ระบบบริหารจัดการและควบคุมการเข้าถึงเอกสารผ่านเว็บ

มุจรินทร์ แพทย์จันลา

สารนิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิศวกรรมเว็บ คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยธุรกิจบัณฑิตย์
พ.ศ. 2556

Web-based System for Document Management and Access Control.

Mucharin Patchanla

Thematic Paper Submitted in Partial Fulfillment of

the Requirements for the Degree of

Master of Science in Web Engineering

Faculty of Information Technology, Dhurakij Pundit University

2013

หัวข้อสารนิพนธ์	ระบบบริหารจัดการและควบคุมการเข้าถึงเอกสารผ่านเว็บ
ชื่อผู้เขียน	มุจรินทร์ แพทย์จันลา
อาจารย์ที่ปรึกษา	ผู้ช่วยศาสตราจารย์.ดร.มัชฌิกา อ่องแตง
สาขาวิชา	วิศวกรรมเว็บ
ปีการศึกษา	2555

บทคัดย่อ

สารนิพนธ์นี้มีวัตถุประสงค์เพื่อศึกษาและจัดทำระบบควบคุมการเอกสารผ่านเว็บแอพพลิเคชั่น โดยใช้โครงสร้างของสมาคมวางแผนครอบครัวแห่งประเทศไทย ในพระราชูปถัมภ์สมเด็จพระศรีนครินทราบรมราชชนนีเป็นกรณีศึกษา โดยนำทฤษฎีและเทคโนโลยีต่างๆ อาทิเช่น เทคโนโลยีเว็บแอพพลิเคชั่น วิศวกรรมความต้องการ เทคโนโลยีความมั่นคงของข้อมูล การกำหนดนโยบายรักษาความปลอดภัย การควบคุมการเข้าถึงระบบ รวมถึงหลักการที่เกี่ยวข้อง มาประยุกต์ใช้ร่วมกัน เพื่อจัดทำระบบที่ตรงกับความต้องการและเพิ่มประสิทธิภาพในการทำงาน โดยระบบที่จัดทำขึ้นนั้นสามารถจัดเก็บและควบคุมการเข้าถึงเอกสาร ที่เดิมได้รับการจัดเก็บไว้ในเครื่องคอมพิวเตอร์ส่วนบุคคล (Personal Computer) และในอุปกรณ์จัดเก็บอื่นๆ นอกจากนี้ยังสามารถแบ่งปันข้อมูลเพื่อใช้งานร่วมกันได้ ภายใต้กฎการเข้าถึงที่จัดทำขึ้นโดยพิจารณาจากบทบาทการทำงานของผู้ใช้ในองค์กรตลอดจนเงื่อนไขเพิ่มเติมอื่นๆ การทำงานของระบบประกอบด้วย 3 ขั้นตอนหลัก ผู้บริหารระดับสูงเป็นผู้อนุญาตโดยหลักการ จากนั้นส่งความต้องการให้ผู้ดูแลระบบสร้างบัญชีผู้ใช้และกำหนดสิทธิให้กับบุคลากรที่ได้รับอนุญาต ตามบทบาทและภาระหน้าที่ที่รับผิดชอบภายในองค์กร สุดท้ายบุคลากรสามารถเข้าใช้งานระบบได้ตามที่ได้รับอนุญาตและสิทธิ์ ทั้งนี้ ระบบได้รับการออกแบบมาให้ทำงานบนบราวเซอร์เพื่ออำนวยความสะดวกให้กับบุคลากรภายในองค์กร สามารถใช้งานระบบผ่านเครือข่ายอินเทอร์เน็ตได้จากทุกที่ทุกเวลา

Thematic Paper Title	Statistical information system: Case study Social Security Office Insured System
Author	Chotika Kumsurmson
Thematic Paper Advisor	Asst.Prof.Dr.Machigar Ongtang
Academic Program	Web Engineering
Academic Year	2012

ABSTRACT

This thematic paper outlines the study, design, and development of a web-based system for document management and access control, which uses the organization of the Planned Parenthood Association of Thailand Under the Patronage of H.R.H. Princess Mother as a case study. The study appropriately employed multiple disciplines and technologies such as web application technology, requirement engineering, data security, security policy development, and access control principles. With such suitable combination, this study aims to develop the system that properly responds to the user requirements and improves working efficiency. The developed system stores the documents which were previously stored in personal computers and other types of storage. It also allows document sharing in a controlled manner, according to the access control policies which are developed based on the users' roles and other conditions. The operation of the system involves three main steps. First, the top-level management directs the granting of access rights by principle. Then, such requirements about the access rights are passed to the system administrator to create user accounts and assign the users' access rights accordingly, based on their roles and job functions within the organization. Lastly, the users access the documents through the system as authorized. For convenience, the system was designed to operate via the web browser to allow the users to use the system remotely through the Internet.

กิตติกรรมประกาศ

การศึกษาวิจัยเรื่อง ระบบบริหารจัดการและควบคุมการเข้าถึงเอกสารผ่านเว็บสำเร็จลุล่วงลงได้ด้วยความกรุณาและการช่วยเหลือจาก ผศ.ดร.มัชฌิกา อ่องแตง อาจารย์ที่ปรึกษาที่ได้ถ่ายทอดความรู้ ให้ข้อแนะนำ ตรวจแก้ไขข้อบกพร่องต่างๆ ตลอดจนช่วยตรวจสอบต้นฉบับและข้อคิดเห็นที่เป็นประโยชน์อย่างยิ่งในการศึกษาวิจัยครั้งนี้ ผู้ศึกษาจึงใคร่ขอกราบขอบพระคุณท่านอาจารย์มา ณ โอกาสนี้ด้วย

ผู้จัดทำสารนิพนธ์ขอขอบคุณ ผู้ช่วยศาสตราจารย์ ดร.วรสิทธิ์ ชูชัยวัฒนา กรุณาให้คำปรึกษาในด้านการศึกษา และคอยช่วยเหลือนักศึกษาทุกอย่างตั้งแต่เริ่มก้าวเข้ามาศึกษาจนกระทั่งจบการศึกษา ขอกราบขอบพระคุณเป็นอย่างสูงมา ณ ที่นี้

ขอขอบคุณคณาจารย์ทุกท่านในคณะเทคโนโลยีสารสนเทศ สาขาวิศวกรรมเว็บ มหาวิทยาลัยธุรกิจบัณฑิตย์ที่ประสิทธิประสาทวิชาความรู้อันเป็นประโยชน์แก่ผู้จัดทำสารนิพนธ์ตั้งแต่ผู้จัดทำสารนิพนธ์ได้เริ่มเข้ามาศึกษาในมหาวิทยาลัยตลอดจนสำเร็จการศึกษา

สุดท้ายนี้ ผู้ศึกษาขอกราบขอบพระคุณบิดา-มารดา ที่เป็นผู้ให้กำเนิดและชุบเลี้ยงผู้ศึกษาจนเติบใหญ่ คอยห่วงใยและพร่ำสอนให้ประพฤติตนเป็นคนดีและเป็นกำลังใจที่สำคัญยิ่งให้กับผู้ศึกษา และขอบคุณพี่ๆ เพื่อนๆ น้องๆทุกคนที่ให้กำลังใจอันสำคัญยิ่งในการทำสารนิพนธ์ประสบความสำเร็จลุล่วงไปด้วยดี หวังว่าสารนิพนธ์ฉบับนี้จักมีประโยชน์และคุณค่าในการบริหารจัดการความเป็นระเบียบเรียบร้อยหากมีข้อผิดพลาดประการใดผู้ศึกษากราบขออภัยมา ณ โอกาสนี้ด้วย

มุจรินทร์ แพทย์จันลา

สารบัญ

สารบัญ (ต่อ)

สารบัญตาราง

สารบัญภาพ

ภาพที่ **หน้า**

สารบัญภาพ(ต่อ)

ภาพที่ **หน้า**

บทที่ 1
บทนำ

1.1 ที่มาและความสำคัญของงาน

การทำงานในองค์กรในปัจจุบันได้นำเอาเทคโนโลยีสารสนเทศเข้ามามีบทบาทในการดำเนินงานเพื่ออำนวยความสะดวกให้แก่เจ้าหน้าที่ภายในองค์กรในการบริหารจัดการเอกสารและข้อมูล ทั้งการจัดเก็บข้อมูล จัดพิมพ์ข้อมูล การแบ่งปันข้อมูล ข้อมูลเหล่านี้ล้วนมีความสำคัญต่อองค์กรทั้งข้อมูลที่เป็นความลับ และข้อมูลที่สามารถเปิดเผยได้ ดังนั้นถ้าหากมีการบริหารจัดการและการควบคุมการเข้าใช้งานข้อมูลทั้งจากผู้ใช้ภายในและภายนอก จะทำให้ข้อมูลเหล่านั้นมีความปลอดภัย สามารถใช้งานร่วมกันได้ และสะดวกสบายต่อผู้ใช้งานภายในองค์กร

สารนิพนธ์ฉบับนี้นำเสนอระบบบริหารจัดการและควบคุมการเข้าถึงเอกสารผ่านเว็บ (Web-based System for Document Management and Access Control.) เพื่อให้เจ้าหน้าที่ในองค์กรมีการจัดเก็บข้อมูลในทิศทางเดียวกันและสามารถใช้ข้อมูลร่วมกันได้ ในการจัดทำระบบได้ประยุกต์ใช้หลักการและเทคโนโลยีการควบคุมการเข้าถึง (Access Control) การจัดการสิทธิ์ของผู้ใช้ตามบทบาทของผู้ใช้ (RBAC) และสิทธิ์การเข้าถึงข้อมูล (Rights) สามารถกำหนดได้ตามโครงสร้างขององค์กร นอกจากนี้ระบบยังสนับสนุนการกำหนดสิทธิ์เพิ่มเติมตามที่ผู้บริหารอนุญาตนอกเหนือจากสิทธิ์ที่กำหนดตามบทบาทภายใต้โครงสร้างองค์กร จะเห็นได้ว่าการอนุญาตนอกเหนือโครงสร้างนี้ ไม่เป็นไปตามนโยบายความมั่นคงและมีแนวโน้มที่จะลดระดับความมั่นคงของข้อมูล อย่างไรก็ตาม การให้สิทธิ์เพิ่มเติมดังกล่าวมีความจำเป็นต่อการดำเนินกิจกรรมขององค์กร และไม่อาจหลีกเลี่ยงได้ ด้วยเหตุนี้ เพื่อให้เอื้อต่อการตรวจสอบสถานะความมั่นคง (Security State) ของข้อมูลในปัจจุบัน ระบบที่พัฒนาขึ้นจึงนำเสนอสถานะการให้สิทธิ์ ผ่านแผนภาพ เพื่อให้ผู้บริหารสามารถมองเห็นภาพรวมของการกำหนดสิทธิ์ของผู้ใช้งานและการเข้าถึงกลุ่มข้อมูล เพื่อใช้ในการพิจารณาในการจัดการสิทธิ์ให้มีความเหมาะสมมากยิ่งขึ้นต่อไป

สารนิพนธ์นี้ใช้สมาคมวางแผนครอบครัวแห่งประเทศไทยในพระบรมราชูปถัมภ์เป็นกรณีศึกษา ในการจัดทำระบบเนื่องจากการดำเนินงานภายในสมาคมฯได้นำคอมพิวเตอร์เข้ามาใช้ในการทำงานแทบทุกกระบวนการ แต่สมาคมฯ ยังไม่มีการจัดเก็บข้อมูลอย่างเป็นระบบ ทำให้การบริหารจัดการเอกสารภายในองค์กรมีรูปแบบที่หลากหลาย ขึ้นอยู่กับความถนัดของแต่ละคน ใน

การจัดเก็บเอกสารดังกล่าวอาจทำให้ข้อมูลเกิดความเสียหายจากอุปกรณ์ชำรุด สูญหาย และการเปิดเผยข้อมูลโดยไม่ตั้งใจของเจ้าของข้อมูลหรือผู้ที่ได้รับข้อมูล เนื่องจากการจัดเก็บอุปกรณ์ที่บันทึกข้อมูลไม่มีความปลอดภัยเพียงพอ

1.1 วัตถุประสงค์ของการพัฒนาระบบ

1. เพื่อพัฒนาระบบการจัดการเอกสารผ่านเว็บที่มีการจัดการสิทธิ์ตามโครงสร้างองค์กรและภาระหน้าที่ที่กำหนดให้กับผู้ใช้และเงื่อนไขการทำงานอื่นๆ
2. เพื่อเป็นแนวทางในการบริหารจัดการข้อมูลให้อยู่ในทิศทางเดียวกันและสามารถแบ่งปันข้อมูลร่วมกันได้
3. เพื่ออำนวยความสะดวกให้กับผู้ใช้งาน สามารถเข้าใช้บริการได้ทุกที่ที่ใช้อินเตอร์เน็ตได้ โดยพัฒนาระบบในรูปแบบของเว็บแอพพลิเคชั่น (Web Application)
4. เพื่อป้องกันข้อมูลจากจากความเสี่ยงทั้งภายในและภายนอก เช่น ภัยธรรมชาติ การสูญหายของข้อมูลจากอุปกรณ์ฮาร์ดแวร์ชำรุด เป็นต้น
5. เพื่อช่วยให้สามารถวิเคราะห์ความปลอดภัยของกลุ่มข้อมูลโดยนำเสนอเป็นแผนภาพในมุมมองต่างๆได้

1.2 **ประโยชน์และผลที่คาดว่าจะได้รับ**

1. ระบบสามารถเป็นต้นแบบเพื่อใช้ในการบริหารจัดการข้อมูล และสามารถพัฒนาเพื่อความเหมาะสมกับองค์กรอื่นๆ
2. ระบบสามารถเพิ่มความน่าเชื่อถือให้กับองค์กรมากยิ่งขึ้นเนื่องจากมีการบริหารจัดการข้อมูลไปในทิศทางเดียวกัน
3. เจ้าหน้าที่ในองค์กรมีการจัดเก็บข้อมูลที่มีความปลอดภัยมากยิ่งขึ้นและแบ่งปันข้อมูลให้สามารถใช้งานร่วมกันได้ตามสิทธิ์ที่ได้รับอนุญาต

1.3 ขอบเขตของระบบ

ระบบบริหารจัดการและควบคุมเอกสารผ่านเว็บ จัดทำขึ้นตามความต้องการของระบบ (System Requirements) ซึ่งนำมาจากการวิเคราะห์โครงสร้างองค์กรและจากความต้องการของผู้ใช้งานจริงภายในองค์กร โดยนำระบบการทำงานของสมาคมวางแผนครอบครัวแห่งประเทศไทยในพระบรมราชูปถัมภ์มาเป็นต้นแบบเพื่อการศึกษา ขอบเขตการทำงานของระบบประกอบด้วยรายละเอียดดังต่อไปนี้

1.3.1 สำหรับผู้ดูแลระบบ

1. กำหนดสิทธิ์การเข้าถึงข้อมูลให้กับผู้ใช้งาน

1.1 R/W (Read/Write) กำหนดสิทธิ์การเข้าถึงและบริหารจัดการข้อมูล (Upload, Download, Delete) ให้กับผู้ใช้ตามบทบาทหน้าที่ที่ได้รับอนุมัติจากผู้บริหารระดับสูง

1.2 R (Read Only) กำหนดสิทธิ์การเข้าถึงข้อมูล (Download) ให้กับผู้ใช้ตามบทบาทหน้าที่ที่ได้รับอนุมัติจากผู้บริหารระดับสูง

1.3 ไม่สามารถเข้าถึงข้อมูลได้

2. บริหารจัดการสิทธิ์การเข้าถึงข้อมูล แก้ไข เปลี่ยนแปลงได้ เมื่อมีการเปลี่ยนแปลงเพิกถอนสิทธิ์การเข้าถึงข้อมูล

2.1 บริหารจัดการบัญชีผู้ใช้ เพิ่ม ลบ ข้อมูลส่วนบุคคลในฐานข้อมูลได้

2.2 สามารถเรียกดูมุมมองภาพรวมสิทธิ์ที่ได้รับและการเข้าถึงกลุ่มข้อมูลได้

1.3.2 สำหรับผู้ใช้งาน

1. สามารถเข้าใช้งานข้อมูลได้ โดยแบ่งออกเป็น 2 ประเภทดังต่อไปนี้

1.1 R/W (Read/Write) ผู้ใช้สามารถเข้าถึงและบริหารจัดการข้อมูล Upload, Download, Delete ได้

1.2 R (Read only) ผู้ใช้สามารถเข้าถึงข้อมูล Download ได้

1.3 สามารถแก้ไขรหัสด้วยตนเองเพื่อป้องกันข้อมูลรั่วไหล

2. สามารถจัดการรหัสผ่านได้ด้วยตนเอง

1.3.3 การทำงานของระบบ

1. สามารถรองรับการทำงานของผู้ใช้ ทั้งในส่วนของผู้ดูแลระบบและผู้ใช้งาน
2. สามารถตรวจสอบสิทธิ์ผู้ใช้ เมื่อมีการล็อกอินเข้าสู่ระบบ
3. สามารถควบคุมสิทธิ์ผู้ใช้ เพื่อให้ใช้งานระบบตามสิทธิ์ที่ได้รับ
4. สามารถรองรับการกำหนดสิทธิ์การเข้าถึงข้อมูลตามที่ผู้ดูแลระบบกำหนดให้
5. สามารถนำเสนอมุมมองแสดงสิทธิ์และการเข้าถึงข้อมูลตามที่ผู้ดูแลระบบหรือผู้บริหารต้องการ

1.5 อุปกรณ์สนับสนุนระบบ

Server ของสมาคมวางแผนครอบครัวแห่งประเทศไทยในพระบรมราชูปถัมภ์

บทที่ 2
วรรณกรรมและงานวิจัยที่เกี่ยวข้อง

ในการจัดทำระบบบริหารจัดการและควบคุมเอกสารผ่านเว็บ (Web-base System for Document Management and Access Control) ได้มีการนำระบบงานของสมาคมวางแผนครอบครัวแห่งประเทศไทยในพระบรมราชูปถัมภ์ มาใช้เป็นกรณีศึกษา โดยผู้จัดทำมุ่งออกแบบระบบเพื่อให้เหมาะสมกับองค์กร ทั้งนี้ผู้จัดทำได้ศึกษาค้นคว้า และทฤษฎีอื่นๆ ที่เกี่ยวข้องเพื่อนำมาประยุกต์ใช้กับระบบดังกล่าว

2.1. ระบบงานภายในสมาคมวางแผนครอบครัวแห่งประเทศไทยฯ (Organization Workflow)

เพื่อให้ได้ระบบที่เหมาะสมกับองค์กร ผู้จัดทำได้วิเคราะห์ประเด็นต่างๆที่อาจมีผลกระทบต่อกระบวนการจัดการเอกสาร ได้แก่

2.1.1 วิเคราะห์โครงสร้างองค์กร

การดำเนินงานภายในสมาคมวางแผนครอบครัวฯ แบ่งงานออกเป็น 2 ส่วน ได้แก่

1. งานหลักภายในสมาคมฯ หมายถึงงานที่เจ้าหน้าที่ภายในสมาคมฯ ปฏิบัติเป็นประจำ ซึ่งถือเป็นงานหลัก สามารถยึดตามโครงสร้างขององค์กรได้ดังต่อไปนี้

1.1 ข้อมูลกลุ่มงานสำนักฯ

1.2 ข้อมูลฝ่ายงานต่างๆที่อยู่ภายใต้งานสำนักฯ

ผู้จัดทำขอยกตัวอย่างกลุ่มงานหลักภายในองค์กรดังนี้

ตัวอย่างงานหลักภายในสมาคมฯ

ข้อมูลกลุ่มงานสำนักบริหารกลาง ประกอบด้วยฝ่ายต่างๆ ดังนี้

ฝ่ายบัญชี

ฝ่ายการเงิน

ฝ่ายพัสดุจัดซื้อ

ฝ่ายบุคลากร

ฝ่ายเลขานุการ

ฝ่ายสารบรรณ

2. งานโครงการ หมายถึง การดำเนินงานที่นอกเหนือจากงานหลักภายในองค์กร มีการกำหนดระยะเวลาในการทำงาน เนื่องจากเป็นงานที่ได้เขียนโครงการเพื่อของบประมาณจากแหล่งทุนและดำเนินงานตามกลุ่มเป้าหมายของแต่ละโครงการ เช่นงานด้านเอดส์ ประกอบไปด้วยโครงการย่อยๆ เพื่อแบ่งตามกลุ่มเป้าหมายของโครงการ โดยขอยกตัวอย่างดังนี้

ตัวอย่างงานโครงการ

ข้อมูลโครงการด้านเอดส์

เอดส์กลุ่มพนักงานบริการหญิง (FSW)

เอดส์กลุ่มชายรักชาย (MSM)

เอดส์กลุ่มเด็กและวัยเจริญพันธ์ (Child live)

ในส่วนการดำเนินงานโครงการผู้ที่มีหน้าที่ในการปฏิบัติงานจะมีทั้งเจ้าหน้าที่ภายในองค์กร (ที่มีการปฏิบัติงานหลักภายในองค์กร) และมีการจัดจ้างเจ้าหน้าที่โครงการเพิ่ม เพื่อให้สามารถดำเนินงานตามพื้นที่และเข้าถึงกลุ่มเป้าหมายของโครงการฯได้

2.1.1 วิเคราะห์ทรัพยากรภายในองค์กรที่ต้องการป้องกัน

ในการดำเนินงานภายในสมาคมฯ ทรัพยากรที่องค์กรต้องการรักษาความปลอดภัยคือข้อมูลหรือเอกสารที่จัดเก็บในเครื่องคอมพิวเตอร์ส่วนบุคคลและอุปกรณ์แบบพกพา (CD , DVD , Flash Drive) ข้อมูลหรือเอกสาร ได้แก่ Microsoft Office (Excel , Word , Power Point) , รูปภาพ เป็นต้น ข้อมูลหรือเอกสารเหล่านี้เป็นข้อมูลที่อยู่ภายใต้การดำเนินงานภายในองค์กร ระบบพัฒนาขึ้นมุ่งที่จะใช้เป็นระบบจัดเก็บ และจัดการทรัพยากรเหล่านี้

2.1.2 การจัดเก็บข้อมูลขององค์กรในปัจจุบัน

การจัดเก็บข้อมูลภายในองค์กร ยังไม่มีระบบจัดเก็บข้อมูลที่ใช้เพื่อให้เกิดทิศทางเดียวกัน เจ้าหน้าที่จะจัดเก็บที่เครื่องคอมพิวเตอร์ส่วนบุคคล โดยมากจะเก็บไว้ที่ไดร์ D หากต้องการนำข้อมูลไปใช้ภายนอกเครื่องคอมพิวเตอร์จะบันทึกที่อุปกรณ์อื่นๆ เช่น CD , DVD , Flash Drive เป็นต้น และการแบ่งปันข้อมูลเพื่อใช้ร่วมกันภายในองค์กรจะใช้วิธีการส่ง e-mail

2.1.3 วิเคราะห์ช่องโหว่

โอกาสของภัยคุกคามและการโจมตี ซึ่งนำไปสู่การสูญเสียหรือความเสียหายให้แก่ข้อมูลที่ต้องการรักษาความปลอดภัยที่อาจเกิดขึ้นภายในองค์กร มีเหตุการณ์ดังต่อไปนี้

1. ความผิดพลาดที่เกิดจากเจ้าของข้อมูล ในการแบ่งปันข้อมูลเพื่อใช้ร่วมกับผู้อื่นที่เกี่ยวข้อง จะส่งข้อมูลทางจดหมายอิเล็กทรอนิกส์ (e-mail) อาจก่อให้เกิดการส่งข้อมูลผิดคน ทำให้ข้อมูลที่เป็นความลับอาจเผยแพร่โดยไม่ได้ตั้งใจ ในบางครั้งการส่งข้อมูลผิดหากปลายทางเป็นผู้ไม่หวังดีอาจจะมีการเปลี่ยนแปลงข้อมูล ทำให้ข้อมูลไม่สมบูรณ์ได้

2. คอมพิวเตอร์ส่วนบุคคลที่ใช้จัดเก็บข้อมูล ไม่ได้มีการตั้ง password ก่อนเข้าใช้งาน ทำให้อาจมีผู้ใช้คนอื่นเข้าไปแก้ไขและขโมยข้อมูล ทำให้ข้อมูลไม่สมบูรณ์และขาดการเป็นความลับ

3. การจัดเก็บข้อมูลไว้ในอุปกรณ์พกพาอื่นๆ เพื่อนำไปใช้ภายนอกเครื่องคอมพิวเตอร์ เช่น CD DVD Flash drive เป็นต้น อุปกรณ์เหล่านี้อาจจะเกิดการสูญหาย ชำรุด หรือผู้ไม่หวังดีเปลี่ยนแปลงข้อมูลหรือขโมย ทำให้ข้อมูลไม่สมบูรณ์และขาดการเป็นความลับ

4. การจัดเก็บข้อมูลในเครื่องคอมพิวเตอร์ ทำให้การเรียกใช้งานข้อมูลนอกเครื่องคอมพิวเตอร์และนอกพื้นที่องค์กรไม่ได้ ทำให้ขาดการพร้อมใช้งาน

เพื่อตอบสนองต่อโครงสร้างและลักษณะการดำเนินงานขององค์กร สารนิพนธ์ฉบับนี้จึงมุ่งที่จะจัดทำระบบจัดเก็บเอกสารที่สนับสนุนการรักษาความมั่นคง เพื่อปกป้องข้อมูลจากบุคคลภายนอกองค์กรและเจ้าหน้าที่ภายในองค์กรที่ไม่ได้รับอนุญาต โดยการเข้าถึงข้อมูลของผู้ใช้สามารถตรวจสอบสิทธิ์จากบทบาทของผู้ใช้ได้ 2 ทาง คือ การเข้าถึงข้อมูลตามกลุ่มของผู้ใช้จะแบ่งตามโครงสร้างขององค์กร และการเข้าถึงข้อมูลตามภาระหน้าที่ของผู้ใช้หมายถึงบทบาทหน้าที่ที่นอกเหนือการทำงานตามโครงสร้าง การตรวจสอบสิทธิ์ของผู้ใช้เพื่อเป็นการอนุญาตให้ผู้ใช้สามารถเข้าถึงข้อมูลได้

2.2 นโยบายการควบคุมการเข้าถึง (Access Control Policies)

นโยบายการรักษาความมั่นคงเป็นข้อบังคับหรือระบุสิ่งที่อาจจะมีการเข้าถึงทรัพยากรแต่ละระบบ โดยกำหนดข้อจำกัดการเข้าถึงที่จะได้รับอนุญาตในแต่ละข้อบังคับที่กำหนด ยกตัวอย่างคำนิยาม ITU-T X.800 ได้ให้คำจำกัดความของ Access Control Policies ว่า “การป้องกันการใช้งานทรัพยากรจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งลักษณะการป้องกันการใช้ทรัพยากรที่ไม่ได้รับอนุญาต” ซึ่งนโยบายการควบคุมการเข้าถึงมี 3 องค์ประกอบดังนี้ [1]

1. Discretionary Access Control Policies

เป็นนโยบายการเข้าถึงที่กำหนดตามวิจารณญาณ (Discretion) ของผู้ใช้ โดยกำหนดขอบเขตระหว่างผู้ใช้กับข้อมูล โดยทั่วไปจะอาศัยการระบุตัวตน (Authentication) และการอนุญาต

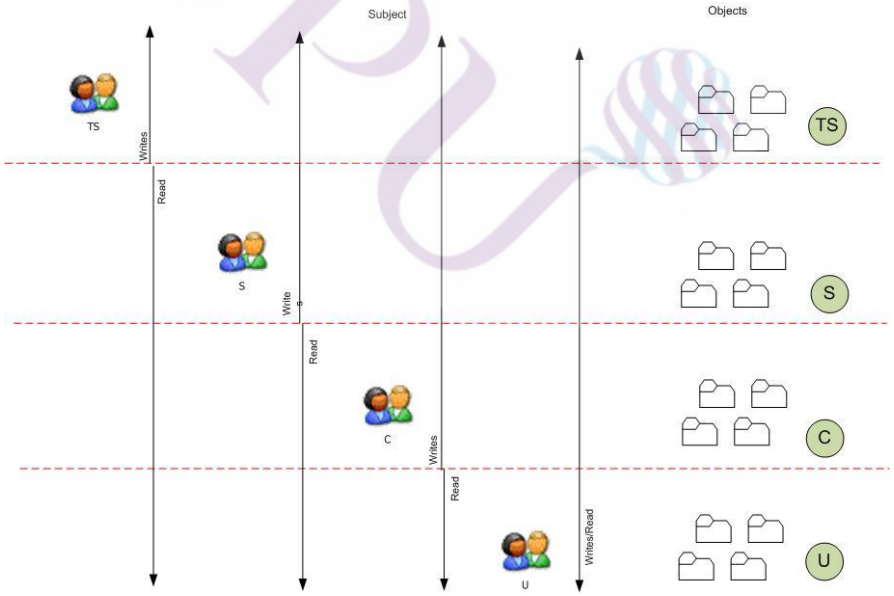
(Authorization) เพื่อใช้ในการตรวจสอบการเข้าสู่ระบบและการเข้าถึงข้อมูลแต่ละ Object และสิทธิ์การเข้าถึง (Read , Write , Execute) ตามคำร้องขอของผู้ใช้ เมื่อต้องการเข้าถึง Object จะถูกตรวจสอบกับการอนุมัติที่ระบุว่าผู้ใช้สามารถเข้าถึง Object ได้ในระดับใด แต่ถ้าผู้ไม่ได้รับอนุญาตจะไม่สามารถเข้าถึงทรัพยากรดังกล่าวได้

