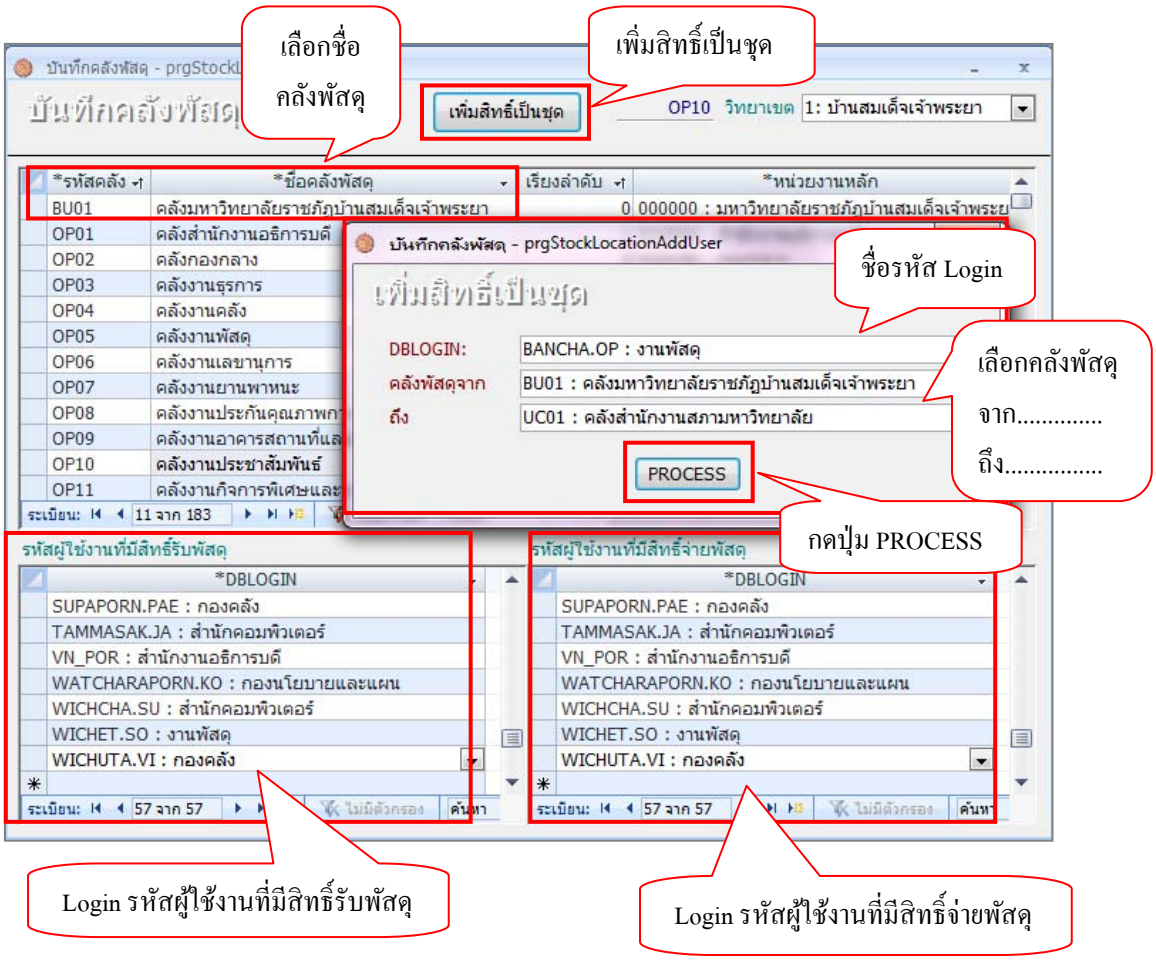


ภาพที่ 4.20 หน้าจอ แสดงการเข้าสู่ระบบคลังพัสดุ

การดำเนินการเพิ่มชื่อผู้ใช้งานให้มองเห็นข้อมูลหน่วยงานของตนเองได้

- เพิ่มสิทธิ์ได้ที่ละรายการ เลือก ชื่อคลังพัสดุ ของหน่วยงานนั้น
- พิมพ์ Login รหัสผู้ใช้งานที่มีสิทธิ์รับพัสดุ ในช่อง *DBLOGIN
- พิมพ์ Login รหัสผู้ใช้งานที่มีสิทธิ์จ่ายพัสดุ ในช่อง *DBLOGIN
- เพิ่มสิทธิ์เป็นชุด ใส่ชื่อรหัส Login ที่ช่อง *DBLOGIN และเลือกคลังพัสดุ

จาก.....ถึง..... กดปุ่ม PROCESS

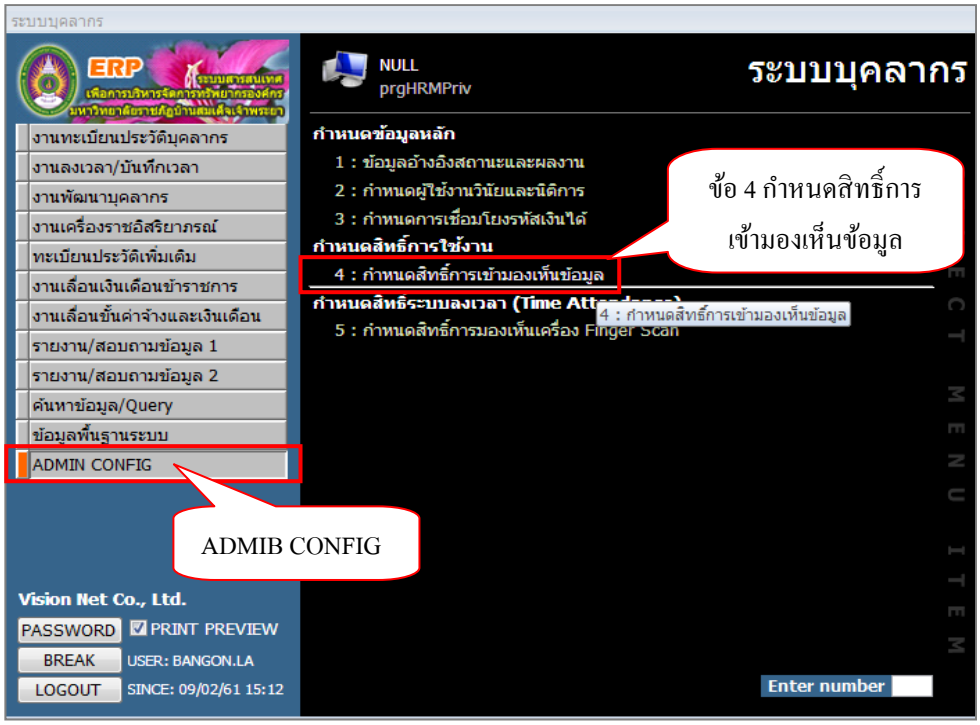


ภาพที่ 4.21 หน้าจอแสดงการเพิ่มชื่อผู้ใช้งานให้มองเห็นข้อมูลหน่วยงานของตนเองได้

5.2.10 ส่วนที่ต้องมีการเพิ่มสิทธิ์ ระบบบุคลากร ให้กับผู้ใช้งาน

เข้าสู่ ระบบบุคลากร

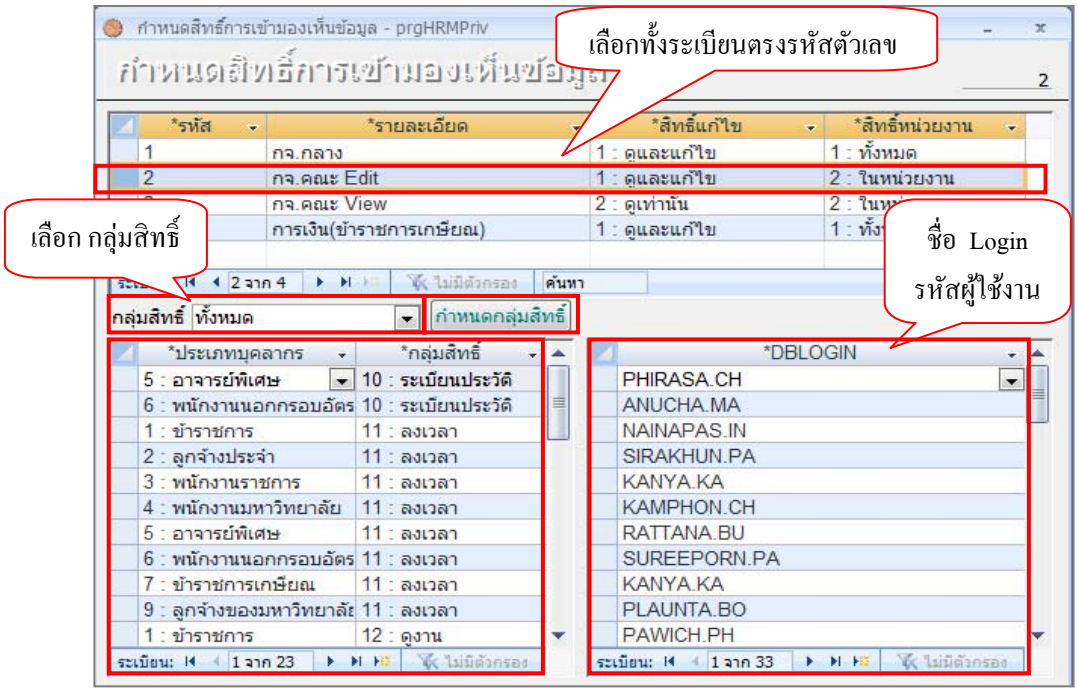
- เลือก เมนู ADMIN CONFIG
- เลือก ข้อ 4 กำหนดสิทธิ์การเข้ามองเห็นข้อมูล



