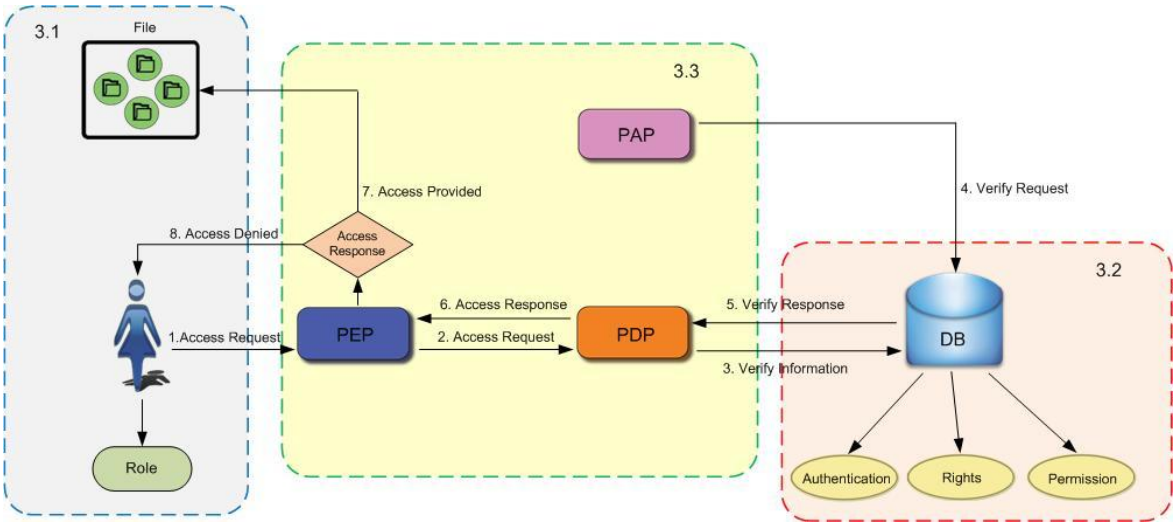
บทที่ 3
การดำเนินการและเครื่องมือ

จากการศึกษาธรรมชาติการทำงานขององค์กร การวิเคราะห์องค์ประกอบต่างๆ ค้นคว้าทฤษฎีและงานวิจัยที่เกี่ยวข้องในบทที่ 2 นั้น ในบทที่ 3 นี้จะกล่าวถึงการออกแบบและขั้นตอนจัดทำระบบงานบริหารจัดการและควบคุมการเข้าถึงเอกสารผ่านเว็บ ทั้งนี้ผู้จัดทำได้แสดงขั้นตอน โดยครอบคลุมรายละเอียดตั้งแต่การศึกษาองค์ประกอบของระบบ วิเคราะห์และออกแบบระบบ และการพัฒนาระบบ ดังรูปที่ 1 แสดงภาพรวมของระบบ



รูปที่ 3.1 ภาพรวมของระบบ

รูปที่ 3.1 แสดงภาพรวมของระบบตั้งแต่ องค์ประกอบของระบบ การจัดเก็บข้อมูลองค์ประกอบของระบบในฐานข้อมูล กระบวนการทำงานของระบบในการอนุญาตและตรวจสอบสิทธิ์ของผู้ใช้ที่เข้าใช้งานระบบ ภาพรวมการทำงานของระบบเริ่มจาก user ใช้ข้อมูลระบุตัวตน (identity) ของตนจากการผ่านการพิสูจน์ตัวตนด้วย username และ password ส่งคำร้องขอ (request) ไป PEP (Policy Enforcement Point) หลังจากนั้น PEP จะส่ง Request ที่ได้รับจากผู้ใช้ไปยัง PDP (Policy Decision Point) เป็นจุดตรวจสอบระหว่างคำร้องขอกับข้อมูลสิทธิ์และข้อมูลนโยบายความ

มั่นคงที่มีอยู่ในระบบ โดย PDP จะเข้าไปดึงเอาข้อมูลเหล่านี้จากฐานข้อมูลเพื่อนำมาตรวจสอบกับคำร้องขอ ทั้งนี้ข้อมูลสิทธิ์และข้อมูลนโยบายความมั่นคงในฐานข้อมูลทั้งกล่าว ได้รับการบริหารจัดการผ่าน PAP (Policy Administrative Point) โดยผู้ดูแลระบบ

หลังจากที่ PDP ดึงข้อมูลที่จำเป็นต่อการตัดสินใจจากฐานข้อมูล และตรวจสอบตามเงื่อนไขที่กำหนดแล้ว PDP จะแจ้งกลับไปยัง PEP เพื่อระบุว่าคำร้องของดังกล่าวได้รับอนุญาตหรือไม่ หากได้รับอนุญาต PEP จะอนุญาตให้ user สามารถเข้าใช้งาน object ได้ มิเช่นนั้น PEP จะไม่อนุญาตให้ user เข้าใช้งาน Object ดังกล่าวได้

จากภาพรวมข้างต้น สามารถอธิบายส่วนประกอบและรายละเอียดต่างๆ ที่เกี่ยวข้องกับกระบวนการดังกล่าวดังต่อไปนี้

3.1 ศึกษาองค์ประกอบของระบบ

3.1.1 การแบ่งกลุ่มข้อมูลขององค์กร (Object Group)

จากบทที่ 2 ทรัพยากรที่ในสมาคมฯ ที่ต้องการบริหารจัดการคือข้อมูลหรือเอกสารในเครื่องคอมพิวเตอร์ส่วนบุคคล ได้แก่ Microsoft Office (Excel , Word , Power Point) รูปภาพ เป็นต้น ในการแบ่งกลุ่มข้อมูลดังกล่าว มีรายละเอียดดังต่อไปนี้

1. การแบ่งกลุ่มข้อมูล (Object) การแบ่งข้อมูลภายในองค์กรสามารถแบ่งกลุ่มข้อมูลด้วยรูปแบบดังต่อไปนี้

1.1 การแยกข้อมูลตามโครงสร้างองค์กร ใช้สำหรับแบ่งข้อมูลที่เป็นงานหลักภายในองค์กร ซึ่งเป็นงานที่เจ้าหน้าที่ปฏิบัติเป็นประจำ ในการแบ่งข้อมูลตามโครงสร้างจะประกอบด้วยกลุ่มข้อมูลดังต่อไปนี้

กลุ่มข้อมูลหลัก หมายถึงกลุ่มข้อมูลที่แบ่งตามสำนักฯ อยู่ภายใต้โครงสร้างองค์กร

กลุ่มข้อมูลรอง หมายถึงกลุ่มข้อมูลย่อยที่อยู่ภายใต้กลุ่มข้อมูลหลัก แบ่งตามฝ่ายงานในกลุ่มข้อมูลหลักซึ่งในแต่ละฝ่ายมีการระบุหน้าที่ได้อย่างชัดเจน

1.2 การแยกข้อมูลตามภาระหน้าที่ ใช้สำหรับแบ่งข้อมูลการดำเนินงานที่นอกเหนือจากงานตามโครงสร้างภายในองค์กร ซึ่งมีการกำหนดระยะเวลาในการทำงาน เนื่องจากเป็นงานที่ได้เขียนโครงการเพื่อของบประมาณจากแหล่งทุนและดำเนินงานตามกลุ่มเป้าหมายของโครงการ

2. การแยกข้อมูลตามแหล่งที่มาของข้อมูล (Source) หมายถึงข้อมูลที่จัดเก็บไว้ในระบบสามารถแบ่งออกเป็น 2 ประเภทดังนี้

2.1. ข้อมูลจากองค์กร (Organization) หมายถึงข้อมูลภายในองค์กรที่เจ้าหน้าที่จัดเก็บไว้ในกลุ่มของข้อมูล ผู้ใช้ที่ไม่เกี่ยวข้องกับกลุ่มข้อมูลนั้นต้องได้รับอนุญาตจึงจะมีสิทธิ์เข้าถึงข้อมูลได้