2. Mandatory Access Control Policies

เป็นนโยบายการเข้าถึงที่กำหนดโดยระบบ ไม่สามารถเปลี่ยนแปลงได้โดยผู้ใช้ (Mandatory) กำหนดการบังคับใช้เพื่อควบคุมการเข้าถึงข้อมูลบนพื้นฐานตามหมวดหมู่ข้อมูล (Object) ในระบบให้กับผู้ใช้ ในแต่ละกลุ่มข้อมูลจะกำหนดระดับความปลอดภัยจะทำให้เห็นสถานะของข้อมูลได้ การกำหนดระดับข้อมูลสามารถแสดงเป็นชุดคำสั่งตามลำดับชั้น ชุดลำดับชั้นโดยทั่วไปประกอบด้วย

ความลับสุดยอด (TS) -> ความลับ (S) -> ความลับเฉพาะกลุ่ม (C) -> ยังไม่แบ่งประเภท (U)

ระดับการรักษาความปลอดภัยจะบอกถึงสถานะของ Object ตามลำดับชั้น การเข้าถึงข้อมูลจะเกิดขึ้นเมื่อมีความสัมพันธ์ระหว่างผู้ใช้ (Subject) และข้อมูล (Object)



รูปที่ 2.1 การแบ่งกลุ่มข้อมูลสำหรับการควบคุมการเข้าถึงข้อมูล

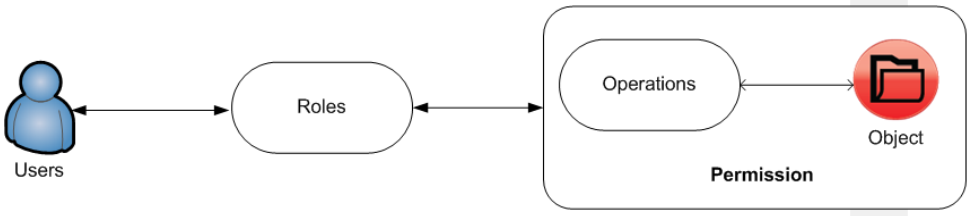
จากรูปที่ 2.1 แสดงตัวอย่างการป้องกันข้อมูลในแต่ละ Object ข้อมูลที่อยู่ในระดับที่สูงกว่าจะมีการรักษาความมั่นคงมากกว่าข้อมูลที่อยู่ในระดับล่าง ผู้ใช้สามารถเข้าใช้งานตามกฎที่ได้รับอนุญาต เพื่อป้องกันความลับให้กับข้อมูลตามระดับที่กำหนด และเพิ่มความน่าเชื่อถือให้แก่กลุ่มข้อมูลจากการรั่วไหลโดยไม่ได้ตั้งใจของเจ้าของข้อมูล ในการกำหนดสามารถเชื่อมโยงความสัมพันธ์ระหว่าง Object และ Subject ตามขอบเขตของการทำงานของผู้ใช้

การจำแนกประเภทการรักษาความปลอดภัย จะสร้างกฎบนพื้นฐานตาม การบังคับควบคุมการเข้าถึง การกำหนดสิทธิ์จะทำให้เห็นระดับความไว้วางใจกับกลุ่มข้อมูลในแต่ละ Object จากผู้มีอำนาจในการกระจายสิทธิ์

3. Role-base Access Control Policies

การกำหนดสิทธิ์ตามบทบาท คือกฎหรือกลุ่มของกฎที่บอกลักษณะหรือขอบเขตบทบาทการจัดการผู้ใช้ตั้งแต่หนึ่งบทบาทขึ้นไป สามารถจัดการการตั้งค่าบัญชีของผู้ใช้และสร้างกลุ่มการได้รับสิทธิ์ได้ การควบคุมการเข้าถึงตามบทบาท (RBAC) เป็นส่วนหนึ่งของรูปแบบสิทธิ์การอนุมัติสิทธิ์ หรือสิทธิ์พิเศษอื่นๆ ที่อนุญาตให้ผู้ใช้ดำเนินงานด้านการจัดการบางอย่างได้ ผู้ใช้สามารถกำหนดค่าและจัดการในบัญชีของผู้ใช้ส่วนตัว กลุ่มที่ผู้ใช้เป็นเจ้าของ และความสามารถในการเข้าร่วมหรือออกจากกลุ่ม การกำหนดสิทธิ์ตามบทบาทเป็นการกำหนดพื้นที่สำหรับผู้ใช้เพื่อให้ผู้ใช้สามารถทำงานได้ในพื้นที่ที่กำหนด การสร้างนโยบายการกำหนดบทบาทเพื่อกำหนดค่าเริ่มต้นและสามารถเปลี่ยนแปลงสิทธิ์ได้ตามความเหมาะสม

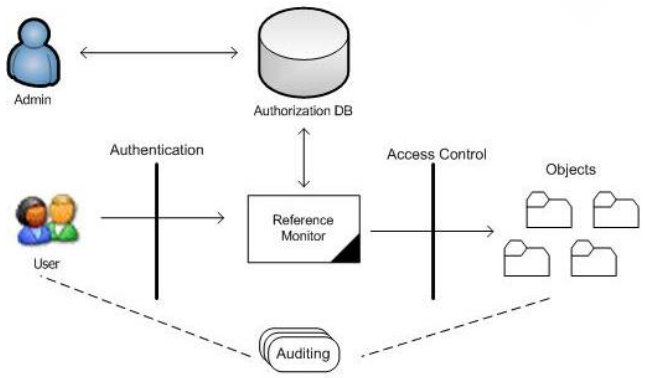
การกำหนดสิทธิ์ตามบทบาทสามารถใช้กำหนดความสามารถกลุ่มผู้ใช้กับการดำเนินงานด้านการจัดการบางอย่าง โดยปรับการตั้งค่าบัญชีที่แต่ละกลุ่มสามารถจัดการได้ ตัวอย่างเช่น ต้องการป้องกันไม่ให้พนักงานทั่วไปเปลี่ยนชื่อที่แสดง แต่ต้องการให้ผู้จัดการสามารถเปลี่ยนชื่อนั้นได้ เมื่อต้องการดำเนินการนี้ต้องเชื่อมโยงการเข้าถึงเริ่มต้นของพนักงาน และนโยบายการเข้าถึงของผู้จัดการ จากนั้นกำหนดค่านโยบายการกำหนดบทบาทที่กำหนดเองเพื่ออนุญาตให้ผู้จัดการเปลี่ยนชื่อที่แสดงได้ ดังรูปที่ 2.2 แสดงการเข้าถึงข้อมูลตาม Roles ที่ได้อนุญาต



รูปที่ 2.2 แสดงการเข้าถึงข้อมูลตามที่ได้รับอนุญาต

2.3 ศึกษากลไกการควบคุมการเข้าถึงข้อมูลและการกำหนดสิทธิ์ (Access Control and Right Management) [2]

การควบคุมการเข้าถึงเป็นการรักษาความปลอดภัยในระบบคอมพิวเตอร์ เป็นนโยบายหรือกลไกในการกำหนดข้อจำกัดของผู้ใช้กับ Object ในระบบตามกฎข้อบังคับการทำงาน เพื่อยับยั้งและป้องกันข้อมูลหรือทรัพยากรจากภัยคุกคามในรูปแบบต่างๆ ในการเข้าใช้งานจะอ้างอิงการเข้าถึงตามผู้ดูแลระบบตั้งค่าอนุมัติในฐานข้อมูลเท่านั้น เพื่อใช้ตรวจสอบการก่อนเข้าใช้งานระบบ ผู้ดูแลระบบจะตั้งค่าการอนุญาตเหล่านั้นบนพื้นฐานของนโยบายความปลอดภัยขององค์กร ผู้ใช้อาจจะสามารถเปลี่ยนข้อมูลบางอย่างที่ได้รับอนุญาต เช่น การเปลี่ยนรหัสผ่าน เป็นต้น ดังรูปที่ 2.3 แสดง logical ของบริการรักษาความปลอดภัยและการโต้ตอบของผู้ใช้ ซึ่งใช้ฐานข้อมูลเก็บบัญชีผู้ใช้เพื่อทำการอนุมัติการเข้าถึง object ทำให้เห็นการทำงานของระบบระหว่าง การตรวจสอบการควบคุมการเข้าถึง สิทธิ์การเข้าถึง และการบริหารระบบ การควบคุมการเข้าถึงจะการตรวจสอบโดยใช้รหัสส่วนตัวที่ได้รับจากผู้ดูแลระบบ ส่วนมากนิยมใช้ขั้นตอนของการระบุและพิสูจน์ตัวตนในระบบคอมพิวเตอร์ด้วยการล็อกอิน (Login) โดยใช้ user name และ password การควบคุมการเข้าถึงไม่ได้เป็นกลไกที่สมบูรณ์สำหรับการรักษาความปลอดภัยระบบ แต่ต้องกระทำควบคู่กับการตรวจสอบ ซึ่งวิเคราะห์จากกิจกรรมของผู้ใช้ระบบและข้อมูลที่เกี่ยวข้อง การตรวจสอบนี้มีประโยชน์ทั้งยับยั้งผู้บุกรุกหรือผู้ที่ไม่ได้รับสิทธิ์ในการเข้าถึงข้อมูล วิเคราะห์พฤติกรรมของผู้ใช้ในการใช้ระบบ นอกจากนี้ยังสามารถพิจารณาข้อบกพร่องที่เป็นไปได้ในระบบรักษาความปลอดภัย

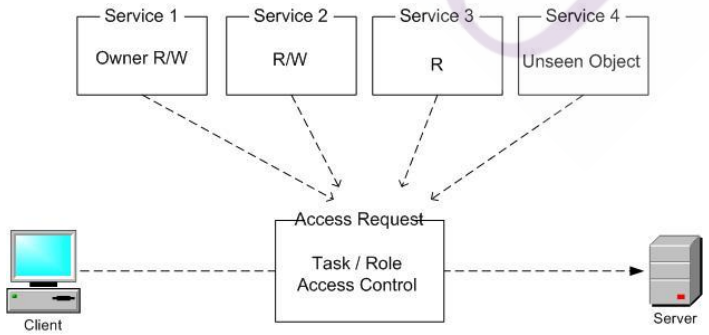


รูปที่ 2.3 การควบคุมการเข้าถึงและการรักษาความมั่นคง

2.4 ศึกษาการให้สิทธิ์ของผู้ใช้ตามบทบาทและภาระหน้าที่ (Distributed Role-based and Task-based Controls)[3]

เป็นการให้สิทธิ์ตามขอบเขตสิทธิ์การเข้าถึงข้อมูลของผู้ใช้ โดยจะกำหนดตามบทบาทและภาระหน้าที่ของผู้ใช้มากำหนดในระบบ ทำให้ประหยัดเวลาและง่ายต่อการควบคุมเมื่อมีการแก้ไข เปลี่ยนแปลง การกระจายสิทธิ์ของผู้ใช้จะเริ่มจากการรวบรวมผู้ที่มีส่วนได้ส่วนเสียกับระบบทั้งหมดและแบ่งหน้าที่ตามความเหมาะสม เช่น ผู้ที่มีอำนาจในการตัดสินใจมีเพียงเจ้าของข้อมูลและผู้ที่สามารถตั้งค่าในระบบจะเป็นผู้ดูแลระบบ เป็นต้น จากนั้นเป็นการกำหนดสิทธิ์การเข้าถึงข้อมูลให้กับผู้ใช้ตามสิทธิ์ที่ได้รับ เช่น การกำหนดให้มีบางข้อมูลที่สามารถเข้าถึงได้ทุกคน หรือกำหนดให้สามารถเข้าถึงข้อมูลเท่านั้น (Read only) และอาจมีบางข้อมูลที่สามารถบริหารจัดการได้ (Read , Write , execute) เป็นต้น ในการกำหนดตามบทบาทจะสามารถกำหนดเป็นกลุ่มผู้ใช้ หรือกลุ่มโปรเจก ทำให้ง่ายต่อการกำหนดสิทธิ์มากกว่าการกำหนดให้ทีละคน

การกำหนดสิทธิ์ตามกลุ่ม ต้องมีการแบ่งกลุ่มของข้อมูล (Object Classes) เป็นหมวดหมู่ข้อมูลตามกิจกรรมของผู้ใช้ การสร้างกลุ่มให้กับ Object เพื่อให้ผู้ใช้สามารถการเรียกใช้งานตามสิทธิ์ที่ได้รับในพื้นที่ที่กำหนด ผู้ใช้สามารถใช้งานร่วมกันได้ตามกลุ่มหรือหมวดหมู่ที่ตั้งไว้ ดังรูปที่ 2 แสดงการกระจายสิทธิ์การเข้าถึงข้อมูลตามบทบาทและภาระหน้าที่ให้กับผู้ใช้



รูปที่ 2.4 แสดงสิทธิ์การเข้าถึงข้อมูลตามบทบาทและภาระหน้าที่ของผู้ใช้

2.5 งานวิจัยและทฤษฎีที่เกี่ยวข้อง [4]

ผู้จัดทำได้ศึกษางานวิจัยที่เกี่ยวข้องกับการจัดทำโครงงาน ซึ่งมีกรณีศึกษาที่น่าสนใจดังต่อไปนี้

การรักษาความปลอดภัยวิศวกรรมความต้องการเพื่อใช้ในการปฏิบัติ : ตามกฎหมายการป้องกันข้อมูลประเทศอิตาลี งานวิจัยนี้ได้นำกรณีศึกษาระบบการรักษาความปลอดภัยวิศวกรรมความต้องการมหาวิทยาลัยเตรนโต ประเทศอิตาลี โดยใช้หลักการดังนี้ วิเคราะห์การสร้างแบบจำลอง การรักษาความปลอดภัย Tropos การศึกษากฎหมายว่าด้วยการคุ้มครองความเป็นส่วนตัว การศึกษากฎหมายคุ้มครองข้อมูลส่วนบุคคลที่ประกาศใช้ในยุโรปและอิตาลี คำนึงถึงสิทธิ์มนุษยชนขั้นพื้นฐานนำเอาหลักการของ ISO-17799 เทคนิคที่ควบคุมการดำเนินงานของมาตการความปลอดภัยคือการตรวจสอบ การอนุมัติ ระบบการป้องกันไวรัส การสำรองข้อมูล การเรียกคืนข้อมูล รวมถึงการจัดตั้งทีมรับมือกรณีเกิดเหตุการณ์ฉุกเฉิน มาตรการทั้งหมดจะลงรายละเอียดไว้ที่ DPS (Document Programmatico sulla sicurezza) มีการศึกษาระบบสารสนเทศขององค์กรโดยรวบรวมข้อมูลได้แก่ กลุ่มผู้รับผิดชอบที่เกี่ยวข้องกับการประมวลผลข้อมูลภายใต้การควบคุมของมหาวิทยาลัย การรักษาความปลอดภัยของฐานข้อมูลและความปลอดภัยบนเครือข่ายในปัจจุบัน การวิเคราะห์ความเสี่ยงที่อาจเกิดขึ้น และการวิเคราะห์การพัฒนาซอฟแวร์ที่เหมาะสมกับมหาวิทยาลัย จากนั้นสร้างแบบจำลองตามความรับผิดชอบของผู้ที่เกี่ยวข้องกับระบบ ระบุหน้าที่ของ Actor และการวิเคราะห์ผู้มีเกี่ยวข้องกับระบบทั้งหมด เพื่อนำมาสร้างแบบจำลองความต้องการการรักษาความปลอดภัย แบบจำลองที่เกี่ยวข้อง การสร้างแบบจำลองความปลอดภัยจะช่วยกำหนดขอบเขตของการจัดการและควบคุมการทำงานของระบบได้เป็นอย่างดี สุดท้ายเป็นการวิเคราะห์รูปแบบและความเพียงพอของความต้องการ ระบบต้องสามารถรับมือกับความซับซ้อนของภัยคุกคามรูปแบบต่างๆและวิธีการสำหรับการอนุญาตหรือการระบุปัญหาที่อาจเกิดขึ้น โดยนำเอาปัญหาของวิทยาลัยเตรนโตมาทำการประเมินความปลอดภัย นอกจากนี้ยังสามารถกำหนดวัตถุประสงค์และความรับผิดชอบไว้ใน DPS

แบบจำลองความต้องการการรักษาความปลอดภัย ความไว้วางใจ ความเป็นเจ้าของ การอนุญาต การมอบหมาย บทความนี้กล่าวถึงวิศวกรรมความต้องการการรักษาความปลอดภัยประกอบด้วยการวิเคราะห์กรอบการทำงานของการรักษาความปลอดภัยและการสร้างแบบจำลองข้อเสนอที่นำมาใช้คือการรักษาความปลอดภัย (CIA) และกลไกของการทำงานที่เกี่ยวข้อง

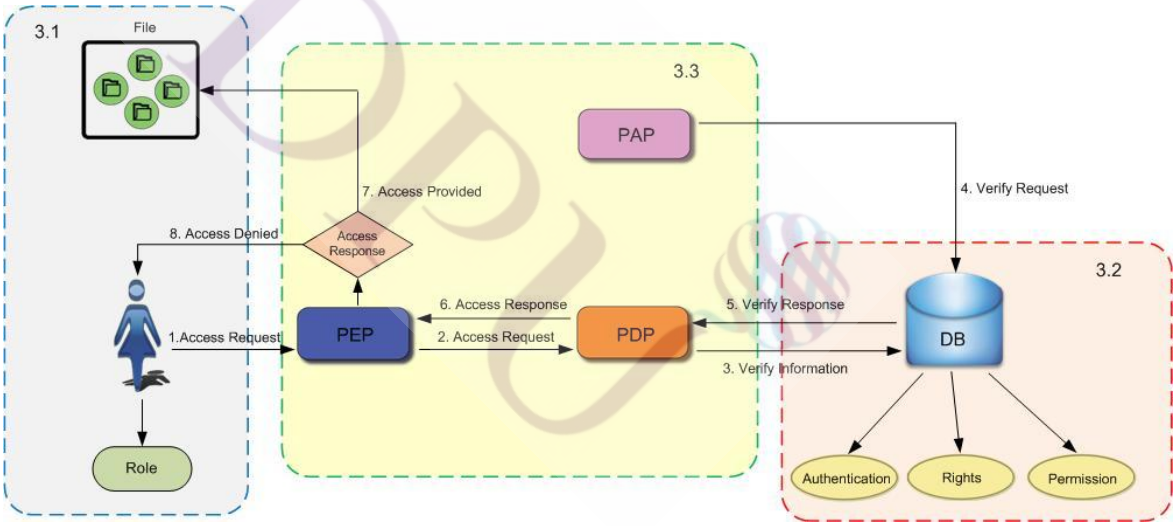
(รหัสผ่าน/การเข้ารหัส) เพื่อสนับสนุนการเป็นเจ้าของ ความไว้วางใจ การมอบหมาย และการสร้างแบบจำลองความต้องการ ในทางปฏิบัติจะประกอบด้วย บริการและ การมอบสิทธิ์ให้กับ Actors โดยใช้กรณีศึกษามหาวิทยาลัยรัฐบาลท้องถิ่นหน่วยการดูแลสุขภาพเพื่อการรักษาความปลอดภัยประเทศอิตาลี การกำหนดความปลอดภัยและนโยบายความเป็นส่วนตัวจะนำเอามาตรฐานการจัดการความปลอดภัย ISO-17799 เป็นต้นแบบ การพัฒนาซอฟแวร์ตามการทำงานของ Actors จะใช้แบบจำลองและการวิเคราะห์ความต้องการซอฟแวร์ ขั้นตอนในการพัฒนาจะหาความแตกต่างของความต้องการของ Actor เพื่อใช้ออกแบบรายละเอียดของ Actors การกำหนดภาระหน้าที่ระหว่าง Actors และการกำหนดระหว่าง Actors กับบริการ การกำหนดจะนำไปสู่ความต้องการของการกระทำและความสามารถในการดำเนินการเพื่อตอบสนองความต้องการ ประกอบด้วยความสัมพันธ์ดังนี้ Ownership (ความสัมพันธ์ระหว่าง Actors กับบริการ) Trust(ความสัมพันธ์ระหว่าง Actor 2 คน กับบริการ) Delegation (ความสัมพันธ์ระหว่าง Actors 2 คน กับบริการ) การเลือกวิธีการมอบหมาย ความไว้วางใจ สามารถสร้างแบบจำลองความปลอดภัยสถานะการณ์ต่างๆ ความแตกต่างของ Actors และการกำหนดสิทธิ์ในการจัดการมากที่สุดและสิทธิ์ในการจัดการน้อยที่สุด การจัดระดับและการแบ่งกลุ่มภายในองค์กร เป็นบริหารจัดการ Actors อย่างมีแบบแผนเพื่อให้สอดคล้องกับความต้องการและการทำงาน การสร้างแบบจำลองการประมวลผลเป็นการยืนยันความต้องการบริการของ Actors การจำลองรูปแบบการอนุญาตจะสอดคล้องกับวิศวกรรมความต้องการความเป็นเจ้าของ เพื่ออนุญาตให้สามารถเข้าถึงบริการและสามารถมอบอำนาจ การแบ่งกลุ่มเพื่อเป็นการตรวจสอบคุณสมบัติและความซับซ้อนของ Actors และบริการ ทำให้ทราบถึงความไว้วางใจระหว่าง Actors หรือใช้ในการตรวจสอบการอนุญาตในการดำเนินการ การตรวจสอบการละเมิดความไว้วางใจ/การตรวจสอบการกระทำของ Actors ตามที่กำหนดไว้ในโครงสร้างภาระหน้าที่ความไว้วางใจและความน่าเชื่อถือของ Actors การตรวจสอบนี้จะทำให้เห็นปัญหาที่เกิดขึ้นและทราบแนวทางการพัฒนาต่อไป

งานวิจัยทั้ง 2 ทฤษฎีที่นำเสนอข้างต้น ถือเป็นแนวทางที่ดีและสามารถรักษาความปลอดภัยของข้อมูลได้เป็นอย่างดี แต่ยังไม่สามารถนำทฤษฎีเหล่านั้นมาสร้างระบบสำหรับสมาคมฯ เนื่องจากองค์กรมีข้อจำกัดในการใช้งานสารสนเทศทั้งทักษะการใช้งานคอมพิวเตอร์และระบบออนไลน์ และขาดบุคลากรทางด้านสารสนเทศ งานวิจัยหัวข้อการรักษาความปลอดภัยวิศวกรรมความต้องการเพื่อใช้ในการปฏิบัติตามกฎหมายการป้องกันข้อมูลประเทศอิตาลี งานวิจัยนี้มีการจัดทำนโยบายการรักษาความปลอดภัยของข้อมูลที่ต้องใช้บุคคลากรสารสนเทศเป็นจำนวนมากให้เพียงพอกับการดูแลรักษาระบบและผู้ใช้งานระบบ รวมทั้งบุคลากรทุกระดับในองค์กรจะต้องเล็งเห็นความสำคัญของระบบสารสนเทศ มีความตั้งใจที่จะเรียนรู้และใช้งานระบบตามนโยบายที่

เจ้าหน้าที่สารสนเทศออกกแบบไว้ แต่โครงสร้างองค์กร ไม่มีตำแหน่งบุคลากรด้านไอทีและสารสนเทศ รวมถึงไม่มีการสร้างนโยบายเกี่ยวกับสารสนเทศที่ดีเพื่อบังคับใช้งานระบบ ส่วนงานวิจัยหัวข้อแบบจำลองความต้องการการรักษาความปลอดภัย ความไว้วางใจ ความเป็นเจ้าของการอนุญาต การมอบหมาย นั้น เหมาะกับองค์กรที่มีเจ้าหน้าที่มีทักษะการใช้งานสารสนเทศมากพอสมควร โดยเฉพาะเจ้าหน้าที่ระดับสูง ที่มีสิทธิ์ให้การมอบหมาย กระจายสิทธิ์ และสามารถกำหนดสิทธิ์ให้กับผู้ใช้อื่นๆ ที่ได้รับวางไว้วางใจในระบบได้ แต่บุคลากรภายในองค์กรขาดความรู้ความเข้าใจเกี่ยวกับการใช้งานระบบสารสนเทศและการใช้คอมพิวเตอร์เท่าที่ควร ดังนั้นในการจัดทำระบบเพื่อให้ผู้ใช้ระดับสูงสามารถกำหนดสิทธิ์ได้เองเป็นเรื่องยากในการเรียนรู้ เนื่องจากระบบจะมีความซับซ้อนมากเกินไป ผู้จัดทำจึงได้ออกแบบระบบให้ผู้ใช้มีหน้าที่ใช้งานตามสิทธิ์ที่ได้รับเท่านั้น ผู้ใช้ไม่ต้องเรียนรู้เทคนิคใดๆ ทำให้ใช้งานง่ายและสะดวกสบาย แต่ในการกำหนดสิทธิ์ทางเทคนิคในระบบ จะมอบหมายให้แก่ผู้ดูแลระบบเป็นผู้กำหนดเท่านั้น ทั้งนี้ระบบได้ออกแบบสำหรับผู้ดูแลระบบให้ใช้งานง่าย สามารถตั้งค่าบัญชีผู้ใช้ผ่านหน้าเว็บ โดยไม่ต้องกำหนดในฐานข้อมูล

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

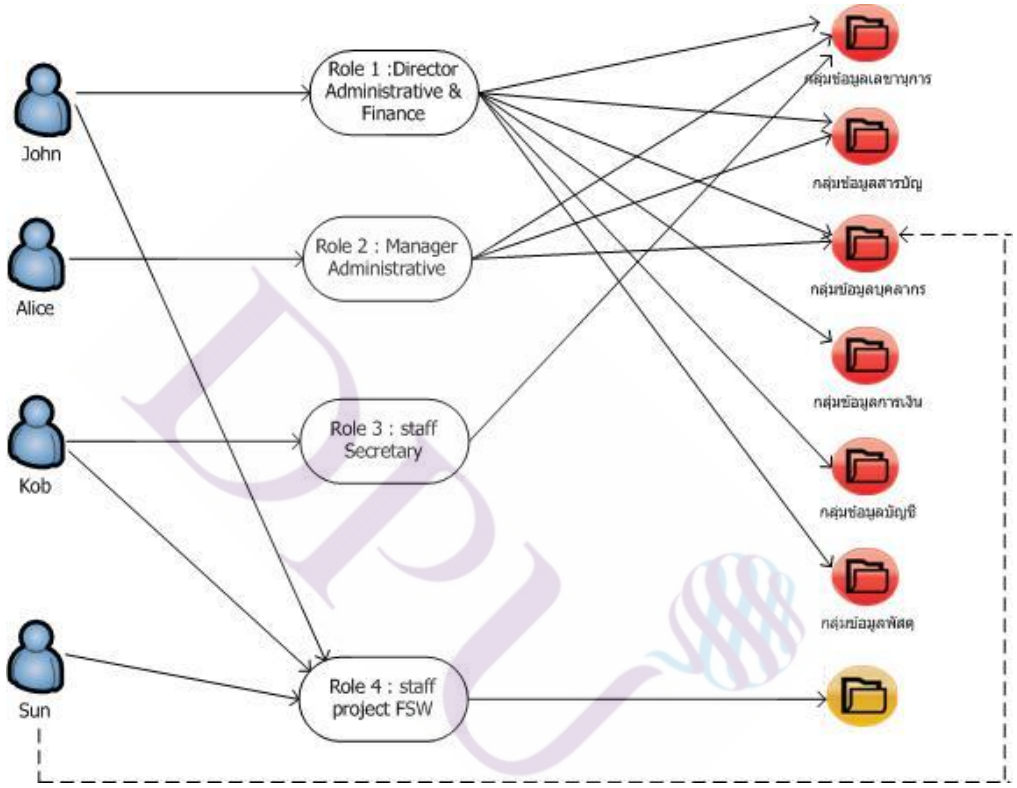
1. Role-base การอนุญาตและกำหนดสิทธิ์ตามบทบาทหน้าที่ที่ได้รับมอบหมาย แบ่งได้ 2 ลักษณะได้แก่