ภาพที่ 4.22 หน้าจอ แสดงการเข้าสู่ระบบบุคลากร

การดำเนินการเพิ่มชื่อผู้ใช้งานให้มองเห็นข้อมูลหน่วยงานของตนเองได้

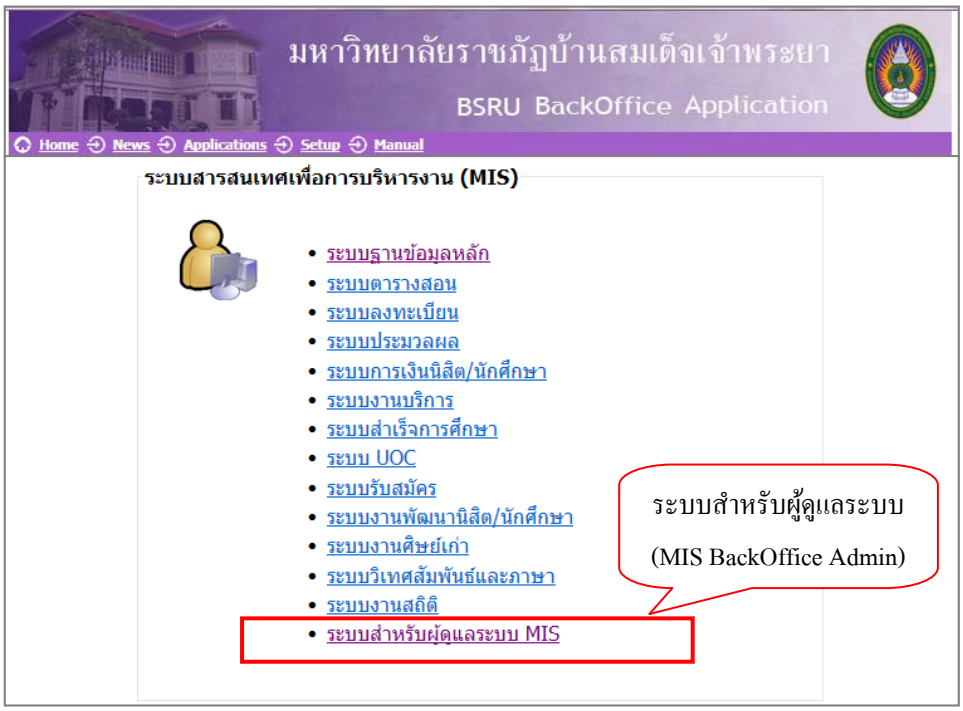
- เลือกทั้งระเบียนตรงรหัสที่มีการกำหนดสิทธิ์การมองเห็นของหน่วยงาน
- เลือก กลุ่มสิทธิ์ เพื่อกำหนดกลุ่มสิทธิ์
- พิมพ์ชื่อ Login รหัสผู้ใช้งาน ในช่อง *DBLOGIN



ภาพที่ 4.23 หน้าจอแสดงการเพิ่มชื่อผู้ใช้งานให้มองเห็นข้อมูลหน่วยงานของตนเองได้

5.3 เข้าระบบสำหรับผู้ปฏิบัติงาน ระบบสารสนเทศเพื่อการบริหารมหาวิทยาลัย (MIS: Management Information System)

5.3.1 คลิกเลือก ระบบสำหรับผู้ดูแลระบบ (MIS BackOffice Admin)

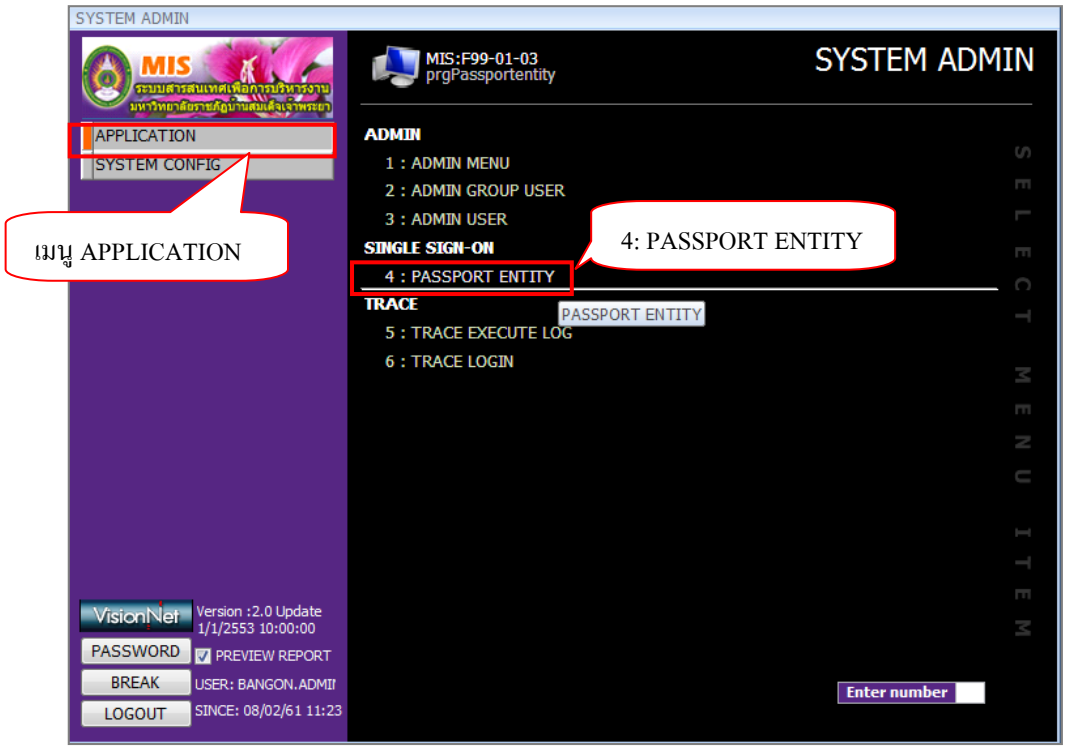


ภาพที่ 4.24 หน้าจอแสดงระบบสารสนเทศเพื่อการบริหารงาน (MIS)

5.3.2 ระบบจะปรากฏหน้าจออีกรูปแบบหนึ่ง เพื่อให้กรอก Username และ Password เพื่อเข้าสู่ระบบสำหรับผู้ดูแลระบบ

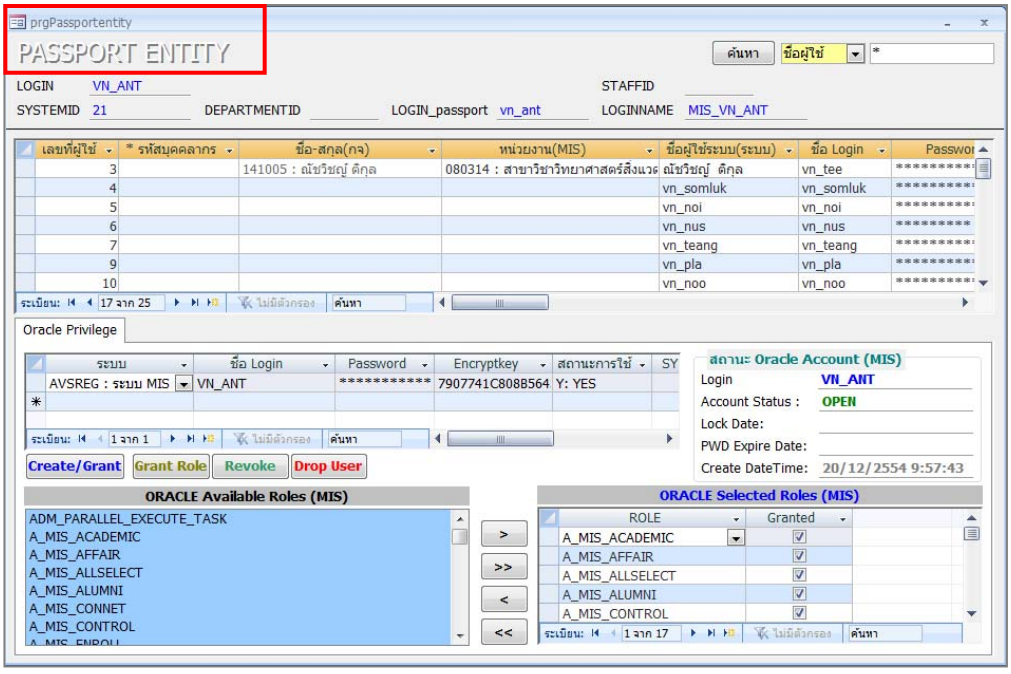
ภาพที่ 4.25 หน้าจอ Login (MIS)