2.2 ข้อมูลจากเจ้าของข้อมูล (Owner) หมายถึงข้อมูลที่ผู้ใช้เป็นคนจัดเก็บไว้ในระบบตามกลุ่มข้อมูลของผู้ใช้

1. การจัดการกลุ่มข้อมูล

กลุ่มข้อมูลที่ได้จากการแบ่งตามโครงสร้างขององค์กร และจากการแบ่งตามงานโครงการต่างๆ ที่ดำเนินงานภายในองค์กร มีลักษณะดังตัวอย่างข้อมูลในตารางที่ 1 ข้อมูลเหล่านี้จะถูกนำมากำหนดสิทธิ์การเข้าถึงต่อไป

ตารางที่ 3.1 ตัวอย่างการแบ่งกลุ่มข้อมูล

ข้อมูลหลัก	ข้อมูลรอง	Group
ข้อมูลงานบริหารกลาง		A
	ข้อมูลงานบริหาร	A1
	ข้อมูลงานเลขา	A1.1
	ข้อมูลงานสารบัญ	A1.2
	ข้อมูลบุคคลากร	A1.3
	ข้อมูลงานด้านบัญชีการเงิน	A2
	ข้อมูลงานบัญชี	A2.1
	ข้อมูลงานการเงิน	A2.2
	ข้อมูลงานพัสดุ	A2.3
ข้อมูลงานโครงการด้านเอดส์		B
	ข้อมูลงานด้านเอดส์กลุ่มพนักงานบริการหญิง	B1
	ข้อมูลงานด้านเอดส์กลุ่มชายรักชาย	B2
	ข้อมูลงานด้านเอดส์กลุ่มเด็กและวัยเจริญพันธ์	B3

จากตารางการแบ่งกลุ่มภายในองค์กร สามารถสร้างตารางการกำหนดสิทธิ์การเข้าถึงข้อมูลได้ดังตารางที่ 3.2

ตารางที่ 3.2 ตารางแสดงสิทธิ์การเข้าถึงข้อมูลของผู้ใช้

รายชื่อเจ้าหน้าที่ภายในองค์กร	**Group**								
	A						B		
	A1.1	A1.2	A1.3	A2.1	A2.2	A2.3	B1	B2	B3
John									
Alicce									
gift									
Kob									
Lee									
la									
Vud									
Pam									

ทั้งนี้ เงื่อนไขในการกำหนดสิทธิ์ขึ้นอยู่กับนโยบายการเข้าถึงในตารางที่ 4 ACLs อันจะกล่าวถึงในหัวข้อที่ 3.2

3.1.2 การควบคุมการเข้าถึงตามบทบาท (Role-based Access Control)

ในการอนุญาตให้สามารถเข้าถึงกลุ่มข้อมูลดังที่ได้แบ่งกลุ่มข้างต้นนั้น สามารถกำหนดการควบคุมการเข้าถึงโดยใช้บทบาทความสามารถและความรับผิดชอบบนพื้นฐานโครงสร้างองค์กร (Role-base) ผู้ใช้จะสามารถใช้งานกลุ่มข้อมูลได้ตามบทบาทที่ได้รับมอบหมาย แต่การทำงานภายในสมาคมฯ (กรณีศึกษา) ไม่ได้กำหนดสิทธิ์การเข้าถึงกลุ่มข้อมูลตามบทบาทเท่านั้น นั่นหมายถึง ผู้ใช้บางคนสามารถเข้าใช้งานกลุ่มข้อมูลนอกเหนือจากบทบาทความสามารถและความรับผิดชอบ ดังนั้นสามารถแบ่งบทบาทออกเป็น 2 ส่วนดังต่อไปนี้

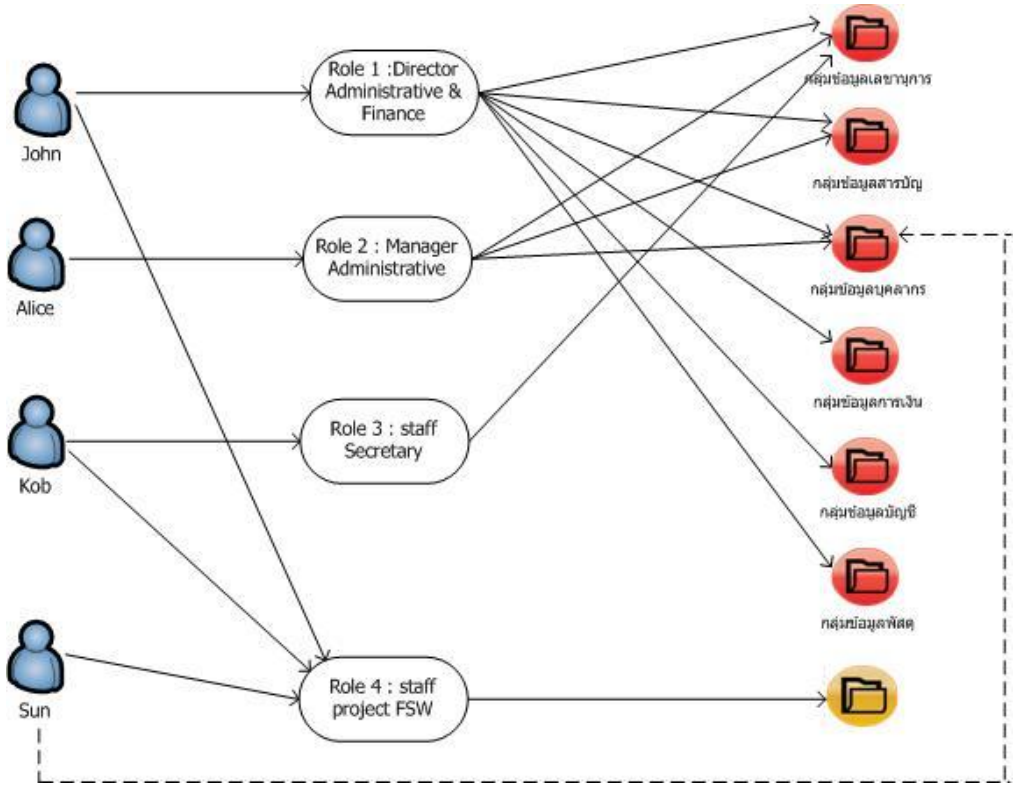
1. Role-base การอนุญาตและกำหนดสิทธิ์ตามบทบาทหน้าที่ที่ได้รับมอบหมาย แบ่งได้ 2 ลักษณะได้แก่

1.1 บทบาทตามโครงสร้าง เป็นการกำหนดสิทธิ์ตามหน้าที่ที่ปฏิบัติเป็นประจำ

1.2 บทบาทตามภาระหน้าที่ เป็นการกำหนดสิทธิ์ตามภาระหน้าที่ที่ได้รับมอบหมายเพิ่มจากงานที่ปฏิบัติเป็นประจำ เช่น งานโครงการ หรือ งานฝ่ายอื่นๆ เป็นต้น

2. Adhocs การอนุญาตและกำหนดสิทธ์ให้สามารถเข้าถึงข้อมูลได้โดยที่ผู้ใช้ไม่ได้มีส่วนเกี่ยวข้องกับกลุ่มข้อมูลนั้น เช่น เจ้าหน้าที่โครงการสามารถเข้าถึงข้อมูลตามบทบาทคือกลุ่มข้อมูลโครงการที่ดำเนินงานอยู่ แต่ได้รับอนุญาตให้สามารถเข้าถึงกลุ่มข้อมูลบุคลากร เป็นต้น

จากบทบาท (Role) ทั้ง 2 ส่วน สามารถแสดงเป็นรูปภาพดังต่อไปนี้



รูปที่ 3.2 แสดงสิทธิ์การเข้าถึงข้อมูลตามบทบาทและนอกเหนือบทบาท (Role and Adhocs)

รูปที่ 3.2 แสดงสิทธิ์การเข้าถึงข้อมูลตามที่ได้รับอนุญาต ซึ่งในการอนุญาตประกอบด้วยการอนุญาตตามบทบาท และนอกเหนือบทบาท สามารถอธิบบายได้ดังนี้