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

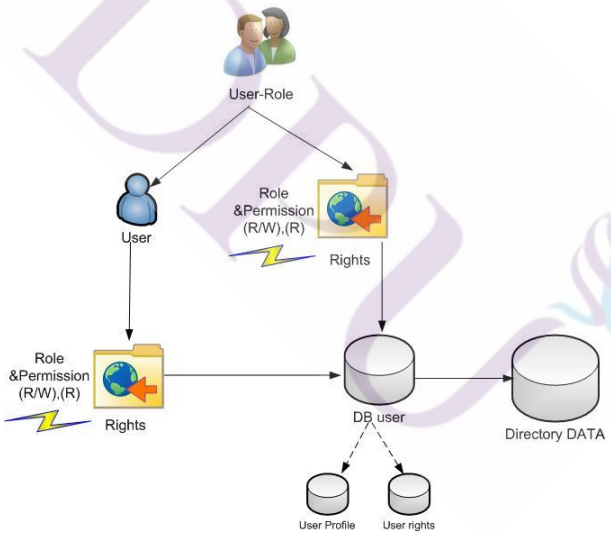
หลังจากกำหนดขอบเขตให้เจ้าหน้าที่ภายในองค์กรสามารถเข้าถึงแหล่งข้อมูลใดได้บ้าง ตามบทบาทและภาระหน้าที่ของผู้ใช้แล้ว จากนั้นเป็นการกำหนดรายละเอียดเกี่ยวกับสิทธิ์ความสามารถในการกระทำกับกลุ่มข้อมูล โดยการประชุมผู้บริหารและผู้ที่มีให้สิทธิ์ในการใช้งานข้อมูล มีรายละเอียดดังต่อไปนี้

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)

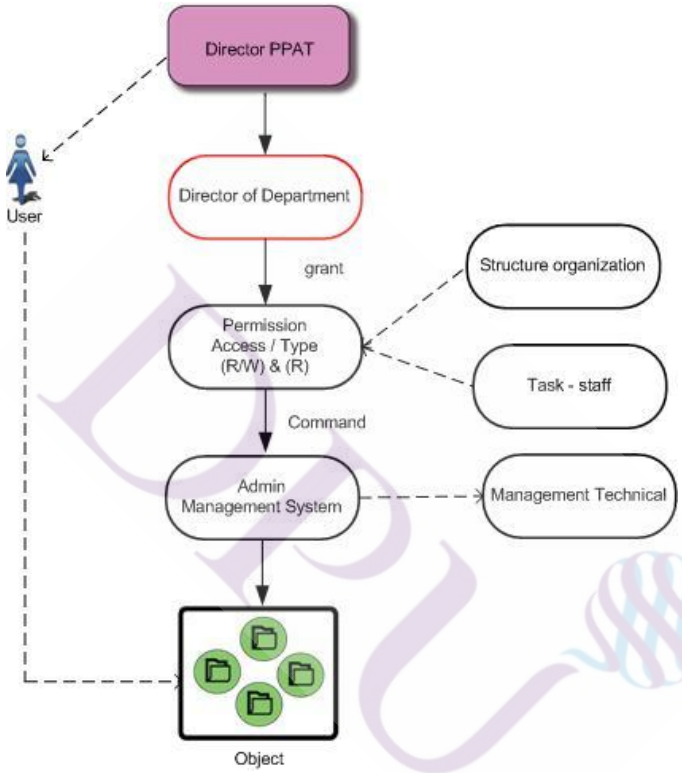
รายชื่อเจ้าหน้าที่	Role No.	Group / Authorization & Authentication								
		สำนักบริหารกลาง						งานโครงการด้านเอดส์		
		งานบริหาร			Finance					
		เลขานุการ	บุคลากร	สารบัญ	บัญชี	การเงิน	พัสดุ	FSW	MSM	Childlive
	Role 3				R/W	R	R			
	Role 11							R		
	Role 12								R/W	
Koi	Role 13									R
	Role 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

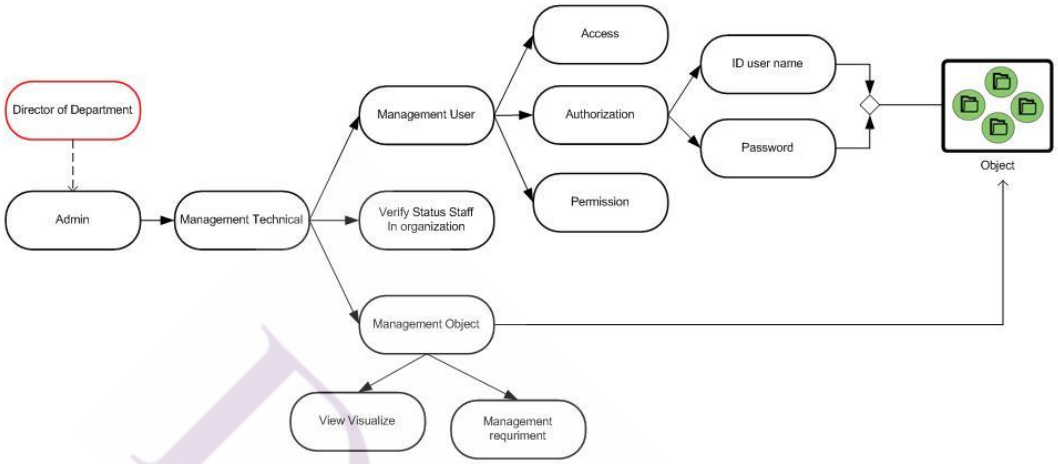


รูปที่ 3.4 กระบวนการดำเนินงานให้สิทธิ์

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

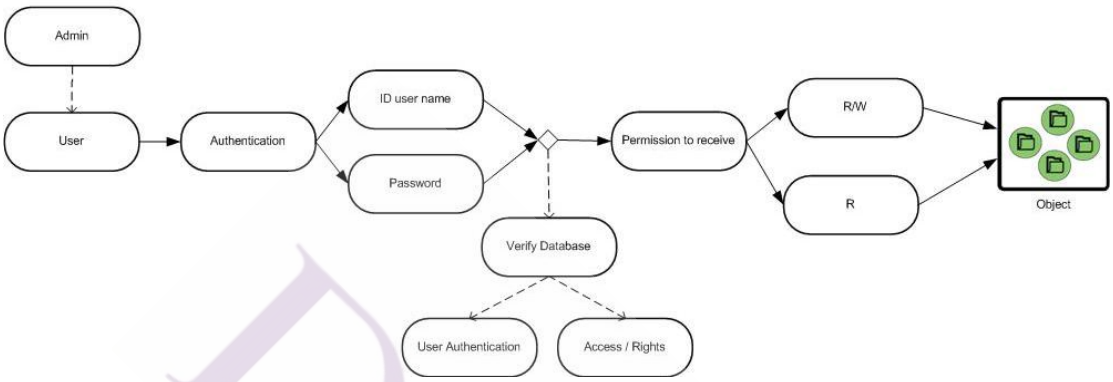
หลังจากที่ผู้อำนวยการสำนักฯ ให้สิทธิ์กับผู้ใช้แล้ว ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงข้อมูลในระบบตามที่ได้รับแจ้งจากผู้อำนวยการสำนักฯ เพื่อป้องกันข้อมูลจากผู้ที่ไม่ได้รับอนุญาต ดังรูปที่ 5 แสดงขั้นตอนการกำหนดสิทธิ์การเข้าถึงข้อมูลให้กับผู้ใช้ มีรายละเอียดดังต่อไปนี้

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

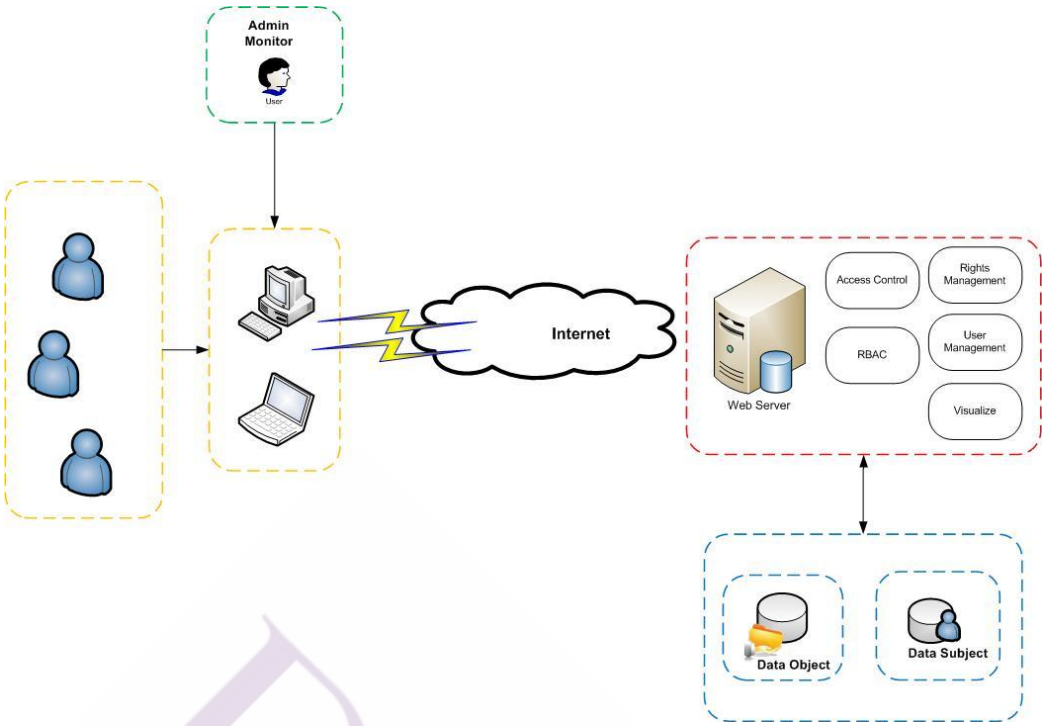
3.4 สามารถควบคุมสิทธิ์การเข้าถึงข้อมูลของผู้ใช้ เพื่อให้ผู้ใช้สามารถใช้งานระบบตามสิทธิ์ที่ได้รับอนุญาตและเพื่อป้องกันการเข้าใช้งานข้อมูลจากผู้ที่ไม่ได้รับอนุญาต

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

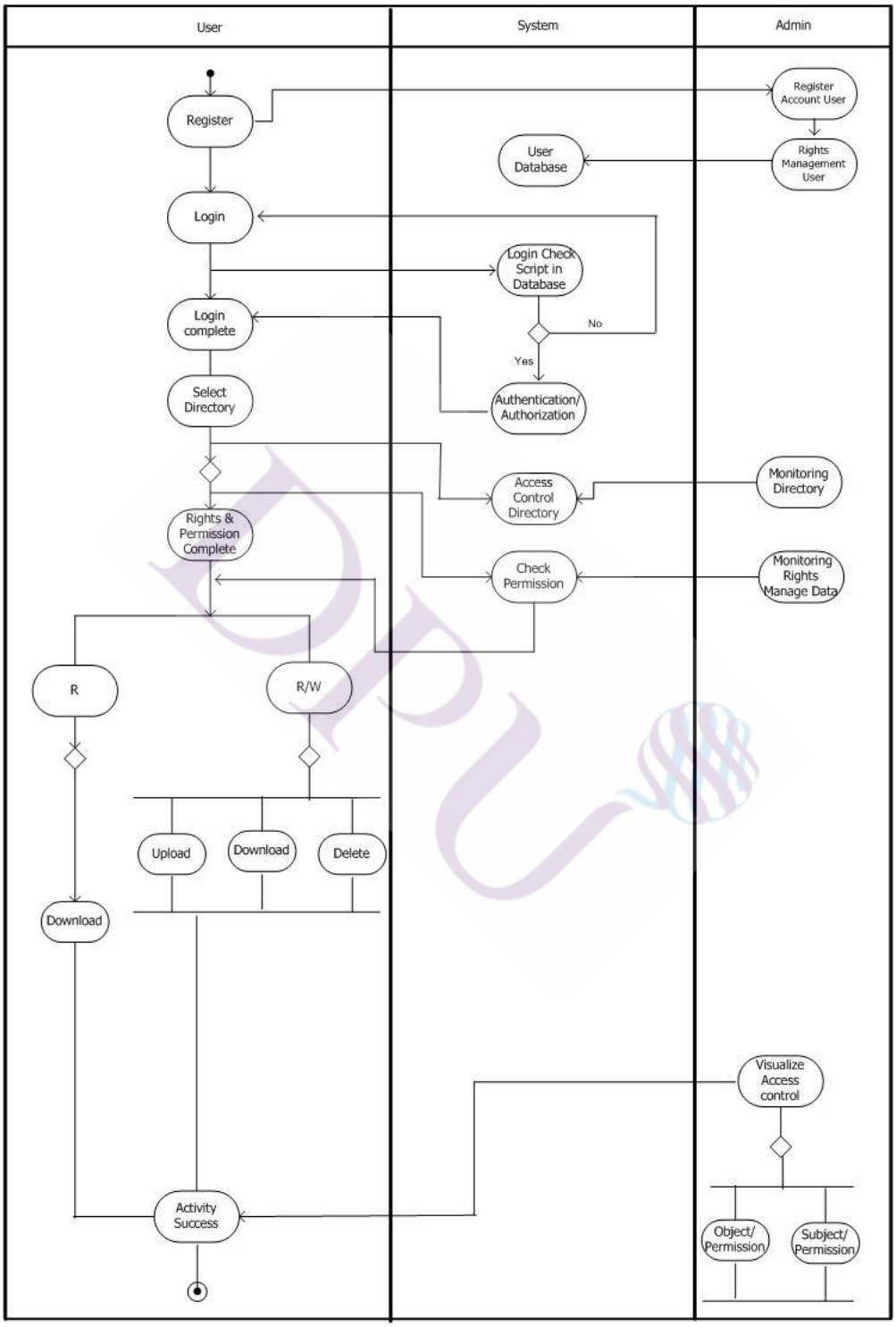
1.4 สามารถแก้ไขหรือเปลี่ยนแปลงสิทธิ์การเข้าถึงข้อมูลของผู้ใช้ได้ กรณีมีการเปลี่ยนแปลงอำนาจหรือปรับโครงสร้างกลุ่มผู้ใช้การเข้าถึงข้อมูล

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									→

บทที่4
ผลการดำเนินงาน

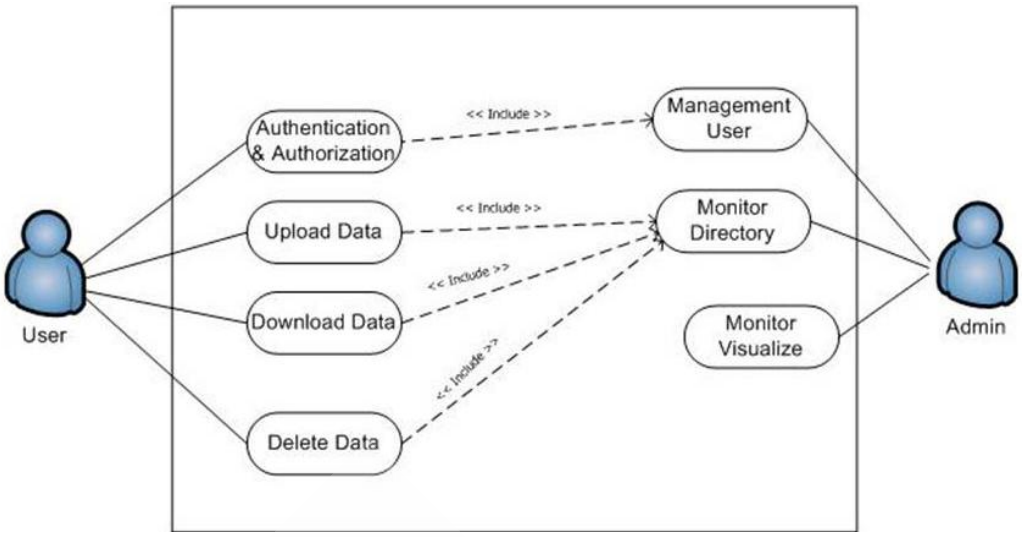
จากการศึกษาข้อมูลที่เกี่ยวข้องและเหมาะสมกับองค์กร ผู้จัดทำได้สร้างแบบจำลองการกำหนดสิทธิ์ การควบคุมการเข้าถึง และออกแบบระบบในบทที่ 3 นั้น เนื้อหาในบทที่ 4 จะกล่าวถึงผลการทำงานของระบบและผลการออกแบบหน้าจอ เพื่อให้เหมาะสมกับผู้ใช้ภายในองค์กร ประกอบด้วยผลการออกแบบขั้นตอนการจัดทำระบบ ผลของการออกแบบหน้าจอการและวิธีการใช้งานระบบ และผลการวิเคราะห์โครงสร้างการให้สิทธิ์และการอนุญาต

4.1 ผลการออกแบบขั้นตอนการจัดทำระบบ

การวิเคราะห์ระบบเพื่อให้สามารถใช้งานได้อย่างมีประสิทธิ์ภาพ ตรงกับความต้องการของผู้ใช้ทุกระดับ และประมวลผลได้ถูกต้องตามที่ผู้ดูแลระบบตั้งค่า ในการจัดทำระบบได้นำกรณีศึกษาสมาคมวางแผนครอบครัวแห่งประเทศไทยในพระบรมราชูปถัมภ์ ผู้จัดทำได้สร้างแบบจำลองแสดงรายละเอียดขั้นตอนกระบวนการทำงานของระบบทำให้เห็นโครงสร้างและรูปแบบการทำงานของเว็บแอปพลิเคชั่นชัดเจนยิ่งขึ้น

4.1.1 กระบวนการทำงานของระบบ

กระบวนการทำงานของระบบทั้งหมดในภาพรวม ประกอบด้วยผู้ที่มีส่วนเกี่ยวข้องกับระบบ ได้แก่ ผู้มีอำนาจมอบหมาย ผู้ใช้งานระบบ และผู้ดูแลระบบ ผู้ที่เกี่ยวข้องจะสามารถเข้าใช้งานตามสิทธิ์ที่ได้รับ ซึ่งสามารถอธิบายอย่างละเอียด Use case Diagram ดังต่อไปนี้



รูปที่ 4.1 Use Case Diagram ของระบบ

ในรูปที่ 4.1 แผนภาพ Use Case Diagram แสดงภาพรวมการทำงานของระบบ และผู้ที่มีส่วนเกี่ยวข้องกับระบบทั้งหมด โดยรายละเอียดของผู้ที่เกี่ยวข้องกับระบบ (Actor Descriptions) แสดงได้ตามตารางที่ 4.1 รายละเอียดของ Actor แต่ละระดับ แสดงไว้ในภาคผนวก ข. Use Case Scenario

ตารางที่ 4.1 แสดงรายละเอียดผู้ที่เกี่ยวข้องกับระบบ

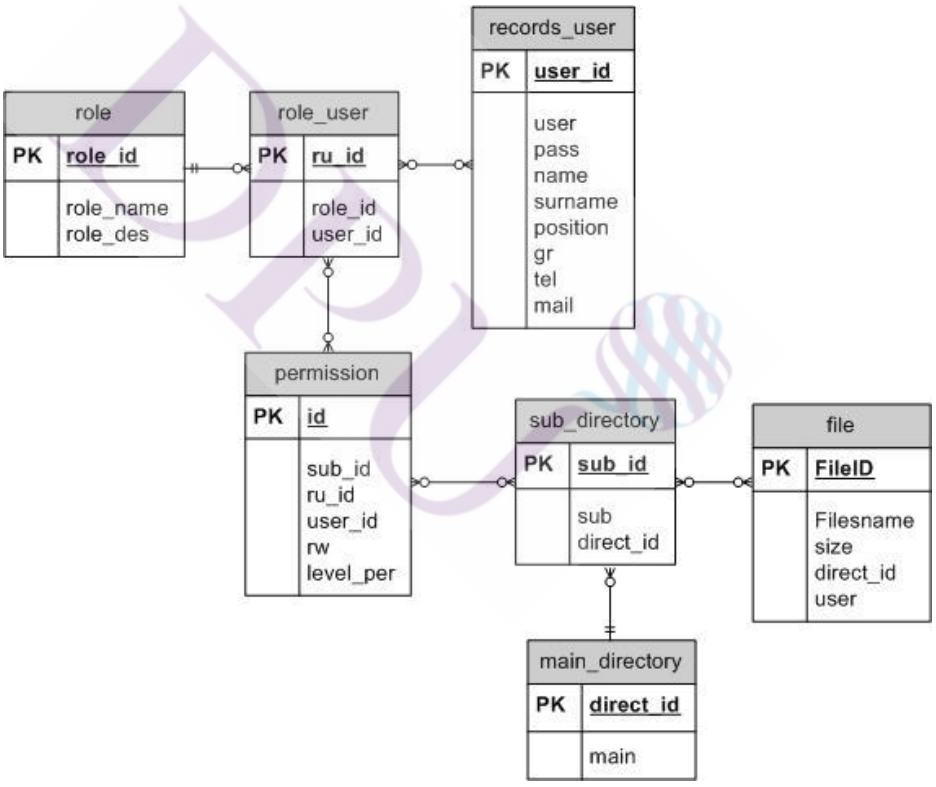
Actor	คำอธิบาย
User	ผู้ใช้งานระบบ (User) สามารถเข้าใช้งานผ่านหน้าเว็บได้ตามที่ได้รับสิทธิ์และตามที่ผู้ดูแลระบบกำหนด
Admin	ผู้ดูแลระบบ (Admin) สามารถกำหนดสิทธิ์ให้กับผู้ใช้งานระบบตามที่ผู้มีอำนาจในการแจกจ่ายสิทธิ์ และสร้างบัญชีผู้ใช้ให้กับ User

4.1.2 การออกแบบระบบฐานข้อมูล

การจัดทำระบบงานเพื่อบริหารจัดการและควบคุมเอกสารบนเว็บ ได้ออกแบบระบบฐานข้อมูลเพื่อจัดเก็บข้อมูล มีโครงสร้างระบบฐานข้อมูลทั้งหมด 6 ตาราง ประกอบด้วยตารางดังต่อไปนี้

1. ตาราง record_user เป็นตารางเก็บรายละเอียดข้อมูลทั่วไปของผู้ใช้งานระบบ (user)
2. ตาราง main directory เป็นตารางเก็บรายชื่อกลุ่มข้อมูลหลัก
3. ตาราง sub directory เป็นตารางเก็บรายชื่อกลุ่มข้อมูลรอง
4. ตาราง file เป็นตารางเก็บรายชื่อเอกสารที่อยู่ในระบบ
5. ตาราง role เป็นตารางเก็บบทบาทตามโครงสร้างขององค์กร
6. ตาราง role_user เป็นตารางเก็บบทบาทของผู้ใช้งานระบบแต่ละคน (user)
7. ตาราง permission เป็นตารางเก็บสิทธิ์การเข้าถึงข้อมูลของผู้ใช้งานระบบแต่ละคน (user)

ตารางเก็บข้อมูลทั้ง 6 ตารางจะมีความสัมพันธ์กันในแต่ละตาราง ดังแสดงในรูปที่ 4.2 สำหรับ Data Dictionary อยู่ในภาคผนวก ก. การออกแบบฐานข้อมูล



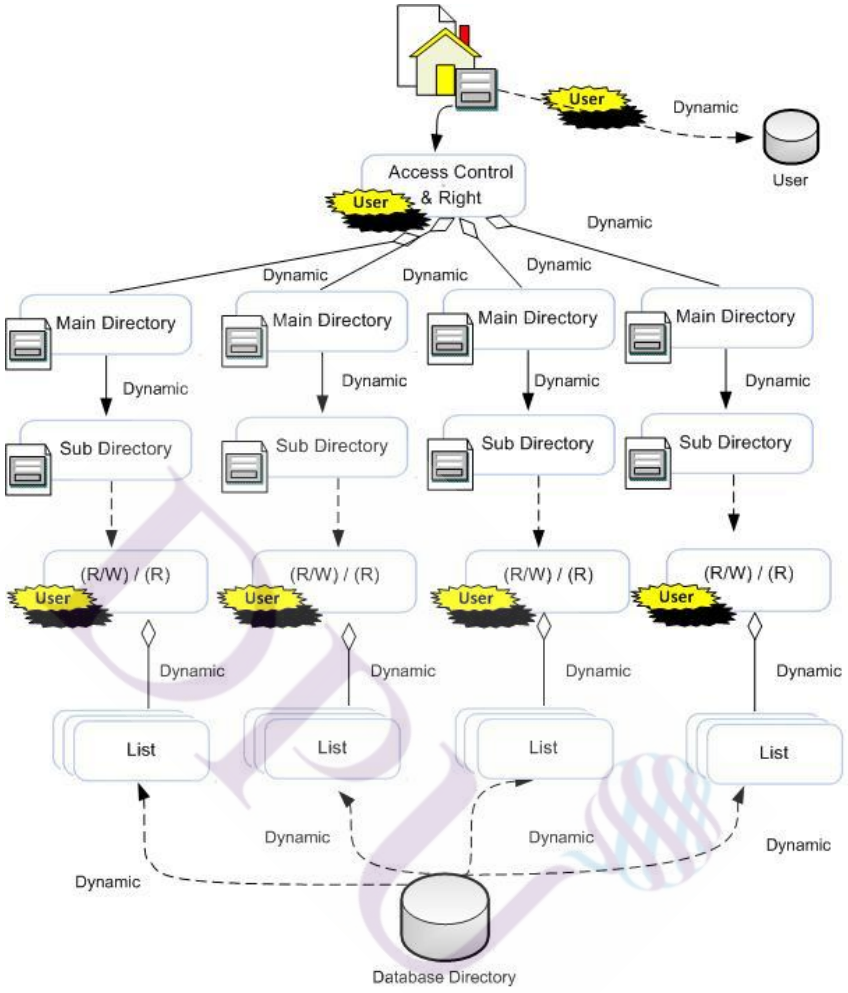
รูปที่ 4.2 แสดงความสัมพันธ์โครงสร้างระบบฐานข้อมูล Relationship

4.1.3 แบบจำลองแสดงรายละเอียดขั้นตอนการทำงานของระบบ

1. โครงสร้างเว็บแอปพลิเคชั่น : Blueprint

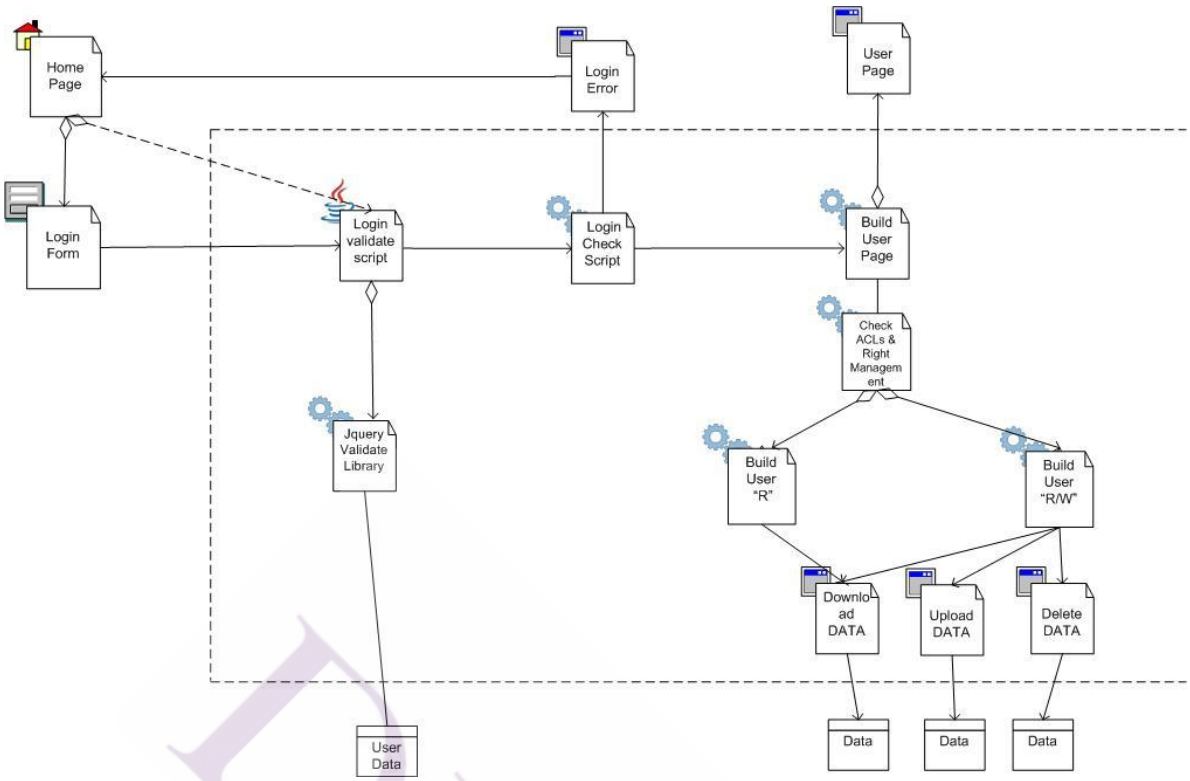
ในการออกแบบโครงสร้างของเว็บแอปพลิเคชั่นการจัดทำระบบงานเพื่อบริหารจัดการและควบคุมเอกสารบนเว็บ โดยใช้การกำหนดสิทธิ์ในการเข้าถึงข้อมูลเพื่อให้ผู้ใช้สามารถใช้งาน