5.3.3 คลิกเลือกที่ เมนู APPLICATION หัวข้อ SINGLE SIGN-NO ข้อ 4 : PASSPORT ENTITY



ภาพที่ 4.26 หน้าจอ SYSTEM ADMIN (MIS)

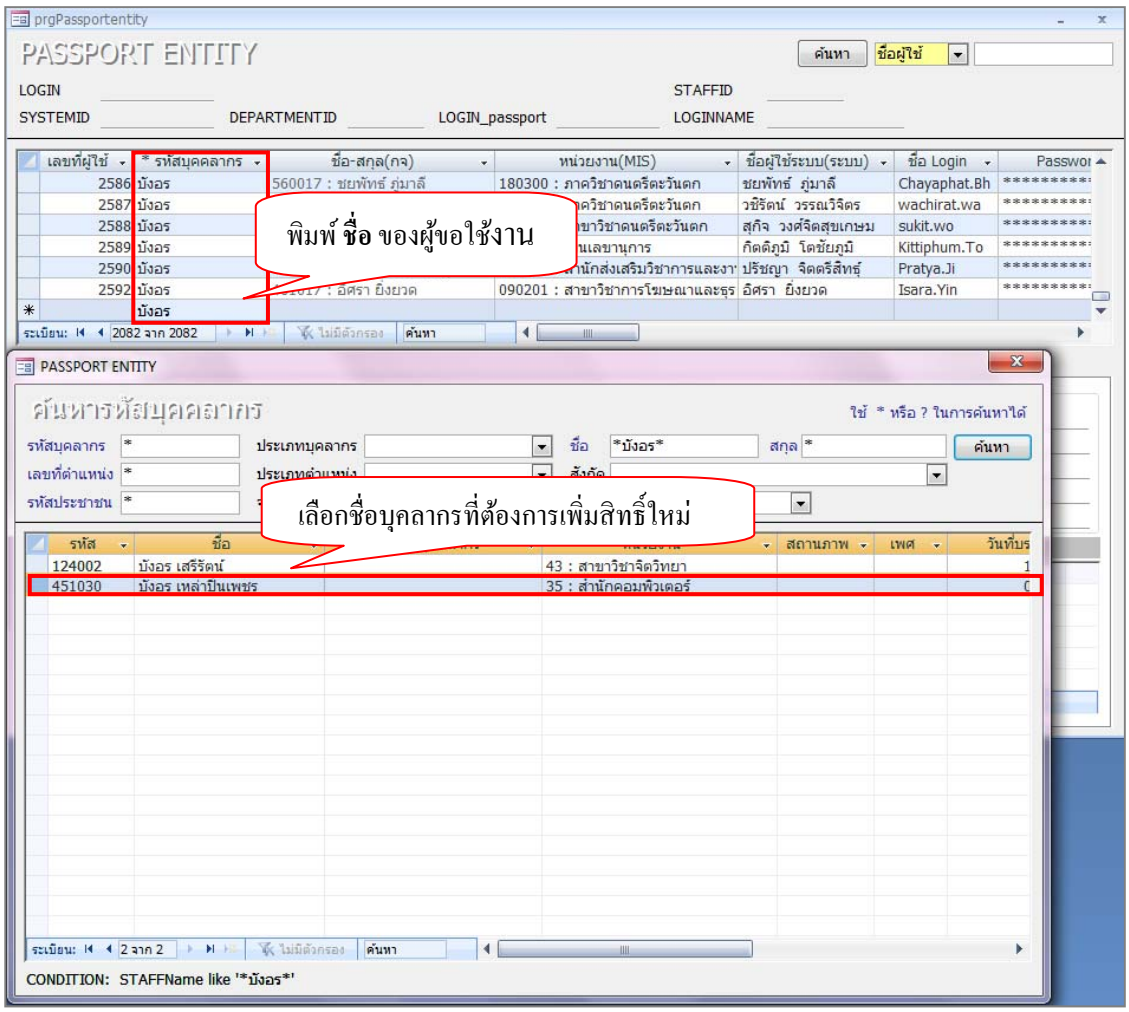
5.3.4 คลิกเลือกที่ ข้อ 4 : PASSPORT ENTITY



ภาพที่ 4.27 หน้าจอ PASSPORT ENTITY (MIS)

5.3.5 วิธีการเพิ่มสิทธิ์ใหม่ของผู้ใช้งาน โดยจะเพิ่มสิทธิ์พื้นฐานของบุคลากรที่ได้

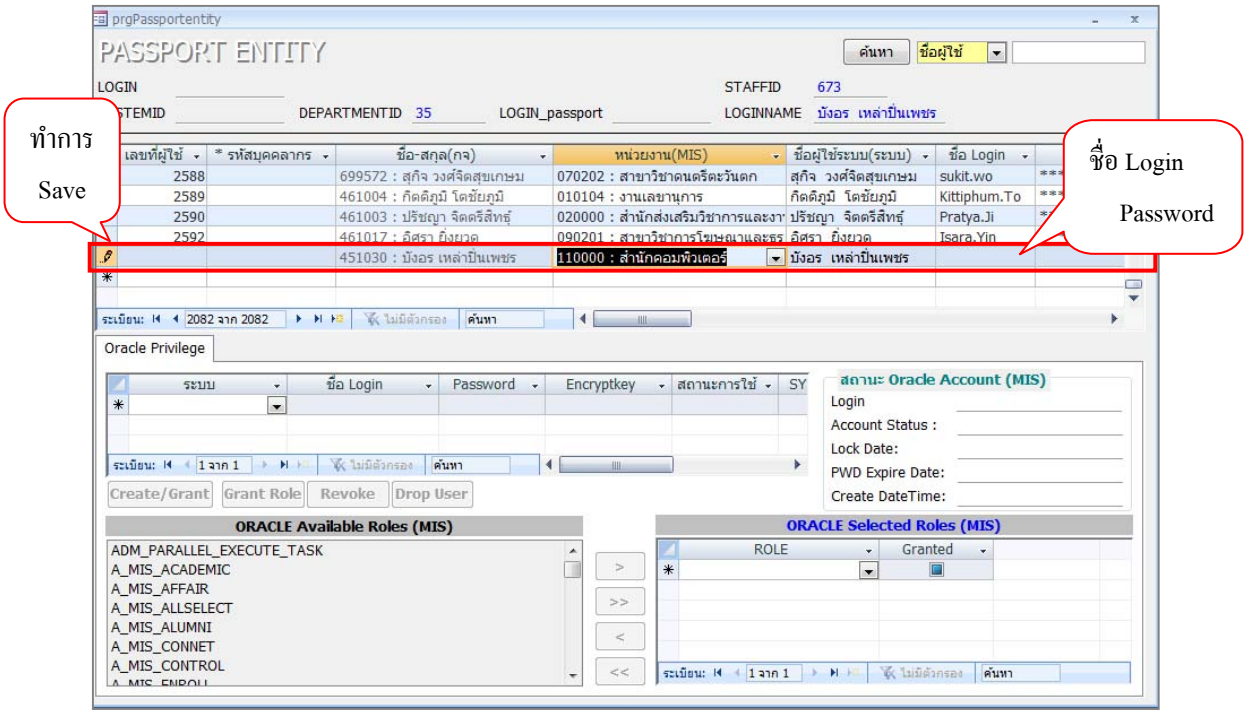
- พิมพ์ **ชื่อ** ของผู้ขอใช้งาน ที่ช่องรหัสบุคลากร
- ในหน้าจอ **ค้นหาบุคลากร** ให้คลิกเลือกชื่อของบุคลากรที่ต้องการเพิ่มสิทธิ์ให้ใหม่



ภาพที่ 4.28 หน้าจอ แสดงการพิมพ์ชื่อ เพื่อค้นหาบุคลากร (MIS)