บทบาทตามโครงสร้าง (Role)

Role 1 : Director Administrative & Finance สามารถเข้าถึงกลุ่มข้อมูลดังนี้ กลุ่มข้อมูลเลขานุการ กลุ่มข้อมูลบุคลากร กลุ่มข้อมูลสารบัญ กลุ่มข้อมูลการเงิน กลุ่มข้อมูลบัญชี กลุ่มข้อมูลพัสดุ ผู้ใช้ได้รับที่สิทธิ์ใน Role นี้คือ John

Role 2 : Manager Administrative สามารถเข้าถึงกลุ่มข้อมูลดังนี้ กลุ่มข้อมูลเลขานุการ กลุ่มข้อมูลบุคลากร กลุ่มข้อมูลสารบัญ ผู้ใช้ที่รับสิทธิ์ใน Role นี้คือ Alice

Role 3 : Staff Secretary สามารถเข้าถึงกลุ่มข้อมูลได้แก่ กลุ่มข้อมูลเลขานุการ ผู้ใช้ที่รับสิทธิ์ใน Role นี้คือ Kob

Role 4 : Staff Project FSW สามารถเข้าถึงกลุ่มข้อมูลได้แก่ กลุ่มข้อมูลโครงการเอดส์ FSW ผู้ใช้ที่รับสิทธิ์ใน Role นี้คือ John , Kob , Sun

บทบาทนอกเหนือโครงสร้าง (Non-Role)

ผู้ใช้ที่ได้รับสิทธิ์ให้สามารถเข้าถึงข้อมูลอื่นๆ นอกเหนือสิทธิ์ที่ได้รับตาม Role ได้แก่ Sun เนื่องจาก Sun ได้รับอนุญาตให้สามารถเข้าถึงข้อมูล กลุ่มข้อมูลบุคลากร ได้แต่ไม่ได้มีส่วนเกี่ยวข้องกับข้อมูล

3.1.3 บทบาทที่มีส่วนเกี่ยวข้องกับระบบ (Role)

ผู้ใช้ที่ปฏิบัติงานภายในสมาคมฯ สามารถแบ่งระดับผู้ใช้ที่มีส่วนเกี่ยวข้องกับระบบมีดังต่อไปนี้

1. ผู้อำนวยการสมาคมฯ (Director) หมายถึง ผู้บริหารสูงสุง เป็นผู้มีอำนาจแต่งตั้งให้ผู้อำนวยการสำนักฯ สามารถให้สิทธิ์ให้กับผู้ใช้งานและกำหนดขอบเขตความสามารถเข้าถึงกลุ่มข้อมูล

2. ผู้อำนวยการสำนักฯ (Director of Department) หมายถึง ผู้ที่ดำรงตำแหน่งเป็นผู้อำนวยการสำนักฯ และได้รับมอบหมายจากผู้อำนวยการสมาคมฯ ในการให้สิทธิ์ให้กับผู้ใช้ที่เกี่ยวข้องกับกลุ่มข้อมูลภายใต้สำนักฯ ที่บังคับบัญชา รวมถึงขอบเขตในการเข้าถึงข้อมูล

3. ผู้ใช้งานระบบ (User) หมายถึง เจ้าหน้าที่ที่ปฏิบัติงานอยู่ภายในสมาคมฯ และดำรงตำแหน่งเจ้าหน้าที่ภายใต้สำนักฯ สามารถเข้าใช้งานระบบตามสิทธิ์ที่ได้รับ

4. ผู้ดูแลระบบ (Admin) หมายถึง ผู้ที่ได้รับมอบหมายให้มีหน้าที่บริหารจัดการระบบตามคำสั่งของผู้อำนวยการสมาคมฯและผู้อำนวยการสำนักฯ

3.2 วิธีการจัดเก็บข้อมูลเพื่อใช้ในกระบวนการควบคุมการเข้าถึง

3.2.1 การกำหนดสิทธิ์และควบคุมการเข้าถึงข้อมูลของผู้ใช้

หลังจากมีการวิเคราะห์โครงสร้าง ทรัพยากร และผู้ใช้ภายในองค์กร ขั้นตอนต่อไปคือการกำหนดสิทธิ์การเข้าถึงข้อมูลให้กับเจ้าหน้าที่ภายในองค์กร โดยการประชุมเพื่อหาข้อตกลงและสรุปการให้สิทธิ์ให้กับเจ้าหน้าที่ที่เกี่ยวข้องกับกลุ่มข้อมูล ผู้ที่เข้าร่วมประชุมได้แก่

1. ผู้อำนวยการสมาคมฯ
2. ผู้อำนวยการสำนักฯ
3. ผู้ดูแลระบบ

ในการประชุมจะมีการกำหนดหัวข้อและรายละเอียดการประชุมดังต่อไปนี้

1. การกำหนดสิทธิ์และควบคุมการเข้าถึงตามโครงสร้างองค์กร

เป็นการหารือเพื่อกำหนดการแบ่งกลุ่มข้อมูลและกำหนดสิทธิ์ให้กับผู้ใช้ภายใต้กลุ่มข้อมูลนั้นตามโครงสร้างขององค์กร รวมถึงการกำหนด Role-base ตามโครงสร้าง ซึ่งเป็นการปฏิบัติงานของเจ้าหน้าที่เป็นประจำอยู่แล้ว โดยจะทำการแยกข้อมูลออกเป็นกลุ่มหลัก และกลุ่มรอง จากนั้นกำหนดสิทธิ์และควบคุมการเข้าถึงข้อมูลให้เจ้าหน้าที่สามารถเข้าถึงข้อมูลได้ตามบทบาทและตามที่ได้รับอนุญาตจากผู้อำนวยการสำนักฯ

2. การกำหนดสิทธิ์และควบคุมการเข้าถึงตามภาระหน้าที่

เป็นการหารือเพื่อกำหนดสิทธิ์ให้กับเจ้าหน้าที่ที่ทำงานนอกเหนือจากงานที่ปฏิบัติเป็นประจำตามโครงสร้าง การทำงานนี้จะเป็นงานโครงการฯ ที่ได้รับงบประมาณจากแหล่งทุนให้ดำเนินงานตามเป้าหมายที่กำหนด เจ้าหน้าที่สมาคมฯ บางคนได้รับมอบหมายให้ดำเนินงานควบคู่ไปกับงานหลักที่ทำเป็นประจำ ดังนั้นการกำหนดสิทธิ์ในกลุ่มข้อมูลนี้ผู้ที่มีหน้าที่ให้สิทธิ์คือผู้อำนวยการโครงการ เพื่อให้เจ้าหน้าที่สามารถเข้าถึงข้อมูลได้ตามที่ได้รับอนุญาตให้สิทธิ์การเข้าถึง

3. การกำหนดสิทธิ์ให้กับเจ้าหน้าที่โครงการฯ

เป็นการหารือเพื่อกำหนดสิทธิ์ให้กับเจ้าหน้าที่ประจำโครงการฯ ซึ่งยังไม่ได้เป็นเจ้าหน้าที่ภายในองค์กร ดังนั้นสิทธิ์การเข้าถึงข้อมูลบางอย่างจะไม่สามารถได้รับอนุญาตจากผู้อำนวยการสำนักฯ เนื่องจากเป็นข้อมูลที่รับทราบกันภายในเท่านั้น ซึ่งการกำหนดนี้จำเป็นต้องได้รับการยืนยันจากผู้อำนวยการสำนักฯต่างๆ ถึงการให้สิทธิ์กับเจ้าหน้าที่โครงการฯ รวมทั้งการกำหนด Role-base ตามโครงการ