ระบบได้ตามความต้องการและสิทธิ์ตามขอบเขตที่ได้รับ การออกแบบโครงสร้างเว็บแอปพลิเคชั่น ทำให้ทราบเนื้อหาในส่วนประกอบของแต่ละหน้าที่เชื่อมโยงกัน สามารถแสดงดังรูป 4.3



รูปที่ 4.3 Blueprint แสดงโครงสร้างเว็บแอปพลิเคชั่น

2 โครงสร้างขั้นตอนการทำงานของระบบ : WAE



รูปที่ 4.4 แสดงขั้นตอนทำงานของระบบ

จากรูปที่ 4.4 สามารถอธิบายรายละเอียดขั้นตอนของการทำงานระบบ ผู้จัดทำขอนำเสนอรูปแบบการเข้าถึงข้อมูลในระบบ ประกอบด้วยการทำงานดังต่อไปนี้

1. User ล๊อกอิน (Login) เข้าสู่ระบบเพื่อพิสูจน์ตัวตนก่อนเข้าใช้งานระบบ โดยใช้ User name และ Password

2. ระบบจะทำการตรวจสอบข้อมูลกับฐานข้อมูล User name และ Password ของ User โดยมีเงื่อนไขดังนี้

2.1 ถ้า User name และ password ไม่ถูกต้อง User จะไม่สามารถเข้าสู่ระบบได้ และระบบจะกลับไปยังหน้าแรก

2.2 ถ้า User name และ password ถูกต้อง User จะสามารถเข้าสู่ระบบได้ และระบบจะเข้าสู่หน้า web page ของ User

3. เมื่อเข้าสู่ระบบได้แล้ว ผู้ใช้จะอยู่ในหน้า user page ของแต่ละคน ประกอบด้วย directory กลุ่มต่างๆ ตามที่ได้รับสิทธิ์ให้สามารถเข้าถึงได้ ซึ่งในแต่ละ directory จะประกอบด้วยรายละเอียดดังนี้

3.1 “R/W” หมายถึง ผู้ใช้สามารถเข้าถึงข้อมูลและบริหารจัดการกลุ่ม directory นั้น ได้แก่ Upload , Download , Delete

3.2 “R” หมายถึง ผู้ใช้สามารถเข้าถึงข้อมูลกลุ่ม directory ได้เท่านั้น ได้แก่ Download

4.2 ผลของการออกแบบหน้าจอการและวิธีการใช้งานระบบ

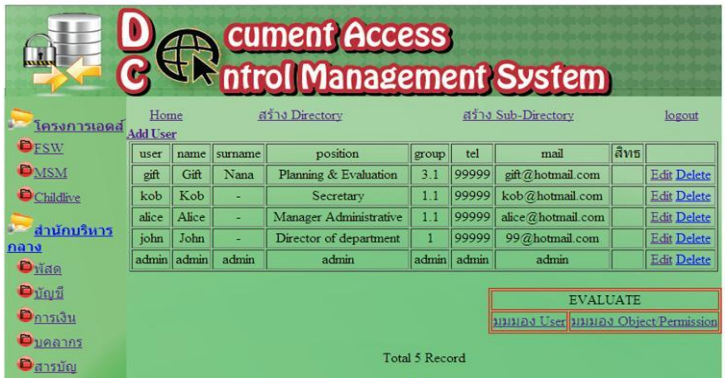
จากการวิเคราะห์และออกแบบระบบของเว็บแอปพลิเคชั่นการจัดทำระบบงานบริหารจัดการและควบคุมเอกสารผ่านเว็บ ผู้จัดทำได้ออกแบบหน้าจอการทำงานของระบบดังนี้

4.2.1 หน้าจอสำหรับผู้ดูแลระบบ (Admin)

หน้าจอสำหรับผู้ดูแลระบบ ผู้เข้าใช้งานต้องต้องล๊อกอิน (Login) เพื่อพิสูจน์ตัวตนในระบบ เพื่อตรวจสอบสิทธิ์การใช้งานระบบกับฐานข้อมูล โดยใช้ User name และ Password ดังรูปที่ 4.5

รูปที่ 4.5 หน้าจอ Login

ระบบแสดงหน้าจอสำหรับผู้ดูแลระบบเพื่อใช้ในการจัดการดังรูปที่ 4.6



รูปที่ 4.6 หน้าจอหลักสำหรับผู้ดูแลระบบ

หน้าจอผู้ดูแลระบบ มีความสามารถดังต่อไปนี้

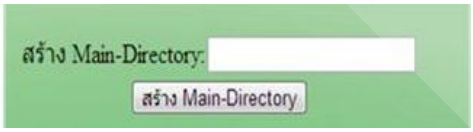
1. หน้าจอสร้างบัญชีผู้ใช้

ในการสร้างบัญชีผู้ใช้ ผู้ดูแลระบบคลิกที่ Add User จากนั้นระบบจะ Alert pop up เพื่อให้ใส่ข้อมูลเบื้องต้นของผู้ใช้

รูปที่ 4.7 หน้าจอบันทึกข้อมูลเบื้องต้นของผู้ใช้งานระบบ

2. หน้าจอสำหรับสร้าง Main Directory

ผู้ดูแลระบบคลิกที่เมนู “สร้าง Main Directory” เพื่อสร้างกลุ่มข้อมูลหลัก



รูปที่ 4.8 หน้าจอบันทึก Main directory

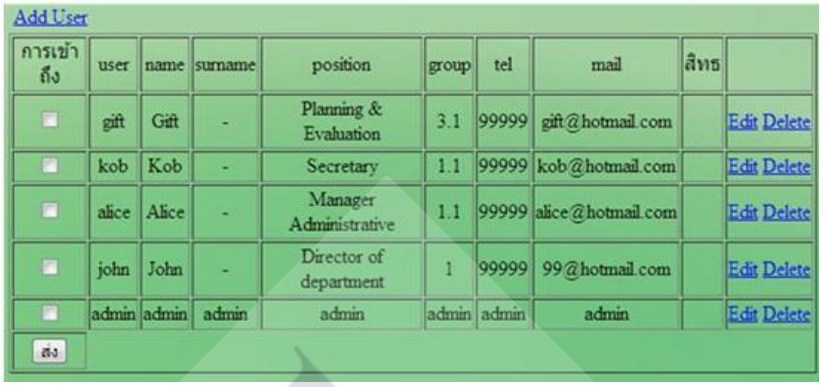
3. หน้าจอสำหรับสร้าง Sub Directory

ผู้ดูแลระบบคลิกที่เมนู “สร้าง sub Directory” เพื่อสร้างกลุ่มข้อมูลรอง ในการสร้าง sub Directory จะทำการเลือกกลุ่มข้อมูลหลัก และเลือกระดับความปลอดภัยของข้อมูล

รูปที่ 4.9 หน้าจอบันทึก Sub director

4. หน้าจอสำหรับกำหนดสิทธิ์ให้กับผู้ใช้

การกำหนดสิทธิ์ให้กับผู้ใช้ จะต้องทำการบันทึกข้อมูลเบื้องต้นก่อน จากนั้นให้คลิกที่ Edit Record User และ เลือกกลุ่มข้อมูลรอง ที่ต้องการกำหนดสิทธิ์ ระบบจะดึงเอาข้อมูลเบื้องต้นมาแสดงยกเว้น password ของผู้ใช้



รูปที่4.10 หน้าจอสำหรับการกำหนดสิทธิ์ให้กับผู้ใช้งานระบบ

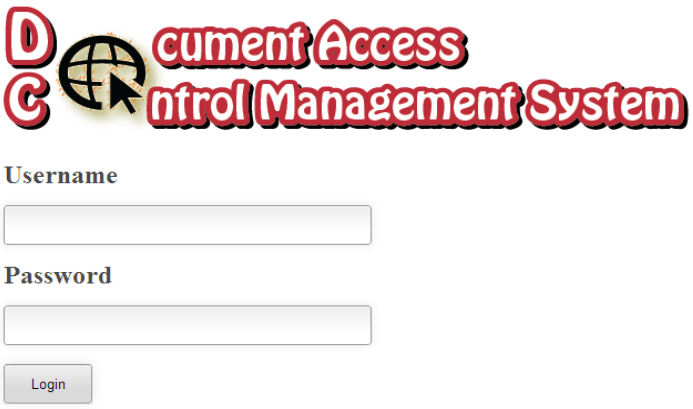
4.2.2 หน้าจอสำหรับผู้ใช้งานระบบ (User)

หน้าจอสำหรับผู้ใช้งานระบบ สามารถใช้งานได้ตามสิทธิ์ที่ได้รับอนุญาตการเข้าใช้งานกลุ่มข้อมูล ในแต่ละกลุ่มข้อมูลนั้นจะขึ้นอยู่กับการกำหนดสิทธิ์ของผู้ดูแลระบบ ซึ่งผู้จัดทำยกตัวอย่างผู้ใช้งาน 2 คน คือ John และ Alice โดยอ้างอิงจาก ตารางที่ 4 ในบทที่ 3 ดังนี้

รายชื่อเจ้าหน้าที่	Group / Authorization & Authentication										
	A (สำนักบริหารกลาง)								B (งานโครงการด้านเอดส์)		
	A1 (งานบริหาร)				A2 (งานบัญชี การเงินและพัสดุจัดซื้อ)				B1	B2	B3
	งานเลขานุการ (A1.1)	งานบุคลากร (A1.2)		งานสารบัญ (A1.3)	งานบัญชี (A2.1)	งานการเงิน (A2.2)		งานพัสดุ (A2.3)	พนักงานบริการหญิง	ชายรักชาย	เด็กและวัยเจริญพันธ์
John	R/W	R/W	R/W	R/W	R/W	R/W	R/W	R/W	R/W	R/W	R/W
Alice	R/W	R/W	R/W	R/W					R	R	R

การทำงานของระบบสำหรับผู้ใช้งาน มีรายละเอียดดังต่อไปนี้

หน้าจอสำหรับผู้ใช้งานระบบ ต้องต้องล๊อกอิน (Login) เพื่อพิสูจน์ตัวตนในระบบ เพื่อตรวจสอบสิทธิ์การใช้งานระบบกับฐานข้อมูล โดยใช้ User name และ Password ดังรูปที่ 4.11



รูปที่ 4.11 หน้าจอ Login เพื่อพิสูจน์ตัวตนของผู้ใช้งานระบบ

หน้าจอสำหรับให้ผู้ใช้สามารถ Upload เอกสร ดังรูปที่ 4.12 เพื่อจัดเก็บเอกสารไว้ในฐานข้อมูล โดยเอกสารที่ Upload ต้องมีขนาดไม่เกิน 10 MB

รูปที่ 4.12 หน้าจอสำหรับ Upload File

หน้าจอสำหรับให้ผู้ใช้สามารถ Download เอกสาร ดังรูปที่ 4.13 เพื่อให้สามารถนำเอกสารที่อยู่ในฐานข้อมูลออกมาใช้งานได้ ทั้งนี้ ระบบไม่ได้รองรับ version control ในการเก็บข้อมูลที่มีการเขียนทับ

รูปที่ 4.13 หน้าจอ Download file

หน้าจอสำหรับให้ผู้ใช้สามารถ Delete เอกสาร ดังรูปที่ 4.14 เพื่อให้สามารถลบเอกสารที่อยู่ในฐานข้อมูลออกได้

รูปที่ 4.14 หน้าจอสำหรับ Delete File

หน้าจอสำหรับให้ผู้ใช้สามารถแก้ไข password ดังรูปที่ 4.15 เพื่อให้สามารถเปลี่ยนแปลง password ส่วนตัวได้ โดยมีเงื่อนไขต้องมีจำนวน 6 ตัวอักษรขึ้นไป

รูปที่ 4.15 หน้าจอสำหรับแก้ไข password

หน้าจอสำหรับให้ผู้ใช้สามารถแก้ไขออกจากระบบ ดังรูปที่ 4.16 เพื่อให้สามารถ logout ออกจากระบบ เมื่อไม่ต้องการใช้งานต่อ

รูปที่ 4.16 หน้าจอสำหรับ logout

1. หน้าจอการใช้กลุ่มข้อมูลตามสิทธิ์ที่ได้รับอนุญาตของ John

ผู้ใช้งาน “John” มีสถานะเป็นผู้บริหารสำนักบริหารกลางทำให้สามารถเข้าถึงและบริหารจัดการข้อมูลภายในสำนักฯ ได้ นอกจากนี้ยังสามารถเข้าถึงและบริหารจัดการโครงการด้านเอดส์ เนื่องจากมีภาระหน้าที่ที่ต้องดำเนินงานโครงการฯ ดังนั้นหน้าจอการทำงานสำหรับ “John” ดังรายละเอียดต่อไปนี้

รูปที่ 4.17 หน้าจอการใช้งานสำหรับ “John” และกลุ่มข้อมูลที่สามารถเข้าถึงได้

รูปที่ 4.18 หน้าจอการใช้งานสำหรับ “John” ที่สามารถบริหารจัดการได้

2. หน้าจอการใช้กลุ่มข้อมูลตามสิทธิ์ที่ได้รับอนุญาตของ Alice

ผู้ใช้งาน “Alice” มีสถานะเป็นหัวหน้าฝ่ายบัญชีการเงิน ทำให้สามารถเข้าถึงและบริหารจัดการข้อมูลภายในฝ่ายได้ นอกจากนี้ยังสามารถเข้าถึงข้อมูลโครงการด้านเอดส์ เนื่องจากมี

ภาระหน้าที่ที่ต้องดำเนินงานโครงการฯ เพื่อนำเอาข้อมูลมาจัดทำรายงาน จึงมีสิทธิ์ในการเข้าถึงข้อมูลเพื่อดาวน์โหลดเอกสารได้เท่านั้น ไม่สามารถบริหารจัดการข้อมูล ดังนั้นหน้าจอการทำงานสำหรับ “Alice” ดังรายละเอียดต่อไปนี้

รูปที่ 4.19 หน้าจอการใช้งานสำหรับ “Alice” ที่สามารถบริหารจัดการได้ (ได้รับสิทธิ์ R/W)

รูปที่ 4.20 หน้าจอการใช้งานสำหรับ “Alice” ที่สามารถเข้าถึงข้อมูลได้ (ได้รับสิทธิ์ R)

4.3 แผนภาพการกำหนดสิทธิ์ (Evaluate Permission)

ในการบริหารจัดการและกำหนดสิทธิ์ความสามารถในการเข้าถึงข้อมูลในแต่ละ Object จากที่ได้กล่าวถึงบทบาทหน้าที่การจัดการระบบในบทที่ 3 นั้น ผู้ที่มีหน้าที่ในการตั้งค่าในระบบคือผู้ดูแลระบบเท่านั้น แต่ผู้ดูแลระบบจะดำเนินงานตามที่ได้รับอนุมัติจากเจ้าของ Object หรือผู้บริหารระดับสูง ดังนั้นเพื่อให้ผู้บริหารหรือเจ้าของข้อมูลมองเห็นภาพที่ได้อนุญาตและกระจายแจกจ่ายสิทธิ์ให้กับเจ้าหน้าที่ทั้งที่เกี่ยวข้อง และไม่เกี่ยวข้องกับข้อมูลเพื่อนำมาใช้ในการพิจารณาในการปรับปรุงเปลี่ยนแปลงให้เหมาะสมและมีความปลอดภัยกับข้อมูลมากยิ่งขึ้น โดยในระบบสามารถเรียกดูเป็นแผนภาพได้ 2 รูปแบบดังต่อไปนี้

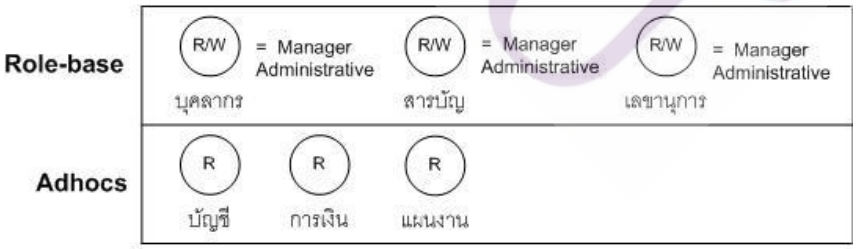
<u>อธิบายสัญลักษณ์</u>

หมายถึง ได้รับอนุญาตให้สามารถเข้าถึงและบริหารจัดการข้อมูลได้ (R/W)

หมายถึง ได้รับอนุญาตให้สามารถเข้าถึงข้อมูลได้เท่านั้น (R)

<u>รูปแบบที่ 1 มุมมองของ Subject</u>

User ชื่อ Alice



รูปที่ 4.21 แสดงความสามารถในการเข้าถึงข้อมูลตามผู้ใช้งานระบบ

รูปที่ 4.21 แสดงความสามารถในการเข้าถึงข้อมูลของ Subject ในแต่ละ Object และความสัมพันธ์กับ Object นั้นๆ สามารถเรียกดูได้จากผู้ใช้งานระบบ โดยแบ่งได้ 3 ระดับ พร้อมทั้งยกตัวอย่างผู้ใช้งานระบบ ชื่อ Koi ดังต่อไปนี้

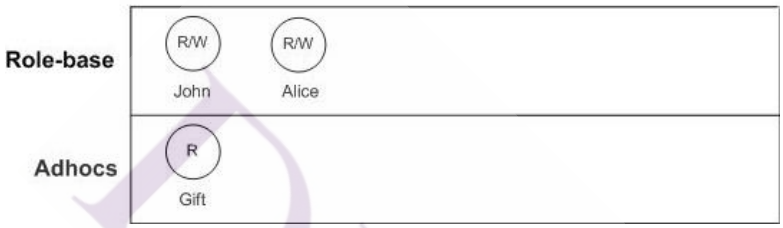
1. Role เป็นการเข้าถึงข้อมูลตามโครงสร้างขององค์กร มีภาระหน้าที่ที่ต้องทำเป็นประจำอยู่แล้วตามตำแหน่งงานที่ได้รับมอบหมาย ดังตัวอย่าง ผู้ใช้งานระบบ Koi ได้รับมอบหมาย

ให้ทำงานในตำแหน่งบัญชี เป็นงานที่ปฏิบัติเป็นประจำตามโครงสร้างองค์กรและได้รับอนุญาตให้สามารถเข้าถึงและบริหารจัดการข้อมูลได้ (R/W)

2. Adhocs เป็นการเข้าถึงข้อมูลตามที่ได้รับอนุญาต แต่ไม่ได้มีภาระหน้าที่ที่รับผิดชอบใน Object นั้นๆ ดังตัวอย่าง ผู้ใช้งานระบบ Koi นอกจากงานที่ได้รับมอบหมายแล้ว ยังได้รับอนุญาตให้สามารถเข้าถึงข้อมูลกลุ่มอื่นๆ ได้แก่ การเงิน บุคลากร เลขานุการ สารบัญ แผนงาน เป็นต้น และได้รับอนุญาตให้สามารถเข้าถึงข้อมูลได้เท่านั้น (R)

<u>รูปแบบที่ 2 มุมมองของ Object และ Role</u>

สำนักบริหารกลาง ฝ่ายการเงิน



รูปที่ 4.22 แสดงผู้ใช้งานระบบที่สามารถเข้าถึงกลุ่มข้อมูล

รูปที่ 4.22 แสดงรายละเอียดผู้ใช้งานระบบที่ได้รับอนุญาตให้สามารถเข้าถึงกลุ่มข้อมูลได้ โดยสามารถเรียกดูได้ตาม Object เมื่อต้องการตรวจสอบว่าแต่ละ Object มีผู้ใช้งานใดเข้าถึงข้อมูลได้ และความสามารถในการใช้งานกลุ่มข้อมูลนั้นเป็นอย่างไร รวมถึงสถานะในกลุ่มข้อมูลนั้นๆ ช่วยในการวิเคราะห์เป็นราย Object เพื่อนำมาพิจารณาต่อไป จากแผนภาพที่ 2 สามารถอธิบายรายละเอียดตามสถานะ 2 ระดับ พร้อมทั้งยกตัวอย่างสำนักบริหารกลาง ฝ่ายการเงินดังต่อไปนี้

สำนักบริหารกลาง ฝ่ายการเงิน มีผู้ใช้งานระบบและสถานะในกลุ่มข้อมูลดังต่อไปนี้

1. Role ผู้ที่ได้รับสิทธิ์ตามสถานะโครงสร้างขององค์กร ได้แก่ John และ John ได้รับอนุญาตให้เข้าถึงและบริหารจัดการข้อมูลได้

2. Adhocs ผู้ที่ได้รับสิทธิ์นอกเหนือจากสถานะตามโครงสร้าง ได้แก่ Koi , May , Jo , Puy , Ann , Jack , Sun ผู้ใช้งานระบบทุกคนได้รับอนุญาตเท่ากันคือ สามารถเข้าถึงข้อมูลได้เท่านั้น (R)

การกำหนดสิทธิ์ในระบบ ผู้ดูแลระบบจะกำหนดตามที่ได้รับอนุญาตจากเจ้าของหรือผู้บริหารระดับสูง ซึ่งในการอนุญาตนี้ไม่ได้มีโครงสร้างในการกำหนดสิทธิ์ที่ชัดเจน ในบางกลุ่ม

ข้อมูลเจ้าของหรือผู้บริหารจะอนุญาตให้ทุกคนสามารถเข้าถึงข้อมูลได้โดยไม่จำกัด ทำให้กลุ่มข้อมูลนั้นๆ ขาดความเป็นความลับและขาดความคงสภาพของข้อมูลไม่มีความปลอดภัยเท่าที่ควร จากแผนภาพที่ 1 และ แผนภาพที่ 2 สามารถแสดงความสัมพันธ์ระหว่างผู้ใช้งานระบบ (User) กับกลุ่มข้อมูล (Object) รวมถึงสิทธิ์ที่ได้รับในการเข้าถึง ทำให้สามารถนำมาวิเคราะห์ต่อยอดเพื่อนำมาพิจารณากลุ่มข้อมูลมีความปลอดภัยมากยิ่งขึ้น

1. ผู้ใช้งานระบบที่ได้รับอนุญาตในการเข้าถึงข้อมูลบางกลุ่มที่อยู่ใน Adhocs สมควรที่จะได้รับสิทธิ์นั้นต่อไปหรือไม่

2. กลุ่มข้อมูลที่อยู่ในระดับ Project ผู้ใช้งานระบบยังต้องรับผิดชอบภาระหน้าที่ที่นอกเหนืองานประจำอยู่ในกลุ่มข้อมูลนั้นๆหรือไม่

3. ผู้ใช้งานระบบแต่ละคนยังมีสิทธิ์เข้าถึงกลุ่มข้อมูลอื่นๆอีกหรือไม่ นอกเหนือจากที่ได้รับอนุญาตในปัจจุบัน

4.4 ผลการวิเคราะห์แบบประเมินความความพึงพอใจของระบบ

เพื่อให้ได้ระบบงานที่มีประสิทธิผลและประสิทธิภาพและตรงตามความต้องการของผู้ใช้มากที่สุด ผู้พัฒนาได้ทำการประเมินผลการใช้งานระบบจากผู้ใช้งาน โดยใช้แบบสอบถามทำการประเมินหาระดับความเหมาะสม/ความพึงพอใจของระบบที่ได้พัฒนาขึ้น แบบสอบถามที่ใช้ในการประเมินแบ่งเนื้อหาออกเป็น 3 ตอน ประกอบด้วย

ตอนที่ 1 ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม

ตอนที่ 2 ข้อมูลความคิดเห็นเกี่ยวกับประสิทธิภาพของระบบ

ตอนที่ 3 ข้อเสนอแนะและแนวทางในการปรับปรุงและพัฒนาระบบ

ตัวอย่างของแบบสอบถามได้กล่าวไว้ในภาคผนวก ข.

มีผู้ตอบแบบสอบถามจำนวน 20 ราย ซึ่งเป็นบุคคลกรของสำนักบริหารเทคโนโลยีสารสนเทศ สำนักงานประกันสังคม โดยผลการตอบแบบสอบถาม ตอนที่ 1 มีดังนี้

1. เพศ แบ่งออกเป็น ชาย จำนวนร้อยละ 30 หญิง จำนวนร้อยละ 70

2. อายุ แบ่งออกเป็น

อายุระหว่าง 25 – 30 ปี	จำนวนร้อยละ 10
อายุระหว่าง 31 – 35 ปี	จำนวนร้อยละ 20
อายุระหว่าง 36 – 40 ปี	จำนวนร้อยละ 30
อายุระหว่าง 41 – 45 ปี	จำนวนร้อยละ 25
อายุมากกว่า 45 ปีขึ้นไป	จำนวนร้อยละ 15

3. ระดับการศึกษา แบ่งออกเป็น

ระดับการศึกษาปริญญาตรี จำนวนร้อยละ 70

ระดับการศึกษาปริญญาโท จำนวนร้อยละ 30

4. มีประสบการณ์ในการเป็นผู้ใช้ระบบบริหารจัดการบนเว็บ

ไม่เคย จำนวนร้อยละ 100

5. มีประสบการณ์ในการเป็นผู้พัฒนาระบบ

ไม่เคย จำนวนร้อยละ 100

6. มีประสบการณ์ในการเป็นผู้ดูแลระบบ

ไม่เคย จำนวนร้อยละ 100

ตอนที่ 2 แบบสอบถามความคิดเห็น แบ่งออกเป็น 4 ด้าน คือ

1. ด้านการตรงตามความต้องการของผู้ใช้ระบบ (Functional Requirement)
2. ด้านการทำงานได้ตามฟังก์ชันงานของระบบ (System Functions)
3. ด้านความง่ายต่อการใช้งานระบบ (Usability)
4. ด้านการรักษาความปลอดภัยของข้อมูลในระบบ (Security Requirements)

มีลักษณะคำตอบเป็นมาตราส่วนประมาณค่า 5 อันดับ ดังต่อไปนี้

5 หมายถึง ความเหมาะสม/ความพึงพอใจในระดับมากที่สุด

4 หมายถึง ความเหมาะสม/ความพึงพอใจในระดับมาก

3 หมายถึง ความเหมาะสม/ความพึงพอใจในระดับปานกลาง

2 หมายถึง ความเหมาะสม/ความพึงพอใจในระดับน้อย

1 หมายถึง ความเหมาะสม/ความพึงพอใจในระดับน้อยที่สุด

เกณฑ์การประเมินจะพิจารณาจากคะแนนเฉลี่ยของความเหมาะสม/ความพึงพอใจ ซึ่งการวิเคราะห์ข้อมูลใช้สถิติเชิงพรรณนา (Descriptive Statistics) ในการวัดค่าของข้อมูลโดยใช้ค่าเฉลี่ยเลขคณิตหรือค่าเฉลี่ย (Mean) และวัดการกระจายของข้อมูลโดยใช้ค่าเบี่ยงเบนมาตรฐาน (Standard Deviation)

ตารางที่ 4.2 แสดงเกณฑ์การกำหนดระดับความเหมาะสม/ความพึงพอใจต่อการใช้งานระบบ

ค่าเฉลี่ยของระดับความเหมาะสม/ความพึงพอใจ	ระดับความเหมาะสม/ความพึงพอใจ
4.50 – 5.00	มากที่สุด
3.50 – 4.49	มาก
2.50 – 3.49	ปานกลาง
1.50 – 2.49	น้อย
1.00 – 1.49	น้อยที่สุด

ตารางที่ 4.3 ผลความเหมาะสม/ความพึงพอใจด้านการตรงตามความต้องการของผู้ใช้ระบบ

รายการประเมิน	$\overline{X}$	ระดับความเหมาะสม /ความพึงพอใจ
ความสามารถของระบบล็อกอินเข้าใช้งาน	5	มากที่สุด
ความสามารถของระบบการใช้งานเอกสารผ่านเว็บ	3.25	ปานกลาง
ความสามารถของระบบการอัพโหลดข้อมูล	3.8	มาก
ความสามารถของระบบการดาวน์โหลดข้อมูล	3.7	มาก
ความสามารถของระบบการลบข้อมูล	3.7	มาก

จากตารางที่ 4.3 เป็นการประเมินผลความถูกต้องและประสิทธิภาพของระบบ สรุปผลการเมินอยู่ในเกณฑ์ระดับความเหมาะสม/ความพึงพอใจของผู้ใช้ในระดับปานกลางถึงมากที่สุด