5.3.6 การสร้างสิทธิ์ผู้ใช้งาน โดยจะมีสิทธิ์ใช้งานระบบสารสนเทศของ(MIS) ดังนี้

- ได้ ชื่อ Login และ Password
- ทำการ Save สัญลักษณ์รูปดินสอ ที่ปรากฏหน้าระเบียน



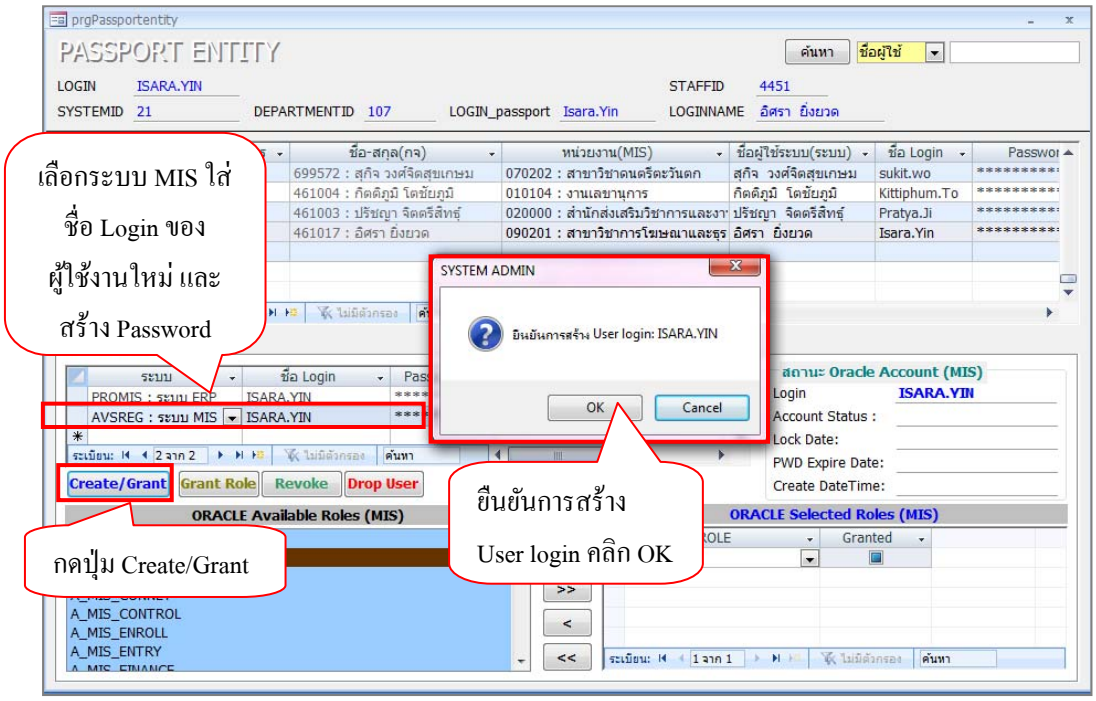
ภาพที่ 4.29 หน้าจอ แสดงการสร้างสิทธิ์ผู้ใช้งาน

เลือกแท็ป Oracle Privilege เพื่อใช้ระบบ MIS

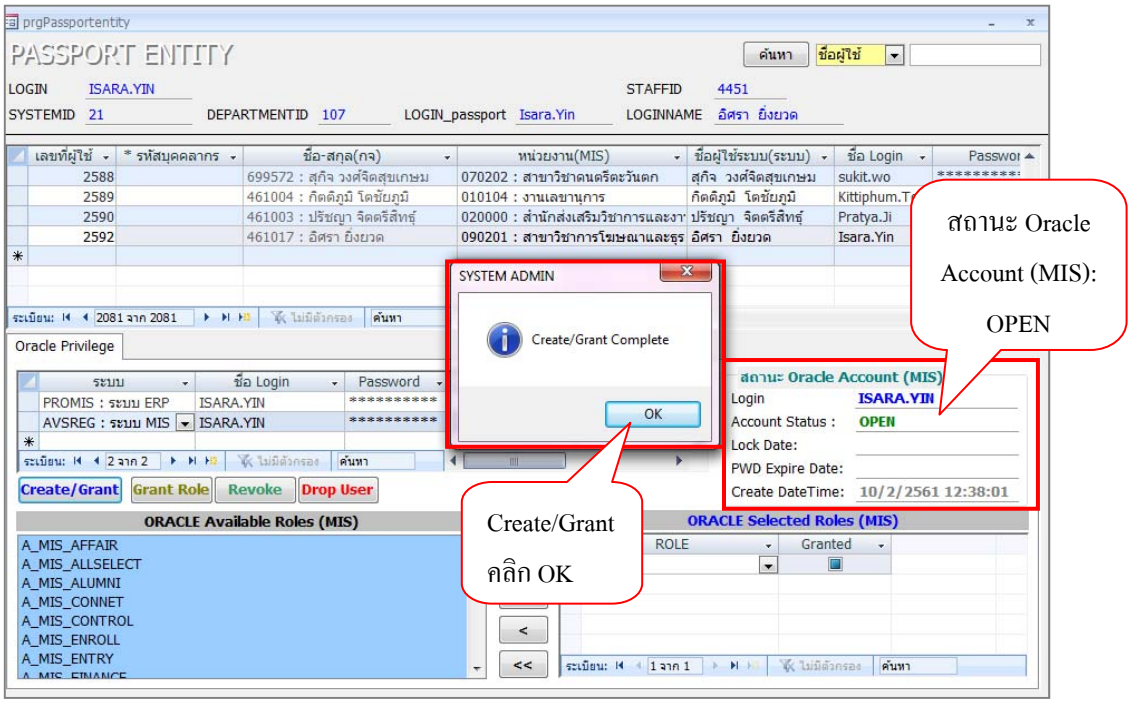
- เลือกระบบ MIS ใส่ชื่อ Login ของผู้ใช้งานใหม่ และสร้าง Password แบบอัตโนมัติ

- กดปุ่ม Create/Grant เพื่อยืนยันการสร้าง User login คลิกปุ่ม OK (แสดงดังภาพที่ 4.30) และเมื่อมี Message Box ขึ้นมาว่า Create/Grant จึงกดปุ่ม OK สถานะ Oracle Account (MIS): OPEN (ดังภาพที่ 4.31)

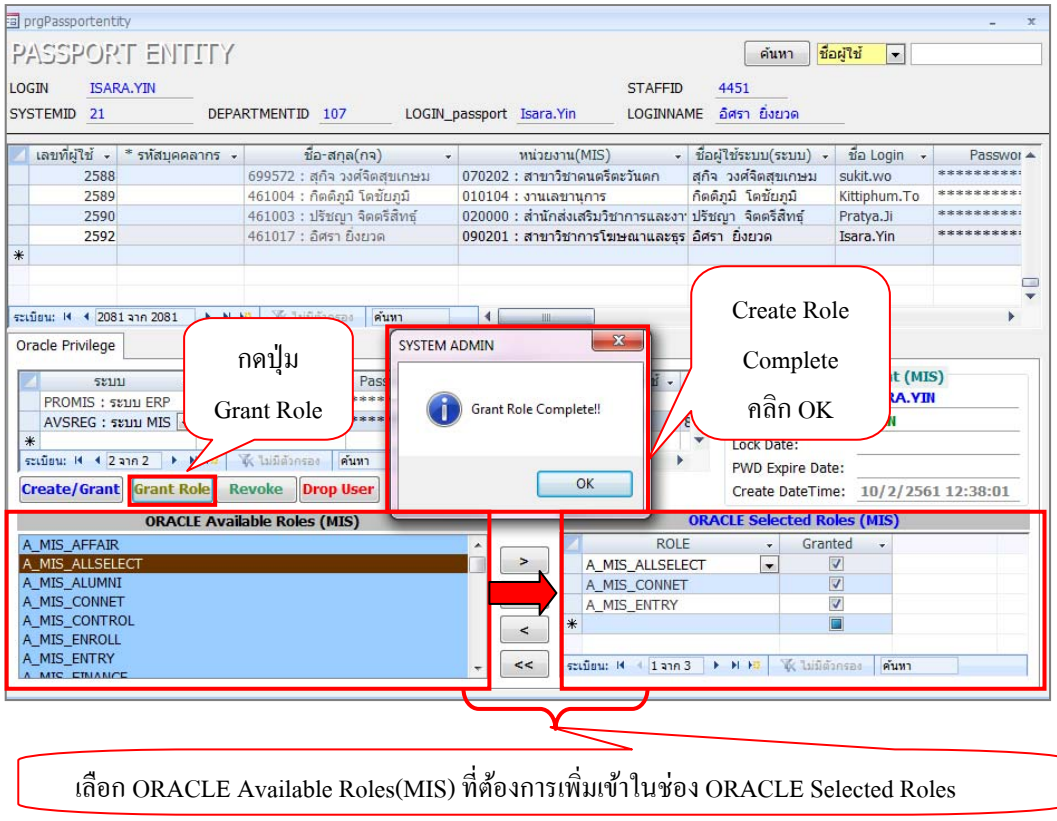
- เมื่อต้องการเพิ่มสิทธิ์ ORACLE Available Roles (MIS) คลิกเลือกRoles ที่ต้องการ เช่น A_MIS_CONNET, A_MIS_ALLSELECT, A_MIS_ENTRY เพิ่มเข้าในช่อง ORACLE Selected Roles (MIS) และกดปุ่ม Grant Role เมื่อมี Message Box ขึ้นมาว่า Create Role Complete จึงกดปุ่ม OK (ดังภาพที่ 4.32)



