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

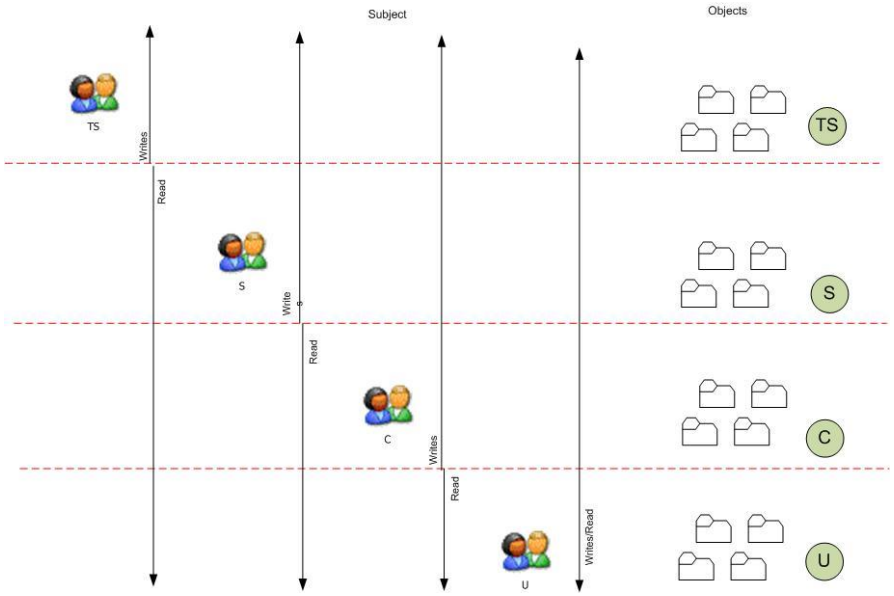
(Authorization) เพื่อใช้ในการตรวจสอบการเข้าสู่ระบบและการเข้าถึงข้อมูลแต่ละ Object และสิทธิ์การเข้าถึง (Read , Write , Execute) ตามคำร้องขอของผู้ใช้ เมื่อต้องการเข้าถึง Object จะถูกตรวจสอบกับการอนุมัติที่ระบุว่าผู้ใช้สามารถเข้าถึง Object ได้ในระดับใด แต่ถ้าผู้ไม่ได้รับอนุญาตจะไม่สามารถเข้าถึงทรัพยากรดังกล่าวได้

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

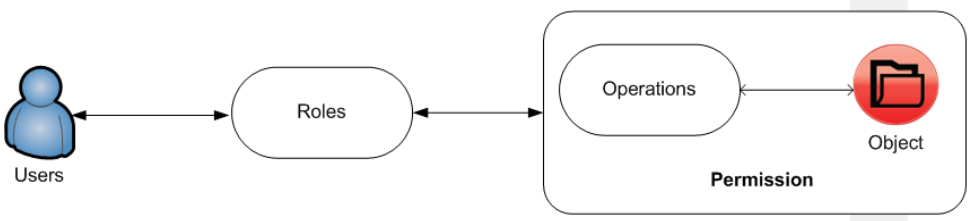
จากรูปที่ 2.1 แสดงตัวอย่างการป้องกันข้อมูลในแต่ละ Object ข้อมูลที่อยู่ในระดับที่สูงกว่าจะมีการรักษาความมั่นคงมากกว่าข้อมูลที่อยู่ในระดับล่าง ผู้ใช้สามารถเข้าใช้งานตามกฎที่ได้รับอนุญาต เพื่อป้องกันความลับให้กับข้อมูลตามระดับที่กำหนด และเพิ่มความน่าเชื่อถือให้แก่กลุ่มข้อมูลจากการรั่วไหลโดยไม่ได้ตั้งใจของเจ้าของข้อมูล 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

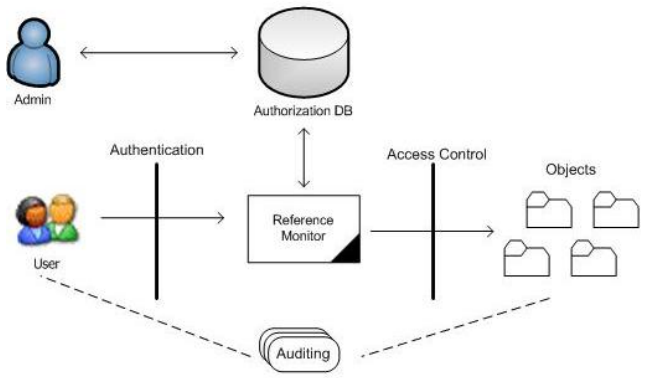
การกำหนดสิทธิ์ตามบทบาทสามารถใช้กำหนดความสามารถกลุ่มผู้ใช้กับการดำเนินงานด้านการจัดการบางอย่าง โดยปรับการตั้งค่าบัญชีที่แต่ละกลุ่มสามารถจัดการได้ ตัวอย่างเช่น ต้องการป้องกันไม่ให้พนักงานทั่วไปเปลี่ยนชื่อที่แสดง แต่ต้องการให้ผู้จัดการสามารถเปลี่ยนชื่อนั้นได้ เมื่อต้องการดำเนินการนี้ต้องเชื่อมโยงการเข้าถึงเริ่มต้นของพนักงาน 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

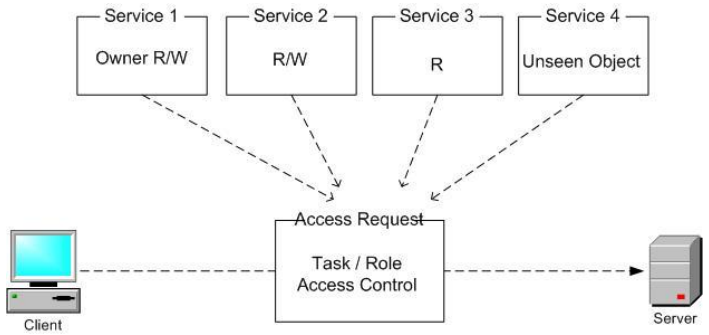


รูปที่ 2.3 การควบคุมการเข้าถึงและการรักษาความมั่นคง

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