ตารางที่ 4.4 ผลความเหมาะสม/ความพึงพอใจด้านการทำงานได้ตามฟังก์ชันงานของระบบ

รายการประเมิน	$\overline{X}$	ระดับความเหมาะสม /ความพึงพอใจ
ความถูกต้องตามที่ได้รับอนุญาต	3.9	มาก
ความถูกต้องสิทธิ์ที่ได้รับ	3.4	ปานกลาง
ความถูกต้องในการแสดงผล	3.85	มาก
ความรวดเร็วในการประมวลผลของระบบ	3.9	มาก
การป้องกันการค้นหาข้อมูลผิดพลาดที่อาจเกิดขึ้น	3.8	ปานกลาง

จากตารางที่ 4.4 เป็นการประเมินความถูกต้องและประสิทธิภาพในการทำงานของระบบ ซึ่งผลการเมินอยู่ในเกณฑ์ความเหมาะสม/ความพึงพอใจของผู้ใช้ในระดับปานกลางถึงระดับปานกลางถึงมาก

ตารางที่ 4.5 ผลความเหมาะสม/ความพึงพอใจด้านความง่ายต่อการใช้งาน

รายการประเมิน	$\overline{X}$	ระดับความเหมาะสม /ความพึงพอใจ
ความง่ายต่อการใช้งานของระบบ	4	มาก
ความเหมาะสมของตำแหน่งการจัดวางส่วนต่างๆ บนจอภาพ	4.05	มาก
ความชัดเจนของข้อความที่แสดงบนจอภาพ	3.8	มาก
ความเหมาะสมของการใช้สีโดยภาพรวม	4.15	มาก
ความเหมาะสมของรูปแบบตัวอักษรที่เลือกใช้	3.85	มาก
การใช้ข้อความและคำแนะนำการใช้โปรแกรมเข้าใจง่าย	4	มาก
ความน่าใช้ของระบบในภาพรวม	3.7	มาก

จากตารางที่ 4.5 เป็นการประเมินลักษณะการออกแบบระบบว่ามีความง่ายต่อการใช้งานของระบบ ซึ่งผลการเมินอยู่ในเกณฑ์ความเหมาะสม/ความพึงพอใจของผู้ใช้ในระดับมาก

ตารางที่ 4.6 ผลความเหมาะสม/ความพึงพอใจด้านการรักษาความปลอดภัยของข้อมูลในระบบ

รายการประเมิน	$\overline{X}$	ระดับความเหมาะสม /ความพึงพอใจ
ความเหมาะสมในการกำหนดชื่อผู้ใช้และรหัสผ่าน	3.7	มาก
ความเหมาะสมของระบบรักษาความปลอดภัย	3.75	มาก
การควบคุมให้ใช้งานตามสิทธิ์ผู้ใช้ได้อย่างถูกต้อง	3.8	มาก
ความสามารถของระบบในการตรวจควบคุมการเข้าถึง	3.65	มาก
ความสามารถของระบบสอบสิทธิ์การเข้าถึง	3.45	มาก
ความน่าเชื่อถือได้ของระบบ	3.85	มาก

จากตารางที่ 4.6 เป็นการประเมินว่าระบบที่พัฒนาขึ้นมานั้น มีความปลอดภัยของข้อมูล ซึ่งผลการเมินอยู่ในเกณฑ์ความเหมาะสม/ความพึงพอใจของผู้ใช้ในระดับมาก

ตอนที่ 3 ในแบบสอบถาม เป็นการสอบถามข้อมูลความคิดเห็นของผู้ตอบแบบสอบถามภายหลังจากที่ได้ทดลองใช้โปรแกรมที่พัฒนาขึ้น ผู้ตอบแบบสอบถามได้มีข้อเสนอแนะที่เป็นประโยชน์ ซึ่งผู้พัฒนาระบบสามารถนำไปปรับปรุงระบบต่อไป ดังนี้

1. ปรับปรุงรูปแบบการแสดงผลให้พื้นหลังมีสีอ่อนๆ
2. ปรับปรุงหน้าจอให้มีข้อความบอกชื่อกลุ่มข้อมูลรองทุกหน้า

บทที่ 5
บทสรุปอภิปรายผลการศึกษาและข้อเสนอแนะ

ในบทนี้จะกล่าวถึง ข้อสรุปจากการดาเนินโครงงาน ปัญหาและอุปสรรคระหว่างการพัฒนา รวมทั้งข้อเสนอแนะต่างๆในการศึกษาต่อไป โดยมีรายละเอียดดังต่อไปนี้

5.1 สรุปผลและวิจารณ์

สารนิพนธ์นี้ได้จัดทำระบบงานบริหารจัดการและควบคุมเอกสารผ่านเว็บ (Web-base System for Document Management and Access Control) ใช้กรณีศึกษาระบบสมาคมวางแผนครอบครัวแห่งประเทศไทยในพระบรมราชูปถัมภ์ มีวัตถุประสงค์เพื่ออำนวยความสะดวกในการจัดเก็บข้อมูลในเครื่องคอมพิวเตอร์ส่วนบุคคล (Personal Computer) ให้บุคลากรภายในองค์กรสามารถจัดเก็บและแบ่งปันข้อมูลใช้ร่วมกันได้ ผู้จัดทำออกแบบระบบให้ผู้ใช้สามารถเรียนรู้และใช้งานง่ายที่สุด เนื่องจากเจ้าหน้าที่ภายในองค์กรมีทักษะในการใช้ระบบออนไลน์น้อยและต้องการความสะดวกสบายในการใช้งาน

การจัดทำระบบผู้พัฒนาได้ศึกษาค้นคว้าทฤษฎี แนวคิดและเทคโนโลยีที่เกี่ยวข้องเพื่อสร้างระบบนี้โดยเริ่มจากการรวบรวมข้อมูล ศึกษาขั้นตอนการทำงานของระบบงานเดิม เพื่อดำเนินการวิเคราะห์การทำงานของระบบงานใหม่ ซึ่งขั้นตอนการพัฒนาผู้พัฒนาได้เขียนโปรแกรมด้วยภาษา PHP ใช้โปรแกรมจัดการฐานข้อมูล MySQL และใช้โปรแกรม Apache เป็นโปรแกรมจำลองเครื่องเป็นเว็บเซิร์ฟเวอร์ รวมถึงศึกษากระบวนการควบคุมการเข้าถึงภายในระบบ โดยใช้ทฤษฎี RBAC (Role-base Access Control)

การทำงานของระบบงานบริหารจัดการและควบคุมเอกสารผ่านเว็บ แบ่งการทำงานออกเป็น 2 ส่วน คือ ส่วนของผู้ดูและระบบ และส่วนของผู้ใช้งานทั่วไป

ส่วนของผู้ดูแลระบบ เมื่อผู้ดูแลระบบทำการล็อกอินเข้าสู่ระบบ จะสามารถสร้างและบริหารจัดการบัญชีผู้ใช้ สร้างกลุ่มข้อมูล กำหนดสิทธิ์ควบคุมการเข้าถึงกลุ่มข้อมูลให้กับผู้ใช้แต่ละคนตามที่มีความสัมพันธ์กัน รวมถึงการตรวจสอบสถานะสิทธิ์และควบคุมการเข้าถึงของผู้ใช้ ในการตั้งค่าผู้ดูแลระบบสามารถตั้งค่าผ่านหน้าเว็บ

ส่วนของผู้ใช้งานทั่วไป เมื่อผู้ใช้งานทั่วไปทำการล็อกอินเข้าสู่ระบบ ผู้ใช้งานสามารถใช้งานกลุ่มข้อมูลตามที่ได้รับอนุญาตจากผู้มีอำนาจในการแจกจ่ายสิทธิ์ และความสามารถในการเข้าถึงและบริหารจัดการข้อมูลตามที่ผู้ดูแลระบบกำหนดในระบบ

5.2 ปัญหาและอุปสรรค

5.2.1 การศึกษาข้อมูลและวิธีที่นำมาเป็นส่วนประกอบในการจัดทำระบบ เนื่องจากลักษณะการทำงานของระบบการรักษาความปลอดภัยของข้อมูลมีความกว้างมาก ผู้จัดทำต้องวางโครงสร้างขอบเขตให้แคบลงเพื่อให้ง่ายต่อการจัดทำระบบ

5.2.2 การออกแบบระบบให้สอดคล้องกับการทำงานของเจ้าหน้าที่ภายในองค์กร สำหรับผู้ใช้งานระบบ การทำงานในองค์กรไม่ได้มีโครงสร้างที่ชัดเจน เจ้าหน้าที่สามารถทำงานได้หลายตำแหน่ง ซึ่งในบางครั้งเป็นภาระหน้าที่ที่ไม่มีความเกี่ยวข้องกับตำแหน่งตามโครงสร้าง เช่น เจ้าหน้าที่บัญชี ทำงานบัญชีในขณะเดียวกันได้รับมอบหมายให้จัดทำรายงานของโครงการฯ เป็นต้น นอกจากนี้ยังต้องออกแบบระบบให้เข้าใจและใช้งานง่ายที่สุด เนื่องจากเจ้าหน้าที่ไม่ต้องการเรียนรู้การใช้งานที่ยากเกินไป ผู้จัดทำต้องทำการวิเคราะห์และรวบรวมพฤติกรรมการใช้งานคอมพิวเตอร์และระบบออนไลน์ที่เจ้าหน้าที่ใช้งานเป็นประจำ และออกแบบการใช้งานระบบให้ใกล้เคียงมากที่สุด เพื่อให้เจ้าหน้าที่ไม่ต้องเรียนรู้เพิ่มเติมมากจนเกินไป

สำหรับผู้ดูแลระบบ ผู้จัดทำต้องออกแบบระบบให้ใช้งานง่าย มีปุ่มในการบริหารจัดการชัดเจน เนื่องจากองค์กรไม่ได้มีเจ้าหน้าที่เกี่ยวกับงานด้านสารสนเทศ ผู้ที่มีหน้าที่เป็นผู้ดูแลระบบอาจจะไม่มีความรู้ ความชำนาญเกี่ยวกับการใช้งานออนไลน์และระบบสารสนเทศเท่าที่ควร ดังนั้นจึงต้องมีการออกแบบให้ใช้งานง่ายมากที่สุด

5.2.3 การจัดทำระบบตามที่ได้ออกแบบระบบที่กล่าวในข้อ 5.2.2 ให้เหมาะสมกับเจ้าหน้าที่ภายในองค์กรก็เป็นเรื่องจากเช่นกัน ตั้งแต่การเลือกตัวอักษร ขนาดตัวอักษร สีที่ใช้ในการจัดทำระบบ เพื่อให้เจ้าหน้าที่ที่ใช้งานระบบสามารถเข้าใจและใช้งานได้ง่ายทั้งผู้ดูแลระบบและผู้ใช้งานระบบ

5.3 ข้อเสนอแนะในการศึกษาขั้นต่อไป

ผู้ที่สนใจสามารถนำระบบที่จัดทำในสารนิพนธ์นี้พัฒนาต่อเพื่อให้เหมาะสมกับสภาพแวดล้อมโครงสร้างและการทำงานของหน่วยงาน/องค์กรนั้นๆ การกำหนดสิทธิ์การควบคุมการเข้าถึงอาจต้องมีการเปลี่ยนแปลงไปตามความเหมาะสมและความต้องการในการนำเสนอ การกำหนด Feature ต่างๆ ก็ต้องเปลี่ยนแปลงไปตามการทำงานและโครงสร้างของหน่วยงาน สำหรับ

ด้านการรักษาความปลอดภัย เนื่องจากระบบใช้งานผ่านเว็บไซต์ดังนั้นจึงควรใช้เครื่องหมายรับรองความปลอดภัยทางอิเล็กทรอนิกส์ หรือ SSL Certificates เป็นมาตรฐานความปลอดภัย ที่ออกให้โดย CA (Certificate Authority) SSL ที่ควรนำมาใช้กับระบบคือประเภท Private SSL เป็นประเภทที่นิยมและมีน่าเชื่อถือมากที่สุด รวมไปถึงการเลือกใช้เทคโนโลยีอื่นๆ เข้ามาจัดทำระบบเพื่อให้สามารถใช้งานได้ดีและมีความปลอดภัยมากยิ่งขึ้น

บรรณานุกรม

บรรณานุกรม

ภาษาไทย

วิทยานิพนธ์

จตุชัย แพงจันทร์. (2553). *Master in Security 2nd Edition* (พิมพ์ครั้งที่ 1). นนทบุรี: ไอดีซีฯ.

กิตติ ภักดีวัฒนะกุล. (2554). *PHP ทีละก้าว*. กรุงเทพฯ: เคทีพี คอมพ์ แอนด์ คอนซัลท์.

บัญชา ปะสีละเตสัง. (2553). *พัฒนาเว็บแอปพลิเคชั่นด้วย PHP ร่วมกับ MySQL และ Dreamweaver.* กรุงเทพฯ : ซีเอ็ดยูเคชั่น.

กาญจนา ตันวิสุทธิ์ (2551). Ajax + PHP. กรุงเทพฯ: วิตตี กรุ๊ป.

Access Control Chapter 1 by Aj. Kusuma Suthakum. สืบค้นเมื่อกรกฎาคม 2555, จาก http://www. nanacm.com/bcom4102o/chapter1.pdf

Policy-based Admission Control. สืบค้นเมื่อกรกฎาคม 2555, จาก http://www.gotoknow.org/posts/238191

Access Control and Site Security (2007). สืบค้นเมื่อกรกฎาคม 2555, จาก *http://www.thai-etc.com/dru_4124905/dru_4124905_schedule.html*

ความมั่นคงปลอดภัยของระบบเครือข่ายและคอมพิวเตอร์ ระดับที่ 3. มหาวิทยาลัยสุโขทัย. สืบค้นเมื่อกรกฎาคม 2555, จาก http://www.stou.ac.th/schools/sst/main/it

วิศวกรรมด้านการรักษาความปลอดภัย Security Engineering. สืบค้นเมื่อกรกฎาคม 2555, จาก http://www. smiledogs.net/SE-C13-f.ppt

ภาษาต่างประเทศ

ARTICLES

Ravi S. Sandhu and Pierangela Samarati . “Access Control : Principles and Practice” , IEEE Communications Magazine (1994)

M.A. Hadavi, V.S. Hamishagi and H.M. Sangchi “Security Requirement Engineering; State of the Art and Research Challenges”. Proceedings of the International MultiConference of Engineers and Computer Scientists (2008).

Benjamin Fabian And faculty. “A comparison of security requirements engineering methods” Requirement Eng (2010)

David Feraiolo And faculty , CISM , CISA. “Role – base Access Control (RBAC)”. Information Systems Audit and Control . All rights reserved. www.isaca.org

Donald G. Firesmith , “Analyzing and Specifying Reusable Security Requirements” , Sotfware Engineering Insitute Carnegie Mellon University Pittsburgh , dgf@sei.cmu.edu.

Axel van Lamsweerds And faculty . “From System Goals to Intruder Anti – Goals :Attack Generation and Resolution for Security Requirements Engineering”, Departement d’ Ingenierie Informatigque Universite catholique de Louvain {avl, sbr, rdl, dja}@info.ucl.ac.be.

Paolo Giorgini And faculty. “Modeling Security Requirement Thorough Ownership , Permission and Delegation”. University of Trento.

Fabio Massacci , Marco Prest and Nicola Zannone. “Using a Security Requirements Engineering Methodology In Practice : The Compliance with the Italian data protection Legislation”. November2004

ภาคผนวก

ภาคผนวก ก

การออกแบบตารางฐานข้อมูล

ตาราง 1 แสดงรายชื่อของตารางและความหมายของตาราง

ลำดับ	ชื่อตาราง	ความหมาย
1	RECORDS_USER	ตารางจัดการรายการเจ้าหน้าที่ภายในองค์กร
2	MAIN_DIRECTORY	ตารางจัดการกลุ่มข้อมูลหลัก
3	SUB_DIRECTORY	ตารางจัดการกลุ่มข้อมูลรอง
4	ROLE	ตารางจัดเก็บ Role ภายในองค์กร
5	ROLE_USER	ตารางจัดการ Role ของ user
6	PERMISSION	ตารางจัดการการอนุญาต
7	FILE	ตารางจัดเก็บรายชื่อข้อมูล

ตาราง 2 แสดงรายละเอียดฟิลด์ข้อมูลของตารางจัดการรายการเจ้าหน้าที่ภายในองค์กร

recorders_user

Fields Name	Type	Size	Description	Key
User_id	int	10	รหัสผู้ใช้	PK
User	varchar	20	ชื่อผู้ใช้ระบบ	
Pass	varchar	20	รหัสผ่าน	
Name	varchar	50	ชื่อเจ้าหน้าที่	
Surname	varchar	50	นามสกุลเจ้าหน้าที่	
Position	varchar	50	ตำแหน่งเจ้าหน้าที่	
Gr	varchar	50	จัดกลุ่มข้อมูลกับผู้ใช้	
Tel	varchar	14	เบอร์โทรศัพท์	
Mail	varchar	20	อีเมลล์เจ้าหน้าที่	

ตาราง 3 แสดงรายละเอียดฟิลด์ข้อมูลของตารางจัดการกลุ่มข้อมูลหลัก

main_directory

Fields Name	Type	Size	Description	Key
Direct_id	int	11	รหัสกลุ่มข้อมูลหลัก	PK
main	varchar	100	ชื่อกลุ่มข้อมูลหลัก	

ตาราง 4 แสดงรายละเอียดฟิลด์ข้อมูลของตารางจัดการกลุ่มข้อมูลรอง

sub_directory

Fields Name	Type	Size	Description	Key
Sub_id	int	11	รหัสกลุ่มข้อมูลรอง	PK
Sub	varchar	150	ชื่อกลุ่มข้อมูลรอง	
Direct_id	int	11	รหัสกลุ่มข้อมูลหลัก	FK

ตาราง 5 แสดงรายละเอียดฟิลด์ข้อมูลของตารางจัดเก็บ Role ภายในองค์กร

role

Fields Name	Type	Size	Description	Key
Role_id	int	3	รหัส Role	PK
Role_name	varchar	10	ชื่อ Role	
Role_des	varchar	11	รายละเอียด Role	

ตาราง 6 แสดงรายละเอียดฟิลด์ข้อมูลของตารางจัดการ Role ของ user

role_user

Fields Name	Type	Size	Description	Key
ru_id	int	3	รหัส role_user	PK
Role_id	int	3	รหัส Role	
User_id	int	3	รหัสผู้ใช้	

ตาราง 7 แสดงรายละเอียดฟิลด์ข้อมูลของตารางจัดการการอนุญาต

permission

Fields Name	Type	Size	Description	Key
Id	int	10	รหัสการอนุญาต	PK
Sub_id	int	3	รหัสกลุ่มข้อมูลรอง	FK
User_id	int	3	รหัสผู้ใช้	FK
rw	varchar	2	การอนุญาต	
Level_per	Varchar	1	ระดับ role	

ตาราง 8 แสดงรายละเอียดฟิลด์ข้อมูลของตารางจัดเก็บรายชื่อข้อมูล

file

Fields Name	Type	Size	Description	Key
File_id	int	11	รหัสข้อมูล	PK
Filesname	varchar	60	ชื่อข้อมูล	
Size	varchar	50	ขนาดข้อมูล	
Direct_id	int	11	รหัสกลุ่มข้อมูลหลัก	FK
Sub_id	int	11	รหัสกลุ่มข้อมูลรอง	FK
user	varchar	100	ชื่อผู้ใช้	

ภาคผนวก ข

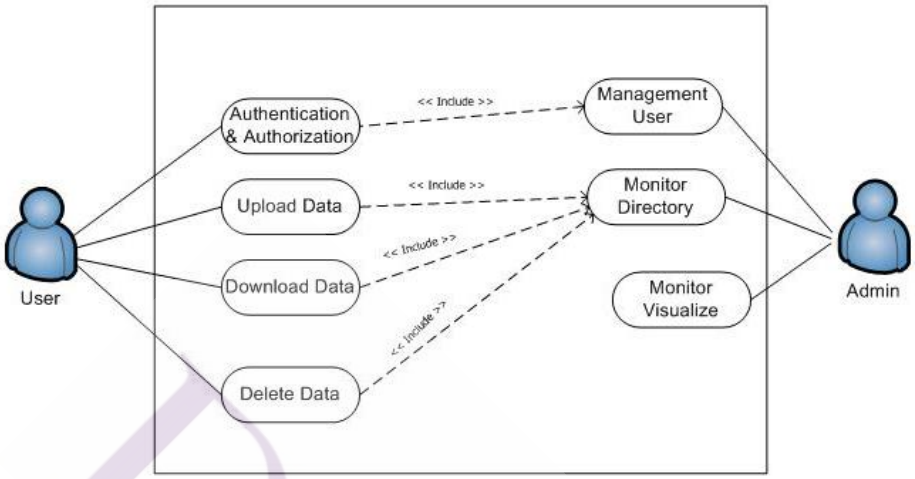
Use Case Scenario

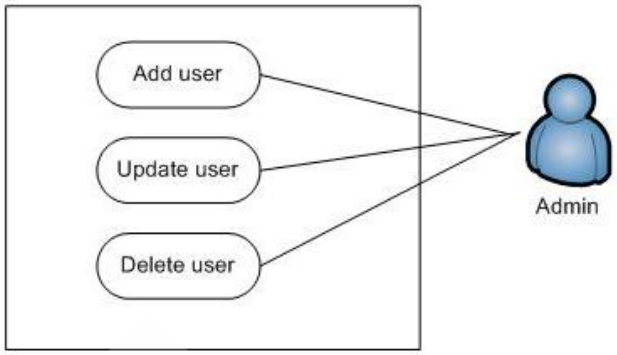
รายละเอียดฟังก์ชั่นการทำงานของระบบ (Use Case Descriptions)

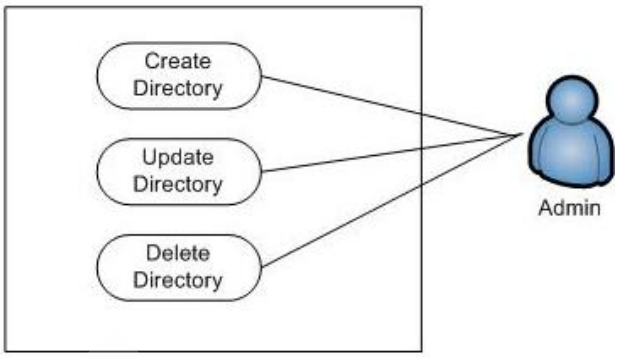
ตารางที่ 8 คำอธิบายรายละเอียดฟังก์ชั่นการทำงานของระบบ (Use Case Descriptions)

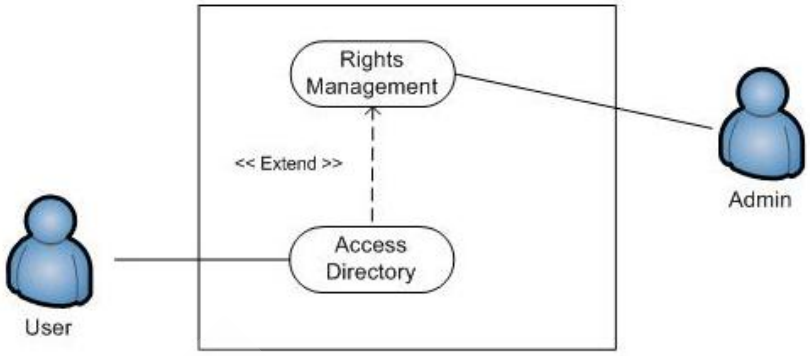
รหัส	Function	คำอธิบาย
UC001	Main System	ระบบการจัดการหลัก
UC002	Member Management	ระบบการบริการจัดการบัญชีผู้ใช้
UC003	Directory Management	ระบบการบริหารจัดการกลุ่มข้อมูล
UC004	Manage Rights	ระบบการบริหารจัดการการกำหนดสิทธิ์
UC005	Assign Permission	ระบบการอนุญาต
UC006	Authentication	ระบบตรวจสอบตัวตนผู้ที่เข้าใช้งานระบบ
UC007	Access Control	ระบบควบคุมสิทธิ์การเข้าถึงข้อมูล
UC008	View Information	ระบบแสดงหน้าจอสิทธิ์ในการเข้าถึงข้อมูล
UC009	R/W (read and write)	ระบบอนุญาตให้ผู้ใช้สามารถบริหารจัดการข้อมูลได้
UC010	R (read only)	ระบบอนุญาตให้ผู้ใช้สามารถเข้าถึงข้อมูลได้เท่านั้น
UC011	Change Password	ระบบอนุญาตให้ผู้ใช้สามารถเปลี่ยนรหัสส่วนตัวได้
UC012	Request view visualize	แจ้งขอดูแผนภาพสิทธิ์
UC013	Update vusialize	ผู้ดูแลระบบแก้ไขสิทธิ์ตามที่ได้รับมอบหมาย

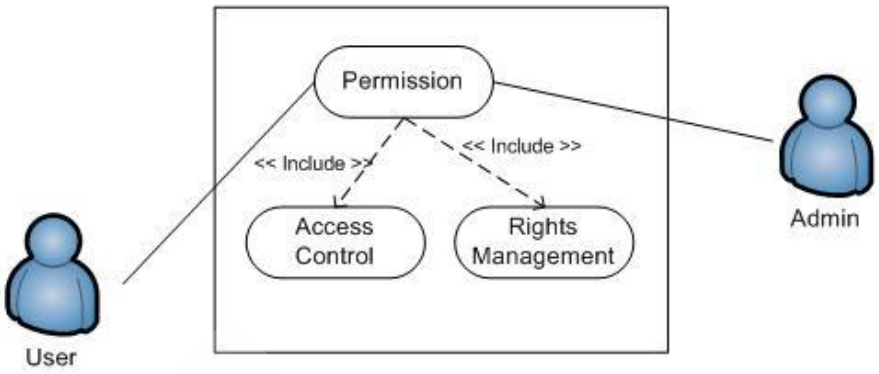
Use Case Diagram

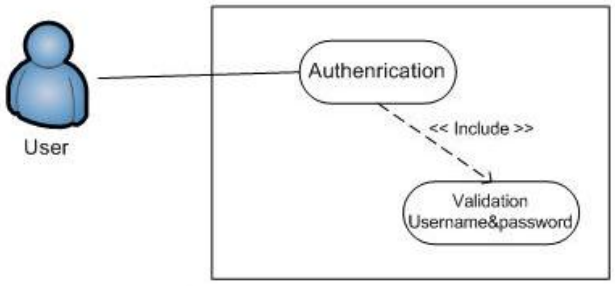
Use Case ID:	**UC001**
	
System :	ระบบงานบริหารจัดการและควบคุมเอกสารผ่านเว็บ
Use Case Name:	Main System
Actors:	Admin , User
Purpose:	เพื่อบริหารจัดการระบบจากผู้ที่มีส่วนเกี่ยวข้องกับระบบ
Overview:	เป็นการบริหารจัดการระบบในภาพรวม
Pre Conditions:	ให้สิทธิ์และตั้งค่าระบบ
Post Conditions:	แสดงการทำงานหลักของการตั้งค่าในระบบ
Flow of Events	
Actor Action	System Response
1. ผู้ดูแลระบบจัดการระบบตาม request จากผู้มีอำนาจ	
	2.ระบบแสดงหน้าจอในการบริหารรจัดการผู้ใช้และการกำหนดสิทธิ์
3. ผู้ใช้สามารถใช้งานตามที่ได้รับอนุญาต	
	4. แสดงกลุ่มข้อมูลที่สามารถเข้าถึงได้
	5. กลับสู่หน้าหลัก
Alternative Flows:	ผู้ใช้งานสามารถเข้าถึงหน้าจอที่ได้รับอนุญาตเท่านั้น