ภาพที่ 4.30 หน้าจอ แสดงการยืนยันการสร้าง User login เพื่อใช้ระบบ MIS



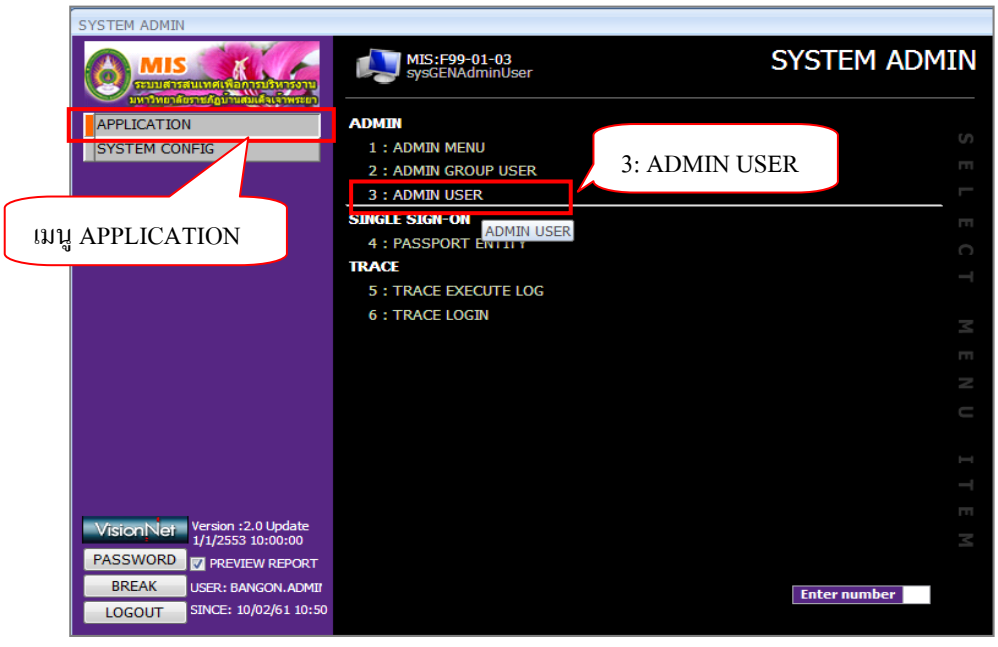
ภาพที่ 4.31 หน้าจอ แสดง Create/Grant เพื่อยืนยันการสร้าง User login



ภาพที่ 4.32 หน้าจอ แสดงการเพิ่มสิทธิ์ ORACLE Available Roles (MIS)

5.3.7 การเพิ่มสิทธิ์ผู้ใช้งาน ในระบบสารสนเทศของ(MIS) ต่างๆ เช่น ระบบตารางสอน, ระบบลงทะเบียน (สำหรับประธานสาขาวิชา) ดังนี้

- คลิกเมนู APPLICATION หัวข้อ ADMIN ข้อ 3 : ADMIN USER



ภาพที่ 4.33 หน้าจอ แสดงการเพิ่มสิทธิ์ผู้ใช้งาน ในระบบสารสนเทศของ(MIS) ต่างๆ

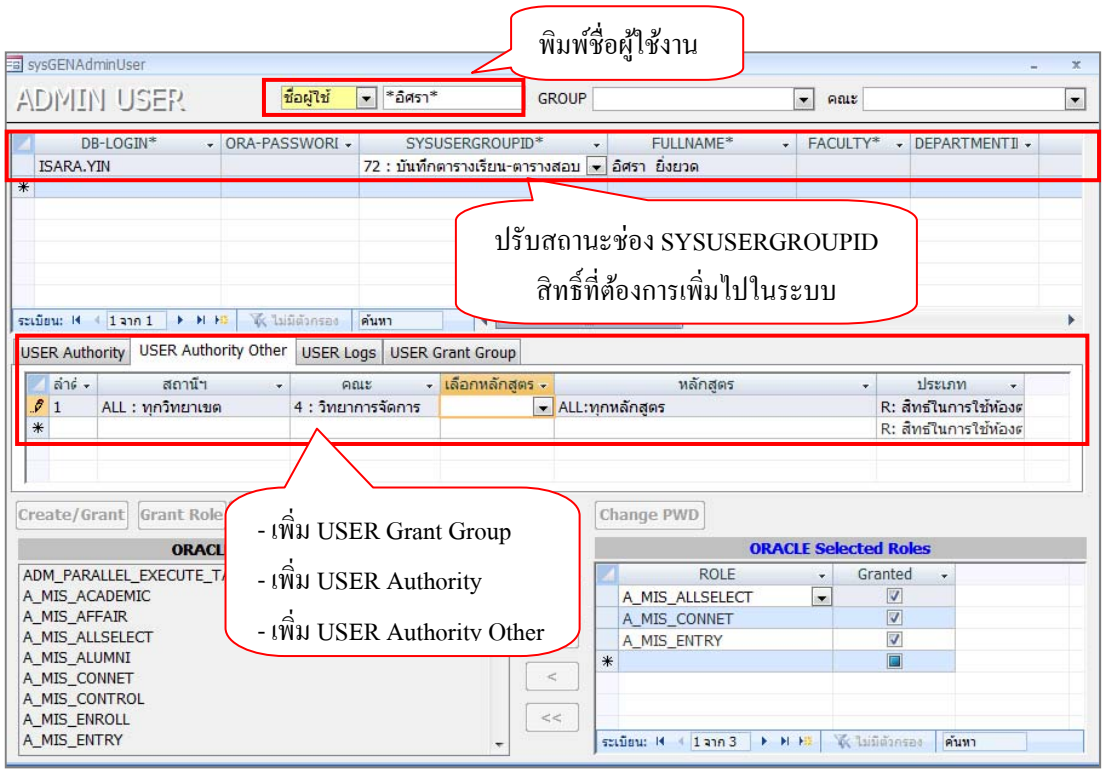
- หน้าจอ ADMIN USER พิมพ์ชื่อผู้ใช้งาน เช่น อิศรา

- ปรับสถานะช่อง SYSUSERGROUPID สิทธิ์ที่ต้องการเพิ่มไปในระบบที่ต้องการ เช่น ระบบตารางเรียน 72: บันทึกตารางเรียน-ตารางสอบ