3.2.2 การกำหนดสิทธิ์และความสามารถในการใช้กลุ่มข้อมูล

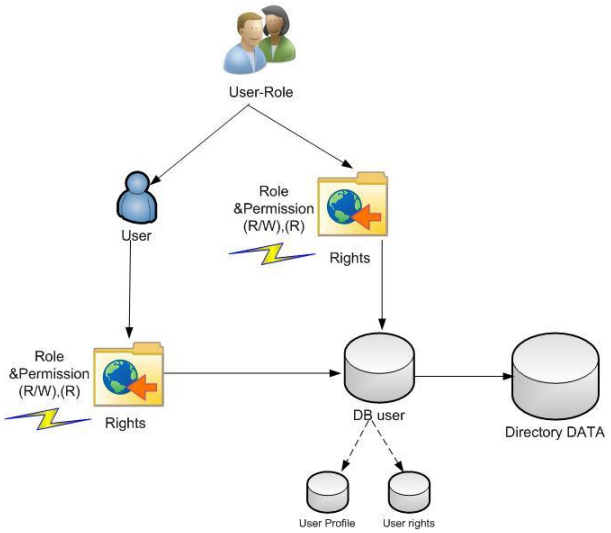
หลังจากกำหนดขอบเขตให้เจ้าหน้าที่ภายในองค์กรสามารถเข้าถึงแหล่งข้อมูลใดได้บ้าง ตามบทบาทและภาระหน้าที่ของผู้ใช้แล้ว จากนั้นเป็นการกำหนดรายละเอียดเกี่ยวกับสิทธิ์ความสามารถในการกระทำกับกลุ่มข้อมูล โดยการประชุมผู้บริหารและผู้ที่มีให้สิทธิ์ในการใช้งานข้อมูล มีรายละเอียดดังต่อไปนี้

1. “R/W” (Read/Write) หมายถึงผู้ใช้ได้รับสิทธิ์ให้สามารถบริหารจัดการข้อมูลภายในกลุ่มข้อมูลนั้น ได้แก่ ดาวน์โหลด อัพโหลด ลบ เอกสารได้

2. “R” (Read only) หมายถึงผู้ใช้ได้รับให้สามารถสิทธิ์เข้าถึงข้อมูลภายในกลุ่มข้อมูลได้แก่ ดาวน์โหลดเอกสาร เท่านั้น

3. ผู้ใช้ไม่ได้รับสิทธิ์ให้สามารถบริหารจัดการข้อมูลและเข้าถึงข้อมูลได้

3.2.3 ความสัมพันธ์ระหว่างบทบาทกับสิทธิ์ (Role and Rights)



รูปที่ 3.3 แสดงความสัมพันธ์ระหวางบทบาทกับสิทธิ์

ในการควบคุมการเข้าถึงและกำหนดสิทธิ์ภายในสมาคมฯ นอกจากจะกำหนดสิทธิ์ตามบทบาทโครงสร้างภายในองค์กรแล้ว ยังกำหนดตามบทบาทตามภาระหน้าที่ที่ได้รับมอบหมายเพิ่มจากบทบาทตามโครงสร้าง ในรูปที่ 3 ผู้ใช้สามารถได้รับสิทธิ์การใช้งานกลุ่มข้อมูลตาม Role ของโครงสร้างองค์กร (user-role) ซึ่งระบุไว้อย่างชัดเจนในสิทธิ์ที่ได้รับและข้อจำกัดของ Role นั้น เพื่อเข้าใช้งานกลุ่มข้อมูลในฐานข้อมูลได้ นอกจากนี้ยังสามารถได้รับสิทธิ์จาก role อื่นๆ ตามภาระหน้าที่ที่ได้รับมอบหมาย เพื่อให้สามารถเข้าใช้งานกลุ่มข้อมูลในฐานข้อมูลได้

ตัวอย่าง การบทบาทผู้ใช้และสิทธิ์

จากตารางที่ 1 แสดงตัวอย่างการแบ่งกลุ่มข้อมูลข้อมูลสำนักบริหารกลาง (Group A) และโครงการเอดส์ (Group B) ประกอบด้วยข้อมูลหลัก และข้อมูลรอง เพื่อใช้ในการกำหนดสิทธิ์ และกำหนดระดับความปลอดภัยของแต่ละกลุ่มข้อมูล จากนั้นสามารถสร้างตารางที่ 3 RBAC เพื่อใช้ในการกำหนดสิทธิ์ตามบทบาทได้ดังนี้

ตารางที่ 3.3 แสดงตัวอย่าง Role-base

Role No.	Role (ตำแหน่ง)	Rights								
		เลขานุการ	บุคลากร	สารบัญ	บัญชี	การเงิน	พัสดุ	FSW	MSM	Childlive
Role 1	ผู้อำนวยการสำนักบริหารกลาง	√	√	√	√	√	√			
Role 2	ผู้จัดการงานบริหาร	√	√	√						
Role 3	ผู้จัดการ Finance				√	√	√			
Role 4	เจ้าหน้าที่เลขานุการ	√								
Role 5	เจ้าหน้าที่บุคลากร		√							
Role 6	เจ้าหน้าที่สารบัญ			√						
Role 7	เจ้าหน้าที่บัญชี				√					
Role 8	เจ้าหน้าที่การเงิน					√				
Role 9	เจ้าหน้าที่พัสดุ						√			
Role 10	ผู้อำนวยการโครงการเอดส์							√	√	√
Role 11	เจ้าหน้าที่โครงการ FSW							√		
Role 12	เจ้าหน้าที่โครงการ MSM								√	
Role 13	เจ้าหน้าที่โครงการ Childlive									√

Access Control Lists (ACLs Group A , B)

การกำหนดสิทธิ์เจ้าหน้าที่ภายในสำนักบริหารกลางและเจ้าหน้าที่โครงการด้านเอดส์

ตารางที่ 3.4 แสดงความสัมพันธ์ของสิทธิ์การเข้าถึงข้อมูลระหว่างผู้ใช้กับกลุ่มข้อมูล

รายชื่อเจ้าหน้าที่	Role No.	Group / Authorization & Authentication								
		สำนักบริหารกลาง						งานโครงการด้านเอดส์		
		งานบริหาร			Finance					
		เลขานุการ	บุคลากร	สารบัญ	บัญชี	การเงิน	พัสดุ	FSW	MSM	Childlive
John	Role 1	R/W	R/W	R/W	R/W	R/W	R/W			
	Role 11							R/W		
	Role 12								R/W	
	Role 13									R/W
Alice	Role 2	R/W	R/W	R/W						
	Role 11							R		
	Role 12								R	
	Role 13									R
Gift	Role 2	R	R	R						
	Role 11							R		
	Role 12								R	
	Role 13									R
Kob	Role 4	R/W								
	Role 11							R/W		
	Role 12								R	
	Role 13									R
Lee	Role 6			R/W						
	Role 11							R		
	Role 12								R	
	Role 13									R

ตารางที่ 3.4 (ต่อ)