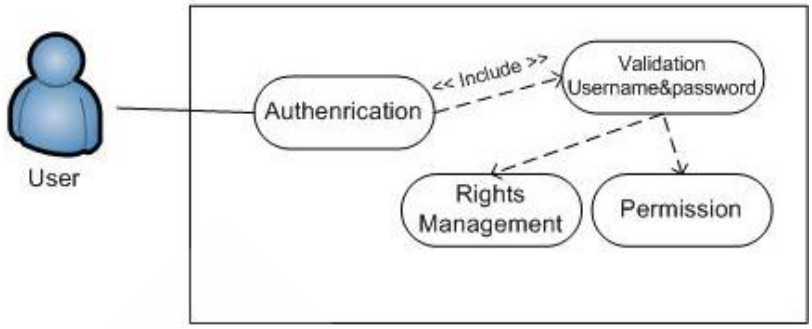
<table>
<tr><td>Use Case ID:</td><td>UC002</td></tr>
<tr><td colspan="2"> 
</td></tr>
<tr><td>System :</td><td>ระบบงานบริหารจัดการและควบคุมเอกสารผ่านเว็บ</td></tr>
<tr><td>Use Case Name:</td><td>Member Management</td></tr>
<tr><td>Actors:</td><td>Admin</td></tr>
<tr><td>Purpose:</td><td>เพื่อสร้างบัญชีผู้ใช้ในระบบ</td></tr>
<tr><td>Overview:</td><td>เป็นการสร้างบัญชีผู้ใช้</td></tr>
<tr><td>Pre Conditions:</td><td>บันทึกบัญชีผู้ใช้ หรือมีการเปลี่ยนแปลง</td></tr>
<tr><td>Post Conditions:</td><td>ระบบมีการจัดเก็บบัญชีผู้ใช้ในฐานข้อมูล</td></tr>
<tr><td colspan="2">Flow of Events</td></tr>
<tr><td>Actor Action</td><td>System Response</td></tr>
<tr><td>1. ผู้ดูแลระบบเข้าสู่ระบบและทำการบันทึกสถานะของผู้ใช้</td><td></td></tr>
<tr><td></td><td>2. ระบบทำการบันทึกข้อมูลตามที่ผู้ดูแลระบบกำหนด</td></tr>
<tr><td>3. ผู้ดูแลระบบสามารถดูรายการที่บันทึก</td><td></td></tr>
<tr><td></td><td>4. กลับสู่หน้าหลัก</td></tr>
<tr><td>Alternative Flows:</td><td>ผู้ดูแลระบบสามารถตั้งค่าได้ตามที่ได้รับมอบหมายเท่านั้น</td></tr>
</table>

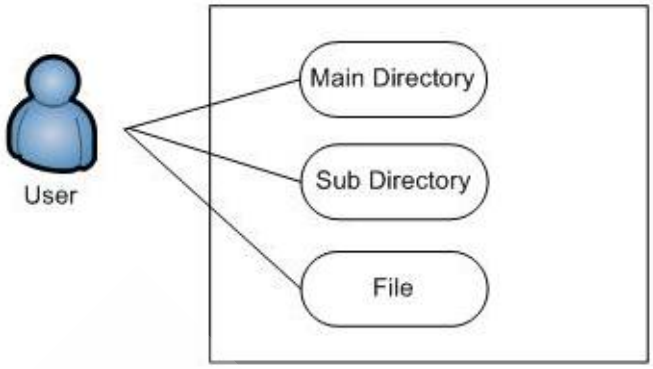
Use Case ID:	**UC003**
	
System :	ระบบงานบริหารจัดการและควบคุมเอกสารผ่านเว็บ
Use Case Name:	Directory Management
Actors:	Admin
Purpose:	เพื่อบริหารจัดการกลุ่มข้อมูลในระบบ
Overview:	เป็นการบริหารจัดการกลุ่มข้อมูลเพื่อให้สอดคล้องกับการทำงานภายในองค์กร
Pre Conditions:	สร้างกลุ่มข้อมูล หรือมีการเปลี่ยนแปลง
Post Conditions:	ระบบมีการจัดเก็บรายชื่อกลุ่มข้อมูลในฐานข้อมูล
Flow of Events	
Actor Action	System Response
1. ผู้ดูแลระบบเข้าสู่ระบบและทำการจัดการกลุ่มข้อมูล	
	2. ระบบทำการบันทึกข้อมูลตามที่ผู้ดูแลระบบกำหนด
3. ผู้ดูแลระบบสามารถดูรายการที่บันทึก	
	4. กลับสู่หน้าหลัก
Alternative Flows:	ผู้ดูแลระบบสามารถตั้งค่าได้ตามที่ได้รับมอบหมายเท่านั้น

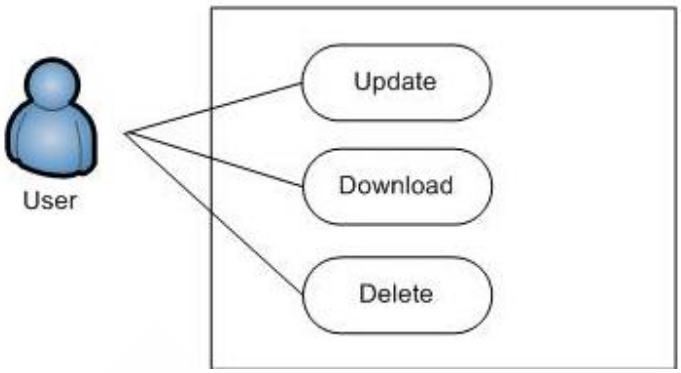
<table>
<tr><td>Use Case ID:</td><td colspan="2">UC004</td></tr>
<tr><td colspan="3"> 
</td></tr>
<tr><td>System :</td><td colspan="2">ระบบงานบริหารจัดการและควบคุมเอกสารผ่านเว็บ</td></tr>
<tr><td>Use Case Name:</td><td colspan="2">Manage Rights</td></tr>
<tr><td>Actors:</td><td colspan="2">Admin , User</td></tr>
<tr><td>Purpose:</td><td colspan="2">เพื่อให้สิทธิ์การใช้งานระบบ</td></tr>
<tr><td>Overview:</td><td colspan="2">เป็นการให้สิทธิ์ให้กับผู้ใช้ภายในองค์กร</td></tr>
<tr><td>Pre Conditions:</td><td colspan="2">ระบุการอนุญาตจากผู้บริหาร</td></tr>
<tr><td>Post Conditions:</td><td colspan="2">ระบบมีการจัดเก็บสิทธิ์ของผู้ใช้แต่ละคนในฐานข้อมูล</td></tr>
<tr><td colspan="3">Flow of Events</td></tr>
<tr><td colspan="2">Actor Action</td><td>System Response</td></tr>
<tr><td colspan="2">1. ผู้ดูแลระบบเข้าสู่ระบบและทำการจัดการสิทธิ์ของผู้ใช้แต่ละคนตามที่ได้รับมอบหมาย</td><td></td></tr>
<tr><td colspan="2"></td><td>2. ระบบทำการบันทึกข้อมูลตามที่ผู้ดูแลระบบกำหนด</td></tr>
<tr><td colspan="2">3. ผู้ดูแลระบบสามารถดูรายการที่บันทึก</td><td></td></tr>
<tr><td colspan="2"></td><td>4. กลับสู่หน้าหลัก</td></tr>
<tr><td>Alternative Flows:</td><td colspan="2">ผู้ดูแลระบบสามารถตั้งค่าได้ตามที่ได้รับมอบหมายเท่านั้น
ผู้ใช้งานสามารถเข้าถึงหน้าจอที่ได้รับอนุญาตเท่านั้น</td></tr>
</table>

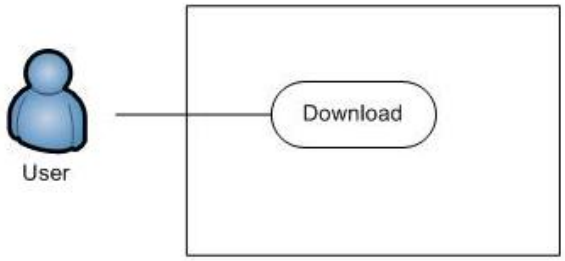
<table>
<tr><td>Use Case ID:</td><td colspan="2">UC005</td></tr>
<tr><td colspan="3"> 
</td></tr>
<tr><td>System :</td><td colspan="2">ระบบงานบริหารจัดการและควบคุมเอกสารผ่านเว็บ</td></tr>
<tr><td>Use Case Name:</td><td colspan="2">Assign Permission</td></tr>
<tr><td>Actors:</td><td colspan="2">Admin , User</td></tr>
<tr><td>Purpose:</td><td colspan="2">เพื่อแสดงการอนุญาตใช้งานระบบ</td></tr>
<tr><td>Overview:</td><td colspan="2">เป็นการแสดงการอนุญาตกำหนดสิทธิ์ของผู้ใช้ภายในองค์กร</td></tr>
<tr><td>Pre Conditions:</td><td colspan="2">ระบุการอนุญาตจากผู้ที่มีอำนาจในการตัดสินใจในการกำหนดสิทธิ์</td></tr>
<tr><td>Post Conditions:</td><td colspan="2">ระบบมีการจัดเก็บสิทธิ์ของผู้ใช้แต่ละคนในฐานข้อมูล</td></tr>
<tr><td colspan="3">Flow of Events</td></tr>
<tr><td colspan="2">Actor Action</td><td>System Response</td></tr>
<tr><td colspan="2">1. ผู้ดูแลระบบเข้าสู่ระบบและทำการจัดการสิทธิ์ของผู้ใช้แต่ละคนตามที่ได้รับมอบหมาย</td><td></td></tr>
<tr><td colspan="2"></td><td>2. ระบบทำการบันทึกข้อมูลตามที่ผู้ดูแลระบบกำหนด</td></tr>
<tr><td colspan="2">3. ผู้ดูแลระบบสามารถดูรายการที่บันทึก</td><td></td></tr>
<tr><td colspan="2"></td><td>4. กลับสู่หน้าหลัก</td></tr>
<tr><td>Alternative Flows:</td><td colspan="2">ผู้ดูแลระบบสามารถตั้งค่าได้ตามที่ได้รับมอบหมายเท่านั้น
ผู้ใช้งานสามารถเข้าถึงหน้าจอที่ได้รับอนุญาตเท่านั้น</td></tr>
</table>

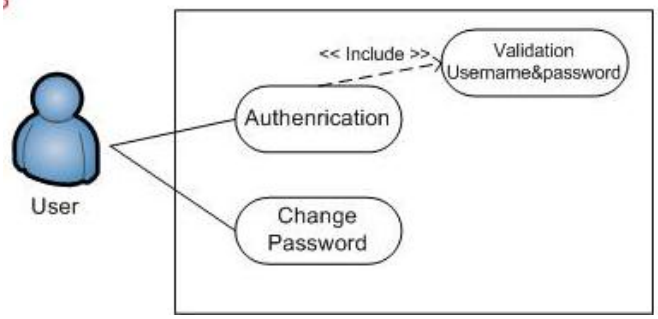
<table>
<tr><td>Use Case ID:</td><td colspan="2">UC006</td></tr>
<tr><td colspan="3"> 
</td></tr>
<tr><td>System :</td><td colspan="2">ระบบงานบริหารจัดการและควบคุมเอกสารผ่านเว็บ</td></tr>
<tr><td>Use Case Name:</td><td colspan="2">Authentication</td></tr>
<tr><td>Actors:</td><td colspan="2">User</td></tr>
<tr><td>Purpose:</td><td colspan="2">เพื่อแสดงระบุตัวตนของผู้ใช้</td></tr>
<tr><td>Overview:</td><td colspan="2">เป็นการแสดงระบุตัวตนของผู้ใช้ภายในองค์กร</td></tr>
<tr><td>Pre Conditions:</td><td colspan="2">ระบุตัวตนของผู้ใช้โดยใช้ Username และ Password</td></tr>
<tr><td>Post Conditions:</td><td colspan="2">ระบบมีการตรวจสอบผลการระบุตัวตนในฐานข้อมูล</td></tr>
<tr><td colspan="3">Flow of Events</td></tr>
<tr><td colspan="2">Actor Action</td><td>System Response</td></tr>
<tr><td colspan="2">1. ผู้ใช้ระบุตัวตนโดยใส่รหัส Username และ Password</td><td></td></tr>
<tr><td colspan="2"></td><td>2. ระบบตรวจสอบ Username และ Password</td></tr>
<tr><td colspan="2">3. ผู้ใช้สามารถเข้าใช้งานได้ถ้าผ่านการตรวจสอบในฐานข้อมูล</td><td></td></tr>
<tr><td colspan="2">4. ผู้ใช้สามารถใช้งานกลุ่มข้อมูลตามที่ได้รับอนุญาต</td><td></td></tr>
<tr><td colspan="2"></td><td>5. กลับสู่หน้าหลัก</td></tr>
<tr><td>Alternative Flows:</td><td colspan="2">ผู้ดูแลระบบสามารถตั้งค่าได้ตามที่ได้รับมอบหมายเท่านั้น
ผู้ใช้งานสามารถเข้าถึงหน้าจอที่ได้รับอนุญาตเท่านั้น</td></tr>
</table>

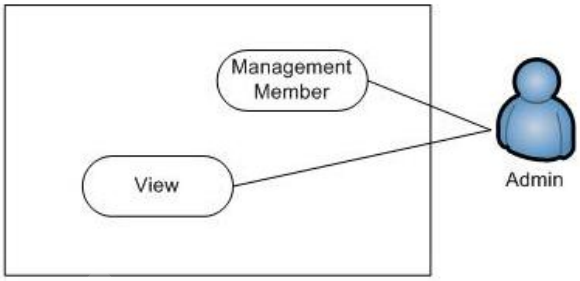
Use Case ID:	UC007
	
System :	ระบบงานบริหารจัดการและควบคุมเอกสารผ่านเว็บ
Use Case Name:	Access Control
Actors:	User
Purpose:	เพื่อควบคุมการเข้าถึงข้อมูลของผู้ใช้กับกลุ่มข้อมูล
Overview:	เป็นการป้องกันเอกสารจากผู้ใช้ที่ไม่ได้รับอนุญาต
Pre Conditions:	ควบคุมการเข้าถึงกลุ่มข้อมูลของผู้ใช้โดยใช้ Identities ที่ผ่านการพิสูจน์ตัวตน
Post Conditions:	ระบบมีการตรวจสอบการได้รับอนุญาตในฐานข้อมูล
Flow of Events	
Actor Action	System Response
1. ผู้ใช้ระบุตัวตนโดยใส่รหัส Username และ Password	
	2. ระบบตรวจสอบ Authentication ของผู้ใช้
	3. ระบบตรวจสอบสิทธิ์และควบคุมการเข้าถึงกลุ่มข้อมูล
4. ผู้ใช้สามารถใช้งานกลุ่มข้อมูลตามที่ได้รับอนุญาต	
	5. กลับสู่หน้าหลัก
Alternative Flows:	ผู้ดูแลระบบสามารถตั้งค่าได้ตามที่ได้รับมอบหมายเท่านั้น ผู้ใช้งานสามารถเข้าถึงหน้าจอที่ได้รับอนุญาตเท่านั้น

<table>
<tr><td>Use Case ID:</td><td>UC008</td></tr>
<tr><td colspan="2"> 
</td></tr>
<tr><td>System :</td><td>ระบบงานบริหารจัดการและควบคุมเอกสารผ่านเว็บ</td></tr>
<tr><td>Use Case Name:</td><td>View Information</td></tr>
<tr><td>Actors:</td><td>User</td></tr>
<tr><td>Purpose:</td><td>เพื่อแสดงกลุ่มข้อมูลที่สามารถเข้าถึงได้</td></tr>
<tr><td>Overview:</td><td>เป็นการเข้าถึงกลุ่มข้อมูลและบริหารจัดการได้ตามที่ได้รับอนุญาต</td></tr>
<tr><td>Pre Conditions:</td><td>ควบคุมการเข้าถึงกลุ่มข้อมูลและแสดงข้อมูลที่ผ่านการควบคุมการเข้าถึง</td></tr>
<tr><td>Post Conditions:</td><td>ระบบมีการตรวจสอบการได้รับอนุญาตในฐานข้อมูล</td></tr>
<tr><td colspan="2">Flow of Events</td></tr>
<tr><td colspan="2"><table>
<tr><td>Actor Action</td><td>System Response</td></tr>
<tr><td>1. ผู้ใช้พิสูจน์ตัวตนโดยใส่รหัส Username และ Password</td><td></td></tr>
<tr><td></td><td>2. ระบบตรวจสอบ Authentication ของผู้ใช้</td></tr>
<tr><td></td><td>3. ระบบตรวจสอบสิทธิ์และควบคุมการเข้าถึงกลุ่มข้อมูล</td></tr>
<tr><td>4. ผู้ใช้สามารถใช้งานกลุ่มข้อมูลตามที่ได้รับอนุญาต</td><td></td></tr>
<tr><td></td><td>6. กลับสู่หน้าหลัก</td></tr>
</table></td></tr>
<tr><td>Alternative Flows:</td><td>ผู้ดูแลระบบสามารถตั้งค่าได้ตามที่ได้รับมอบหมายเท่านั้น
ผู้ใช้งานสามารถเข้าถึงหน้าจอที่ได้รับอนุญาตเท่านั้น</td></tr>
</table>

Use Case ID:	**UC009**
	
System :	ระบบงานบริหารจัดการและควบคุมเอกสารผ่านเว็บ
Use Case Name:	R/W (read and write)
Actors:	User
Purpose:	เพื่อแสดงกลุ่มข้อมูลที่สามารถบริหารจัดการข้อมูลได้
Overview:	เป็นการเข้าถึงกลุ่มข้อมูลและบริหารจัดการได้ตามที่ได้รับอนุญาต
Pre Conditions:	การอนุญาตให้สามารถเข้าถึงกลุ่มข้อมูลและบริหารจัดการกลุ่มข้อมูลได้
Post Conditions:	ระบบมีการตรวจสอบการได้รับอนุญาตในฐานข้อมูล
Flow of Events	
Actor Action	System Response
1. ผู้ใช้ระบุตัวตนโดยใส่รหัส Username และ Password	
	2. ระบบตรวจสอบ Authentication ของผู้ใช้
	3. ระบบตรวจสอบสิทธิ์และอนุญาตให้สามารถเข้าถึงกลุ่มข้อมูล
4. ผู้ใช้สามารถบริหารจัดการกลุ่มข้อมูลตามที่ได้รับอนุญาตได้แก่ Upload , Download , Delete	
	5. กลับสู่หน้าหลัก
Alternative Flows:	ผู้ดูแลระบบสามารถตั้งค่าได้ตามที่ได้รับมอบหมายเท่านั้น ผู้ใช้งานสามารถเข้าถึงหน้าจอที่ได้รับอนุญาตเท่านั้น

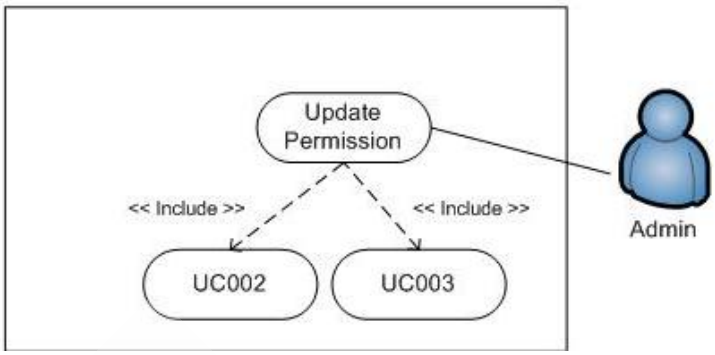
Use Case ID:	**UC010**
	
System :	ระบบงานบริหารจัดการและควบคุมเอกสารผ่านเว็บ
Use Case Name:	R (read only)
Actors:	User
Purpose:	เพื่อแสดงกลุ่มข้อมูลที่สามารถเข้าถึงได้เท่านั้น
Overview:	เป็นการเข้าถึงกลุ่มข้อมูลได้ตามที่ได้รับอนุญาต
Pre Conditions:	การอนุญาตให้สามารถเข้าถึงกลุ่มข้อมูลได้
Post Conditions:	ระบบมีการตรวจสอบการได้รับอนุญาตในฐานข้อมูล
Flow of Events	
Actor Action	System Response
1. ผู้ใช้ระบุตัวตนโดยใส่รหัส Username และ Password	
	2. ระบบตรวจสอบ Authentication ของผู้ใช้
	3. ระบบตรวจสอบสิทธิ์และอนุญาตให้สามารถเข้าถึงกลุ่มข้อมูล
4. ผู้ใช้สามารถบริหารจัดการกลุ่มข้อมูลตามที่ได้รับอนุญาตได้แก่ Download	
	5. กลับสู่หน้าหลัก
Alternative Flows:	ผู้ดูแลระบบสามารถตั้งค่าได้ตามที่ได้รับมอบหมายเท่านั้น ผู้ใช้งานสามารถเข้าถึงหน้าจอที่ได้รับอนุญาตเท่านั้น

<table>
<tr><td>Use Case ID:</td><td>UC011</td></tr>
<tr><td colspan="2"> 
</td></tr>
<tr><td>System :</td><td>การพัฒนาระบบงานเพื่อบริหารจัดการและควบคุมเอกสารบนเว็บ</td></tr>
<tr><td>Use Case Name:</td><td>Change Password</td></tr>
<tr><td>Actors:</td><td>User</td></tr>
<tr><td>Purpose:</td><td>เพื่อใช้ในการเปลี่ยนรหัสผ่านเพื่อป้องกันการแอบอ้างใช้สิทธิ์</td></tr>
<tr><td>Overview:</td><td>เป็นการเปลี่ยนรหัสผ่านตามที่ผู้ใช้ต้องการ</td></tr>
<tr><td>Pre Conditions:</td><td>การเปลี่ยนรหัสผ่านในระบบโดยมีเงื่อนไขต้องมี 6 ตัวอักษรขึ้นไป</td></tr>
<tr><td>Post Conditions:</td><td>ระบบมีการตรวจสอบการได้รับอนุญาตในฐานข้อมูล</td></tr>
<tr><td colspan="2">Flow of Events</td></tr>
<tr><td>Actor Action</td><td>System Response</td></tr>
<tr><td>1. ผู้ใช้ระบุตัวตนโดยใส่รหัส Username และ Password</td><td></td></tr>
<tr><td></td><td>2. ระบบตรวจสอบ Authentication ของผู้ใช้</td></tr>
<tr><td></td><td>3. ระบบตรวจสอบสิทธิ์และอนุญาตให้เข้าใช้งานระบบได้</td></tr>
<tr><td>4. ผู้ใช้สามารถแก้ไขรหัสผ่านส่วนตัวได้โดยต้องเกิน 6 ตัวอักษรขึ้นไป</td><td></td></tr>
<tr><td>5. ผู้ดูแลระบบสามารถบริหารจัดการได้เมื่อผู้ใช้จำรหัสผ่านไม่ได้</td><td></td></tr>
<tr><td></td><td>6. กลับสู่หน้าหลัก</td></tr>
<tr><td>Alternative Flows:</td><td>ผู้ดูแลระบบสามารถตั้งค่าได้ตามที่ได้รับมอบหมายเท่านั้น
ผู้ใช้งานสามารถเข้าถึงหน้าจอที่ได้รับอนุญาตเท่านั้น</td></tr>
</table>

Use Case ID:	**UC012**
	
System :	ระบบงานบริหารจัดการและควบคุมเอกสารผ่านเว็บ
Use Case Name:	view visualize
Actors:	Admin
Purpose:	เพื่อใช้ในการเรียกดูมุมมองสิทธิ์ของผู้ใช้ และการเข้าถึงกลุ่มข้อมูล
Overview:	เป็นการนำเสนอสิทธิ์ของผู้ใช้ และการเข้าถึงกลุ่มข้อมูล ในภาพรวมเพื่อใช้ในการวิเคราะห์ ความเหมาะสมต่อไป
Pre Conditions:	เรียกดูมุมมอง Object , Subject
Post Conditions:	ระบบมีแสดงผลการนำเสนอเพื่อใช้ในการวิเคราะห์และเปลี่ยนแปลง Permission

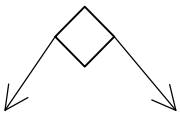
Flow of Events	
Actor Action	System Response
1. ผู้ดูแลระบบเรียกข้อมูลตามที่ผู้บริหารร้องขอ	
	2. ระบบแสดงผลตามที่ผู้ดูแลระบบเรียกดู
3. ผู้ดูแลระบบนำเสนอแผนภาพตามที่ผู้บริหารร้องขอ	
	4. กลับสู่หน้าหลัก

Alternative Flows:	ผู้ดูแลระบบสามารถเรียกดูข้อมูลได้ทั้ง มุมมองสิทธิ์ของผู้ใช้ และมุมมองการเข้าถึงกลุ่มข้อมูล

Use Case ID:	**UC013**
	
System :	ระบบงานบริหารจัดการและควบคุมเอกสารผ่านเว็บ
Use Case Name:	Update Visualize
Actors:	Admin
Purpose:	เพื่อใช้ในการแก้ไขสิทธิ์การเข้าถึงข้อมูล (ต่อจาก UC012)
Overview:	เป็นการแก้ไข เปลี่ยนแปลง เพิกถอนสิทธิ์การเข้าถึงข้อมูลให้กับผู้ใช้ตามความเหมาะสมเพื่อความปลอดภัยของข้อมูล
Pre Conditions:	ผู้ดูแลระบบแก้ไข เปลี่ยนแปลง เพิกถอน ตามที่ได้รับแจ้งจากผู้บริหาร
Post Conditions:	ระบบเปลี่ยนแปลงข้อมูลตามที่ผู้ดูแลระบบแก้ไขการตั้งค่า
Flow of Events	
Actor Action	System Response
1. ผู้ดูแลระบบเปลี่ยนแปลงการตั้งค่าในระบบ	
	2. ระบบบันทึกข้อมูลที่ผู้ดูแลระบบตั้งค่า
3. ผู้ดูแลระบบสามารถตรวจสอบการตั้งค่าโดยดูภาพรวมใน UC0014	
	4. กลับสู่หน้าหลัก
Alternative Flows:	ผู้ดูแลระบบสามารถตั้งค่าสิทธิ์และผู้ใช้ตามที่ได้รับแจ้งจากผู้บริหารเท่านั้น

ภาคผนวก ค
ผังแสดงกิจกรรมที่เกิดขึ้นของกิจกรรม

ตารางที่ 9 ส่วนประกอบของแอคทิวิตี้ไดอะแกรม

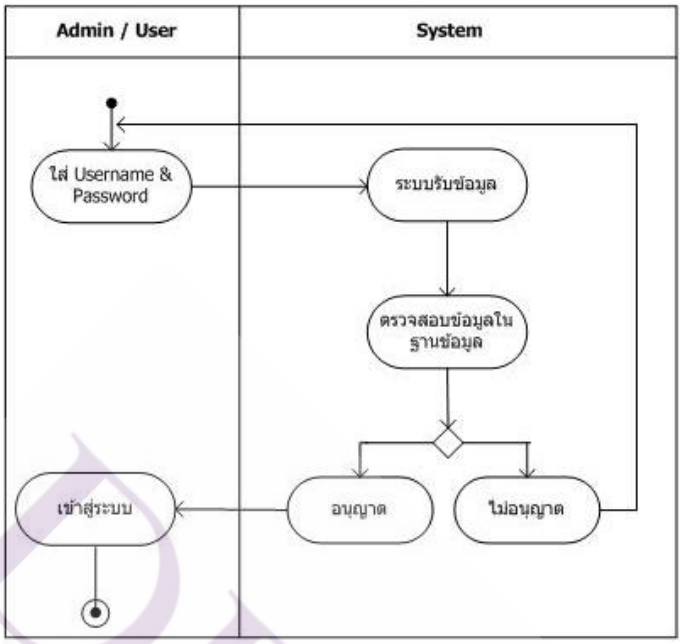
ชื่อสัญลักษณ์	ความหมาย	สัญลักษณ์
Initial Activity	แสดงจุดเริ่มต้นของการทำกิจกรรม	
Activity	กำหนดกิจกรรมที่กระทำโดยผู้ที่มีส่วนเกี่ยวข้องกับระบบหรือกิจกรรมที่ระบบกระทำ	
Decision	เงื่อนไขที่ใช้ในการตัดสินใจหรือเป็นทางเลือกในการทำกิจกรรม	
Final Activity	แสดงจุดสิ้นสุดของการทำกิจกรรม	

รายละเอียดการทำงานของระบบ (Activity Diagram Descriptions)

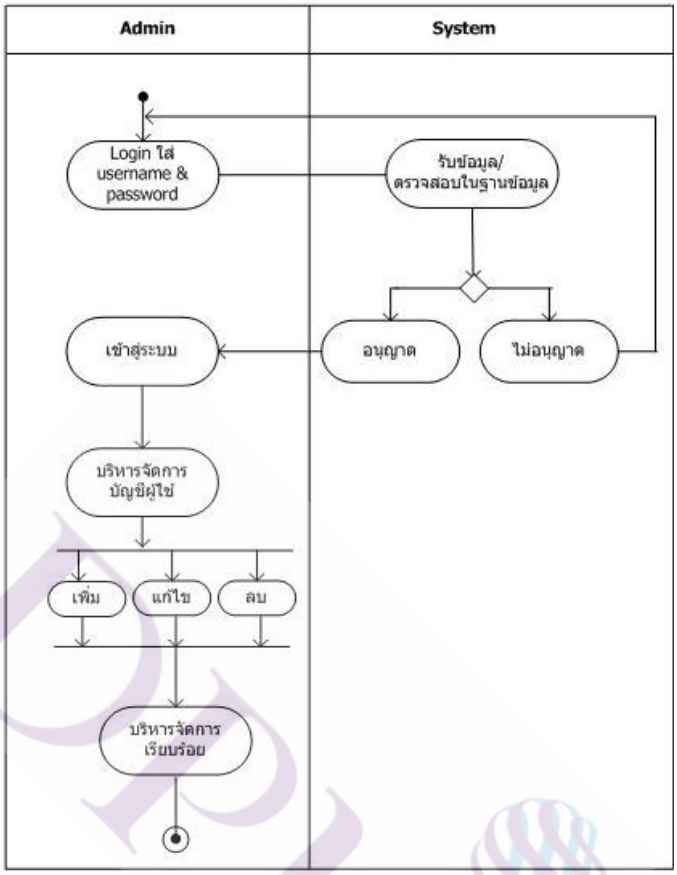
ตารางที่ 10 คำอธิบายรายละเอียดการทำงานของระบบ (Activity diagram Descriptions)