- เพิ่ม USER Grant Group ที่ใช้งานระบบนั้น เช่น 72: บันทึกตารางเรียน-ตารางสอบ

- เพิ่ม USER Authority ดังนี้ สถานี ระดับ คณะ เลือกหลักสูตรสาขาวิชา

- เพิ่ม USER Authority Other ดังนี้ สถานี คณะ เลือกหลักสูตรสาขาวิชา

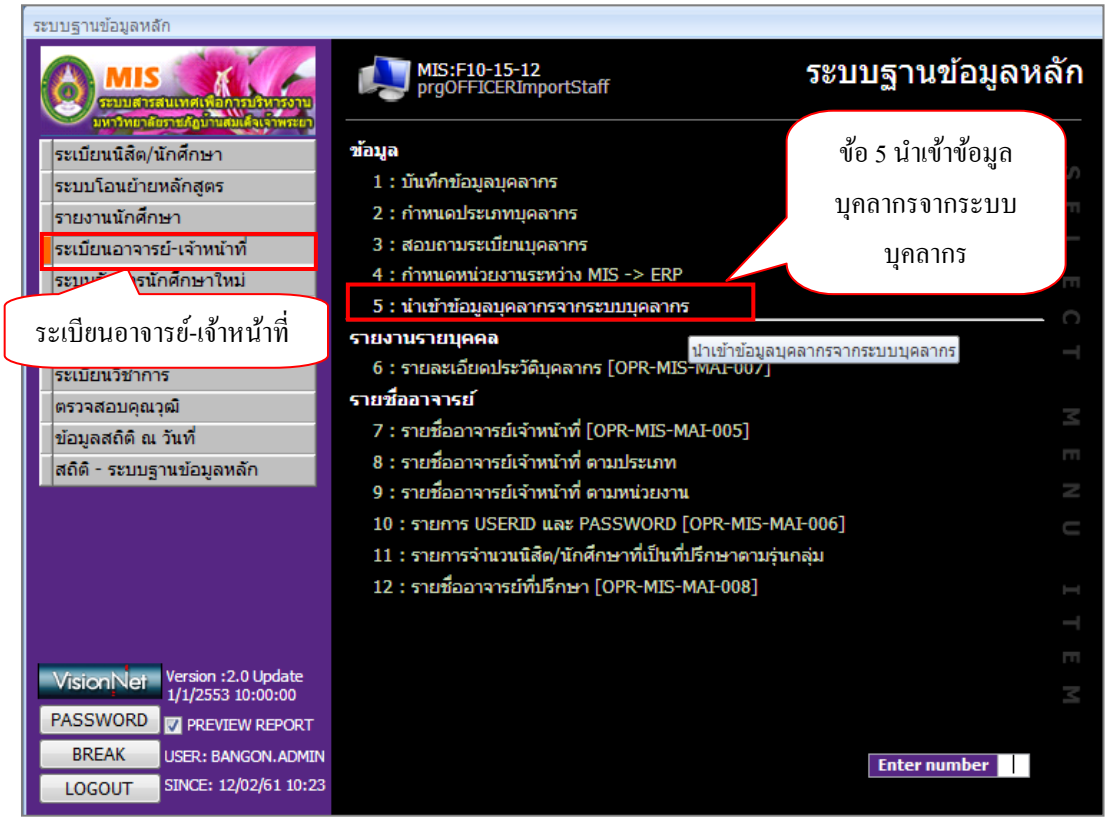


ภาพที่ 4.34 หน้าจอ แสดงการเพิ่มสิทธิ์ ADMIN USER

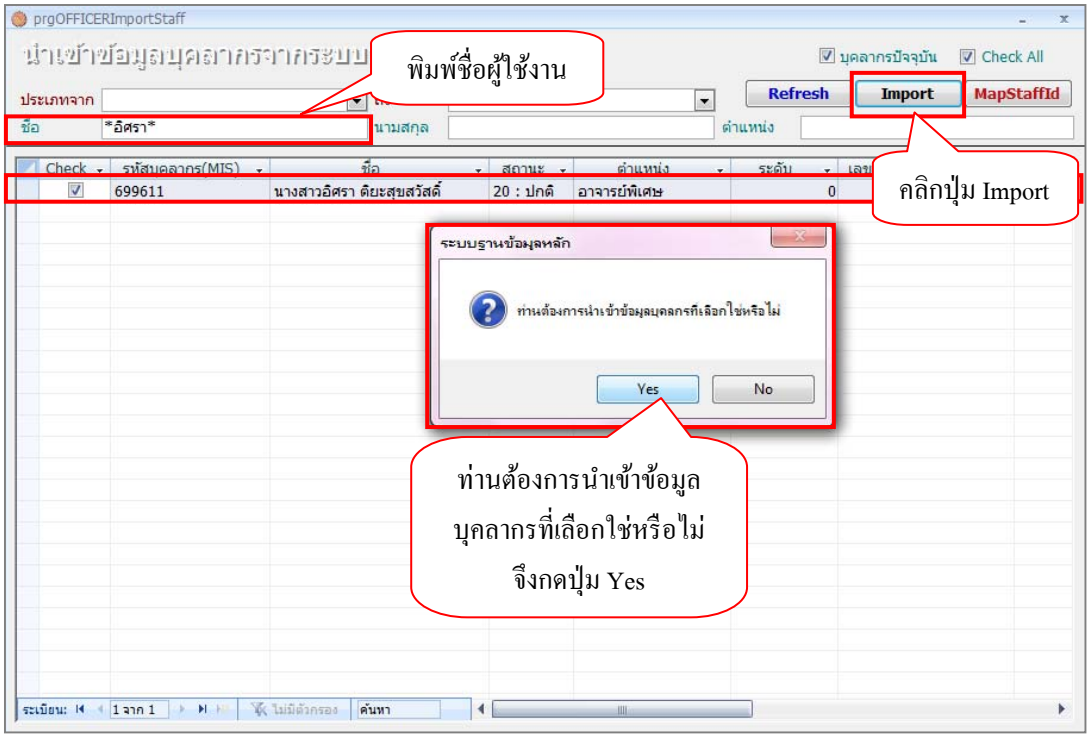
5.3.8 ส่วนที่ต้องมีการเพิ่มสิทธิ์ ระบบฐานข้อมูลหลัก ให้กับผู้ใช้งานระบบ MIS เข้าสู่ ระบบฐานข้อมูลหลัก

- คลิกเมนู ระเบียนอาจารย์-เจ้าหน้าที่ หัวข้อ ข้อมูล ข้อ 5 : นำเข้าข้อมูลบุคลากรจากระบบบุคลากร (ดังภาพที่ 4.35)

- หน้าจอ นำเข้าข้อมูลบุคลากรจากระบบบุคลากร พิมพ์ชื่อผู้ใช้งานที่ช่องคำว่า ชื่อ เช่น *อิศรา แล้วคลิกปุ่ม Import เมื่อมี Message Box ขึ้นมาว่า ท่านต้องการนำเข้าข้อมูลบุคลากรที่เลือกใช่หรือไม่ จึงกดปุ่ม Yes (ดังภาพที่ 4.36)



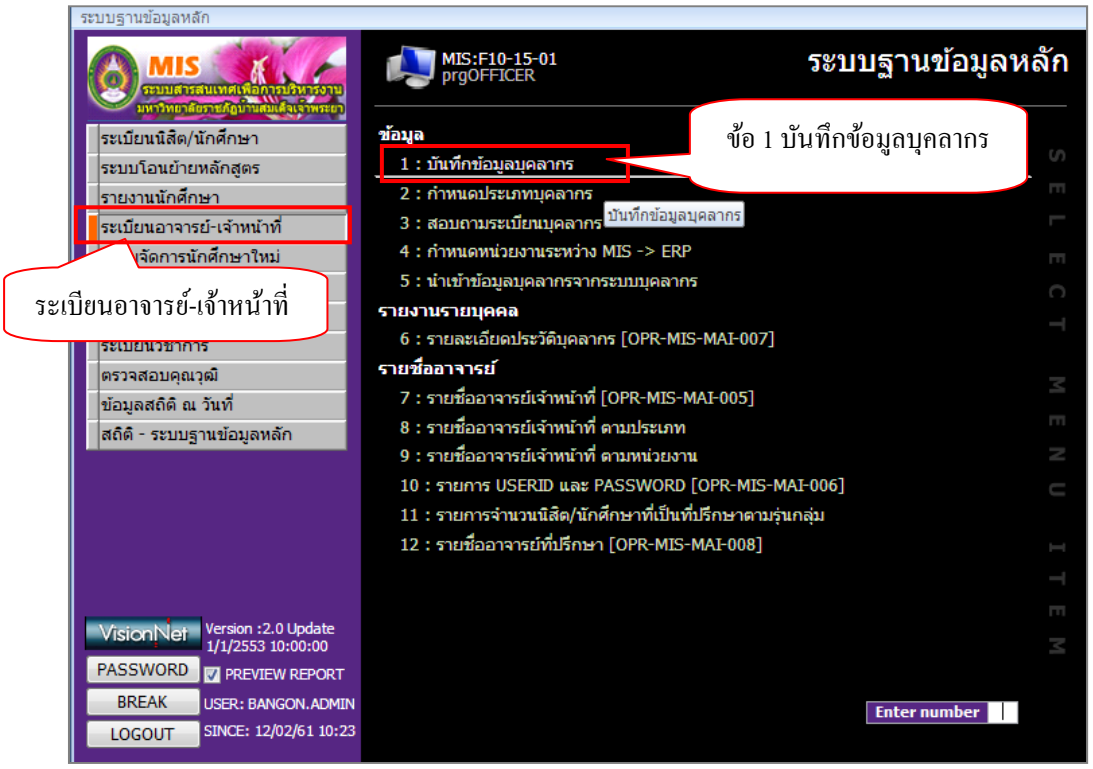
ภาพที่ 4.35 หน้าจอ แสดงการเพิ่มสิทธิ์ ADMIN USER



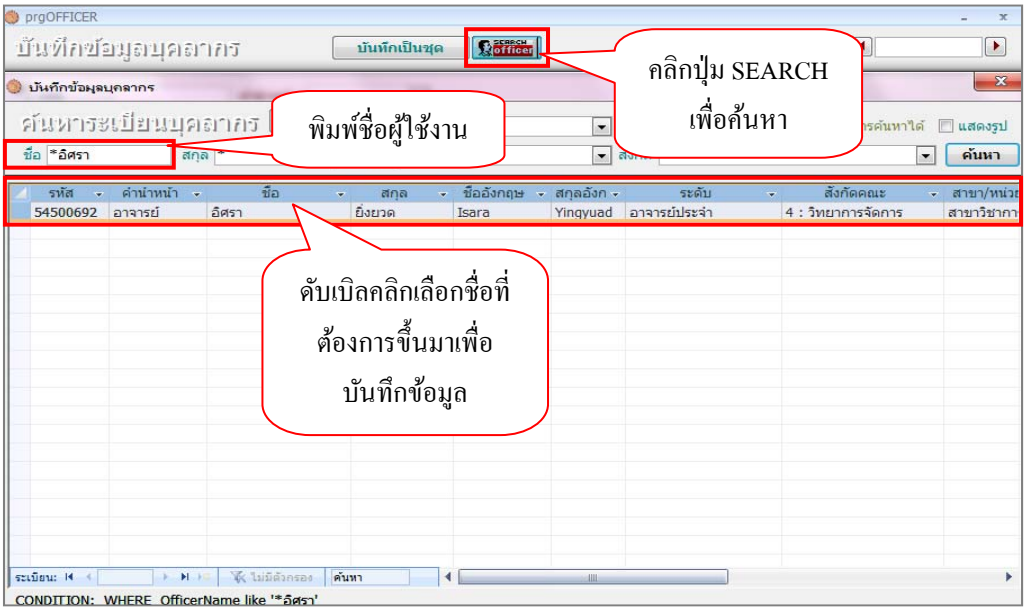
ภาพที่ 4.36 หน้าจอ แสดงการนำเข้าข้อมูลบุคลากรจากระบบบุคลากร