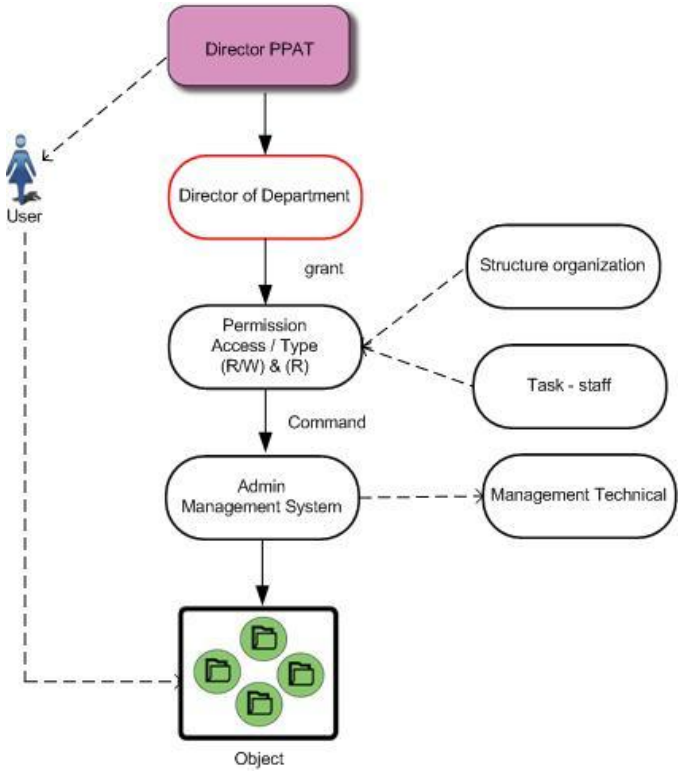
รายชื่อเจ้าหน้าที่	Role No.	Group / Authorization & Authentication								
		สำนักบริหารกลาง						งานโครงการด้านเอดส์		
		งานบริหาร			Finance					
		เลขานุการ	บุคลากร	สารบัญ	บัญชี	การเงิน	พัสดุ	FSW	MSM	Childlive
	Role 3				R/W	R	R			
	Role 11							R		
	Role 12								R/W	
Koi	Role 13									R
	Role 2	R	R	R						
	Role 8					R/W				
Jo	Role 9						R			
	Role 2	R	R	R						
	Role 8					R				
	Role 9						R			
Puy	Role 13									R/W
	Role 2	R	R	R						
	Role 8					R				
	Role 9						R			
Jack	Role 10							R/W	R/W	R/W
	Role 5		R			R	R	R/W		
	Role 8									
	Role 9									
Sun	Role 11									
	Role 5		R							
	Role 8							R		
	Role 9								R/W	
Paw	Role 11									R

ในตารางที่ 3.4 แสดงภาพรวมรายละเอียดสิทธิ์การเข้าถึงกลุ่มข้อมูลของผู้ใช้แต่ละคนที่ผู้ใช้ได้รับการอนุญาต โดย Role No. สามารถดูได้จากตารางที่ 3 หากมีการเปลี่ยนแปลง โยกย้าย หรือยกเลิกสิทธิ์ สามารถตรวจสอบและบริหารจัดการได้ง่ายขึ้น

3.3 ระบบและกลไกการรักษาความปลอดภัย

จากข้อ 3.1.3 ได้อธิบายผู้ที่เกี่ยวข้องกับระบบภายในสมาคมฯ ในข้อ 3.3 นี้จะกล่าวถึงกระบวนการทำงานของผู้ที่มีส่วนเกี่ยวข้องระบบ มีดังต่อไปนี้

3.3.1 กระบวนการให้สิทธิ์

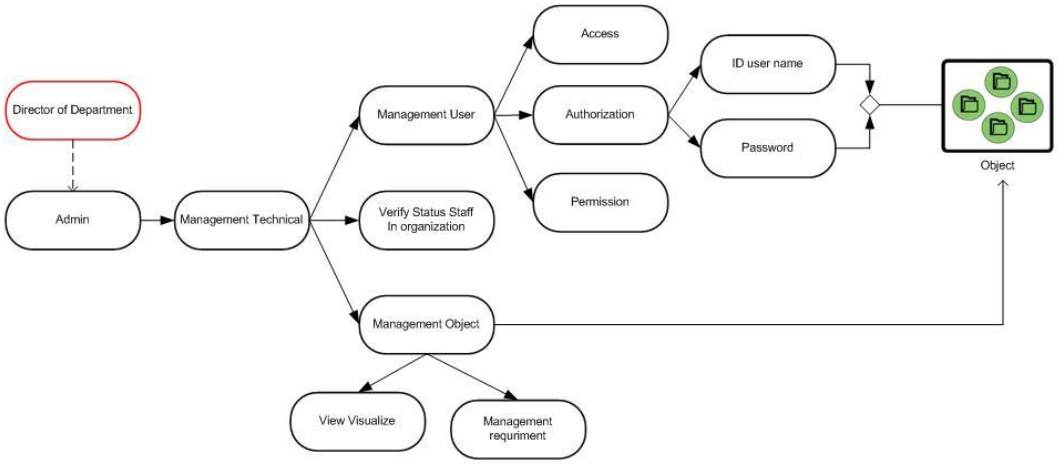


รูปที่ 3.4 กระบวนการดำเนินงานให้สิทธิ์

รูปที่ 3.4 แสดงขั้นตอนการให้สิทธิ์การเข้าถึงข้อมูลให้กับผู้ใช้แต่ละคน เริ่มจากผู้อำนวยการสมาคมฯ มอบหมายให้ผู้อำนวยการสำนักฯ เป็นผู้ให้สิทธิ์ผู้ใช้ โดยในกรณีเจ้าหน้าที่สมาคมฯ สามารถให้สิทธิ์ตามโครงสร้างองค์กร และงานอื่นตามภาระหน้าที่ที่ได้รับมอบหมายนอกเหนือจากงานตามโครงสร้าง เช่น Kob เป็นเจ้าหน้าที่บัญชี และในขณะเดียวกันให้รับผิดชอบงานโครงการเอดส์ FSW เป็นต้น ในการให้สิทธิ์กับผู้ใช้จะต้องควบคู่ไปกับขอบเขตของการเข้าถึงข้อมูลได้แก่ R/W (ดาวน์โหลด อัพโหลด ลบ) และ R (ดาวน์โหลดเท่านั้น) จากนั้นผู้อำนวนการสำนักฯ จะแจ้งให้ผู้ดูแลระบบเป็นผู้สร้างบัญชีผู้ใช้ และกำหนดความสามารถในการเข้าใช้งานระบบ เพื่อป้องกันไม่ให้ผู้ใช้เข้าใช้งานระบบเกินความสามารถที่ได้ระบุไว้ หลังจากผู้ดูแลระบบ

กำหนดค่าแล้วจะแจ้งให้ผู้ใช้สามารถเข้าใช้งานระบบ พร้อมทั้งแจ้งขอบเขตการใช้งานระบบและกลุ่มข้อมูลให้ผู้ใช้รับทราบ

3.3.2 การกำหนดสิทธิ์การเข้าถึงข้อมูลในระบบ



รูปที่ 3.5 การกำหนดสิทธิ์การเข้าถึงข้อมูลให้กับผู้ใช้

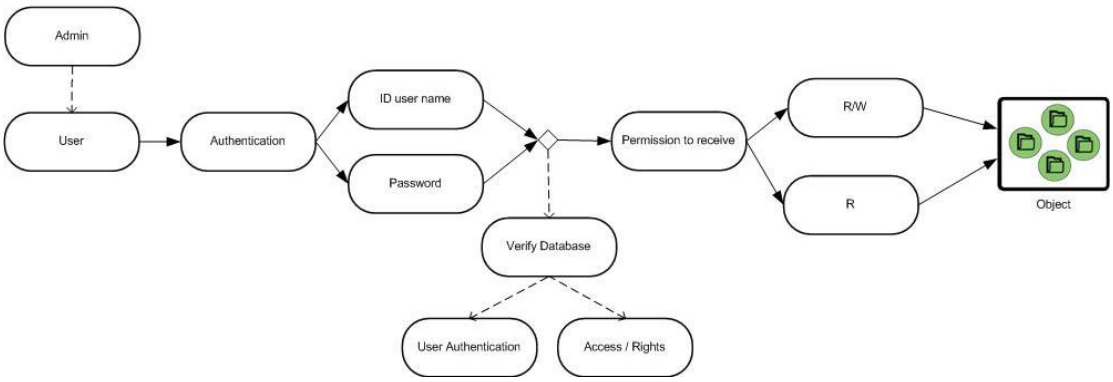
หลังจากที่ผู้อำนวยการสำนักฯ ให้สิทธิ์กับผู้ใช้แล้ว ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงข้อมูลในระบบตามที่ได้รับแจ้งจากผู้อำนวยการสำนักฯ เพื่อป้องกันข้อมูลจากผู้ที่ไม่ได้รับอนุญาต ดังรูปที่ 5 แสดงขั้นตอนการกำหนดสิทธิ์การเข้าถึงข้อมูลให้กับผู้ใช้ มีรายละเอียดดังต่อไปนี้