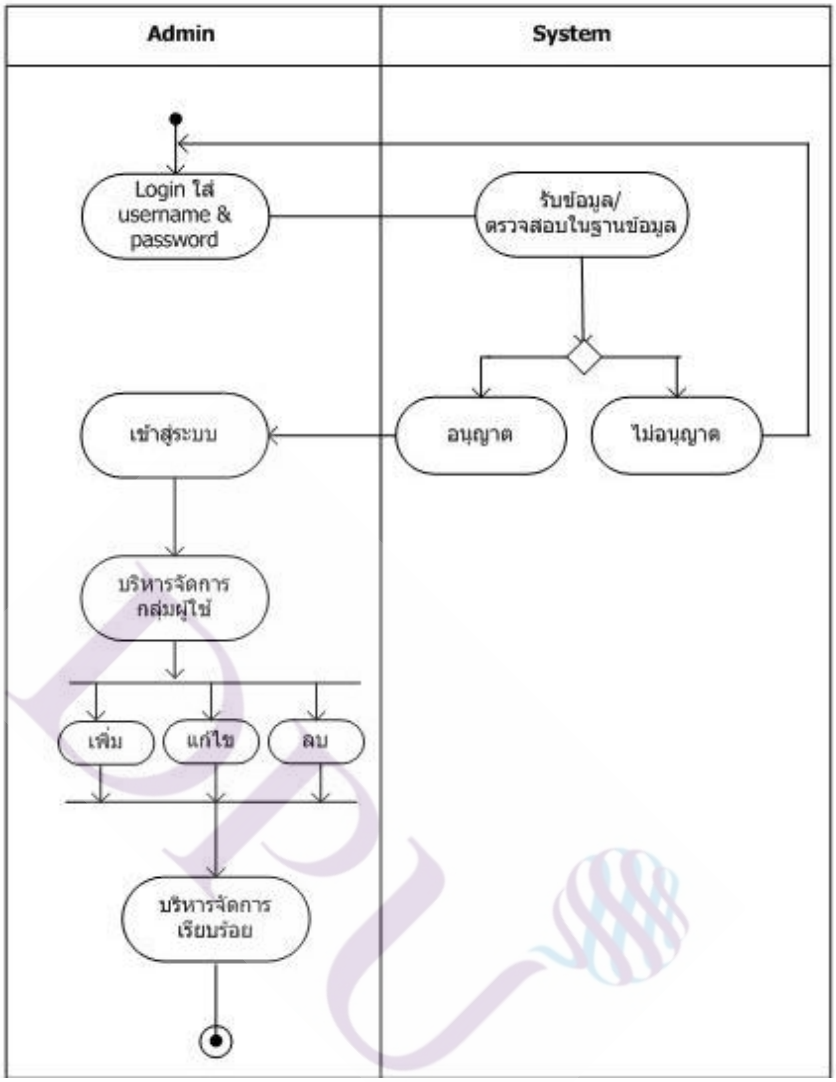
รหัส	Function	คำอธิบาย
AD001	Authentication	การทำงานพิสูจน์ตัวตน
AD002	Management User	การทำงานบริหารจัดการผู้ใช้
AD003	Management Diretory	การทำงานบริหารจัดการกลุ่มผู้ใช้
AD004	Access Control	การทำงานบริหารจัดการสิทธิ์การเข้าถึง
AD005	Change Password	การทำงานเปลี่ยนรหัสผ่าน
AD006	Management file	การทำงานบริหารจัดการเอกสาร
AD007	View Visualize	การทำงานเรียกดูมุมมองเพื่อนำเสนอภาพรวม

Activity Diagram ID:	AD001

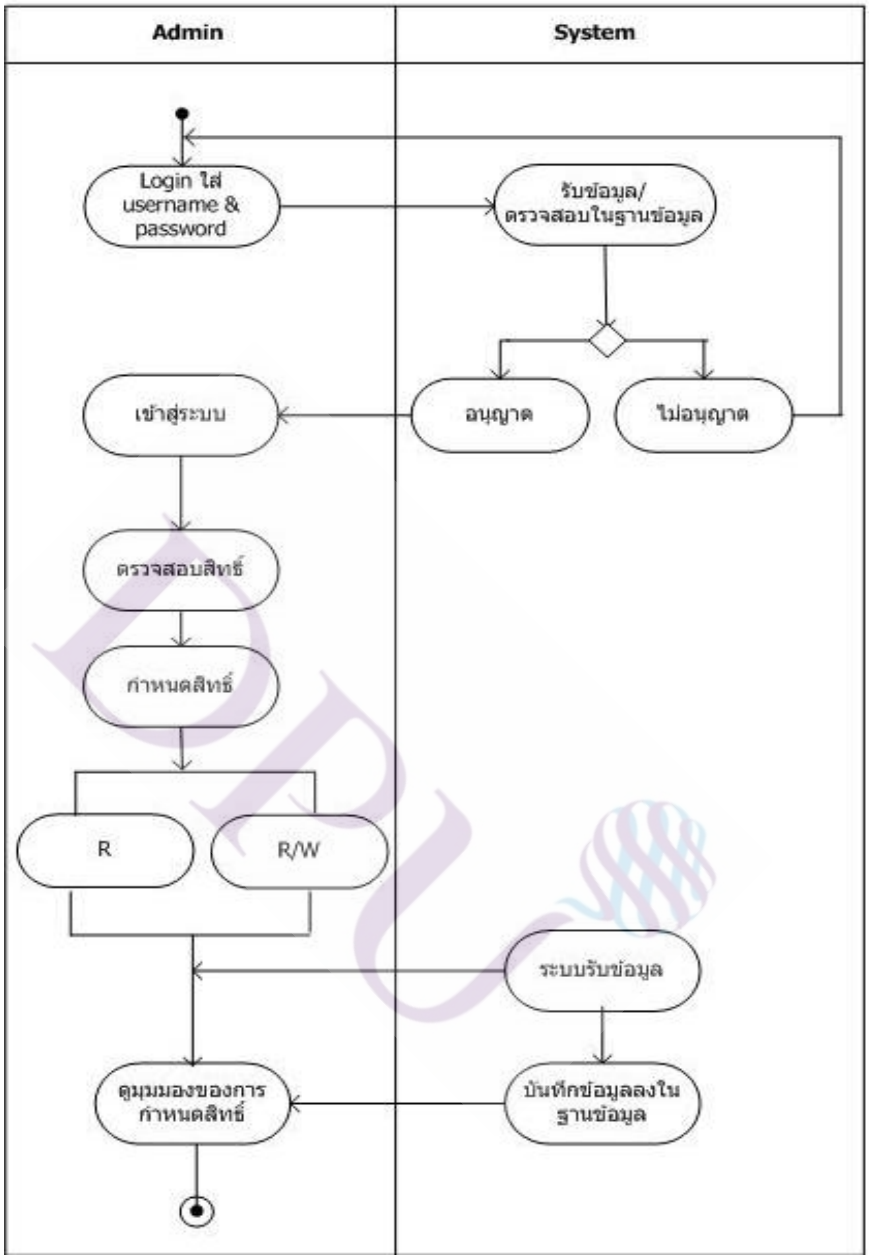


Activity Diagram ID:	AD002

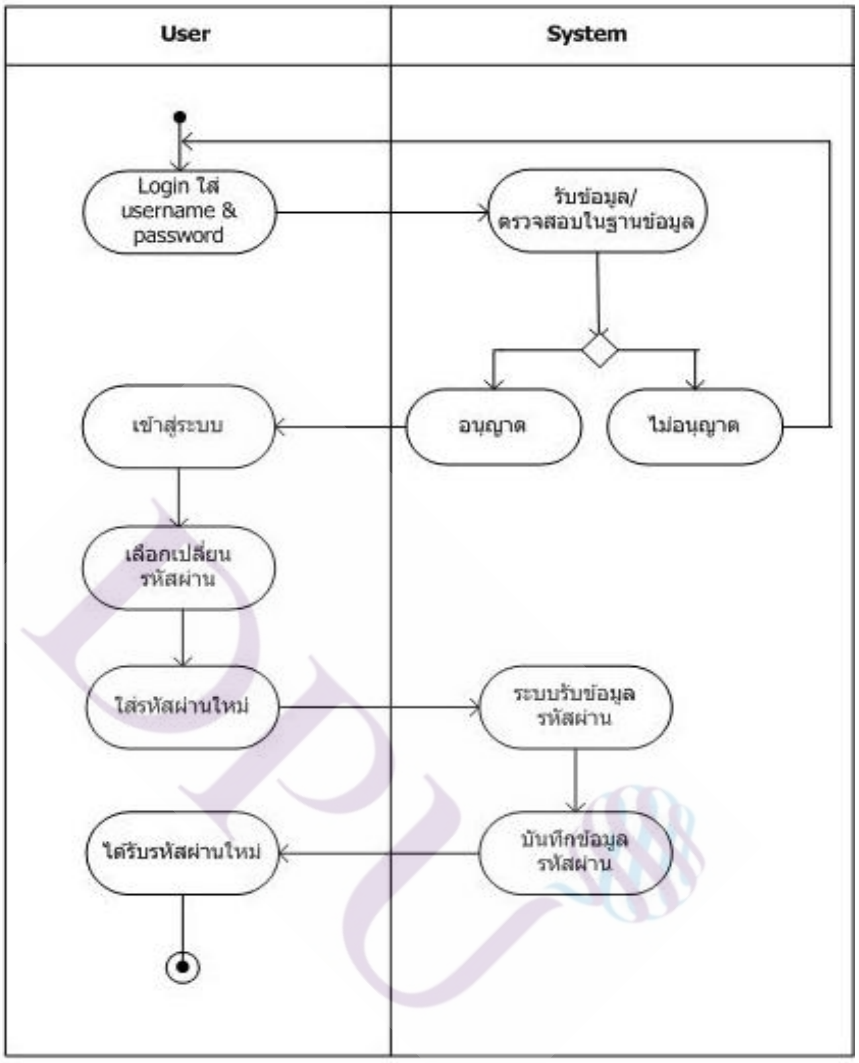



Admin
System
Login ใส่ username & password
รับข้อมูล/ ตรวจสอบในฐานข้อมูล
เข้าสู่ระบบ
อนุญาต
ไม่อนุญาต
บริหารจัดการ กลุ่มผู้ใช้
เพิ่ม
แก้ไข
ลบ
บริหารจัดการ เรียบร้อย

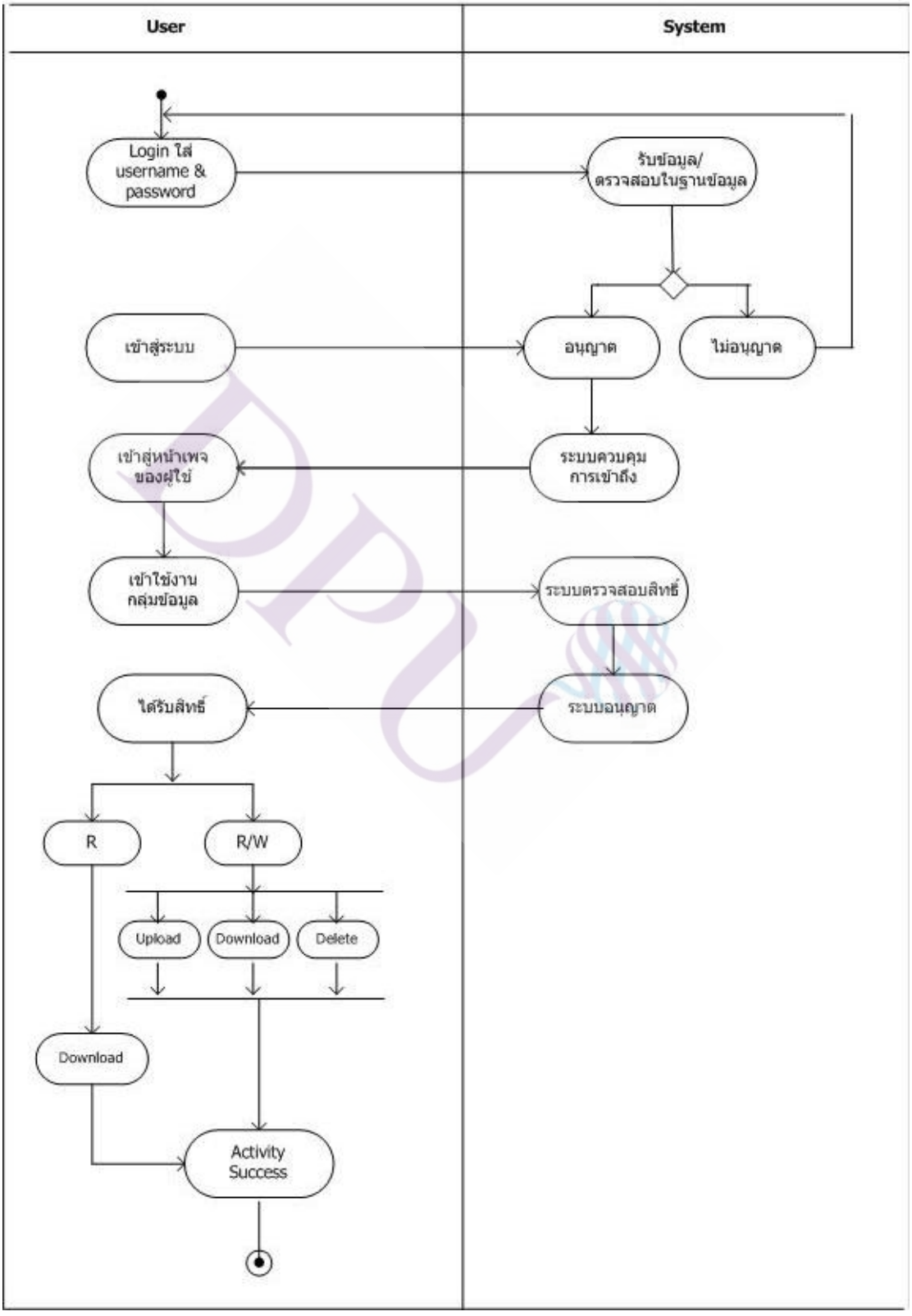
Activity Diagram ID:	AD004



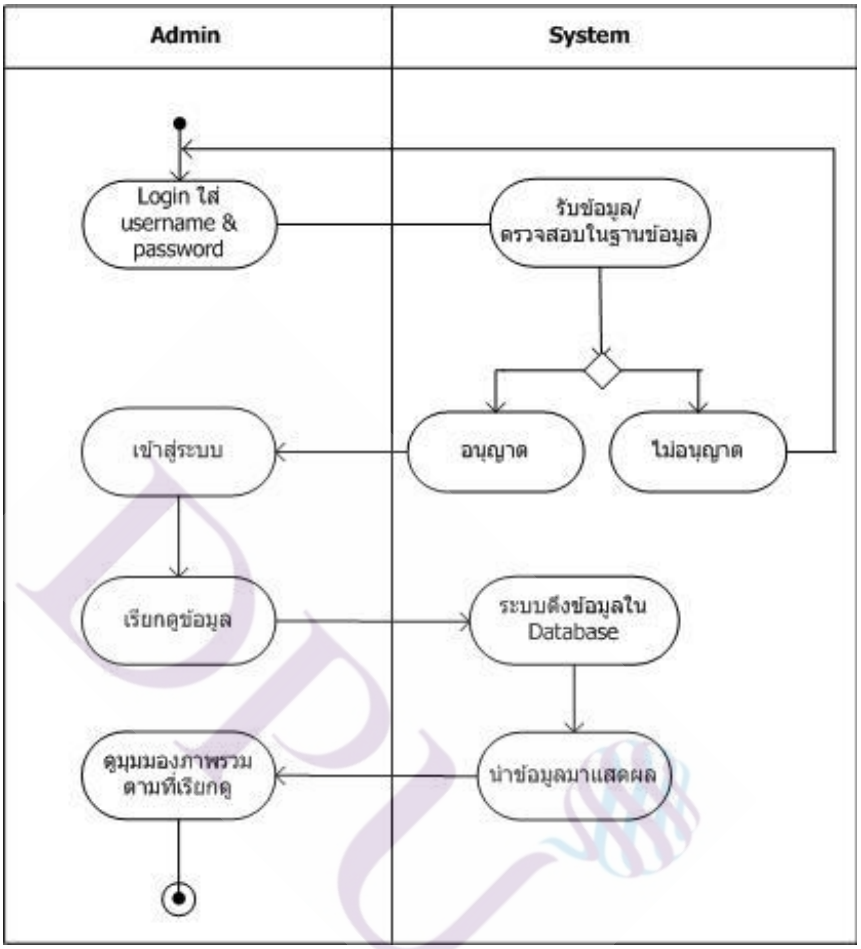
Activity Diagram ID:	AD005



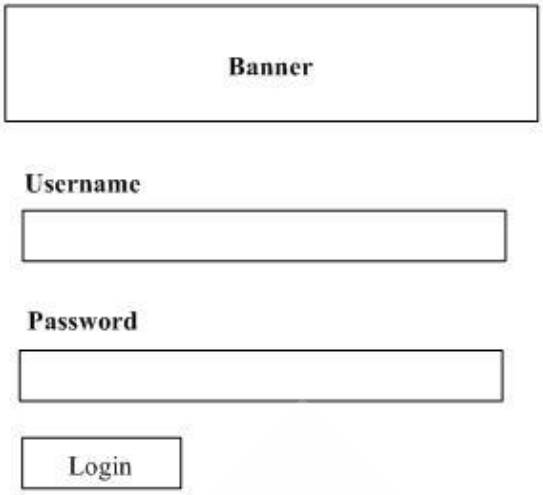
Activity Diagram ID:	AD006



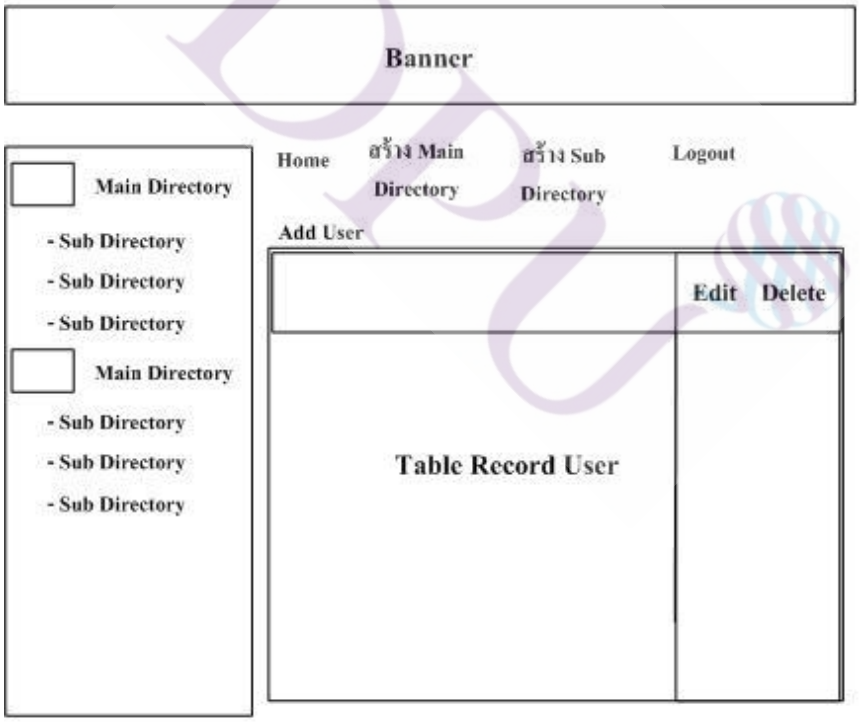
Activity Diagram ID:	AD007



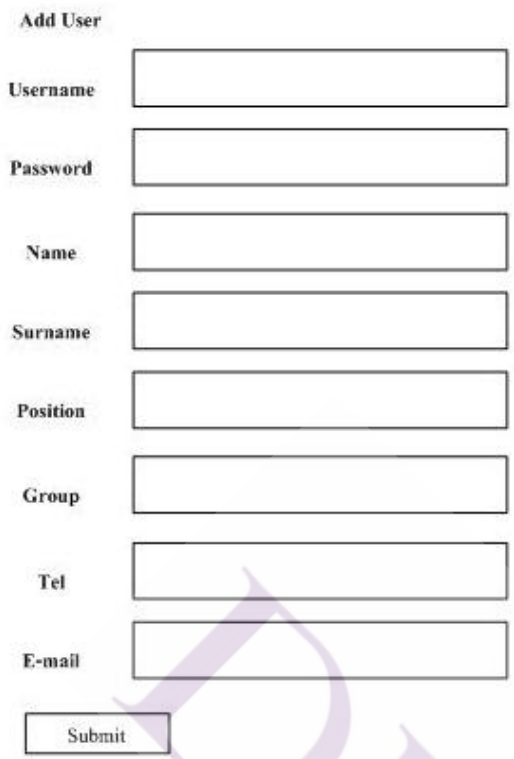
ภาคผนวก ง
การออกแบบส่วนประสานงานผู้ใช้ (Graphical User Interface)



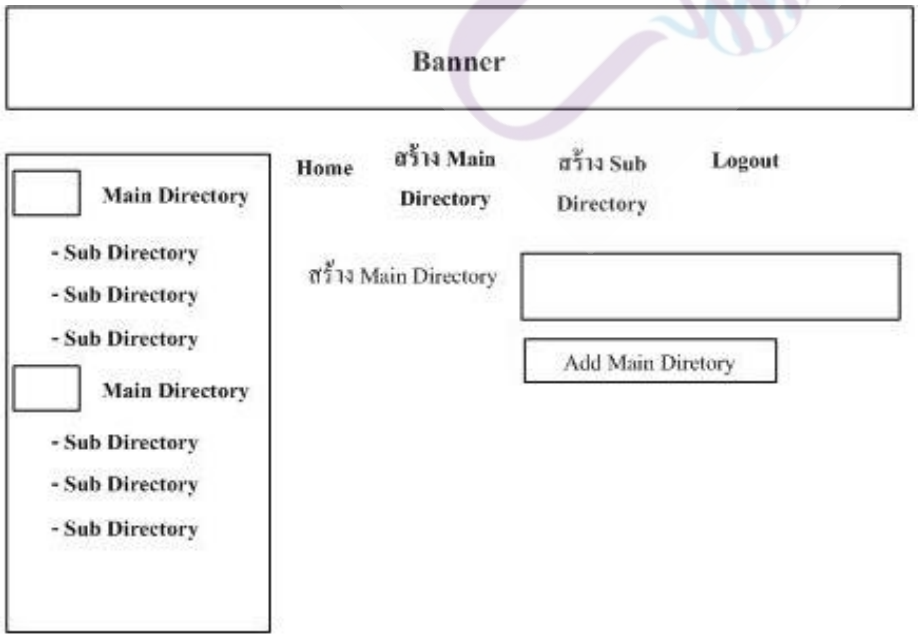
รูปที่ 1 Layout แสดงหน้าจอเข้ารหัสเพื่อพิสูจน์



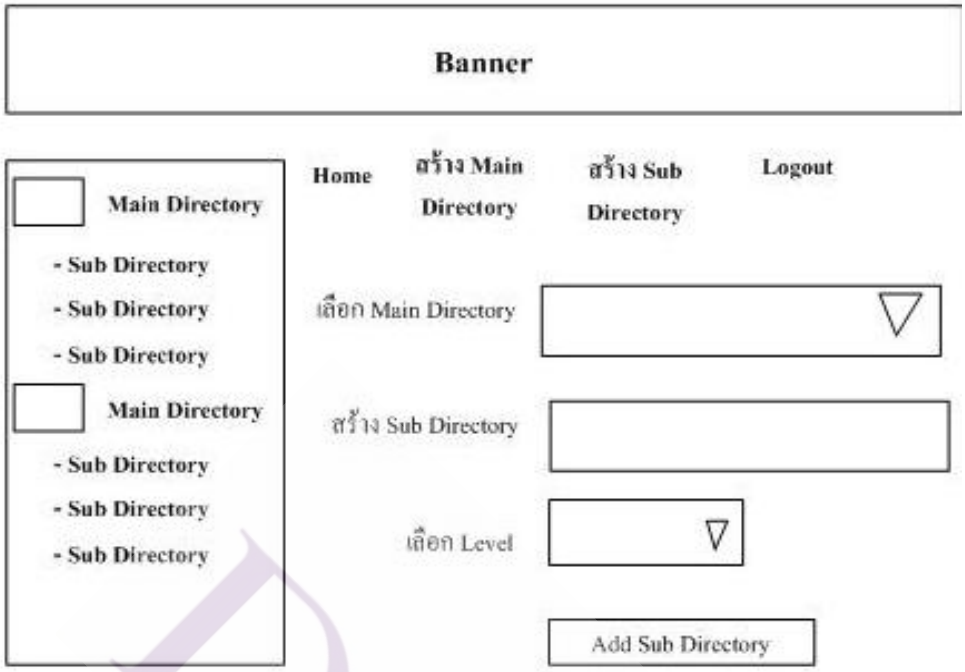
รูปที่ 2 Layout แสดงหน้าจอการเก็บรายชื่อของผู้ใช้งานระบบ



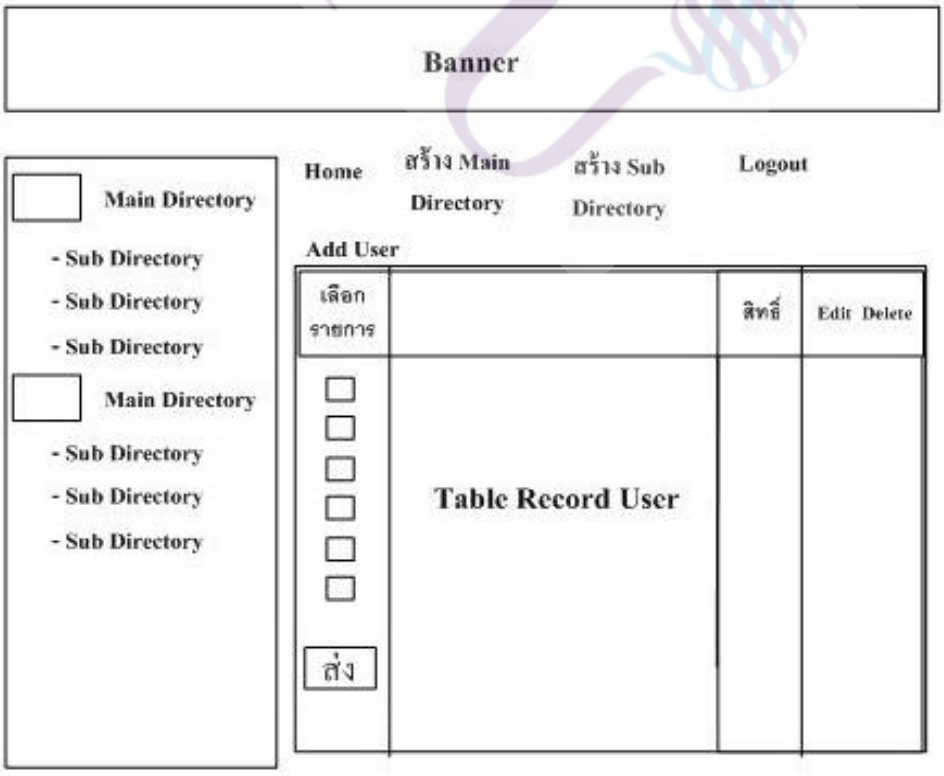
รูปที่ 3 Layout แสดงหน้าจอการบันทึกข้อมูลเบื้องต้นของผู้ใช้