- คลิกเมนู ระเบียนอาจารย์-เจ้าหน้าที่ หัวข้อ ข้อมูล ข้อ 1 : บันทึกข้อมูลบุคลากร (ดังภาพที่ 4.37)

- หน้าจอ บันทึกข้อมูลบุคลากร คลิกปุ่ม SEARCH แล้วพิมพ์ชื่อผู้ใช้งานที่ช่องคำว่า ชื่อ เช่น *อิศรา และดับเบิลคลิกเลือกชื่อที่ต้องการขึ้นมาเพื่อบันทึกข้อมูล (ดังภาพที่ 4.38)

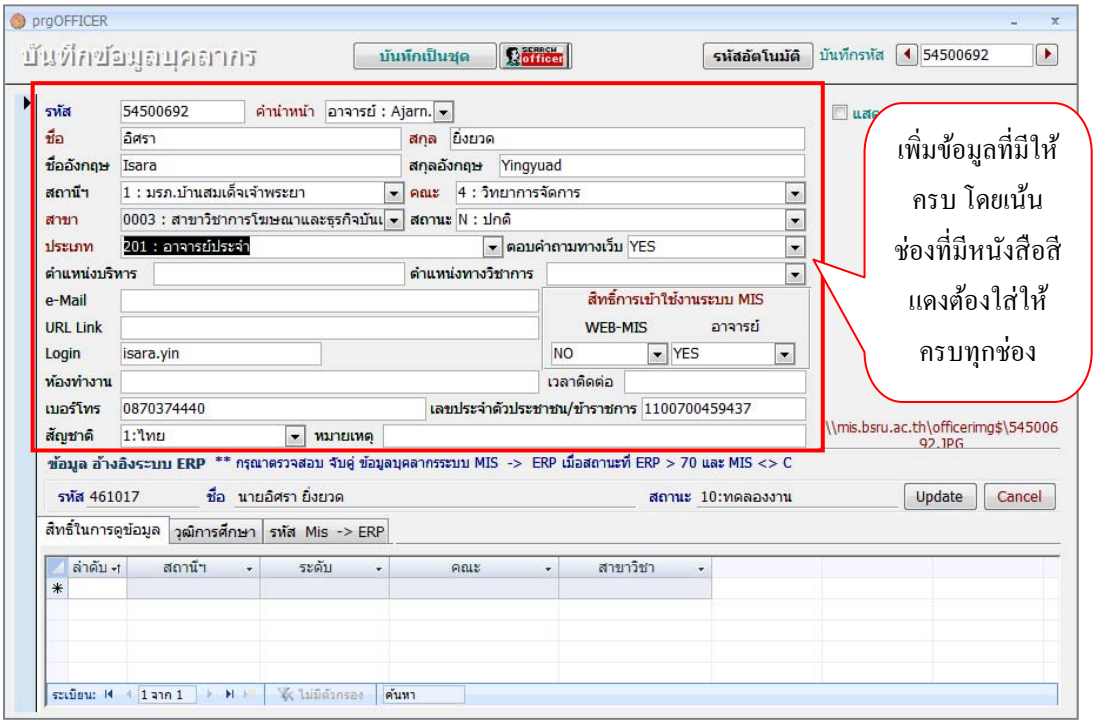


ภาพที่ 4.37 หน้าจอ แสดงเมนู บันทึกข้อมูลบุคลากร



ภาพที่ 4.38 หน้าจอ แสดงการค้นหาข้อมูลบุคลากร

- หน้าจอ บันทึกข้อมูลบุคลากร เมื่อพบชื่อผู้ใช้งานที่ต้องการเรียบร้อยแล้ว ให้ดำเนินการเพิ่มข้อมูลที่มีให้ครบ โดยเน้นช่องที่มีหนังสือสีแดงต้องใส่ให้ครบทุกช่อง



ภาพที่ 4.39 หน้าจอ แสดงการบันทึกข้อมูลบุคลากร

6. ผู้ปฏิบัติงานประสานงานตอบกลับผู้ใช้งานไปยังสาขาวิชา/คณะ ที่แจ้งขอมา

6.1 ผ่านช่องทางการสื่อสารต่างๆ

- ทางระบบสารบรรณอิเล็กทรอนิกส์
- จัดส่งบันทึกข้อความตามหน่วยงาน
- ผ่านช่องทางโทรศัพท์ภายในและมือถือ

6.2 อธิบายขั้นตอนการเข้าใช้งานเบื้องต้นแก่ผู้ใช้งานให้รับทราบสิทธิ์ของตนเองและวิธีการเข้าใช้งานได้ถูกต้อง

7. ผู้ปฏิบัติงานจัดเก็บเอกสารบันทึกข้อความหรือแบบฟอร์มการขอใช้สิทธิ์การใช้งานระบบสารสนเทศต่างๆ ลงในแฟ้ม ไว้เพื่อเป็นหลักฐานในการตรวจสอบสิทธิ์ที่ขอมาในภายหลังได้

การติดตามประเมินผลการปฏิบัติงาน

การดำเนินงานในการกำหนดสิทธิ์การใช้งานของผู้ใช้งานระบบสารสนเทศเพื่อการบริหารมหาวิทยาลัย (MIS: Management Information System) และระบบสารสนเทศเพื่อการบริหารทรัพยากรองค์กร (ERP: Enterprise Resource Resource Planning) ของบุคลากรในมหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา แต่ละครั้งมีวัตถุประสงค์เพื่อสร้างสิทธิ์และเพิ่มสิทธิ์การใช้งานระบบสารสนเทศทั้งหมดที่มีให้กับผู้รับบริการที่เป็นบุคลากรของมหาวิทยาลัยแล้ว ควรมีการติดตามผลการปฏิบัติงานของผู้ใช้งานระบบหลังจากได้รับสิทธิ์การใช้งานไปแล้วนั้น ว่ายังคงมีการใช้งานระบบดังกล่าวอยู่เป็นปัจจุบันหรือไม่ หรือมีการเปลี่ยนแปลงหน้าที่การปฏิบัติงานของผู้ใช้คนนั้นไปเป็นท่านอื่นแล้ว จึงต้องมีการตรวจสอบสิทธิ์การใช้งานให้เป็นปัจจุบัน ซึ่งมีการดำเนินการเป็นเวลาประมาณ 1 ปีงบประมาณ หลังจากผู้ใช้ได้รับสิทธิ์ไปแล้ว โดยมีขั้นตอนการติดตามและประเมินผล ดังนี้

1. จัดทำบันทึกข้อความเป็นแบบเวียนทุกหน่วยงานในมหาวิทยาลัย เพื่อแจ้งข้อมูลของการใช้สิทธิ์ระบบ (MIS-ERP) แต่ละระบบที่มีในปัจจุบันของบุคลากรตามรายชื่อที่สังกัดหน่วยงานต่างๆ ให้รับทราบข้อมูลที่เป็นปัจจุบันของแต่ละท่าน
2. หน่วยงานได้รับบันทึกข้อความดังกล่าวแล้ว ให้หัวหน้าหน่วยงานนั้นๆ มอบหมายงานให้บุคลากรตรวจสอบสิทธิ์ของตัวเอง ว่ายังมีสิทธิ์ในการปฏิบัติงานตามระบบดังกล่าวที่แจ้งมาหรือไม่
3. กรณีที่มีสิทธิ์เกินหรือยังไม่ได้รับสิทธิ์ระบบการใช้งานที่เคยขอมาแล้ว ให้หน่วยงานทำบันทึกข้อความหรือกรอกแบบฟอร์มการขอใช้สิทธิ์เพิ่มเติม แจ้งกลับมายังสำนักคอมพิวเตอร์ เพื่อขอเพิ่มสิทธิ์ระบบอื่นๆ เข้ามาได้ด้วย
4. ระยะเวลาในการตรวจสอบสิทธิ์ให้เป็นปัจจุบันจะมีการตรวจสอบทุกๆ 1 ปีงบประมาณ
5. ผู้ปฏิบัติงานสรุปเป็นรายงานการติดตามผลและประเมินผลการตรวจสอบสิทธิ์ระบบสารสนเทศให้เป็นไปตามแผนที่กำหนดไว้เป็นที่เรียบร้อย