1. การบริหารจัดการบัญชีผู้ใช้ (Management User) ประกอบด้วยการสร้างบัญชีผู้ใช้เพื่อให้สามารถพิสูจน์ตัวตนด้วยการใช้ user name และ password เพื่อให้สามารถเข้าสู่ระบบได้ และการกำหนดให้ผู้ใช้สามารถเข้าถึง Object ได้ มีองค์ประกอบในการตัดสินใจได้แก่ การควบคุมการเข้าถึง การอนุญาต การให้สิทธิ์ โดยใช้ Identity ที่ผ่านการตรวจสอบ user name และ password ของผู้ใช้ล๊อกอินเข้าสู่ระบบ

2. การตรวจสอบสถานะผู้ใช้ภายในองค์กรเป็นประจำ (verify status staff in organization) เพื่อป้องกันผู้ใช้ที่พ้นสภาพการเป็นเจ้าหน้าที่ หรือเมื่อมีการเพิกถอนสิทธิ์ ไม่ให้สามารถเข้าถึงข้อมูลได้

3. การบริหารจัดการข้อมูล(Management Object) เป็นการกำหนดกลุ่มข้อมูลตามที่ได้รับแจ้งจากผู้อำนวยการสำนักฯ และการเรียกดูมุมมองเมื่อผู้บริหารต้องการประเมินหรือวิเคราะห์สิทธิ์ของผู้ใช้ต่อไป

3.3.3 กระบวนการเข้าถึง Object



รูปที่ 3.6 แสดงกระบวนการเข้าถึงเอกสาร

ในกระบวนการเข้าถึงเอกสารจะประกอบด้วยการพิสูจน์ตัวตนของผู้ใช้ ในรูปที่ 3.6 เริ่มจากผู้ใช้ได้รับแจ้งจากผู้ดูแลระบบให้สมารถเข้าใช้งานระบบได้ ผู้ใช้จะทำการพิสูจน์ตัวตนด้วย user name และ password เพื่อให้สามารถเข้าสู่ระบบได้ จากนั้นนำเอา Identity ที่ผ่านการพิจสูจน์ตัวตน มาตรวจสอบสิทธิ์การเข้าถึงข้อมูล ซึ่งการได้รับสิทธิ์ให้สามารถเข้าถึงกลุ่มข้อมูลนั้นจะกำหนดขอบเขตการใช้งานกลุ่มข้อมูลนั้นๆด้วย ได้แก่ R/W (ดาวน์โหลด อัพโหลด เพิ่ม ลบ) , R (ดาวน์โหลดเท่านั้น)

3.4. วิเคราะห์ความต้องการของระบบและออกแบบระบบ

จากการวิเคราะห์ปัญหาและศึกษาค้นคว้าข้อมูล ในการจัดทำระบบงานบริหารจัดการและควบคุมเอกสารผ่านเว็บ ผู้จัดทำระบบได้ทำการศึกษาจากความต้องการ (Requirement System) เพื่อใช้ในการออกแบบระบบ สามารถอธิบายรายละเอียดดังนี้

3.4.1 วิเคราะห์ความต้องการที่เกี่ยวข้อง

ผู้จัดทำได้วิเคราะห์ความต้องการจากสภาพแวดล้อม ทั้งความต้องการของผู้ใช้ ความต้องการของผู้ดูแลระบบ และความต้องการการทำงานของระบบ โดยสามารถอธิบายรายละเอียดดังต่อไปนี้

1. ความต้องการของผู้ใช้ (User) หมายถึง ความสามารถในการเข้าใช้งานระบบและกลุ่มข้อมูล มีรายละเอียดดังต่อไปนี้

1.1 ความสามารถบริหารจัดการข้อมูล ตามสิทธิ์ที่ได้รับอนุญาต แยกได้ 2 ประเภท ดังนี้

1. ผู้ใช้สามารถเข้าถึงข้อมูลและสามารถบริหารจัดการข้อมูล (R/W) ได้แก่ Upload Download Delete ข้อมูลได้

2. ผู้ใช้สามารถเข้าถึงข้อมูล (R) ได้แก่ Download ข้อมูลได้เท่านั้น

1.2 ผู้ใช้สามารถเปลี่ยนรหัสผ่านส่วนตัวได้ เพื่อป้องกันบุคคลที่ไม่ได้รับอนุญาตแอบอ้างในการเข้าใช้งานระบบและการเข้าถึง แก้ไข เปลี่ยนแปลงข้อมูล

2. ความต้องการผู้ดูแลระบบ (Admin) หมายถึง ผู้ที่ได้รับมอบหมายให้สามารถตั้งค่าในระบบเพื่อกำหนดสิทธิ์การเข้าใช้งานระบบให้กับผู้ใช้ตามที่ได้รับอนุญาตจากผู้อำนวยการสำนักฯ ความสามารถของผู้ดูแลระบบมีรายละเอียดดังต่อไปนี้

2.1 ผู้ดูแลระบบสามารถกำหนดสิทธิ์และบริหารจัดการสิทธิ์การเข้าใช้งานระบบและกลุ่มข้อมูลให้กับผู้ใช้แต่ละคน ตามที่ได้รับอนุญาต

1. สามารถกำหนดสิทธิ์การเข้าถึงและบริหารจัดการข้อมูล (R/W) ให้กับผู้ใช้ตามบทบาทหน้าที่ที่ได้รับอนุมัติจากผู้อำนวยการสำนักฯ ได้แก่ Upload, Download, Delete

2. สามารถกำหนดสิทธิ์การเข้าถึงข้อมูล (R) ให้กับผู้ใช้ตามบทบาทหน้าที่ที่ได้รับอนุมัติจากผู้อำนวยการสำนักฯ ได้แก่ Download ได้เท่านั้น

3. สามารถเปลี่ยนแปลงสิทธิ์การเข้าถึงข้อมูลให้กับเจ้าหน้าที่ในฐานข้อมูลเมื่อมีการเปลี่ยนแปลง เพิกถอน ตามที่ได้รับอนุมัติจากผู้อำนวยการสำนักฯ

2.2 ความสามารถในการบริหารจัดการกลุ่มข้อมูล เมื่อมีการเปลี่ยนแปลงกลุ่มข้อมูลจากโครงสร้างเดิม เช่น องค์กรได้รับงานจากโครงการอื่นๆ เพิ่มจากที่มีอยู่เดิม หรือ โครงการที่มีอยู่เดิมได้ดำเนินงานจนสิ้นสุดโครงการ ผู้ดูแลระบบสามารถบริหารจัดการกลุ่มข้อมูลและกลุ่มผู้ใช้ดังต่อไปนี้

1. สามารถเพิ่มกลุ่มข้อมูลตามที่ได้รับอนุมัติจากผู้อำนวยการสำนักฯ

2. สามารถกำหนดสิทธิ์กลุ่มผู้ใช้กับกลุ่มข้อมูลเมื่อมีการเปลี่ยนแปลงได้

2.3 ความสามารถในการบริหารจัดการบัญชีผู้ใช้

1. บริหารจัดการบัญชีผู้ใช้ เพิ่ม ลบ ข้อมูลส่วนบุคคลในฐานข้อมูลได้

2. สามารถเปลี่ยนแปลงข้อมูลส่วนบุคคลให้กับเจ้าหน้าที่ในฐานข้อมูล

2.4 ความสามารถในการเรียกดูมุมมองภาพรวมหลังจากการกำหนดสิทธิ์ระหว่างผู้ใช้กับกลุ่มข้อมูลหากผู้บริหารร้องขอ เพื่อให้สามารถนำมาวิเคราะห์ความปลอดภัยของกลุ่มข้อมูลและความเหมาะสมของผู้ใช้

3 ความต้องการระบบ

3.1 ระบบสามารถรองรับการจัดเก็บบัญชีผู้ใช้และสามารถบริหารจัดการบัญชีผู้ใช้ได้ ได้แก่ Add , Update , Delete ได้

3.2 ระบบสามารถรองรับการทำงานของผู้ใช้ ตามที่ผู้ดูแลระบบกำหนดสิทธิ์การเข้าถึงข้อมูล