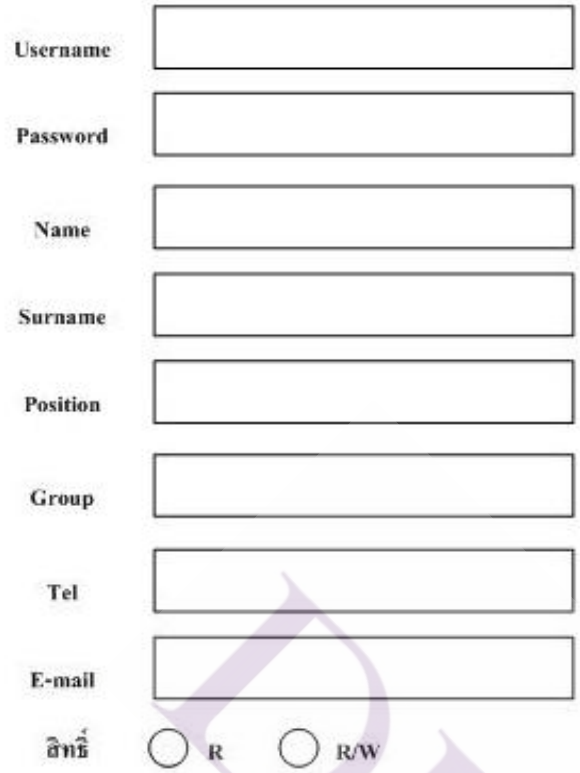
รูปที่ 4 Layout แสดงหน้าจอการบันทึกกลุ่มข้อมูลหลัก



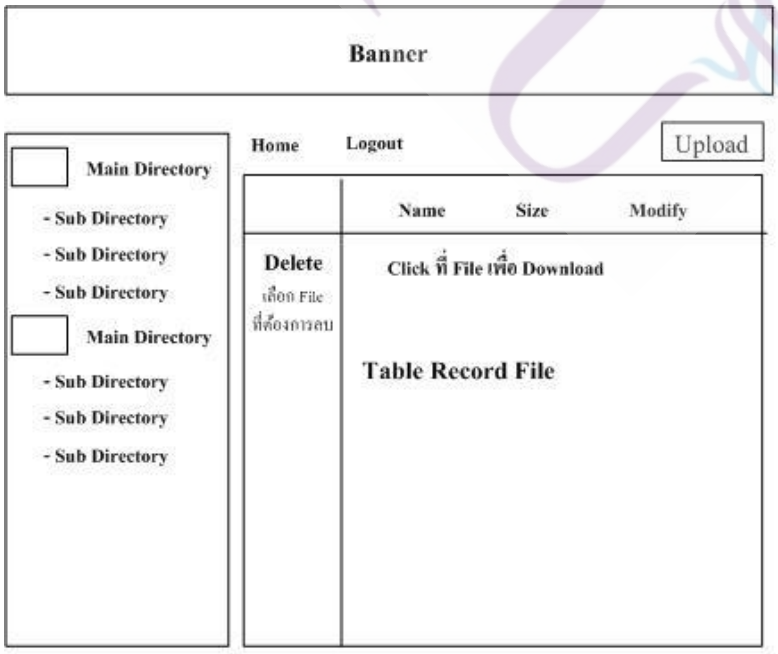
รูปที่ 5 Layout แสดงหน้าจอการบันทึกกลุ่มข้อมูลรอง



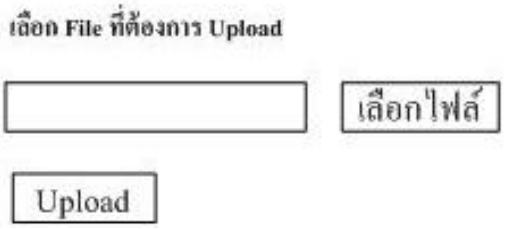
รูปที่ 6 Layout แสดงหน้าจอเลือกรายการบัญชีผู้ใช้เพื่อกำหนดสิทธิ์



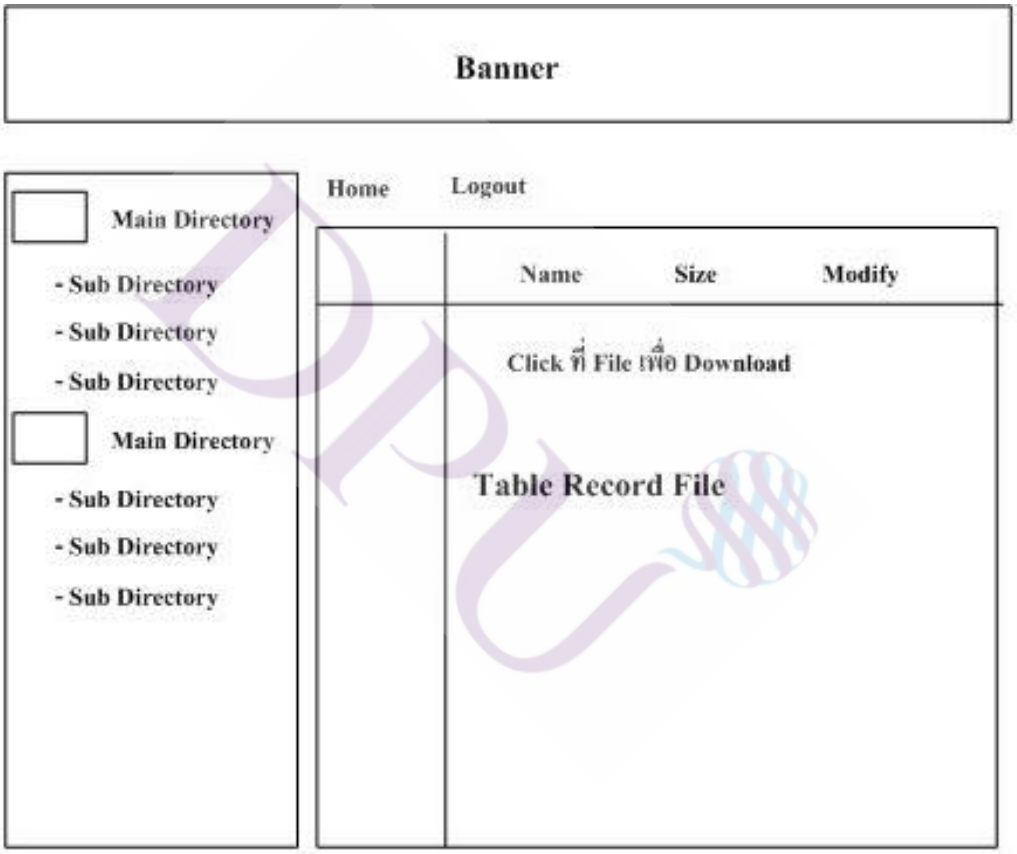
รูปที่ 7 Layout แสดงหน้าจอเพื่อกำหนดสิทธิ์บัญชีผู้ใช้



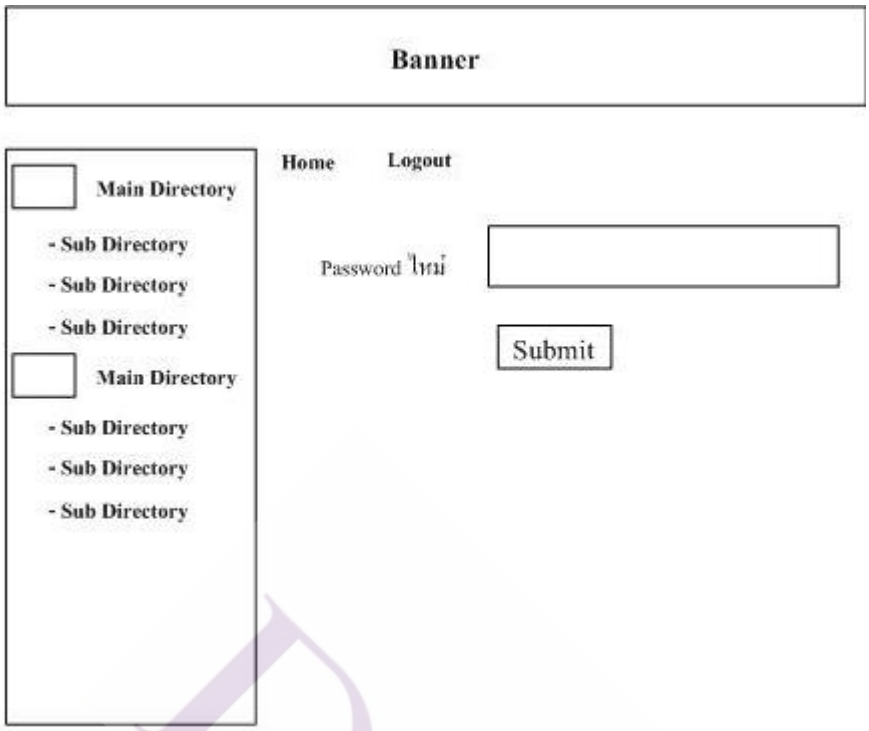
รูปที่ 8 Layout แสดงหน้าจอผู้ใช้งานที่ได้รับสิทธิ์ R/W (Upload , Download , Delete)



รูปที่ 9 Layout แสดงหน้าจอ Upload เอกสาร



รูปที่ 10 Layout แสดงหน้าจอผู้ใช้งานที่ได้รับสิทธิ์ R (Download)



รูปที่ 11 Layout แสดงหน้าจอเปลี่ยนรหัสผ่านส่วนตัว

ภาคผนวก จ

การประเมินผล (Evaluate)

ระบบงานบริหารจัดการและควบคุมเอกสารผ่านเว็บ (Web-Based System for Document Management and Access Control) กรณีศึกษาระบบสมาคมวางแผนครอบครัวแห่งประเทศไทยในพระบรมราชูปถัมภ์ เพื่อช่วยในการวิเคราะห์พิจารณาสิทธิ์การเข้าถึงที่ได้รับอนุญาตทั้งด้าน Subject และ Object ทำให้ช่วยเห็นภาพรวมของสิทธิ์ที่ได้รับแล้ว ทั้งนี้ ผู้จัดทำได้วิเคราะห์ปัญหาและแนวทางพัฒนาระบบให้มีความปลอดภัยและยืดหยุ่นมากยิ่งขึ้น มีรายละเอียดดังต่อไปนี้

1. วิเคราะห์ปัญหาที่พบและปัญหาที่อาจจะเกิดขึ้น

1.1 องค์กรไม่มีการวางโครงสร้างระบบสารสนเทศและข้อบังคับใช้ที่ดี เนื่องจากเจ้าหน้าที่ภายในองค์กรไม่ได้ให้ความสำคัญกับเทคโนโลยีสารสนเทศใหม่ๆ และไม่มีการกำหนดข้อบังคับเพื่อบังคับให้ผู้ใช้ทำตามข้อตกลง ในการใช้เทคโนดลยีอื่นๆ ในปัจจุบันธรรมชาติการทำงานของเจ้าหน้าที่จะทำงานโดยใช้ Microsoft Office (word , excel , power point) จัดเก็บข้อมูลเหล่านี้ไว้ที่เครื่องคอมพิวเตอร์ส่วนบุคคล หรือ บันทึกไว้ในแผ่น CD , DVD ส่วนการแบ่งปันข้อมูลเพื่อใช้ข้อมูลร่วมกันจะใช้วิธีการส่งข้อมูลทาง e-mail ภายในองค์กรจะใช้ Free mail เช่น hotmail , yahoo , gmail เป็นต้น ทำให้องค์กรไม่มีระบบสารสนเทศเพื่อรองรับการทำงานทุกส่วน ในการสร้างระบบนี้จึงไม่สามารถใช้ฐานข้อมูลร่วมกับระบบอื่นๆได้

1.2 การกำหนดสิทธิ์ให้กับผู้ใช้ที่เป็นเจ้าหน้าที่ประจำภายในองค์กรมีงานที่ปฏิบัติเป็นประจำตามโครงสร้างอยู่แล้ว จะกำหนดตามบทบาทโครงสร้างขององค์กร ทำให้ค่อนข้างมีความชัดเจนและง่ายต่อการแก้ไขเมื่อมีการเปลี่ยนแปลง สำหรับผู้ใช้ที่เป็นเจ้าหน้าที่ประจำบางคนได้ได้รับภาระหน้าที่เพิ่มจากงานที่ปฏิบัติเป็นประจำตามโครงสร้าง เช่น ได้รับมอบหมายให้ทำงานโครงการฯเพิ่ม งานโครงการฯแต่ละโครงการฯ จะมีการกำหนดระยะเวลาในการดำเนินงานตามที่แหล่งทุนกำหนด ทั้งนี้งานโครงการฯ จะมีเพิ่ม-ลด อยู่ตลอดเวลา อีกทั้งในบางครั้งได้มีการเปลี่ยนแปลงภาระหน้าที่กะทันหัน ทำให้การกำหนดสิทธิ์ตามภาระหน้าที่ที่ได้รับมอบหมายเพิ่มจากงานที่ปฏิบัติประจำ ให้กับเจ้าหน้าที่ประจำไม่มีโครงสร้างที่ชัดเจน

1.3 การกำหนดสิทธิ์ให้กับผู้ใช้ที่เป็นเจ้าหน้าที่โครงการฯที่ทำงานเฉพาะกิจหรืองานโครงการฯที่ได้รับมอบหมายเท่านั้น ไม่ได้เป็นเจ้าหน้าที่ประจำภายในองค์กรและไม่ได้ปฏิบัติงานตามโครงสร้างขององค์กร อีกทั้งสวัสดิการที่ได้รับยังแตกต่างกันจากเจ้าหน้าที่ประจำ แต่เจ้าหน้าที่โครงการฯ บางคนได้รับอนุญาตให้สามารถเข้าถึงข้อมูลบาง Object จากผู้บริหารระดับสูง ซึ่งข้อมูลที่เกี่ยวข้องกับเจ้าหน้าที่โครงการฯ มีเพียงข้อมูลบางอย่างเท่านั้นไม่ใช่ทั้ง Object ทำให้ข้อมูลที่ไม่เกี่ยวข้องภายใน Object นั้น ไม่มีความปลอดภัยเพียงพอ เนื่องจากขัดแย้งกับความต้องการที่ไม่ให้บุคคลภายนอกเข้าถึงข้อมูลภายในองค์กรได้

1.4 การกำหนดสิทธิ์ให้กับผู้ใช้ ที่มีหน้าที่กำหนดสิทธิ์ในระบบ มีเพียงผู้ดูแลระบบเท่านั้นและผู้ดูแลระบบจะกำหนดสิทธิ์ในระบบตามที่ได้รับแจ้งจากผู้บริหารเท่านั้น ดังนั้นถ้ามีการปรับเปลี่ยนภาระหน้าที่ โยกย้าย หรือเพิกถอนสิทธิ์ หากผู้บริหารหรือผู้ที่ได้รับมอบหมายให้แจ้งแทนผู้บริหารไม่ได้แจ้งให้ผู้ดูแลระบบเปลี่ยนแปลงสิทธิ์ในระบบ ผู้ใช้ก็ยังสามารถใช้สิทธิ์ได้ ทำให้ข้อมูลไม่เป็นความลับ และถ้าผู้ดูแลระบบเป็นผู้ไม่หวังดี อาจจะก่อให้เกิดความไม่ปลอดภัยของข้อมูลได้

2. ขั้นตอนและแนวทางพัฒนาระบบ

จากที่ได้วิเคราะห์ปัญหาที่พบและปัญหาที่อาจจะเกิดขึ้นทำให้เห็นว่าระบบที่จัดทำตามธรรมชาติการทำงานขององค์กรยังไม่มีความปลอดภัยเพียงพอ หากองค์กรต้องการให้ข้อมูลมีความปลอดภัยและยืดหยุ่นมากยิ่งขึ้น สามารถพัฒนาระบบเพิ่มจากเดิมดังต่อไปนี้

2.1 เจ้าหน้าที่ภายในองค์กร จะต้องเห็นความสำคัญของระบบสารสนเทศมากยิ่งขึ้น อย่างน้อยต้องเห็นความสำคัญของระบบภายในองค์กร เพื่อให้มีการจัดโครงสร้างของสารสนเทศภายในองค์กรที่ดีและกำหนดข้อบังคับในการใช้งานระบบสารสนเทศ เพื่อให้เจ้าหน้าที่ภายในองค์กรให้อยู่ในทิศทางเดียวกัน

2.2 ฝึกอบรมเพื่อพัฒนาทักษะการใช้งานคอมพิวเตอร์และระบบภายในองค์กรให้กับเจ้าหน้าที่ เพื่อให้เจ้าหน้าที่สามารถแก้ปัญหาเฉพาะหน้าเกี่ยวกับการใช้งานคอมพิวเตอร์และใช้งานระบบ

2.3 พัฒนาระบบเพื่อให้มีความปลอดภัยมากยิ่งขึ้น แต่ในการพัฒนาจะต้องสอดคล้องกับเจ้าหน้าที่และโครงสร้างภายในองค์กร ในการพัฒนาระบบที่สามารถพัฒนาได้มีดังต่อไปนี้

2.3.1 จัดระดับผู้ใช้งานภายในองค์กรและสิทธิ์ในการใช้งานระบบแต่ละระดับ ในแต่ละระดับจะมีหน้าที่ดังต่อไปนี้

1. ผู้ดูแลระบบ เป็นผู้บันทึกข้อมูลผู้ใช้งานระบบ สร้างกลุ่มข้อมูลตามโครงสร้าง และเป็นผู้กำหนดสิทธิ์ในการเข้าถึงกลุ่มข้อมูลตามที่ได้รับแจ้งจากผู้บริหารหรือผู้ที่ได้รับมอบหมายให้สามารถตัดสินใจแทนผู้บริหารได้

2. ผู้บริหาร เป็นผู้ที่มีอำนาจในการตัดสินใจในการกำหนดให้สิทธิ์ผู้ใช้งานระบบ และสามารถกำหนดสิทธิ์ในการเข้าถึงข้อมูลได้เอง ภายในกลุ่มข้อมูลที่ได้รับสิทธิ์ นอกจากนี้ยังสามารถแต่งตั้งมอบหมายให้ผู้ที่เชื่อถือได้ให้ปฏิบัติการแทนได้

3. ผู้ที่ได้รับแต่งตั้งมอบหมายให้ปฏิบัติงานแทนผู้บริหาร เป็นผู้ที่สามารถกระทำการใดๆ ในระบบพร้อมทั้งสามารถสั่งงานผู้ดูแลระบบแทนผู้บริหารตามที่ได้รับมอบหมายได้

4. เจ้าหน้าที่ หรือผู้ใช้งานทั่วไป เป็นผู้ใช้งานระบบ มีสิทธิ์ในการเข้าใช้งานข้อมูลตามที่ได้อนุญาตจากผู้บริหารหรือผู้ที่ได้รับแต่งตั้งมอบหมายให้ปฏิบัติงานแทนผู้บริหาร และผู้ดูแลระบบได้ทำการกำหนดสิทธิ์ในระบบให้เรียบร้อยแล้ว

2.3.2 ในการพัฒนาระบบ นอกจากจะต้องสอดคล้องกับลักษณะของผู้ใช้ระดับต่างๆ ดังที่กล่าวไว้ข้างต้นแล้ว ระบบจะต้องเหมาะสมกับโครงสร้างขององค์กรอีกด้วย Feature ที่เพิ่มจากระบบเดิม คือ ผู้ใช้ที่อยู่ในระดับผู้บริหารและผู้ที่ได้รับการแต่งตั้งมอบหมายให้ปฏิบัติงานแทนผู้บริหาร จะสามารถกำหนดสิทธิ์อนุญาตให้ผู้ใช้คนอื่นๆ สามารถการเข้าถึงข้อมูล และเปลี่ยนแปลงสิทธิ์การอนุญาตได้เอง โดยไม่ต้องให้ผู้ดูแลระบบเป็นผู้จัดการทั้งหมด แต่จะต้องภายใต้กลุ่มข้อมูลหลักที่อยู่ในอำนาจหน้าที่เท่านั้น การเพิ่ม Feature นี้จะสามารถช่วยลดขั้นตอนการทำงาน และแก้ปัญหา กรณีมีการเปลี่ยนแปลง โยกย้าย เพิกถอน ผู้บริหารสามารถเปลี่ยนแปลงได้เองทันที

ภาคผนวก ฉ
ตัวอย่างแบบสอบถาม

แบบสอบถาม

ระบบบริหารจัดการและควบคุมการเข้าถึงเอกสารผ่านเว็บ

คำชี้แจง

แบบสอบถามนี้เป็นส่วนหนึ่งของการศึกษาระดับปริญญาโท หลักสูตรวิทยาศาสตรมหาบัณฑิตสาขาวิศวกรรมเว็บ มหาวิทยาลัยธุรกิจบัณฑิตย์ จัดทำขึ้นเพื่อใช้สอบถามความคิดเห็นเกี่ยวกับการใช้งานระบบบริหารจัดการและควบคุมเอกสารผ่านเว็บ

แบบสอบถามนี้มีวัตถุประสงค์เพื่อประเมินหาระดับความพึงพอใจของระบบดังกล่าวที่ได้พัฒนาขึ้น โดยแบ่งเป็น 3 ตอน ประกอบด้วย

ตอนที่ 1 ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม

ตอนที่ 2 ข้อมูลความคิดเห็นเกี่ยวกับประสิทธิภาพของระบบ

ตอนที่ 3 ข้อเสนอแนะและแนวทางในการปรับปรุงและพัฒนาระบบ

กรุณาตอบคำถามให้ครบทุกข้อตามความเป็นจริง เพราะคำตอบของท่านจะเป็นประโยชน์อย่างยิ่งต่อการพัฒนาระบบในครั้งนี้ เพื่อที่ผู้พัฒนาจะได้นำข้อมูลไปวิเคราะห์และประเมินความพึงพอใจของระบบต่อไป

ขอขอบพระคุณเป็นอย่างยิ่งที่ท่านได้กรุณาให้ความร่วมมือในการตอบแบบสอบถามในครั้งนี้

มุจรินทร์ แพทย์จันลา

ตอนที่ 1: ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม

คำชี้แจง: โปรดทำเครื่องหมาย ✓ ลงในช่อง O ที่ตรงกับความเป็นจริง

1. เพศ
   - O ชาย
   - O หญิง
2. อายุ
   - O ต่ำกว่า 25 ปี
   - O 25 – 30 ปี
   - O 31 – 35 ปี
   - O 36 – 40 ปี
   - O 41 – 45 ปี
   - O มากกว่า 45 ปีขึ้นไป
3. ระดับการศึกษา
   - O ต่ำกว่าปริญญาตรี
   - O ปริญญาตรี
   - O ปริญญาโท
   - O ปริญญาเอก
4. มีประสบการณ์ในการเป็นผู้ใช้ระบบบริหารจัดการข้อมูลผ่านเว็บ
   - O เคย
   - O ไม่เคย
5. มีประสบการณ์ในการเป็นผู้พัฒนาระบบ
   - O เคย
   - O ไม่เคย
6. มีประสบการณ์ในการเป็นผู้ดูแลระบบ
   - O เคย
   - O ไม่เคย

ตอนที่ 2: ข้อมูลเกี่ยวกับระดับความพึงพอใจของผู้ใช้งานระบบ

คำชี้แจง: -

1. แบบสอบถามความคิดเห็นตอนที่ 2 นี้ เป็นการสอบถามข้อมูลความคิดเห็นของผู้ตอบแบบสอบถามภายหลังจากที่ได้ทดลองใช้ระบบที่พัฒนาขึ้น ซึ่งแบบสอบถามแบ่งออกเป็น 4 ด้าน คือ

1. ด้านการตรงตามความต้องการของผู้ใช้ระบบ Functional Requirement Test เป็นการประเมินผลความถูกต้องและประสิทธิภาพของระบบว่าตรงตามความต้องการของผู้ใช้มากน้อยเพียงใด

2. ด้านการทำงานได้ตามฟังก์ชันงานของระบบ Functional Test เป็นการประเมินความถูกต้องและประสิทธิภาพในการทำงานของระบบว่าสามารถทำงานได้ตามฟังก์ชั่นของระบบมากน้อยเพียงใด

3. ด้านความง่ายต่อการใช้งานระบบ Usability Test เป็นการประเมินลักษณะการออกแบบระบบว่ามีความง่ายต่อการใช้งานมากน้อยเพียงใด

4. ด้านการรักษาความปลอดภัยของข้อมูลในระบบ Security Test เป็นการประเมินว่าระบบที่พัฒนาขึ้นมานั้น มีความปลอดภัยของข้อมูลมากน้อยเพียงใด

2. ในการตอบแบบสอบถามตอนที่ 2 นี้ ขอความกรุณาให้ท่านดำเนินการดังนี้

ทำเครื่องหมาย ✓ ลงในช่องในแบบสอบถามที่ตรงกับระดับความคิดเห็นของท่านมากที่สุด โดยตัวเลขของระดับความพึงพอใจแต่ละด้านมีความหมายดังนี้

5 หมายถึง ความเหมาะสม/ความพึงพอใจในระดับมากที่สุด

4 หมายถึง ความเหมาะสม/ความพึงพอใจในระดับมาก

3 หมายถึง ความเหมาะสม/ความพึงพอใจในระดับปานกลาง

2 หมายถึง ความเหมาะสม/ความพึงพอใจในระดับน้อย

1 หมายถึง ความเหมาะสม/ความพึงพอใจในระดับน้อยที่สุด

ตัวอย่างการประเมิน

รายการประเมิน	**ระดับความเหมาะสม / ความพึงพอใจ**				
	5	**4**	**3**	**2**	**1**
การออกแบบหน้าจอมีความเป็นมาตรฐานเดียวกัน		✓			

แบบสอบถามความพึงพอใจด้านการตรงตามความต้องการของผู้ใช้ระบบ

(Functional Requirement Test)

รายการประเมิน	ระดับความเหมาะสม / ความพึงพอใจ				
	5	4	3	2	1
ความสามารถของระบบล็อกอินเข้าใช้งาน					
ความสามารถของระบบการใช้งานเอกสารผ่านเว็บ					
ความสามารถของระบบการอัพโหลดข้อมูล					
ความสามารถของระบบการดาวน์โหลดข้อมูล					
ความสามารถของระบบการลบข้อมูล					

แบบสอบถามความพึงพอใจด้านการทำงานได้ตามฟังก์ชันงานของระบบ (Function Test)

รายการประเมิน	ระดับความเหมาะสม / ความพึงพอใจ				
	5	4	3	2	1
ความถูกต้องตามที่ไดรับอนุญาต					
ความถูกต้องสิทธิ์ที่ได้รับ					
ความถูกต้องในการแสดงผล					
ความรวดเร็วในการประมวลผลของระบบ					
การป้องกันการค้นหาข้อมูลผิดพลาดที่อาจเกิดขึ้น					

แบบสอบถามความพึงพอใจด้านความง่ายต่อการใช้งานระบบ (Usability Test)

รายการประเมิน	ระดับความเหมาะสม / ความพึงพอใจ				
	5	4	3	2	1
ความง่ายต่อการใช้งานของระบบ					
ความเหมาะสมของตำแหน่งการจัดวางส่วนต่างๆ บนจอภาพ					
ความชัดเจนของข้อความที่แสดงบนจอภาพ					
ความเหมาะสมของการใช้สีโดยภาพรวม					
ความเหมาะสมของรูปแบบตัวอักษรที่เลือกใช้					
การใช้ข้อความและคำแนะนำการใช้โปรแกรมเข้าใจง่าย					
ความน่าใช้ของระบบในภาพรวม					

แบบสอบถามความพึงพอใจด้านการรักษาความปลอดภัยของข้อมูลในระบบ (Security Test)

รายการประเมิน	ระดับความเหมาะสม / ความพึงพอใจ				
	5	4	3	2	1
ความเหมาะสมในการกำหนดชื่อผู้ใช้และรหัสผ่าน					
ความเหมาะสมของระบบรักษาความปลอดภัย					
การควบคุมให้ใช้งานตามสิทธิ์ผู้ใช้ได้อย่างถูกต้อง					
ความสามารถของระบบในการตรวจควบคุมการเข้าถึง					
ความสามารถของระบบสอบสิทธิ์การเข้าถึง					
ความน่าเชื่อถือได้ของระบบ					

ตอนที่ 3: ข้อเสนอแนะโปรดแสดงความคิดเห็นและข้อเสนอแนะเกี่ยวกับการพัฒนาระบบ

.....

.....

.....

.....

.....

ขอขอบพระคุณเป็นอย่างสูงในการให้ความร่วมมือในการตอบแบบสอบถาม

ประวัติผู้เขียน

ชื่อ-นามสกุล	มุจรินทร์ แพทย์จันลา
ประวัติการศึกษา	สำเร็จการศึกษาระดับปริญญาตรีสาขาวิชาเทคโนโลยีสารสนเทศธุรกิจ มหาวิทยาลัยธุรกิจบัณฑิตย์ ปีการศึกษา 2549
ตำแหน่งและสถานที่ทำงานปัจจุบัน	เจ้าหน้าที่แผนงานและพัฒนาโครงการ (ระดับ 4 ขั้น 11) สมาคมวางแผนครอบครัวแห่งประเทศไทย ในพระราชูปถัมภ์สมเด็จพระศรีนครินทราบรมราชชนนี