บทที่ 5
ปัญหาอุปสรรคและข้อเสนอแนะ

คู่มือการปฏิบัติงาน เรื่อง การกำหนดสิทธิ์การใช้งานของผู้ใช้งานระบบสารสนเทศเพื่อการบริหารมหาวิทยาลัย (MIS: Management Information System) และระบบสารสนเทศเพื่อการบริหารทรัพยากรองค์กร (ERP: Enterprise Resource Resource Planning) ของบุคลากรในมหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา ผู้เขียนได้รวบรวมปัญหาอุปสรรค แนวทางการแก้ไขและข้อเสนอแนะเพื่อการพัฒนา จากการกำหนดสิทธิ์การใช้งานของผู้ใช้งานระบบสารสนเทศของมหาวิทยาลัยและการปฏิบัติงานจริงของเจ้าหน้าที่ผู้รับผิดชอบด้านระบบสารสนเทศ โดยสรุปไว้ดังนี้

ปัญหาอุปสรรคในการปฏิบัติงาน และแนวทางแก้ไข

การกำหนดสิทธิ์การใช้งานของผู้ใช้งานระบบสารสนเทศเพื่อการบริหารมหาวิทยาลัย (MIS: Management Information System) และระบบสารสนเทศเพื่อการบริหารทรัพยากรองค์กร (ERP: Enterprise Resource Resource Planning) ของบุคลากรในมหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา เป็นการมอบสิทธิประโยชน์ให้กับบุคลากรที่มีการปฏิบัติงานของมหาวิทยาลัยให้สามารถปฏิบัติงานด้านระบบสารสนเทศตามหน้าที่ของตนเองที่ได้รับมอบหมายในการมองเห็นข้อมูลส่วนตัวผ่านระบบสารสนเทศและการปฏิบัติงานด้านวิชาการของอาจารย์ผู้สอนที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศขึ้นด้วย แต่ผู้รับผิดชอบในการปฏิบัติงานการกำหนดสิทธิ์ระบบสารสนเทศให้ผู้ขอรับบริการ ยังพบปัญหาจากผู้ใช้งานอยู่ เพื่อให้เป็นแนวทางในการศึกษาปัญหาและอุปสรรค จึงได้มีการรวบรวมปัญหาและแนวทางการแก้ไข ไว้ดังนี้

ขั้นตอนดำเนินงาน	ปัญหา/อุปสรรค	แนวทางแก้ไข
การกำหนดสิทธิ์การใช้งานของผู้ใช้งานระบบสารสนเทศ	1. ขอสิทธิ์โดยไม่มีเอกสารบันทึกข้อความหรือแบบฟอร์มขอใช้งานระบบ	- ทำการตรวจสอบจากผู้ใช้โดยตรงด้วยการติดต่อสื่อสารกับตัวบุคคลนั้นและทางโทรศัพท์เพื่อยืนยันข้อมูลที่เป็นความจริงและถูกต้อง

ขั้นตอนดำเนินงาน	ปัญหา/อุปสรรค	แนวทางแก้ไข
การกำหนดสิทธิ์การใช้งานของผู้ใช้งานระบบสารสนเทศ	2. การสร้างสิทธิ์ในระบบเกิดความซ้ำซ้อนกันกับที่มีอยู่ในระบบ จากสาเหตุที่บุคลากรมีการเปลี่ยนสถานะภาพการบรรจุแต่งตั้งใหม่	- ดำเนินการตรวจสอบข้อมูลเบื้องต้นภายในระบบ เพื่อตรวจเช็คข้อมูลเบื้องต้นและสอบถามโดยตรงจากผู้ขอใช้งานและผู้ที่เกี่ยวข้อง
	3. การยกเลิกสิทธิ์ของผู้ใช้งานเมื่อมีการเปลี่ยนสถานะภาพ เช่น ลาออก, เปลี่ยนหน่วยงาน, เปลี่ยนตำแหน่งการปฏิบัติงานภายในหน่วยงานนั้น เป็นต้น โดยไม่มีเอกสารแจ้งกลับมาที่สำนักคอมพิวเตอร์	- ผู้ปฏิบัติงานได้รับแจ้งโดยตรงจากผู้ใช้งานเองหรือบุคลากรในหน่วยงานติดต่อเข้ามาเพื่อขอยกเลิกสิทธิ์ของบุคคลนั้น พร้อมแจ้งให้หน่วยงานต้นสังกัดทำบันทึกข้อความยกเลิกสิทธิ์การใช้งานของบุคลากรดังกล่าวด้วย
	4. ไม่มีขั้นตอนที่ชัดเจนให้บุคลากรที่เข้าใหม่หรือบุคลากรเดิมที่ต้องการขอสิทธิ์ใช้งานระบบเพิ่มเติมให้สามารถขอใช้งานได้ทันที	- จัดทำขั้นตอน (Flowchart) เกี่ยวกับลำดับการขอใช้สิทธิ์ใหม่ และเพิ่มเติม
	5. ไม่มีคู่มือการปฏิบัติงานในการกำหนดสิทธิ์การใช้งานของผู้ใช้งานระบบสารสนเทศ (MIS - ERP)	- จัดทำคู่มือหรือขั้นตอนการกำหนดสิทธิ์การใช้งานของผู้ใช้งานระบบสารสนเทศ (MIS - ERP) ที่แสดงรายละเอียดการปฏิบัติตั้งแต่เริ่มจนสิ้นสุดกระบวนการกำหนดสิทธิ์การใช้งานของผู้ใช้งานระบบสารสนเทศ

ข้อเสนอแนะเพื่อการพัฒนา

จากปัญหาอุปสรรคในปฏิบัติงานการกำหนดสิทธิ์การใช้งานของผู้ใช้งานระบบสารสนเทศเพื่อการบริหารมหาวิทยาลัย (MIS: Management Information System) และระบบสารสนเทศเพื่อการบริหารทรัพยากรองค์กร (ERP: Enterprise Resource Resource Planning) ของบุคลากรในมหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา ผู้ปฏิบัติงานได้เสนอแนวทางแก้ไขปัญหาข้างต้นภายใต้ข้อจำกัดและปัจจัยต่างๆ ซึ่งล้วนแต่เป็นปัญหาที่ผู้ปฏิบัติงานไม่สามารถควบคุมได้ ผู้ปฏิบัติงานจึงขอเสนอแนะเพื่อการพัฒนางานให้มีประสิทธิภาพและประสิทธิผลต่อไปไว้ ดังนี้

1. ควรมีการแจ้งประชาสัมพันธ์ขั้นตอนการยื่นขอกำหนดสิทธิ์การใช้งานระบบสารสนเทศของมหาวิทยาลัยให้กับบุคลากรที่บรรจุใหม่ให้รับทราบ

2. หน่วยงานที่ดูแลระบบสารสนเทศ ควรมีการจัดทำบันทึกข้อความส่งหน่วยงานภายในเรื่อง การขอสิทธิ์การใช้งานของผู้ใช้งานระบบสารสนเทศของบุคลากรที่บรรจุใหม่ และบุคลากรเดิมที่ต้องการสิทธิ์เพิ่มเติมจากการเปลี่ยนตำแหน่งหน้าที่ในการปฏิบัติงานให้เป็นปัจจุบัน

3. หากมีการจัดประชุมหรือการจัดอบรมบุคลากรที่บรรจุใหม่ ควรมีการแนะนำการให้บริการด้านระบบสารสนเทศของมหาวิทยาลัยที่ควรได้รับสิทธิประโยชน์ของระบบต่างๆ เบื้องต้นได้

4. ผู้บริหารควรให้ความสำคัญกับสิทธิ์การเข้าใช้งานของระบบสารสนเทศในการเปลี่ยนแปลง ยกเลิกสิทธิ์ของบุคลากรในสังกัดหน่วยงานของตนในการปฏิบัติงาน เพื่อให้เกิดความปลอดภัยของข้อมูลส่วนตัวด้วย

บรรณานุกรม

เรืองชัย จรุงศิรวัฒน์. (2553). **เทคนิคการเขียนคู่มือการปฏิบัติงาน.**ขอนแก่น : ศูนย์ผลิตเอกสาร มหาวิทยาลัยขอนแก่น.

สำนักคอมพิวเตอร์ มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา. (2560). **รายงานประจำปี 2560** ค้นเมื่อวันที่ 3 มกราคม 2560. จาก http://cc.bsru.ac.th/

สำนักงานคณะกรรมการพัฒนาระบบราชการ. (2552). **การจัดทำคู่มือการปฏิบัติงาน**.กรุงเทพฯ : โรงพิมพ์ ก.กลพิมพ์.

ประวัติผู้เขียน

ชื่อ-สกุล นางสาวบังอร เหล่าปิ่นเพชร

วัน เดือน ปีเกิด 10 มิถุนายน พ.ศ. 2526

ประวัติการศึกษา

ระดับปริญญาตรี วิทยาศาสตรบัณฑิต
สาขาวิชาวิทยาการคอมพิวเตอร์
มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา
พ.ศ. 2550

ระดับปริญญาโท ครุศาสตร์อุตสาหกรรมมหาบัณฑิต
สาขาวิชาคอมพิวเตอร์และเทคโนโลยีสารสนเทศ
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี
พ.ศ. 2556

ประวัติการทำงาน นักวิชาการคอมพิวเตอร์
สำนักคอมพิวเตอร์
มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา
พ.ศ. 2551 – ปัจจุบัน