3.3 สามารถตรวจสอบสิทธิ์ผู้ใช้งานระบบ เมื่อมีการล๊อกอิน (Login) เข้าสู่ระบบ

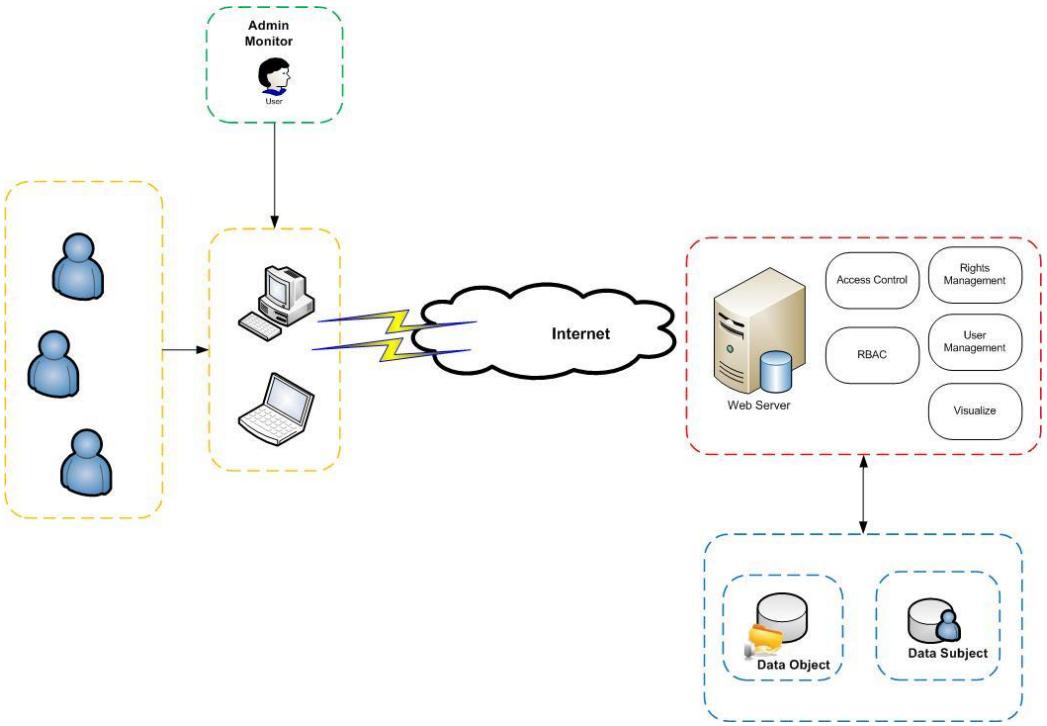
3.4 สามารถควบคุมสิทธิ์การเข้าถึงข้อมูลของผู้ใช้ เพื่อให้ผู้ใช้สามารถใช้งานระบบตามสิทธิ์ที่ได้รับอนุญาตและเพื่อป้องกันการเข้าใช้งานข้อมูลจากผู้ที่ไม่ได้รับอนุญาต

3.5 สามารถแก้ไขการกำหนดสิทธิ์เมื่อมีการเปลี่ยนแปลงผู้ใช้ หรือปรับเปลี่ยนโครงสร้างองค์กร

3.6 สามารถแสดงผลเพื่อนำเสนอมุมมองภาพรวมของสิทธิ์ระหว่างกลุ่มข้อมูลและผู้ใช้ได้อย่างถูกต้อง

3.4.2 การออกแบบระบบ

1. สถาปัตยกรรมระบบ (System Architecture)



รูปที่ 3.7 System Architecture สถาปัตยกรรมการทำงานของระบบ

สถาปัตยกรรมการทำงานของระบบดังรูปที่ 3.7 แสดงรายละเอียดความสามารถการทำงานของระบบในภาพรวม อธิบายดังต่อไปนี้

ผู้ใช้งานระบบสามารถเข้าใช้งานระบบโดยอุปกรณ์คอมพิวเตอร์ (Personal Computer) หรือโน้ตบุค (Notebook) เชื่อมต่อกับอินเตอร์เน็ต (Internet) ผ่านเว็บบราวเซอร์ (Web Browser) เมื่อสามารถเชื่อมต่อได้ระบบจะให้พิสูจน์ตัวตนด้วยการล็อกอิน (Login) เพื่อเข้าสู่การใช้งานระบบในเว็บเซอร์เวอร์ (Web Server) มีองค์ประกอบที่เกี่ยวข้องคือ Access Control (ระบบไม่ได้รองรับ version control) , Rights Management , RBAC , User Management และแผนภาพ ซึ่งองค์ประกอบเหล่านี้จะเป็นส่วนที่นำมากำหนดสิทธิ์ตามที่ได้รับอนุญาตในดาต้าเบส (Database) ได้แบ่งการจัดการและจัดเก็บข้อมูลออกเป็น 2 ส่วนได้แก่

1.1 Data Object เป็นการจัดเก็บและบริหารจัดการในส่วนของกลุ่มข้อมูล

1.2 Data Subject เป็นการจัดเก็บและบริหารจัดการในส่วนของผู้ใช้งานระบบ

ทั้งนี้ Database ทั้ง 2 ส่วน จะนำมากำหนด Permission และควบคุมการเข้าถึงข้อมูล กำหนดขอบเขตความสามารถในการบริหารจัดการข้อมูลตามสิทธิ์ของผู้ใช้แต่ละคนกับข้อมูลประกอบด้วยสิทธิ์ดังนี้

1. R/W (Read and Write) ความสามารถในการบริหารจัดการข้อมูล ได้แก่ Upload Download , Delete ได้

2. R (Read) ความสามารถในการเข้าถึงข้อมูล ได้แก่ Download ได้

3. ไม่สามารถเข้าถึงข้อมูลและบริหารจัดการข้อมูลได้

ผู้ที่มีหน้าที่ในการบริหารจัดการ Database ทั้ง 2 ส่วน คือผู้ดูแลระบบ (Admin Monitoring) เท่านั้น โดยผู้ดูแลระบบจะสามารถบริหารจัดการ Database ดังต่อไปนี้

1. สามารถกำหนดสิทธิ์การเข้าถึงข้อมูลให้กับผู้ใช้ ประกอบด้วยสิทธิ์ดังนี้

1.1 R/W กำหนดให้ผู้ใช้สามารถเข้าถึงและบริหารจัดการข้อมูล ได้แก่ Upload , Download , Delete ได้

1.2 R กำหนดให้ผู้ใช้สามารถเข้าถึงข้อมูลได้เท่านั้น ได้แก่ Download ได้

1.3 กำหนดให้ผู้ใช้ไม่สามารถเข้าถึงกลุ่มข้อมูลได้

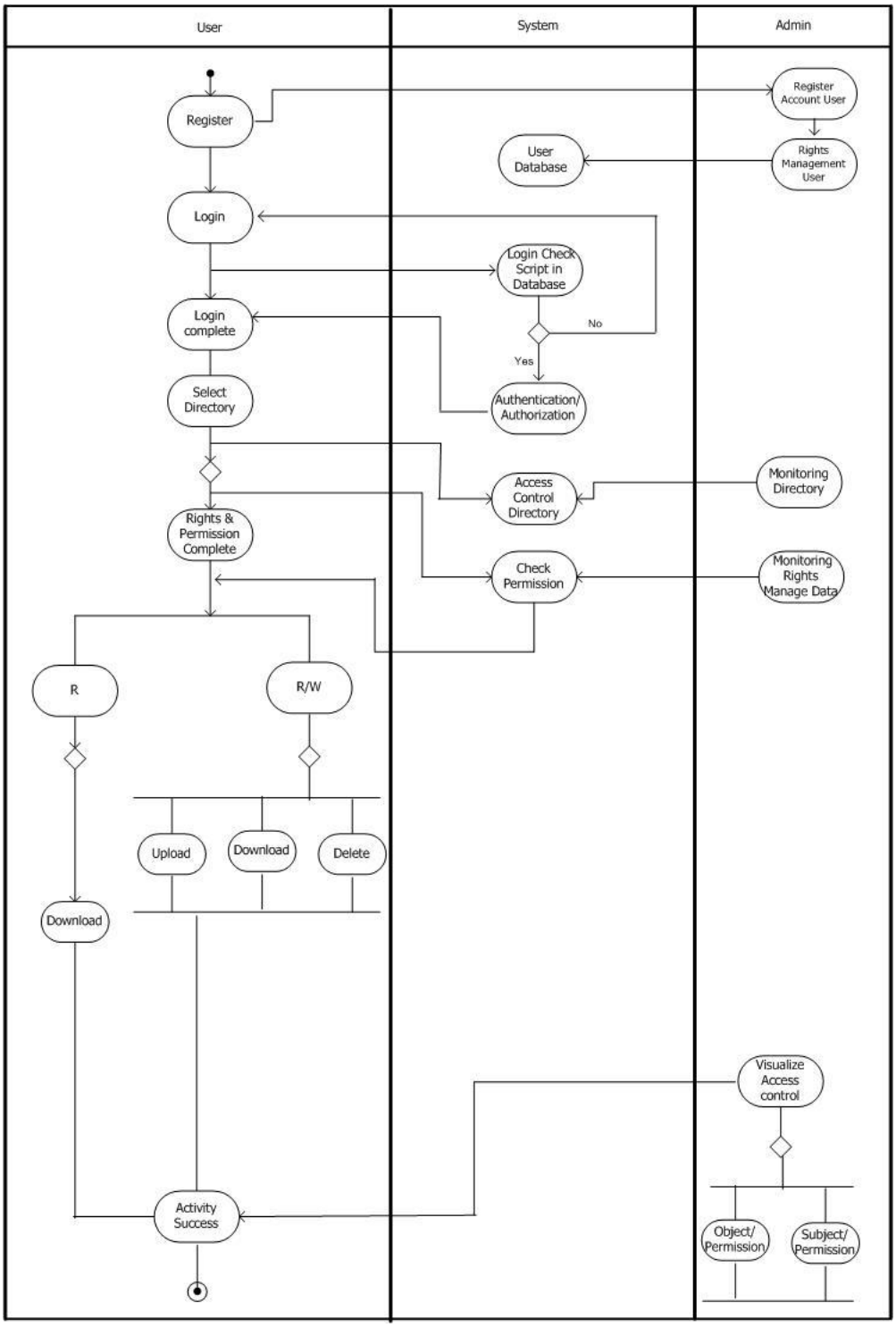
1.4 สามารถแก้ไขหรือเปลี่ยนแปลงสิทธิ์การเข้าถึงข้อมูลของผู้ใช้ได้ กรณีมีการเปลี่ยนแปลงอำนาจหรือปรับโครงสร้างกลุ่มผู้ใช้การเข้าถึงข้อมูล

2. สามารถบริหารจัดการบัญชีผู้ใช้ ได้แก่ Add , Update , Delete ข้อมูลบัญชีผู้ใช้ได้

3. สามารถเพิ่มกลุ่มข้อมูลได้

ทั้งนี้ในการบริหารจัดการฐานข้อมูลทั้ง 2 ส่วน จะสามารถทำให้ระบบสร้างแผนภาพเพื่อนำเสนอมุมมองของสิทธิ์การเข้าถึงระหว่างกลุ่มข้อมูลและผู้ใช้

3.4.3 Activity Diagram



รูปที่ 3.8 Activity Diagram แสดงการทำงานของระบบ

รูปที่ 3.8 Activity Diagram จะแสดงการทำงานภาพรวมของระบบซึ่งประกอบด้วย การทำงานของผู้ใช้ การทำงานของระบบ และการทำงานผู้ดูแลระบบ สามารถอธิบายการทำงานได้ดังต่อไปนี้

1. เมื่อผู้ใช้ต้องการเข้าใช้ระบบจะทำการร้องขออนุมัติการเข้าถึงกับผู้ดูระบบ

2. ผู้ดูแลระบบตรวจสอบข้อมูลผู้ใช้และสิทธิ์การเข้าถึงข้อมูล ที่ได้รับอนุมัติจากผู้บริหาร

3. ผู้ดูแลระบบจะทำการสร้างบัญชีผู้ใช้ พร้อมทั้งกำหนดสิทธิ์การเข้าถึงกลุ่มข้อมูลแต่ละส่วน เพื่อให้ผู้ใช้สามรถบริหารจัดการข้อมูลภายใน Directory ได้

4. ผู้ใช้ทดสอบการเข้าสู่ระบบ ถ้าชื่อผู้ใช้กับรหัสผ่านไม่ถูกต้องจะไม่สามารถเข้าสู่ระบบได้ ถ้าชื่อผู้ใช้กับรหัสผ่านถูกต้องผู้ใช้จะสามารถเข้าสู่ระบบได้

5. ระบบจะแสดงกลุ่มข้อมูลที่ผู้ใช้ได้รับตามสิทธิ์ที่ได้รับอนุญาต ในแต่ละกลุ่มข้อมูลจะแตกต่างกันตามบทบาทและภาระหน้าที่

6. ผู้ใช้เลือกใช้งานกลุ่มข้อมูลที่ต้องการได้ตามบทบาท ภาระหน้าที่ ที่สามารถเข้าถึงได้ ทั้งนี้ผู้ดูแลระบบจะเป็นผู้บริหารรจัดการกลุ่มข้อมูลให้กับผู้ใช้

7. ระบบจะมีการตรวจสอบและควบคุมการเข้าถึงข้อมูลของผู้ใช้ถ้ามีสิทธิ์เข้าใช้ Directory ระบบจะตรวจสอบเงื่อนไข ประกอบด้วย 2 ทางเลือกได้แก่

7.1 Read / Write (R/W) ผู้ใช้สามารถเข้าถึงและบริหารจัดการข้อมูลภายใน Directory นั้นๆ คือ Upload , Download , Delete

7.2 Read Only (R) ผู้ใช้สามารถเข้าถึงข้อมูลภายใน Directory นั้นๆ คือ Download จากนั้นผู้ใช้สามารถเข้าใช้และบริหารจัดการ Directory ตามความต้องการได้

8. ผู้ใช้สามารถใช้งานระบบและได้ผลลัพธ์ตามความต้องการ

9. เมื่อตั้งค่าทั้งหมดเรียบร้อยตามที่ได้รับแจ้งจากผู้บริหารและผู้ใช้สามารถใช้งานได้ตามสิทธิ์ที่ได้รับ ระบบจะสามารถนำเสนอแผนภาพเพื่อให้ผู้บริหารเห็นภาพรวม โดยนำเสนอมุมมองได้ทั้ง มุมมองสิทธิ์ผู้ใช้งาน และมุมมองการเข้าถึงกลุ่มข้อมูล

ตารางที่ 3.5 แสดงแผนการดำเนินงานและระยะเวลาในการดำเนินงาน

ลำดับที่	รายละเอียดการดำเนินงาน	ระยะเวลาดำเนินงาน								
		1	2	3	4	5	6	7	8	9
1	ศึกษาธรรมชาติขององค์กร ปัญหาและข้อจำกัดต่างๆ การพัฒนาระบบ และรวบรวมความต้องการของผู้ใช้	→								
2	ศึกษาเครื่องมือและภาษาที่ใช้ในการเขียนโปรแกรม ทฤษฎีและเทคโนโยลีต่างๆที่เกี่ยวข้องในการพัฒนาระบบ	→	→	→						
3	ออกแบบหน้าจอการทำงานและจัดทำฐานข้อมูลของระบบ				→	→				
4	ขั้นตอนการพัฒนาและจัดทำระบบ					→	→	→		
5	ทดสอบการทำงานของระบบและแก้ไขข้อผิดพลาดของระบบ							→	→	
6	สรุปผลงานและนำเสนอแนะระบบ									→